



Data Encoding Specification for the IC Full Service Directory Schema

Version 1.0

Date of Release: 14 Dec 2011

Table of Contents

1. INTRODUCTION.....	1
1.1 Purpose	1
1.2 Background and Needs.....	1
1.3 Audience and Applicability.....	2
1.4 Conventions.....	3
1.5 Conformance	3
2. IC FSD SYSTEM DESCRIPTION	4
3. IC FSD SCHEMA	5
3.1 IC FSD Schema for IC Person	5
3.2 IC FSD Schema for IC Non-Person Entity	7
3.3 IC FSD Attribute Definitions	7
3.3.1 buildingName.....	8
3.3.2 c, countryName	8
3.3.3 cn, commonName	9
3.3.4 companyName	9
3.3.5 displayName	10
3.3.6 employeeType.....	11
3.3.7 expertCountry	11
3.3.8 expertFunctionalArea.....	12
3.3.9 facsimileTelephoneNumber.....	13
3.3.10 generationQualifier	13
3.3.11 givenName	14
3.3.12 icEmail	14
3.3.13 icNetworks	15
3.3.14 icServerAddress	15
3.3.15 initials.....	16
3.3.16 internetEmail.....	16
3.3.17 isICMember	17
3.3.18 l, localityName	18
3.3.19 languageProficiency.....	18
3.3.20 mail	19
3.3.21 militaryTelephoneNumber	19
3.3.22 nationality-Extended	20
3.3.23 NiprnetEmail.....	21
3.3.24 personalTitle	21
3.3.25 postalAddress	22
3.3.26 postalCode.....	22
3.3.27 productionManager	23
3.3.28 rank	23
3.3.29 resourceSecurityMark	24
3.3.30 secureFacsimileNumber.....	25
3.3.31 secureTelephoneNumber	25

3.3.32 serverPOC	26
3.3.33 serverURL.....	26
3.3.34 serviceOrAgency.....	27
3.3.35 SiprnetEmail	28
3.3.36 sn	29
3.3.37 st, stateOrProvinceName.....	29
3.3.38 street.....	29
3.3.39 telephoneNumber.....	30
3.3.40 title	30
3.3.41 uid	31
3.3.42 userCertificate	32
4. MANDATORY, POLICY-BASED, AND OPTIONAL ATTRIBUTES.....	33
5. SECURING ACCESS TO IC FSD ATTRIBUTES	35
6. EFFECTIVE DATE.....	37
APPENDIX A – IC FSD SCHEMA FOR ICPKI ROOT AND INTERMEDIATE CERTIFICATE AUTHORITIES	38
A.1 authorityRevocationList	38
A.2 certificateRevocationList	39
A.3 cACertificate	39
APPENDIX B – CHANGE HISTORY	41
APPENDIX C – MODIFICATIONS TO PREVIOUS IC FSD SCHEMA	42
APPENDIX D – ACRONYMS	43
APPENDIX E – BIBLIOGRAPHY.....	45
APPENDIX F – POINTS OF CONTACT	47
APPENDIX G - IC CIO APPROVAL MEMO	48

1. INTRODUCTION

1.1 Purpose

This technical specification codifies the set of Lightweight Directory Access Protocol (LDAP) attributes that IC elements are expected to provide to the Intelligence Community Full Service Directory (IC FSD). It will facilitate the availability, accuracy, and standardization of these attributes across the IC TS/SCI enterprise, building a consistent basis for capabilities including directory services, email functions, and attribute-based access control decisions. The specification defines:

- IC-specific Schema and supporting objectClasses for IC Entities
- Attributes, both standard and IC-defined, that must be managed by IC Elements
- Controlled vocabulary for those attributes whose use requires standard values
- Authentication requirements for the attributes

1.2 Background and Needs

In operation since 1999, the IC FSD provides enterprise-level directory services to both IC personnel and applications on the US TS/SCI fabric. This IC-wide directory is made possible by IC elements sharing attributes amongst themselves via the IC FSD's hub and spoke replication model. Under this model, each participating IC element is responsible for providing attributes about their personnel and non-person entities such as servers and service applications. The IC FSD supports:

- The IC White Pages, a web-based service with which TS/SCI users can locate colleagues' email addresses, phone numbers, and other organizational information.¹
- The sharing of user email attributes between IC Elements' internal address books, to facilitate cross-agency and S/MIME-enabled email capabilities.
- The sharing of user email attributes with the TS/SCI Allied and Collaborative Shared Services environment, to facilitate US-5 Eyes collaboration.
- Attribute-Based Access Control, by resources directly accessing an IC FSD Border Directory or indirectly via the Unified Authorization and Attribute Service (UAAS) Federation, within which the IC FSD serves as a repository for authoritative authorization attributes.

The IC FSD also provides two attributes that are required for replicating content to other SCI networks (JWICS, NSANET, ACSS):

- Resource Security Mark – an overall data classification and control marking for each entry in the IC FSD.

¹ URL = <http://directory.csp.ic.gov/eGuide/index.html>

- 38 ■ icNetworks - a releasability attribute specifying the IC-approved network on which the
39 object is allowed to be replicated (JWICS, NSANET, ACSS) .

40
41 Planning and partnerships between IC Elements have made current IC Full Service Directory
42 capabilities possible. However, as the IC FSD has become increasingly important, some
43 limitations have been identified that must be addressed to realize the IC FSD's full potential. The
44 following limitations affect consistent identity management, IC ONEmail initiatives, emerging
45 Attribute-Based Access Control capabilities, and overall user productivity:

- 46
47 • Instances of attributes populated incompletely by IC Elements
48 • Instances of attributes populated with inconsistent values, making resource providers unable
49 to rely on them for access control
50 • No authentication requirements designed to limit access to the attributes, which has become
51 more important with their dissemination to diverse TS/SCI environments, making some
52 elements hesitant to share some attributes

53
54 Beginning in 2010, IC elements again demonstrated partnership by addressing these limitations
55 together, resulting in this document, which:

- 56
57 • Formally documents the IC FSD attribute schema
58 • Increases the number of IC FSD attributes required for each entry
59 • Defines attribute names
60 • Identifies the attributes requiring controlled values
61 • Defines those controlled values
62 • Establishes authentication requirements for each attribute
63 • Ensures interoperability with the IC enterprise authorization attributes exchanged through the
64 Unified Authorization and Attribute Service federation, as documented in *Logical Data*
65 *Specification for IC Enterprise Authorization Attributes*.

66 67 **1.3 Audience and Applicability**

68 The primary audience for this document includes those responsible for implementing and
69 managing the capabilities that create, provide, modify, store, exchange, search, display, or
70 further process IC FSD attributes.

71
72 This document applies to all attributes shared via the IC FSD about IC Entities on the TS/SCI
73 fabric, with the majority of attributes pertaining to IC Persons.

74
75 Each IC FSD entry about a person provides attributes about a “persona”, which means that one
76 person may have several IC FSD records, each with distinct attributes about that persona. A
77 persona is an electronic identity that can be unambiguously associated with a single person. A

78 single person may have multiple personas, with each persona being managed by the same or by
79 different organizations (such as a DNI contractor who is also an Army reservist).

80
81 Since the concept of personas applies to IC FSD records, it is an important concept to remember
82 when reading portions of the IC FSD schema which reference persons.
83

84 **1.4 Conventions**

85 The key words MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD
86 NOT, RECOMMENDED, MAY, and OPTIONAL in this service description are to be
87 interpreted as described in the IETF RFC 2119 [RFC 2119]. These keywords are thus capitalized
88 when used to unambiguously specify requirements over protocol and application features and
89 behavior that affect the interoperability and security of implementations. When these words are
90 not capitalized, they are meant in their natural-language sense.

91 Certain typography is used throughout the body of this document to convey certain meanings, in
92 particular:

- 93 ▪ *Italics* – A title of a referenced work or a specialized or emphasized term
- 94 ▪ *Courier* – A class, package, or attribute name.

95
96 **1.5 Conformance**

97 This specification defines a business object to which an implementation and a subsequent
98 deployment MUST conform. For an implementation to conform to this specification, it MUST
99 adhere to all mandatory aspects of the specification.

100 Within this document, class diagrams are normative for the class name, attribute names, attribute
101 multiplicity, attribute visibility, and class inheritance. All tables describing the class attributes
102 are normative for descriptions of the attributes and informative for all other aspects of the class.

103 For the purposes of this document, normative and informative are defined as:

- 104 • Normative: considered to be prescriptive and necessary to conform to the standard.
- 105 • Informative: serving to instruct or enlighten or inform.

106 Additional guidance that is either classified or has handling controls can be found in separate
107 annexes, which are distributed to the appropriate networks and environments, as necessary.
108 Systems and services operating in those environments must consult the appropriate annexes.

109

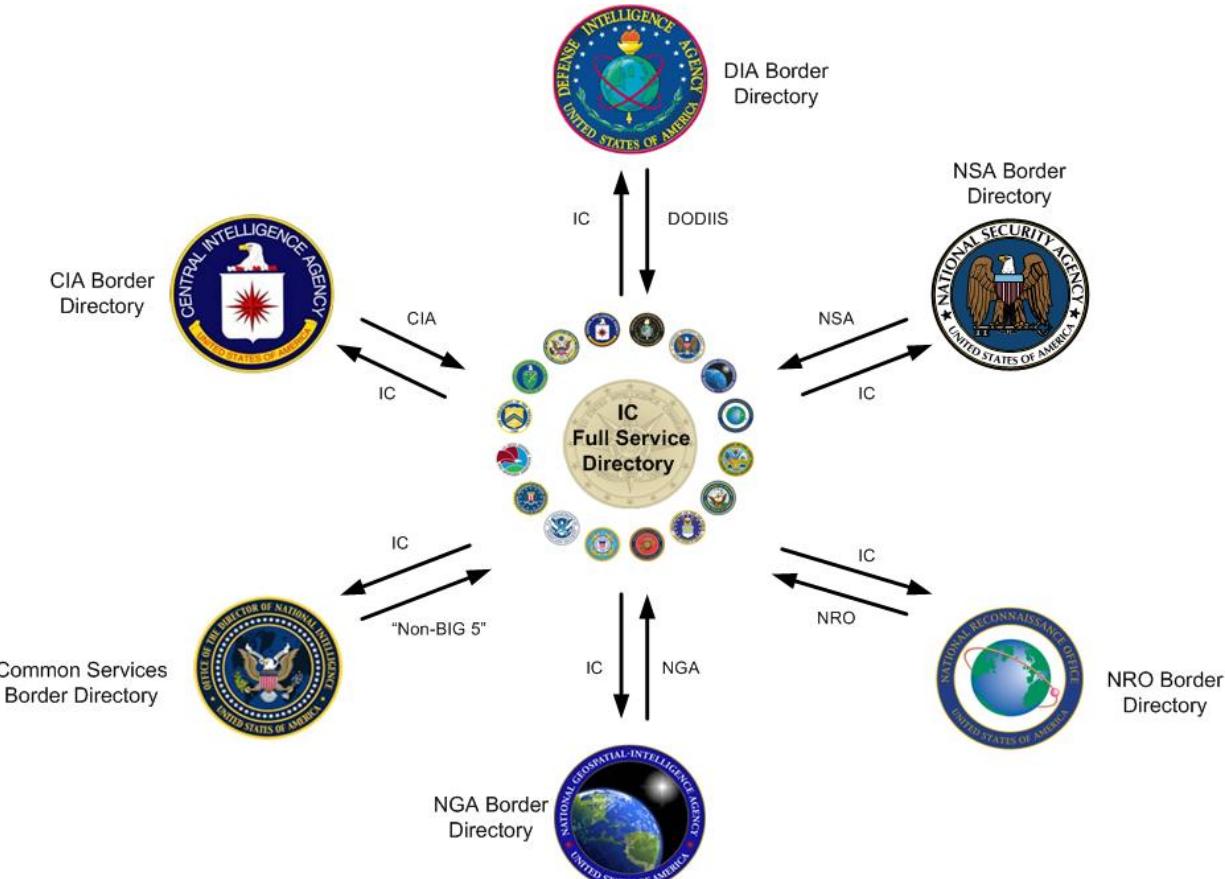
110

111 2. IC FSD SYSTEM DESCRIPTION

112 The IC FSD is based on the X.500 standard for electronic directory services. It is a fully
 113 replicated directory framework in which each participating IC Element holds a full and accurate
 114 copy of the IC FSD content. The architecture is based on a hub and spoke model, with the central
 115 IC FSD serving as the master replication hub. When a participating IC Element adds, deletes, or
 116 modifies data in its border directory, the IC FSD detects and replicates the updated content to
 117 itself and all other border directories. This full replication scenario strengthens the IC FSD's
 118 disaster recovery posture. Figure 1 below depicts the IC FSD replication model.

119

120 **Figure 1. IC FSD Replication**



121

122

123 The IC FSD, acting in its role as the master replication manager, is designed to only
 124 communicate with authorized border directories. The IC FSD always initiates communications
 125 with the authorized border directories; no IC Element border directory can initiate
 126 communication with the IC FSD.

127

128 The IC FSD maintains redundancy through two geographically diverse locations, each with three
129 servers. The first server communicates with authorized border directories (currently CIA, DIA,
130 NGA, NRO, and NSA), retrieving updates hourly and immediately replicating any changes to the
131 other border directories. The second server replicates information to and from the Common
132 Services border directory. The third server provides local redundancy and, in the event of a
133 complete failure of one of the first two servers, can serve as the replication engine for either.

134

135 **3. IC FSD SCHEMA**

136

137 The IC FSD Schema is defined by several standard LDAP objectClasses and two derived
138 auxiliary objectClasses that designate additional attributes about IC Entities. IC Entities fall into
139 the categories of an “IC Person” or “IC Non-Person Entity”, with the latter being used to define
140 objects such as servers, devices, appliances, applications, and services that exist within the IC
141 enterprise.

142

143 **3.1 IC FSD Schema for IC Person**

144

145 Attributes that characterize an “IC Person” are defined through a combination of standard LDAP
146 objectClasses and a derived IC-defined objectClass called “icOrgPerson”. The specific
147 implementation of an “icOrgPerson” objectClass may vary depending on the directory server
148 in use, so the definition of the actual objectClass is left to the discretion of the implementing IC
149 Element. The suggested objectClass hierarchy used to hold the various attributes about an IC
150 Person is as follows:

151

152

```
objectclass (2.5.6.6 NAME 'person' SUP top
    DESC 'RFC2256: Person'
    STRUCTURAL
    MUST (sn $ cn)
    MAY ( userPassword $ telephoneNumber $ seeAlso $ description)
)
```

153

```
objectclass (2.5.6.7 NAME 'organizationalPerson' SUP person
    DESC 'RFC2256: organizationalPerson'
    STRUCTURAL
    MAY (title $ x121Address $ registeredAddress $
```

```

destinationIndicator $ preferredDeliveryMethod $  

telexNumber $ teletexTerminalIdentifier $  

telephoneNumber $ internationaliSDNNumber $  

facsimileTelephoneNumber $ street $ postOfficeBox $  

postalCode $ postalAddress $  

physicalDeliveryOfficeName $ ou $ st $ l )  

)

```

154

```

objectclass (2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson'  

DESC 'RFC2798: Internet Organizational Person'  

SUP organizationalPerson  

STRUCTURAL  

MAY ( audio $ businessCategory $ carLicense $  

departmentNumber $ displayName $ employeeNumber $  

employeeType $ givenName $ homePhone $  

homePostalAddress $ initials $ jpegPhoto $  

labeledURI $ mail $ manager $ mobile $ o $ pager $  

photo $ roomNumber $ secretary $ uid $  

userCertificate $ x500uniqueIdentifier $  

preferredLanguage $userSMIMECertificate $  

userPKCS12 )  

)

```

155

```

objectclass (2.16.840.1.101.2.2.3.73 NAME 'icOrgPerson'  

DESC 'Intelligence Community Person'  

SUP inetOrgPerson  

STRUCTURAL  

MUST ( nationality-Extended $ serviceOrAgency $  

icNetworks $ resourceSecurityMark )  

MAY ( icEmail $ secureTelephoneNumber $ companyName $  

internetEmail $ nippnetEmail $ sippnetEmail $  

rank $ buildingName $ countryName $  

militaryTelephoneNumber $  

secureFacsimileNumber $ uid $ expertCountry $  

expertFunctionalArea $ productionManager $  

languageProficiency $ isICMember )

```

```
)
```

156

157

158 **3.2 IC FSD Schema for IC Non-Person Entity**

159

160 Attributes that characterize an IC Non-Person Entity are defined through a combination of
161 standard LDAP objectClasses and a derived IC-defined objectClass called “icOrgServer”.
162 The “icOrgServer” objectClass used to hold the various attributes about an IC Non-Person
163 Entity is defined below. As is the case with “icOrgPerson”, the actual objectClass hierarchy
164 used to implement “icOrgServer” is left to the discretion of the implementing IC element.

165

```
objectclass (2.16.840.1.101.2.2.3.74 NAME 'icOrgServer'  
    DESC 'Intelligence Community Non-Person Entity'  
    SUP <implementation specific>  
    STRUCTURAL  
    MUST ( cn $ icServerAddress $ serviceOrAgency $  
        uid $ userCertificate $ resourceSecurityMark $  
        icNetworks $ serverPOC )  
    MAY ( description $ serverURL )  
)
```

166

167

168 **3.3 IC FSD Attribute Definitions**

169

170 The following section defines a collection of attributes from the objectClasses described in
171 sections 3.1 and 3.2 that participating IC Elements should attempt to support so that the IC FSD
172 can realize its full potential as an IC Enterprise-level directory service. Each attribute is
173 described using the formal attribute definition format as defined in *RFC 2252 section 4.2*. A
174 tabular format will also be used to provide additional information and a controlled vocabulary
175 (when appropriate) for each attribute.

176 In terms of IC Element provisioning requirements, this specification organizes attributes about
177 an IC entity into mandatory, policy-based or optional categories and is further described in
178 Section 4.

179 This specification establishes three authentication tiers, providing graded authentication for
180 attributes of varying sensitivity and is further described in Section 5.

181 All attributes are assumed to be MULTI-VALUE unless specifically identified as SINGLE-
182 VALUE.

183 Several of the designated attributes are “children” of the SUPERIOR (SUP) attribute called
 184 ‘name’. As a result, each child attribute inherits the properties of ‘name’, described as follows:

185

186 attributetype (2.5.4.41 NAME ‘name’
 187 EQUALITY caseIgnoreMatch
 188 SUBSTR caseIgnoreSubstringsMatch
 189 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 190)
 191

192 **3.3.1 buildingName**

193

194 attributetype (0.9.2342.19200300.100.1.48 NAME ‘buildingName’
 195 EQUALITY caseIgnoreMatch
 196 SUBSTR caseIgnoreSubstringsMatch
 197 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 198)
 199

Attribute Name	buildingName
Reference	RFC 1274
Object Class	icOrgPerson
Friendly Name	Physical Building Name
Description	Defines the building name associated with an IC Person
Allowable Values	IC Person’s community recognized building name
Example	LX2 NBP-304
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

200

201 **3.3.2 c, countryName**

202

203 attributetype (2.5.4.6 NAME (‘c’ ‘countryName’) SUP name SINGLE-VALUE)
 204

Attribute Name	c, countryName
Reference	RFC 2256
Object Class	icOrgPerson

Friendly Name	Physical Country
Description	Country where IC Person's physical work facility is located
Allowable Values	ISO 3166 two-letter country code
Example	US AU
Provisioning	Optional
Authentication	Strong User
Single/Multi	SINGLE-VALUE

205

206 **3.3.3 cn, commonName**

207

208 attributetype (2.5.4.3 NAME ('cn' 'commonName') SUP name)

209

Attribute Name	cn, commonName
Reference	RFC 2256
Object Class	Person
Friendly Name	Common Name
Description	This is the X.500 commonName attribute, which contains a name of an object. When the object corresponds to an IC Entity, it typically matches the CN component of the entity's Distinguished Name in its/his/her ICPKI certificate.
Allowable Values	For the IC, the <i>Intelligence Community Public Key Infrastructure Interface Specification</i> provides the basis for specifying Common Names for both IC Person and Non-Person Entities. Consult Chapter 6 - CERTIFICATE DISTINGUISHED NAME (DN) SCHEMA of the ICPKI Interface Specification for allowable values
Example	Smith John A dijasmi webserver.dni.ic.gov
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

210

211 **3.3.4 companyName**

212

213 IC-defined attribute. Suggested definition for implementation by IC Element:

214 attributetype (2.16.840.1.101.2.2.1.148 NAME 'companyName'

215 EQUALITY caseIgnoreMatch

216 SUBSTR caseIgnoreSubstringsMatch

217 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

218 SINGLE-VALUE
 219)
 220

Attribute Name	companyName
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Company Name
Description	Company name of an IC Person with CTR employeeType
Allowable Values	Legal name of company provided by authoritative source
Example	Company Inc.
Provisioning	Optional
Authentication	Strong User
Single/Multi	SINGLE-VALUE

221
 222 **3.3.5 displayName**
 223
 224 attributetype (2.16.840.1.113730.3.1.241 NAME 'displayName'
 225 EQUALITY caseIgnoreMatch
 226 SUBSTR caseIgnoreSubstringsMatch
 227 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 228 SINGLE-VALUE
 229)
 230

Attribute Name	displayName
Reference	RFC 2798 <i>Intelligence Community Standard 500-13, Intelligence Community Optimized Network E-Mail Display Name Format</i>
Object Class	inetOrgPerson
Friendly Name	Display Name
Description	Preferred name of an IC Person to be used when displaying entries. Especially useful in displaying a preferred name within a one-line summary list, such as the case with an IC email client.

Allowable Values	Format as defined in ICS 500-13: Last Name<space>First Name<space>Middle Name/ Initial<space>Generation ID<space> Title/Rank<space>Agency<space> Citizenship<space>EmployeeType In terms of corresponding directory attribute names: <sn givenName initials generationQualifier title/rank serviceOrAgency nationality-Extended employeeType>
Example	Smith John M Jr Maj DIA USA MIL
Provisioning	Policy-based
Authentication	Network
Single/Multi	SINGLE-VALUE

231

232 **3.3.6 employeeType**

233

234 attributetype (2.16.840.1.113730.3.1.4 NAME ‘employeeType’

235 EQUALITY caseIgnoreMatch

236 SUBSTR caseIgnoreSubstringsMatch

237 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

238)

239

Attribute Name	employeeType
Reference	RFC 2798
Object Class	inetOrgPerson
Friendly Name	Employee Type
Description	Indicates whether an IC Person is a US federal government employee, military service member, or contractor
Allowable Values	GOV, MIL, or CTR
Example	GOV MIL CTR
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE (per RFC 2798)

240

241 **3.3.7 expertCountry**

242

243 IC-defined attribute. Suggested definition for implementation by IC Element:
 244 attributetype (2.16.840.1.101.2.2.1.149 NAME ‘expertCountry’
 245 EQUALITY caseIgnoreMatch
 246 SUBSTR caseIgnoreSubstringsMatch
 247 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 248 SINGLE-VALUE
 249)
 250

Attribute Name	expertCountry
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Expert Country
Description	3-letter country code describing an IC Person’s expertise area
Allowable Values	3-letter country code as defined in ISO 3166-1
Example	USA GBR AUS
Provisioning	Optional
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

251
 252 **3.3.8 expertFunctionalArea**
 253

254 IC-defined attribute. Suggested definition for implementation by IC Element:
 255 attributetype (2.16.840.1.101.2.2.1.150 NAME ‘expertFunctionalArea’
 256 EQUALITY caseIgnoreMatch
 257 SUBSTR caseIgnoreSubstringsMatch
 258 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 259 SINGLE-VALUE
 260)
 261

Attribute Name	expertFunctionalArea
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Expert Functional Area
Description	IC Person’s functional area expertise

Allowable Values	DIA Intelligence Functional Code
Example	IFC1000 IFC2800
Provisioning	Optional
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

262

263

264 **3.3.9 facsimileTelephoneNumber**

265

266 attributetype (2.5.4.23 NAME ('facsimileTelephoneNumber' 'fax')

267 SYNTAX 1.3.6.1.4.1.1466.115.121.1.22

268)

269

Attribute Name	facsimileTelephoneNumber
Reference	RFC 2256
Object Class	organizationalPerson
Friendly Name	Unclassified Telephone FAX Number
Description	IC Person's unclassified/commercial FAX number
Allowable Values	<Country Code (if applicable)> (Area Code) <Prefix><Suffix>
Example	(703) 561-0000
Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

270

271 **3.3.10 generationQualifier**

272

273 attributetype (2.5.4.44 NAME 'generationQualifier' SUP name)

274

Attribute Name	generationQualifier
Reference	RFC 2256
Object Class	<i>Implementation Dependent</i>
Friendly Name	Generational Qualifier
Description	The generationQualifier attribute contains the part of the IC Person's name which typically is the suffix
Allowable Values	JR,, SR, etc.
Example	JR SR

Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

275

276 **3.3.11 givenName**

277

278 attributetype (2.5.4.42 NAME 'givenName' SUP name)

279

Attribute Name	givenName
Reference	RFC 2256
Object Class	inetOrgPerson
Friendly Name	First Name
Description	The givenName attribute is used to hold the part of a person's name which is not their surname nor middle name
Allowable Values	For IC Persons, this should reflect a person's legal first name
Example	Joseph Katherine
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

280

281 **3.3.12 icEmail**

282

283 IC-defined attribute. Suggested definition for implementation by IC Element:

284 attributetype (2.16.840.1.101.2.2.1.154 NAME 'icEmail'

285 EQUALITY caseIgnoreMatch

286 SUBSTR caseIgnoreSubstringsMatch

287 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

288 SINGLE-VALUE

289)

290

Attribute Name	icEmail
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	IC Email Address
Description	IC Email address of an IC Person

Allowable Values	Official email address of the IC Person as given by their email provider
Example	jsmith@intelink.ic.gov
Provisioning	Policy-based
Authentication	Network
Single/Multi	SINGLE-VALUE

291

292 **3.3.13 icNetworks**

293

294 IC-defined attribute. Suggested definition for implementation by IC Element:

295 attributetype (2.16.840.1.101.2.2.1.160 NAME ‘icNetworks’

296 EQUALITY caseIgnoreMatch

297 SUBSTR caseIgnoreSubstringsMatch

298 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

299)

300

Attribute Name	icNetworks
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson, icOrgServer
Friendly Name	IC Networks
Description	icNetworks is used to specify what networks an object may exist on. This attribute provides the capability for other security domains to be listed. Directory objects include both IC Person and Non-Person Entities.
Allowable Values	ACSS, NSANET, JWICS
Example	ACSS NSANET JWICS
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	MULTI-VALUE

301

302 **3.3.14 icServerAddress**

303

304 IC-defined attribute. Suggested definition for implementation by IC Element:

305 attributetype (2.16.840.1.101.2.2.2.200 NAME ‘icServerAddress’

306 EQUALITY caseIgnoreMatch

307 SUBSTR caseIgnoreSubstringsMatch

308 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 309 SINGLE-VALUE
 310)
 311

Attribute Name	icServerAddress
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgServer
Friendly Name	IP Address
Description	IP Address of IC Non-Person Entity
Allowable Values	Valid IPv4 or IPv6 address
Example	10.1.2.3 3ffe:1900:4545:3:200:f8ff:fe21:67cf
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

312
 313 **3.3.15 initials**
 314
 315 attributetype (2.5.4.43 NAME ‘initials’ SUP name)
 316

Attribute Name	initials
Reference	RFC 2256
Object Class	inetOrgPerson
Friendly Name	Middle Initial
Description	IC Person’s middle initial
Allowable Values	Single, first letter of the middle name with no periods, if one is available
Example	K L N, etc.
Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

317
 318 **3.3.16 internetEmail**
 319
 320 IC-defined attribute. Suggested definition for implementation by IC Element:
 321 attributetype (2.16.840.1.101.2.2.1.155 NAME ‘internetEmail’
 322 EQUALITY caseIgnoreMatch

323 SUBSTR caseIgnoreSubstringsMatch
 324 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 325 SINGLE-VALUE
 326)
 327

Attribute Name	internetEmail
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Internet Email Address
Description	Internet email address of an IC Person
Allowable Values	Official Internet email address of the IC Person as given by their email provider
Example	jsmith@ugov.gov
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

328
 329 **3.3.17 isICMember**
 330
 331 IC-defined attribute. Suggested definition for implementation by IC Element:
 332 attributetype ('**OID TBD**' NAME 'isICMember'
 333 EQUALITY booleanMatch
 334 SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
 335 SINGLE-VALUE
 336)
 337

Attribute Name	isICMember
Reference	DES for the IC Full Service Directory Schema, ICD 501, Executive Order 12333
Object Class	icOrgPerson
Friendly Name	IC Membership
Description	Value that denotes an individual's IC membership status for ICD 501 purposes
Allowable Values	Boolean True/False (false by default)
Example	False
Provisioning	Policy-based
Authentication	Strong User
Single/Multi	SINGLE-VALUE

338

339 The isICMember attribute is a flag that reflects whether the persona is a member of the
 340 Intelligence Community (IC).

341 This is a Boolean attribute that will be set to False by default. Null values for this attribute
 342 should be treated as False by applications using this attribute for access control purposes.

343 Each IC organization will make the determination as to which of its users will have a True value
 344 for this attribute. This process will be documented by the organization and approved by the
 345 organization's senior leadership and general counsel. The ODNI will then review and approve
 346 the process. The following, from Executive Order 12333, is used as general guidance in making
 347 this determination: an IC member is "a person employed by, assigned or detailed to, or acting for
 348 an element within the IC".

349

350 **3.3.18 l, localityName**

351

352 attributetype (2.5.4.7 NAME ('l' 'localityName') SUP name)

353

Attribute Name	l, localityName
Reference	RFC 2256
Object Class	organizationalPerson
Friendly Name	Physical City
Description	IC Person's physical city or location name
Allowable Values	City or location name
Example	Fairfax
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

354

355 **3.3.19 languageProficiency**

356

357 IC-defined attribute. Suggested definition for implementation by IC Element:

358 attributetype (2.16.840.1.101.2.2.1.151 NAME 'languageProficiency'

359 EQUALITY caseIgnoreMatch

360 SUBSTR caseIgnoreSubstringsMatch

361 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

362 SINGLE-VALUE

363)

364

Attribute Name	languageProficiency
----------------	---------------------

Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Language Proficiency
Description	Individual's evaluated ability to read, write and speak a second language other than English. Based on Defense Language Proficiency Test.
Allowable Values	Contains a reading level and listening level based on the Defense Language Proficiency Test results
Example	Reading Level 1 Listening Level 0+
Provisioning	Optional
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

365

366 **3.3.20 mail**

367

368 attributetype (0.9.2342.19200300.100.1.3 NAME ('mail' 'rfc822Mailbox')
 EQUALITY caseIgnoreIA5Match
 SUBSTR caseIgnoreIA5SubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
)
 373

Attribute Name	mail
Reference	RFC 2798
Object Class	inetOrgPerson
Friendly Name	Email Address
Description	Email address of an object on a particular network
Allowable Values	Official email address of the IC Person as given by their email provider
Example	jsmith@intelink.ic.gov
Provisioning	Policy-based
Authentication	Network
Single/Multi	MULTI-VALUE

374

375 **3.3.21 militaryTelephoneNumber**

376

377 IC-defined attribute. Suggested definition for implementation by IC Element:
 378 attributetype (2.16.840.1.101.2.2.1.120 NAME 'militaryTelephoneNumber'
 EQUALITY caseIgnoreMatch

380 SUBSTR caseIgnoreSubstringsMatch
 381 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 382 SINGLE-VALUE
 383)
 384

Attribute Name	militaryTelephoneNumber
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	DSN Voice Telephone Number
Description	IC Person's Defense Switched Network (DSN) phone number
Allowable Values	Authoritative DSN telephone number provided by the user's home agency
Example	867-5309
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

385

3.3.22 nationality-Extended

387

388 IC-defined attribute. Suggested definition for implementation by IC Element:
 389 attributetype (2.16.840.1.101.2.2.1.61 NAME 'nationality-Extended'

390 EQUALITY caseIgnoreMatch
 391 SUBSTR caseIgnoreSubstringsMatch
 392 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 393 SINGLE-VALUE
 394)
 395

Attribute Name	nationality-Extended
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Citizenship
Description	3-letter country code describing an IC Person's citizenship
Allowable Values	3-letter country code as defined in ISO 3166-1
Example	USA GBR AUS
Provisioning	Mandatory

Authentication	Network
Single/Multi	SINGLE-VALUE

396

397 **3.3.23 NiprnetEmail**

398

399 IC-defined attribute. Suggested definition for implementation by IC Element:

400 attributetype (2.16.840.1.101.2.2.1.156 NAME 'NiprnetEmail'

401 EQUALITY caseIgnoreMatch

402 SUBSTR caseIgnoreSubstringsMatch

403 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

404 SINGLE-VALUE

405)

406

Attribute Name	NiprnetEmail
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Niprnet Email Address
Description	Niprnet email address of an IC Person
Allowable Values	Official Niprnet email address of the IC Person as given by their DOD email provider
Example	jsmith@af.mil
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

407

408 **3.3.24 personalTitle**

409

410 attributetype (0.9.2342.19200300.100.1.40 NAME 'personalTitle'

411 EQUALITY caseIgnoreMatch

412 SUBSTR caseIgnoreSubstringsMatch

413 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

414)

415

Attribute Name	personalTitle
Reference	RFC 1274
Object Class	<i>Implementation Dependent</i>
Friendly Name	Personal Title

Description	The title attribute contains the personal title of an IC Person
Allowable Values	Dr, Mr, Ms, Prof, etc.
Example	Mr Dr Ms
Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

416

417

418 **3.3.25 postalAddress**

419

420 attributetype (2.5.4.16 NAME ‘postalAddress’

421 EQUALITY caseIgnoreListMatch

422 SUBSTR caseIgnoreListSubstringsMatch

423 SYNTAX 1.3.6.1.4.1.1466.115.121.1.41

424)

425

Attribute Name	postalAddress
Reference	RFC 2256
Object Class	organizationalPerson
Friendly Name	Mailing Address
Description	IC Person’s address for receiving mail
Allowable Values	Full address used to receive mail
Example	1 Main St., Fairfax, VA 22030-4345
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

426

427 **3.3.26 postalCode**

428

429 attributetype (2.5.4.17 NAME ‘postalCode’

430 EQUALITY caseIgnoreMatch

431 SUBSTR caseIgnoreSubstringsMatch

432 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

433)

434

Attribute Name	postalCode
Reference	RFC 2256
Object Class	organizationalPerson
Friendly Name	Physical Postal Code
Description	IC Person's physical postal code
Allowable Values	XXXXX-XXXX (if last four digits are known)
Example	22030-4345
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

435

436 **3.3.27 productionManager**

437

438 IC-defined attribute. Suggested definition for implementation by IC Element:

439 attributetype (2.16.840.1.101.2.2.1.152 NAME 'productionManager'

440 EQUALITY caseIgnoreMatch

441 SUBSTR caseIgnoreSubstringsMatch

442 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

443 SINGLE-VALUE

444)

445

Attribute Name	productionManager
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Production Manager
Description	IC Person's Production Manager
Allowable Values	Distinguished Name of production manager
Example	cn=Smith Joe K Jr smithj,ou=test,o=u.s.government,c=us
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

446

447 **3.3.28 rank**

448

449 IC-defined attribute. Suggested definition for implementation by IC Element:

450 attributetype (2.16.840.1.101.2.2.1.133 NAME 'rank'

451 EQUALITY caseIgnoreMatch

452 SUBSTR caseIgnoreSubstringsMatch
 453 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 454 SINGLE-VALUE
 455)
 456

Attribute Name	rank
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Grade/Rank
Description	Individual's GSA defined grade level
Allowable Values	GSA defined grades with two digit level required <Schedule>-<Level>
Example	GS-01 O-01 E-09, etc.
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

457
 458 **3.3.29 resourceSecurityMark**
 459
 460 IC-defined attribute. Suggested definition for implementation by IC Element:
 461 attributetype (2.16.840.1.101.2.2.1.161 NAME 'resourceSecurityMark'
 462 EQUALITY caseIgnoreMatch
 463 SUBSTR caseIgnoreSubstringsMatch
 464 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 465 SINGLE-VALUE
 466)
 467

Attribute Name	resourceSecurityMark
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson, icOrgServer
Friendly Name	Resource Classification
Description	The classification markings for the associated directory object for both IC Person and Non-Person Entities.
Allowable Values	Classification banner as described in the latest published version of the CAPCO Register and Implementation Manual
Example	UNCLASSIFIED//FOUO

Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

468

469 **3.3.30 secureFacsimileNumber**

470

471 IC-defined attribute. Suggested definition for implementation by IC Element:

472 attributetype (2.16.840.1.101.2.2.1.127 NAME 'secureFacsimileNumber'

473 EQUALITY caseIgnoreMatch

474 SUBSTR caseIgnoreSubstringsMatch

475 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

476 SINGLE-VALUE

477)

478

Attribute Name	secureFacsimileNumber
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Secure FAX Number
Description	IC Person's secure/classified FAX number
Allowable Values	<Country Code> (Area Code) <Prefix> <Suffix>
Example	(703) 561-0000
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

479

480 **3.3.31 secureTelephoneNumber**

481

482 IC-defined attribute. Suggested definition for implementation by IC Element:

483 attributetype (2.16.840.1.101.2.2.1.128 NAME 'secureTelephoneNumber'

484 EQUALITY caseIgnoreMatch

485 SUBSTR caseIgnoreSubstringsMatch

486 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

487 SINGLE-VALUE

488)

489

Attribute Name	secureTelephoneNumber
----------------	-----------------------

Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Secure Telephone Number
Description	IC Person's secure/classified phone number
Allowable Values	Authoritative secure telephone number provided by the user's home agency (seven digits in length)
Example	867-5309
Provisioning	Policy-based
Authentication	Network
Single/Multi	SINGLE-VALUE

490

491 **3.3.32 serverPOC**

492

493 IC-defined attribute. Suggested definition for implementation by IC Element:

494 attributetype (2.16.840.1.101.2.2.2.201 NAME 'serverPOC'

495 EQUALITY caseIgnoreMatch
 496 SUBSTR caseIgnoreSubstringsMatch
 497 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 498 SINGLE-VALUE
 499)
 500

Attribute Name	serverPOC
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgServer
Friendly Name	Server Point of Contact
Description	Name of an IC Person or IC Element organizational point of contact responsible for an IC Non-Person Entity
Allowable Values	Name of an IC Person or IC Element organizational POC
Example	Valid name
Provisioning	Mandatory
Authentication	Strong User
Single/Multi	SINGLE-VALUE

501

502 **3.3.33 serverURL**

503

504 IC-defined attribute. Suggested definition for implementation by IC Element:

505 attributetype (2.16.840.1.101.2.2.2.202 NAME 'serverURL'

506 EQUALITY caseIgnoreMatch

507 SUBSTR caseIgnoreSubstringsMatch
 508 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 509 SINGLE-VALUE
 510)
 511

Attribute Name	serverURL
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgServer
Friendly Name	Server URL
Description	Uniform/Universal Resource Locator (URL) for IC Non-Person Entity when applicable
Allowable Values	Valid URL for IC Non-Person Entity
Example	https://myserver.dni.ic.gov
Provisioning	Optional
Authentication	Strong User
Single/Multi	SINGLE-VALUE

512
 513 **3.3.34 serviceOrAgency**
 514
 515 IC-defined attribute. Suggested definition for implementation by IC Element:
 516 attributetype (2.16.840.1.101.2.2.1.82 NAME ‘serviceOrAgency’
 517 EQUALITY caseIgnoreMatch
 518 SUBSTR caseIgnoreSubstringsMatch
 519 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 520 SINGLE-VALUE
 521)
 522

Attribute Name	serviceOrAgency
Reference	IC FSD Technical Reference
Object Class	icOrgPerson, icOrgServer
Friendly Name	Home Organization
Description	IC Person’s owning organization (e.g. CIA, DIA, NGA, etc.) If military, this attribute contains the agency to which they are assigned. If a contractor, this attribute contains the agency that holds their contract. IC Non-Person Entity’s owning organization.

Allowable Values	Commonly recognized agency acronym or identifier (CIA, DIA, DNI, NSA, NGA, NRO, DOJ, DOS, DOE, DHS, DOT, DOI, HHS, DOC, TREA, USDA, EOP, NRC, FRB, USCP, U.S. Congress, USAID, USPS, USPIS, NASA, EPA, DVA). DoD values not covered above will be determined and included in a later issuance of the Data Encoding Specification for the IC Full Service Directory Schema.
Example	CIA NSA NGA, etc.
Provisioning	Mandatory
Authentication	Network
Single/Multi	SINGLE-VALUE

523

524 **3.3.35 SiprnetEmail**

525

526 IC-defined attribute. Suggested definition for implementation by IC Element:

527 attributetype (2.16.840.1.101.2.2.1.157 NAME ‘SiprnetEmail’

528 EQUALITY caseIgnoreMatch
 529 SUBSTR caseIgnoreSubstringsMatch
 530 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 531 SINGLE-VALUE
 532)
 533

Attribute Name	SiprnetEmail
Reference	DES for the IC Full Service Directory Schema
Object Class	icOrgPerson
Friendly Name	Siprnet Email Address
Description	Siprnet email address of an IC Person
Allowable Values	Official Siprnet email address of the IC Person as given by their email provider
Example	jsmith@intelink.sgov.gov
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

534

535 **3.3.36 sn**

536

537 attributetype (2.5.4.4 NAME 'sn' SUP name)

538

Attribute Name	sn
Reference	RFC 2256
Object Class	Person
Friendly Name	Surname, Last Name
Description	This is the X.500 surname attribute, which contains the family name of a person.
Allowable Values	For IC Persons, this should reflect a person's legal last name
Example	Smith Jones
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

539

540 **3.3.37 st, stateOrProvinceName**

541

542 attributetype (2.5.4.8 NAME ('st' 'stateOrProvinceName') SUP name)

543

Attribute Name	st, stateOrProvinceName
Reference	RFC 2256
Object Class	organizationalPerson
Friendly Name	Physical State or Province
Description	IC Person's physical state or province name
Allowable Values	Standard Post Office abbreviation for state or province name
Example	VA
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

544

545 **3.3.38 street**

546

547 attributetype (2.5.4.9 NAME ('street' 'streetAddress')

548 EQUALITY caseIgnoreMatch

549 SUBSTR caseIgnoreSubstringsMatch

550 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

551)

552

Attribute Name	street, streetAddress
Reference	RFC 2256
Object Class	organizationalPerson
Friendly Name	Physical Address
Description	IC Person's physical street address location
Allowable Values	Street address of a physical location
Example	1 Main St.
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

553

554 **3.3.39 telephoneNumber**

555

556 attributetype (2.5.4.20 NAME 'telephoneNumber'

557 EQUALITY telephoneNumberMatch

558 SUBSTR telephoneNumberSubstringsMatch

559 SYNTAX 1.3.6.1.4.1.1466.115.121.1.50

560)

561

Attribute Name	telephoneNumber
Reference	RFC 2256
Object Class	organizationalPerson
Friendly Name	Unclassified Telephone Number
Description	IC Person's unclassified/commercial phone number
Allowable Values	<Country Code (when applicable)> (Area Code) <Prefix> <Suffix>
Example	(703) 561-0000
Provisioning	Policy-based
Authentication	Network
Single/Multi	MULTI-VALUE

562

563 **3.3.40 title**

564

565 attributetype (2.5.4.12 NAME 'title' SUP name)

566

Attribute Name	title
----------------	-------

Reference	RFC 2256
Object Class	organizationalPerson
Friendly Name	Title
Description	The title attribute contains the title of an IC Person in their organizational context
Allowable Values	Major, Captain, Vice President, etc.
Example	Major Captain Vice President
Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

567

568 **3.3.41 uid**

569

570 attributetype (0.9.2342.19200300.100.1.1 NAME (‘uid’)

571 EQUALITY caseIgnoreMatch

572 SUBSTR caseIgnoreSubstringsMatch

573 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

574)

575

Attribute Name	uid
Reference	RFC 2798
Object Class	inetOrgPerson
Friendly Name	Agency Unique ID
Description	IC Element assigned unique identifier for IC Person IC Element assigned unique identifier for IC Non-Person Entity
Allowable Values	IC Element unique identifiers
Example	jsmith jsmith1234 12345, etc.
Provisioning	Optional, Mandatory for NPE
Authentication	Network
Single/Multi	MULTI-VALUE

576

577

578

579 **3.3.42 userCertificate**

580

581 userCertificate attributes must be transferred using the binary encoding, by requesting or
582 returning the attributes via ‘usercertificate;binary’

583

584 attributetype (2.5.4.36 NAME ‘userCertificate’

585 SYNTAX 1.3.6.1.4.1.1466.115.121.1.8)

586)

587

Attribute Name	userCertificate
Reference	RFC 2256, ICPKI Interface Specification
Object Class	inetOrgPerson
Friendly Name	PKI Certificate
Description	X.509-compliant PKI certificate issued to either an IC Person or IC Non-Person Entity
Allowable Values	Certificate issued by a trusted Certificate Authority operating within a trusted PKI
Example	ICPKI certificate
Provisioning	Policy-based, Mandatory for NPE
Authentication	Network
Single/Multi	MULTI-VALUE

588

589

590

591 **4. MANDATORY, POLICY-BASED, AND OPTIONAL**
 592 **ATTRIBUTES**

593

594 This Data Encoding Specification for the IC Full Service Directory Schema organizes attributes
 595 about an “IC Person” or “IC Non-Person Entity” into mandatory, policy-based or optional
 596 categories. These categories are defined as follows:

597

- 598 • Mandatory: Attributes that IC Elements MUST include in FSD records, without which
 599 the record will not be added to the IC FSD.
- 600 • Policy-based: Attributes which IC Elements MAY provide, if present in that IC
 601 Element’s internal directories.
- 602 • Optional: Attributes which IC Elements MAY provide to the IC FSD, depending on that
 603 IC Element’s security requirements and capabilities. Most optional attributes are not
 604 populated.

605

Attribute Name	Mandatory	Policy-Based	Optional
buildingName			
c			
cn			
companyName			
displayName			
employeeType			
expertCountry			
expertFunctionalArea			
facsimileTelephoneNumber			
generationQualifier			
givenName			
icEmail			
icNetworks			
icServerAddress			
initials			
internetEmail			

Attribute Name	Mandatory	Policy-Based	Optional
isICMember			
languageProficiency			
locality			
mail			
militaryTelephoneNumber			
nationality-Extended			
NiprnetEmail			
personalTitle			
postalAddress			
postalCode			
productionManager			
rank			
resourceSecurityMark			
secureFacsimileNumber			
secureTelephoneNumber			
serverPOC			
serverURL			
serviceOrAgency			
SiprnetEmail			
Sn			
St			
street			
telephoneNumber			
Title			
Uid	Mandatory only for NPE		
userCertificate	Mandatory only for NPE		

607 **Note:** employeeType and givenName are not mandatory attributes in terms of the
608 inetOrgPerson objectClass. Compliance with the mandatory requirement for
609 employeeType and givenName is enforced through the replication agreements in place
610 between the master IC FSD and participating IC Element Border directories.

611 **Note:** Once all supporting policies and IC Element workflow processes are in place to manage
612 the population of the isICMember attribute, it is envisioned that this attribute will be promoted to
613 Mandatory.

614

615 **5. SECURING ACCESS TO IC FSD ATTRIBUTES**

616

617 In the current implementation of the IC FSD, there are no stated requirements for controlling
618 access to the attributes. This technical specification establishes three authentication tiers,
619 providing graded authentication for attributes of varying sensitivity. These tiers are defined as
620 follows:

621

- 622 • Network authentication

- 623 ○ Permits end user access to content
- 624 ○ Primarily used to support IC White Pages functionality, for attributes viewable by
625 users through the IC White Pages.
- 626 ○ Relies on authentication at the user's desktop login.
- 627 ○ Applies to attributes such as name, citizenship, employee type, organization, email,
628 phone numbers, etc.

629

- 630 • Strong user authentication

- 631 ○ Permits end user access to content
- 632 ○ Used for attributes more sensitive than those above
- 633 ○ Requires users to present an IC PKI certificate
- 634 ○ Applies to attributes such as isICMember, mailing or physical address, company, etc.

635

- 636 • Strong server/application authentication

- 637 ○ Attributes which end users have no need to view in the IC FSD
- 638 ○ Attributes used by servers and applications
- 639 ○ Requires those servers and applications to present an IC PKI certificate
- 640 ○ Applies to attributes such as Language Proficiency, or Certificate Revocation List

641

642 The IC FSD operator and IC elements are expected to maintain the authentication levels defined
643 for each attribute, in whatever locations IC FSD data resides: border directories, element address
644 books, etc. A reduction from three to two IC FSD authentication tiers is foreseen (eliminating

645 network authentication and requiring strong user authentication to all user accessible content)
 646 when requirements are defined and supporting technology capabilities exist.
 647

Attribute Name	Network	Strong User	Strong Server
buildingName			
c			
cn			
companyName			
displayName			
employeeType			
expertCountry			
expertFunctionalArea			
facsimileTelephoneNumber			
generationQualifier			
givenName			
icEmail			
icNetworks			
icServerAddress			
initials			
internetEmail			
isICMember			
languageProficiency			
locality			
mail			
militaryTelephoneNumber			
nationality-Extended			
NiprnetEmail			
personalTitle			
postalAddress			
postalCode			
productionManager			

Attribute Name	Network	Strong User	Strong Server
rank			
resourceSecurityMark			
secureFacsimileNumber			
secureTelephoneNumber			
serverPOC			
serverURL			
serviceOrAgency			
SiprnetEmail			
sn			
st			
street			
telephoneNumber			
title			
uid			
userCertificate			

648

649 The IC FSD operator and IC elements are expected to perform audit at a minimum as indicated
 650 through applicable security controls mandated by ICD 503 and subordinate policy documents,
 651 and as directed by IC-wide audit policies.

652

653 **6. EFFECTIVE DATE**

654

655 TBD

656

657 **APPENDIX A – IC FSD SCHEMA FOR ICPKI ROOT AND**
 658 **INTERMEDIATE CERTIFICATE AUTHORITIES**

659

660 For those IC Elements providing Certification Authority (CA) capabilities under the Intelligence
 661 Community Public Key Infrastructure (ICPKI), the following objectClass and associated
 662 attributes should be used as a basis to propagate critical CA information into the IC FSD
 663 architecture. This CA information is vital to the proper PK-enablement of services and
 664 applications within the IC TS/SCI enterprise.

665

```
objectclass (2.5.6.16 NAME 'certificationAuthority' SUP top
AUXILIARY
  DESC 'RFC2256: certificationAuthority'
  MUST ( authorityRevocationList $ 
          certificateRevocationList $ cACertificate )
  MAY crossCertificatePair
)
```

666

667 **Note:** the objectClass hierarchy in support of certificationAuthority may vary
 668 depending on the commercial Certificate Authority product implementation. In addition, the
 669 crossCertificatePair attribute is not applicable to the ICPKI.

670

671 **A.1 authorityRevocationList**

672

673 The use and support of authority revocation lists by the ICPKI is not specifically identified in the
 674 ICPKI Certificate Policy or Interface Specifications. However, it is a mandatory attribute within
 675 the certificationAuthority objectClass and is currently supported by all ICPKI
 676 Certificate Authorities.

677 This attribute is to be stored and requested in binary form, as
 678 'authorityRevocationList;binary'

679

680 attributetype (2.5.4.38 NAME 'authorityRevocationList'
 681 SYNTAX 1.3.6.1.4.1.1466.115.121.1.9
 682)

683

Attribute Name	authorityRevocationList
Reference	RFC 2256

Object Class	certificationAuthority
Friendly Name	Authority Revocation List
Description	An authority revocation list is a form of CRL containing certificates issued to certificate authorities, contrary to CRLs which contain revoked end-entity certificates
Allowable Values	Valid authority revocation list
Example	Any ARL issued by an ICPKI Certificate Authority
Provisioning	Mandatory (LDAP object class requirement)
Authentication	Network
Single/Multi	Multi

684

685 **A.2 certificateRevocationList**

686

687 This attribute is to be stored and requested in binary form, as
688 ‘certificateRevocationList;binary’

689

690 attributetype (2.5.4.39 NAME ‘certificateRevocationList’

691 SYNTAX 1.3.6.1.4.1.1466.115.121.1.9

692)

693

Attribute Name	certificateRevocationList
Reference	RFC 2256, RFC 5280
Object Class	certificationAuthority
Friendly Name	Certificate Revocation List, CRL
Description	A CRL lists all unexpired certificates, within the scope of a specific Certificate Authority, that have been revoked for one of the reasons as defined in the <i>Intelligence Community Public Key Infrastructure Certificate Policy</i>
Allowable Values	A valid X.509 V2 CRL as defined in RFC 5280 and the <i>Intelligence Community Public Key Infrastructure Interface Specification</i>
Example	Any CRL issued by an ICPKI Certificate Authority
Provisioning	Mandatory
Authentication	Network
Single/Multi	Multi

694

695 **A.3 cACertificate**

696

697 This attribute is to be stored and requested in binary form, as ‘cACertificate;binary’

698

699 attributetype (2.5.4.37 NAME ‘cACertificate’
700 SYNTAX 1.3.6.1.4.1.1466.115.121.1.8
701)
702

Attribute Name	cACertificate
Reference	RFC 2256, RFC 5280
Object Class	certificationAuthority
Friendly Name	CA Certificate
Description	A Certificate Authority’s X.509 v3 compliant certificate
Allowable Values	A valid X.509 V3 certificate as defined in RFC 5280 and the <i>Intelligence Community Public Key Infrastructure Interface Specification</i>
Example	Any ICPKI Certificate Authority certificate
Provisioning	Mandatory
Authentication	Network
Single/Multi	Multi

703 Appendix B – Change History

704 This table summarizes the version identifier history for this Data Encoding Specification.

705 **Identifier History**

Version	Date	Purpose
1.0	14 DEC 2011	Initial Release

706

707 This table summarizes the changes made to Version 1.0 in developing Version X.

708 **Change History**

Change	Artifacts Changed	Compatibility Notes

709

APPENDIX C – MODIFICATIONS TO PREVIOUS IC FSD SCHEMA

This IC Technical Specification revises certain aspects of the IC FSD Schema previously in use. These changes are outlined as follows:

New Attributes

`isICMember` and `generationQualifier` are being introduced as new attributes to be managed and populated by participating IC Elements.

Retired Attributes

The `COI` objectClass and all attributes contained within are no longer being included as part of the IC FSD schema due to lack of use.

Mandatory Attributes

`cn`, `employeeType`, `icNetworks`, and `resourceSecurityMark` are being promoted to Mandatory attributes.

employeeType Controlled Vocabulary

`GOV`, `MIL`, and `CTR` are being defined as the controlled vocabulary for the `employeeType` attribute.

serviceOrAgency Controlled Vocabulary

A finite set of Agency acronyms are being proposed as the controlled vocabulary for the `serviceOrAgency` attribute.

Authentication

In addition to schema changes, this technical specification establishes three authentication tiers for controlling access to IC FSD attributes of varying sensitivity. For a description of these new authentication requirements, please consult section 5 – *Securing Access to IC FSD Attributes* of this technical specification.

APPENDIX D – ACRONYMS

742

Acronym	Definition
ABAC	Attribute-Based Access Control
ACSS	Allied Collaborative Shared Services
CAPCO	Controlled Access Program Coordination Office
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CRL	Certificate Revocation List
DIA	Defense Intelligence Agency
DN	Distinguished Name
FSD	Full Service Directory
IC	Intelligence Community
ICD	IC Directive
ICS	IC Standard
ICTS	IC Technical Specification
ISO	International Organization for Standardization
JWICS	Joint Worldwide Intelligence Communications System
LDAP	Lightweight Directory Access Protocol
NGA	National Geospatial-Intelligence Agency
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
ONEMail	Optimized Network Email
PKI	Public Key Infrastructure
RFC	Request For Comments
SAML	Security Assertion Markup Language
SCI	Sensitive Compartment Information
SLA	Service Level Agreement
TS	Top Secret
UAAS	Unified Authorization and Attribute Services
XML	Extensible Markup Language

X.509	X.509: Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks
X.520	X.520: Information Technology – Open Systems Interconnection – The Directory: Selected Attribute Types

743

APPENDIX E – BIBLIOGRAPHY

- 744 (ICD 500)
745 Director of National Intelligence Chief Information Officer. Intelligence Community Directive
746 Number 500. 7 August 2008. Office of the Director of National Intelligence.
747 http://www.dni.gov/electronic_reading_room/ICD_500.pdf.
- 749
- 750 (ICD 501)
751 Discovery and Dissemination or Retrieval of Information within the IC. Intelligence Community
752 Directive 501. 21 January 2009. Office of the Director of National Intelligence.
753 http://www.dni.gov/electronic_reading_room/ICD_501.pdf.
- 754
- 755 (ICD 503)
756 Intelligence Community Information Technology Systems Security, Risk Management,
757 Certification and Accreditation. Intelligence Community Directive 503. 15 September 2008.
758 Office of the Director of National Intelligence.
759 http://www.dni.gov/electronic_reading_room/ICD_503.pdf.
- 760
- 761 (ICS 500-13)
762 Intelligence Community Optimized Network Email Display Name Format Intelligence
763 Community Standard
764 Number 500-13. 16 October 2008. Office of the Director of National Intelligence
765 http://www.dni.gov/electronic_reading_room/ICS-500-13.pdf.
766
- 767 (ICS 500-14)
768 Intelligence Community Optimized Network Email Public Key Infrastructure Intelligence
769 Community Standard
770 Number 500-14. 16 October 2008. Office of the Director of National Intelligence
771 http://www.dni.gov/electronic_reading_room/ICS-500-14.pdf.
772
- 773 (ICS 500-15)
774 Intelligence Community Optimized Network E-Mail Full Service Directory Intelligence
775 Community Standard
776 Number 500-15. 16 October 2008. Office of the Director of National Intelligence
777 http://www.dni.gov/electronic_reading_room/ICD_500_15.pdf.
778
- 779 (ICS 500-20)
780 Intelligence Community Enterprise Standards Compliance Intelligence Community Standard
781 Number 500-20. 16 December 2010. Office of the Director of National Intelligence.
782 http://www.dni.gov/electronic_reading_room/ ICS_500-20.pdf.
783

784 (ICS 500-21)
785 Tagging of Intelligence and Intelligence-related Information. Intelligence Community Standard
786 Number 500-21. 28 January 2011. Office of the Director of National Intelligence.
787 http://www.dni.gov/electronic_reading_room/ICS_500-21.pdf.
788
789 (ICS 500-xx) TBD
790 Intelligence Community Enterprise Authorization Attributes. Intelligence Community Technical
791 Specification Number 500-XX. Date. TBD Office of the Director of National Intelligence.
792 http://www.dni.gov/electronic_reading_room/ICD_500_XX.pdf.
793
794 (RFC 2119)
795 Key words for use in RFCs to Indicate Requirement Levels
796 <http://www.ietf.org/rfc/rfc2110.txt>
797
798 (RFC 2256)
799 A Summary of the X.500(96) User Schema for use with LDAPv3
800 <http://www.ietf.org/rfc/rfc2256.txt>
801
802 (RFC 2798)
803 Definition of the inetOrgPerson LDAP Object Class
804 <http://www.ietf.org/rfc/rfc2798.txt>
805
806 (RFC 2252)
807 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
808 <http://www.ietf.org/rfc/rfc2252.txt>
809
810 (RFC 1274)
811 The COSINE and Internet X.500 Schema
812 <http://www.ietf.org/rfc/rfc1274.txt>
813
814 (RFC 5280)
815 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)
816 Profile
817 <http://www.ietf.org/rfc/rfc5280.txt>
818
819 (ISO-3166-1)
820 Codes for the representation of names of countries and their subdivisions – part 1: Country
821 codes. International Organization for Standardization.
822 Alpha-3 character codes are available for purchase at
823 http://www.iso.org/iso/country_codes/iso_3166_databases.htm
824

APPENDIX F – POINTS OF CONTACT

The Intelligence Community Chief Information Officer (IC CIO) facilitates one or more collaboration and coordination forums charged with the adoption, modification, development, and governance of IC technical specifications of common concern. This technical specification was produced by the IC CIO and coordinated with these forums, approved by the IC CIO or a designated representative, and made available at ODNI-sponsored web sites. Direct all inquiries about this IC technical specification to the IC CIO Identity and Access Management Program.

833 Appendix G - IC CIO Approval Memo

834 An Office of the Intelligence Community Chief Information Officer (OCIO) Approval
835 Memo should accompany this enterprise technical data specification bearing the signature of the
836 Intelligence Community Chief Information Officer (IC CIO) or an IC CIO-designated official(s).
837 If an OCIO Approval Memo is not accompanying this specification's version release package,
838 then refer back to the authoritative web location(s) for this specification to see if a more
839 complete package or a specification update is available.

840 Specification artifacts display a date representing the last time a version's artifacts as a
841 whole were modified. This date most often represents the conclusion of the IC element
842 collaboration and coordination process. Once the IC element coordination process is complete,
843 the specification goes through an internal OCIO staffing and coordination process leading to
844 signature of the OCIO Approval Memo. The signature date of the OCIO Approval Memo will be
845 later than the last modified date shown on the specification artifacts by an indeterminable time
846 period.

847 Upon signature of the OCIO Approval Memo, IC elements may begin to use this
848 specification version in order to address mission and business objectives. However, it is critical
849 for IC elements, prior to disseminating information encoded with this new specification version,
850 to ensure that key enterprise services and consumers are prepared to accept this information. IC
851 elements should work with enterprise service providers and consumers to orchestrate an orderly
852 implementation transition to this specification version in concert with mandatory and retirement
853 usage decisions captured in the IC Enterprise Standards Baseline as defined in Intelligence
854 Community Standard (ICS) 500-20.