



# **Intelligence Community Technical Specification**

---

## **Data Encoding Specification for IC Full Service Directory Schema**

**Version 2021-NOV**

December 1, 2022

Distribution Notice:

This document has been approved for Public Release and is available for use without restriction.

# Table of Contents

Chapter 1 - Introduction .....	1
1.1 - Purpose .....	1
1.2 - Scope .....	1
1.3 - Enterprise Need .....	3
1.4 - Conventions .....	4
1.4.1 - Multiplicity .....	4
1.5 - Dependencies .....	5
1.5.1 - Specification Dependencies .....	5
1.5.2 - Inverse Dependencies .....	8
Chapter 2 - Development Guidance .....	9
2.1 - IC FSD System Description .....	9
2.2 - IC FSD Policy Statements .....	10
2.2.1 - Duplicate Entries .....	10
2.2.2 - Account Disablement .....	10
Chapter 3 - Constraints .....	11
Chapter 4 - Conformance Validation .....	12
Chapter 5 - IC FSD Schema .....	13
5.1 - IC FSD Schema for IC Person .....	13
5.2 - IC FSD Schema for IC Non-Person Entity .....	15
5.3 - IC FSD Attribute Definitions .....	15
5.3.1 - adminOrganization .....	16
5.3.2 - auditRoutingOrganization .....	17
5.3.3 - ATOSStatus .....	18
5.3.4 - buildingName .....	19
5.3.5 - c, countryName .....	20
5.3.6 - cn, commonName .....	20
5.3.7 - companyName .....	21
5.3.8 - countryOfAffiliation .....	22
5.3.9 - displayName .....	22
5.3.10 - dn, distinguishedName .....	23
5.3.11 - dutyOrganization .....	24
5.3.12 - dutySubOrganization .....	26
5.3.13 - employeeType .....	26
5.3.14 - expertCountry .....	28
5.3.15 - expertFunctionalArea .....	28
5.3.16 - facsimileTelephoneNumber .....	29
5.3.17 - generationQualifier .....	29
5.3.18 - givenName .....	30
5.3.19 - icEmail .....	30
5.3.20 - icNetworks .....	31
5.3.21 - icServerAddress .....	32
5.3.22 - initials .....	33
5.3.23 - instantMessageAddress .....	33
5.3.24 - internetEmail .....	34
5.3.25 - isICMember .....	34
5.3.26 - l, localityName .....	35

5.3.27 - languageProficiency .....	36
5.3.28 - lifeCycleStatus .....	37
5.3.29 - mail .....	37
5.3.30 - militaryTelephoneNumber .....	38
5.3.31 - nationality-Extended .....	38
5.3.32 - niprnetEmail .....	39
5.3.33 - personalTitle .....	40
5.3.34 - personaUID .....	41
5.3.35 - postalAddress .....	41
5.3.36 - postalCode .....	42
5.3.37 - preferredName .....	42
5.3.38 - productionManager .....	43
5.3.39 - rank .....	44
5.3.40 - resourceSecurityMark .....	45
5.3.41 - secureFacsimileNumber .....	45
5.3.42 - secureTelephoneNumber .....	46
5.3.43 - serverPOC .....	47
5.3.44 - serverURL .....	47
5.3.45 - serviceOrAgency .....	48
5.3.46 - siprnetEmail .....	49
5.3.47 - sn, surname .....	50
5.3.48 - st, stateOrProvinceName .....	50
5.3.49 - street, streetAddress .....	51
5.3.50 - telephoneNumber .....	51
5.3.51 - title .....	52
5.3.52 - uid .....	52
5.3.53 - userCertificate .....	53
Chapter 6 - Attribute Status .....	55
Chapter 7 - Securing Access to IC FSD Attributes .....	58
Chapter 8 - IC FSD Schema for PKI Root and Intermediate Certificate Authorities .....	61
8.1 - authorityRevocationList .....	61
8.2 - certificateRevocationList .....	62
8.3 - cACertificate .....	63
8.4 - icNetworks .....	63
8.5 - resourceSecurityMark .....	64
Appendix A - Feature Summary .....	66
A.1 - FSD Feature Summary .....	66
A.1.1 - Features from V2015-AUG to V2021-NOV .....	66
A.1.2 - Features from V2 to V2015-AUG .....	67
A.1.3 - Features from V1 to V2 .....	67
Appendix B - Change History .....	68
B.1 - V2021-NOVChange Summary .....	68
B.2 - V2019-SEP Change Summary .....	69
B.3 - V2016-SEP Change Summary .....	70
B.4 - V2015-AUG Change Summary .....	70
B.5 - V2014-DEC Change Summary .....	71
B.6 - V3 Change Summary .....	72
B.7 - V2 Change Summary .....	72
B.8 - V1 Change Summary .....	73

Appendix C - Glossary .....	75
Appendix D - List of Abbreviations .....	77
Appendix E - Bibliography .....	81
Appendix F - Points of Contact .....	86
Appendix G - IC CIO Approval Memo .....	87

## List of Figures

Figure 1 - Related Specifications .....	7
Figure 2 - IC FSD Replication .....	9

## List of Tables

Table 1 - Definitions of Multiplicities .....	4
Table 2 - Dependencies .....	5
Table 3 - adminOrganization .....	16
Table 4 - Foreign Government adminOrganization Countries .....	17
Table 5 - auditRoutingOrganization .....	18
Table 6 - ATOSStatus .....	19
Table 7 - buildingName .....	19
Table 8 - c, countryName .....	20
Table 9 - cn, commonName .....	20
Table 10 - companyName .....	21
Table 11 - countryOfAffiliation .....	22
Table 12 - displayName .....	23
Table 13 - dn, distinguishedName .....	24
Table 14 - dutyOrganization .....	25
Table 15 - Foreign Government dutyOrganization Countries .....	25
Table 16 - dutySubOrganization .....	26
Table 17 - employeeType .....	27
Table 18 - expertCountry .....	28
Table 19 - expertFunctionalArea .....	29
Table 20 - facsimileTelephoneNumber .....	29
Table 21 - generationQualifier .....	30
Table 22 - givenName .....	30
Table 23 - icEmail .....	31
Table 24 - icNetworks .....	31
Table 25 - icServerAddress .....	32
Table 26 - initials .....	33
Table 27 - instantMessageAddress .....	33
Table 28 - internetEmail .....	34
Table 29 - isICMember .....	35
Table 30 - l, localityName .....	35
Table 31 - languageProficiency .....	36
Table 32 - lifeCycleStatus .....	37
Table 33 - mail .....	37
Table 34 - militaryTelephoneNumber .....	38
Table 35 - nationality-Extended .....	39
Table 36 - niprnetEmail .....	40
Table 37 - personalTitle .....	40
Table 38 - personaUID .....	41
Table 39 - postalAddress .....	42
Table 40 - postalCode .....	42
Table 41 - preferredName .....	43
Table 42 - productionManager .....	43
Table 43 - rank .....	44
Table 44 - resourceSecurityMark .....	45
Table 45 - secureFacsimileNumber .....	46
Table 46 - secureTelephoneNumber .....	46

Table 47 - serverPOC .....	47
Table 48 - serverURL .....	48
Table 49 - serviceOrAgency .....	48
Table 50 - siprnetEmail .....	50
Table 51 - sn, surname .....	50
Table 52 - st, stateOrProvinceName .....	50
Table 53 - street, streetAddress .....	51
Table 54 - telephoneNumber .....	52
Table 55 - title .....	52
Table 56 - uid .....	53
Table 57 - userCertificate .....	53
Table 58 - IC Person Attributes Mandatory, Policy-Based, Optional or Deprecated .....	55
Table 59 - IC Non-Person Entity Attributes Mandatory, Policy-Based, Optional or Deprecated ...	57
Table 60 - Securing Access to IC FSD IC Person Attributes .....	58
Table 61 - Securing Access to IC FSD IC Non-Person Entity Attributes .....	60
Table 62 - authorityRevocationList .....	62
Table 63 - certificateRevocationList .....	62
Table 64 - cACertificate .....	63
Table 65 - icNetworks .....	64
Table 66 - resourceSecurityMark .....	64
Table 67 - Feature Summary Legend .....	66
Table 68 - FSD Feature Comparison V2015-AUG to V2021-NOV .....	66
Table 69 - FSD Feature Comparison V2 to V2015-AUG .....	67
Table 70 - FSD Feature Comparison V1 to V2 .....	67
Table 71 - Identifier History .....	68
Table 72 - Data Encoding Specification V2021-NOV Change Summary .....	69
Table 73 - Data Encoding Specification V2019-SEP Change Summary .....	69
Table 74 - Data Encoding Specification V2016-SEP Change Summary .....	70
Table 75 - Data Encoding Specification V2015-AUG Change Summary .....	71
Table 76 - Data Encoding Specification V2014-DEC Change Summary .....	71
Table 77 - Data Encoding Specification V3 Change Summary .....	72
Table 78 - Data Encoding Specification V2 Change Summary .....	72
Table 79 - Data Encoding Specification V1 Change Summary .....	73



## Chapter 1 - Introduction

### 1.1 - Purpose

This *Data Encoding Specification for IC Full Service Directory Schema* (FSD), codifies the set of Lightweight Directory Access Protocol (LDAP) Attributes that Intelligence Community (IC) elements are expected to provide to the IC Full Service Directory (FSD). It will facilitate the availability, accuracy, and standardization of these Attributes across the IC Top Secret (TS)/ Sensitive Compartmented Information (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 accessing the attributes.

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

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

Each IC FSD entry about a person provides attributes about a “persona”, which means that one person may have several IC FSD records, each with distinct attributes about that persona. A persona is an electronic identity that can be unambiguously associated with a single person. A single person may have multiple personas, with each persona being managed by the same or by different organizations (such as a Director of National Intelligence (DNI) contractor who is also an Army reservist).

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

### 1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML<sup>[10]</sup>) defines the basic conceptual structure and outlines the core philosophy of IC technical specifications. For convenience, a copy of this framework is included in every package.

This specification is applicable to the IC and access to the information produced by, stored within, or shared throughout the IC's IC TS/SCI information domain as defined in Intelligence Community Program Guidance (ICPG) 500.1, *Intelligence Community Policy Guidance, Digital Identity*<sup>[14]</sup>. Identity Attributes defined at the enterprise level within the IC may have relevance outside the scope of the IC; however, prior to applying outside of this defined scope, the models should be closely scrutinized and differences separately documented and assessed for applicability.

This document lists 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; and Authentication requirements for the attributes.

FSD Attributes are assigned per persona. A persona is an electronic identity that is unambiguously associated with a single person or non-person entity Non-Person Entity (NPE). A single person or NPE may have multiple personas, with each persona being managed by the same or by different organizations (e.g., a DNI contractor who is also an Army reservist).

The IC FSD provides enterprise-level directory services to both IC personnel and applications on the United States (US) IC 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 its 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 IC TS/SCI users can locate colleagues' email addresses, phone numbers, and other organizational information <sup>1</sup>
- The sharing of user email attributes between IC Elements' internal address books, to facilitate cross-agency and Secure/Media Type (S/MIME)-enabled email capabilities
- The sharing of user email attributes with the IC TS/ SCI Allied 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 Services (UAAS) Federation, within which the IC FSD serves as a repository for authoritative authorization attributes.

The IC FSD also provides two attributes that indicate where attributes can be passed (e.g., Joint Worldwide Intelligence Communications System (JWICS,) The National Security Agency intranet (NSANET), Allied Collaborative Shared Services (ACSS)):

- **@resourceSecurityMark** – an overall data classification and control marking for each entry in the IC FSD (e.g., “UNCLASSIFIED//FOUO”).
- **@icNetworks** - a releasability attribute specifying the IC-approved network on which the object is allowed to be passed (e.g., JWICS, NSANET, ACSS).

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

- Instances of attributes populated incompletely by IC Elements
- Instances of attributes populated with inconsistent values, making resource providers unable to rely on them for access control

---

<sup>1</sup> Uniform Resource Locator (URL) = <http://directory.csp.ic.gov/eGuide/index.html>

- Lack of clear authentication requirements to secure access to attributes, which has become increasingly important with the dissemination of attributes to other environments, makes some elements hesitant to share and populate certain attributes.

IC elements again demonstrated partnership by addressing these limitations together, resulting in this document, which:

- Formally documents the IC FSD attribute schema
- Increases the number of IC FSD attributes required for each entry
- Defines attribute names
- Identifies the attributes requiring controlled values
- Defines those controlled values
- Establishes authentication requirements for each attribute
- Ensures interoperability with the IC enterprise authorization attributes exchanged through the Unified Authorization and Attribute Service federation, as documented in *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set* (UIAS.XML<sup>[33]</sup>)

## 1.3 - Enterprise Need

The IC FSD provides a replication hub for identity attribute related information. The IC FSD replicates identity information to and from IC agency border directories. This centralized repository of select IC user information is automatically populated from each participating agency's border directories and consolidated in the IC FSD. The IC FSD is critical to the operation of many programs within the IC. The IC FSD provides an industry standard LDAP interface for attribute retrieval of multiple records at one time.

Defining the set of IC enterprise directory attributes and values for sharing through LDAP supports the opportunity for consistent and assured information sharing across the enterprise. Implementers of IC FSD require coordination of attribute definitions. This requires the usage of standardized attribute names and values when exchanging attributes between agencies.

Both enterprise needs and requirements for this specification can be found in the following policies and implementation guidance:

- 500 Series:
  - Intelligence Community Directive (ICD) 500, *Director Of National Intelligence Chief Information Officer*<sup>[11]</sup>
  - ICPG 500.1, *Digital Identity*<sup>[14]</sup>
  - ICPG 500.2, *Attribute-based Authorization and Access Management*<sup>[15]</sup>
  - Intelligence Community Standard (ICS) 500-13, *Intelligence Community Optimized Network Email Display Name Format*<sup>[16]</sup>
  - ICS 500-15, *Intelligence Community Optimized Network Email Full Service Directory*<sup>[17]</sup>
  - ICS 500-20, *IC Enterprise Standards Compliance*<sup>[18]</sup>
  - ICS 500-29, *IC Digital Identifier*<sup>[20]</sup>

- ICS 500-30, *Enterprise Authorization Attributes: Assignment, Authoritative Sources, and Use for Attribute-Based Access Control of Resources* [\[21\]](#)
- IC CIO Directives:
  - *Intelligence Community Public Key Infrastructure Certificate Policy* [\[7\]](#)

## 1.4 - Conventions

Certain technical and presentation conventions are used in the creation of the IC technical specifications to ensure readability and understanding. For details, please see the “Specification Conventions” chapter in the IC-SF.XML [\[10\]](#).

Several key terms in this document are to be interpreted as defined in ICS 500-30, *Intelligence Community Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources* [\[21\]](#), Appendix B. These terms, with their definitions are defined in the [Appendix C - Glossary](#) and include the following: Attribute, Integree, NPE, and PE.

### 1.4.1 - Multiplicity

Throughout this document, references are made to the multiplicity of attributes and parameters. Multiplicity defines the allowed number of occurrences of an attribute value, and whether the attribute is required or optional.

Table [Table 1](#) follow Object Management Group (OMG)'s UML, *Unified Modeling Language* [\[34\]](#) and International Organization for Standardization (ISO) 11179-3, *SO/IEC 11179, Information Technology -- Metadata registries (MDR), Part 3: Registry metamodel and basic attributes* [\[29\]](#).

**Table 1 - Definitions of Multiplicities**

Multiplicity	Description
[1..1]	Indicates the attribute is mandatory and must contain one and only one value.
[0..1]	Indicates the attribute is optional and may contain at most one value.
[0..*]	Indicates the attribute is optional and may contain any number of values, including none.
[1..*]	Indicates the attribute is mandatory and may contain one or more values.
[0..n]	Indicates the attribute is optional and may contain at most n values, where n is a finite integer. An example in this specification is the multiplicity of <b>auditRoutingOrganization</b> , which is [0..10].
[n..m]	Indicates the attribute is mandatory having at least n values, and may contain at most m values, where n and m are finite integers.

In some cases within this specification, attribute value multiplicity requirements for an attribute will vary depending on whether the entity is a person entity or a non-person entity. In these situations,

multiplicity requirements will be noted with "PE" for person entities, and "NPE" for non-person entities.

## 1.5 - Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. For specific definitions of dependency terminology used throughout this section, please see the "Dependency Definitions" chapter in the IC-SF.XML<sup>[10]</sup>.

### 1.5.1 - Specification Dependencies

This technical specification directly depends on the technical specifications, documentation, and implementations listed in [Table 2](#). The dependencies listed below are directly referenced in this specification (e.g., Schema, Schematron), and are normative or informative as indicated.

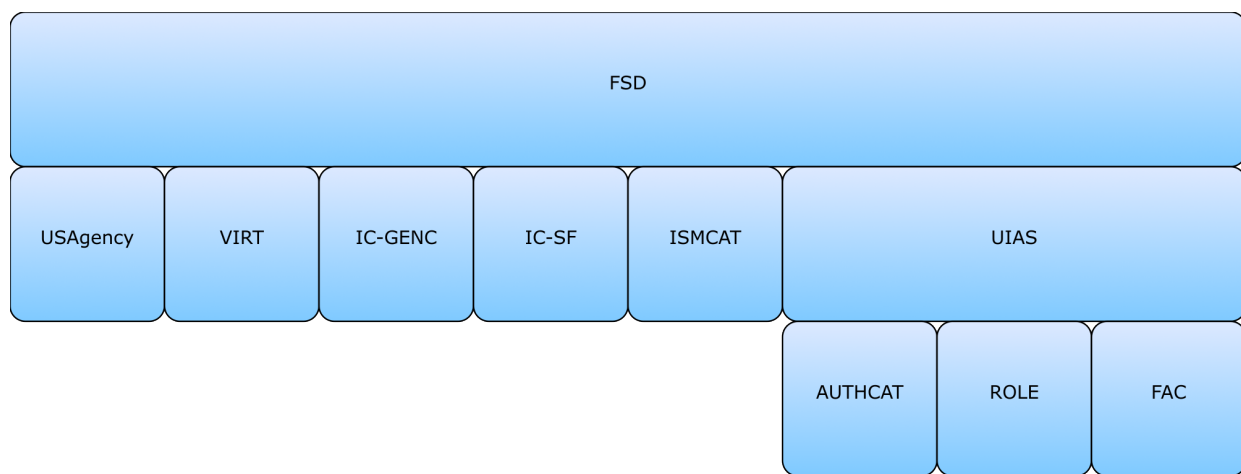
The subsequent figure, [Figure 1](#), is an informative graphical representation of all of the Intelligence Community Chief Information Officer (IC CIO) specifications related to this specification. The graphic depicts dependencies. However, the representations may not match an exact schema import tree or dependency diagram that an analysis of the Schema, Schematron or other documents would yield. For example, the graphic only shows a given specification once even though it may actually be imported by many specifications or be a direct dependency. All IC CIO specifications listed in [Table 2](#) will be shown in [Figure 1](#); however not all IC CIO specifications listed in [Figure 1](#) may appear in [Table 2](#). [Figure 1](#) is to aid users in gaining a general understanding of all dependencies whether direct or transitive.

**Table 2 - Dependencies**

Name	Dependency Description
Internet Engineering Task Force (IETF)- Request for Comments (RFC) 4510, <i>Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map</i> <sup>[23]</sup>	Internet Engineering Task Force standard for Lightweight Directory Access Protocol

Name	Dependency Description
Schematron <sup>[32]</sup>	<p>Schematron — ISO/International Electrotechnical Commission (IEC) 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative.</p> <p>The Schematron rules are normative in the sense that they convey criteria that a document <b>MUST</b> adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers <b>MAY</b> use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification.</p> <p>Note: The Schematron rules in this specification use Transformations (XSLT) 2.0<sup>[37]</sup> query binding.</p>
<i>CVE Encoding Specification for Geopolitical Entities, Names, and Codes</i> (IC-GENC.CES.V2019-SEP+ <sup>[9]</sup> )	This specification depends on the LATEST technically sound, approved version of IC-GENC.CES <sup>[9]</sup> . At the time of this release, the latest version of IC-GENC.CES is 2019-SEP and <b>MUST</b> be used unless a later, technically sound, approved version of IC-GENC.CES has been released. The requirement to use the latest technically sound, approved version is based on authoritative source compliance <sup>[31]</sup> .
<i>CVE Encoding Specification for US Agency</i> (USAgency.CES.V2017-MARr2018-FEB+ <sup>[35]</sup> )	The specification does not depend on a specific version of USAgency.CES <sup>[35]</sup> ; versions later than version 2017-MARr2018-FEB <b>MAY</b> be used. The minimum version was based on the earliest non-retired version; Enterprise Standards Baseline (ESB) 21-2 was used for determining the version.
<i>Data Encoding Specification for Unified Identity Attribute Set</i> (UIAS.XML.V2019-SEP+ <sup>[33]</sup> )	This specification does not depend on a specific version of UIAS.XML <sup>[33]</sup> ; versions later than version 2019-SEP <b>MAY</b> be used. The minimum version was based on the earliest non-retired version; ESB 21-2 was used for determining the version.

Name	Dependency Description
<i>XML Data Encoding Specification for Virtual Coverage</i> (VIRT.XML.V2020-OCT+ <sup>[36]</sup> )	This specification does not depend on a specific version of VIRT.XML <sup>[36]</sup> ; versions later than version 2020-OCT MAY be used. The minimum version was based on the earliest non-retired version; ESB 21-2 was used for determining the version.
<i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ <sup>[10]</sup> )	This specification does not depend on a specific version of IC-SF.XML <sup>[10]</sup> ; versions later than version 2021-NOV MAY be used, however, the newest version of IC-SF.XML SHOULD be used as IC-SF.XML is expected to always replace its preceding version. The minimum version was based on technical dependencies on IC-SF.XML; IC-SF.XML is the basic structure of and philosophy behind intelligence community technical specifications.



**Figure 1 : Related Specifications**

## 1.5.2 - Inverse Dependencies

Generally, it is only necessary to think of the *dependencies* in the dependency tree. However, with the specification versions being decoupled, it is also important to consider the *inverse dependencies*, for compatibility with newer versions of a given specification. The changes introduced to a given specification can sometimes make it incompatible with current versions of its inverse dependencies (specifications that uses the given specification).

This specification is not used by other specifications released by the IC CIO, and therefore does not contain an Inverse Dependency Diagram.

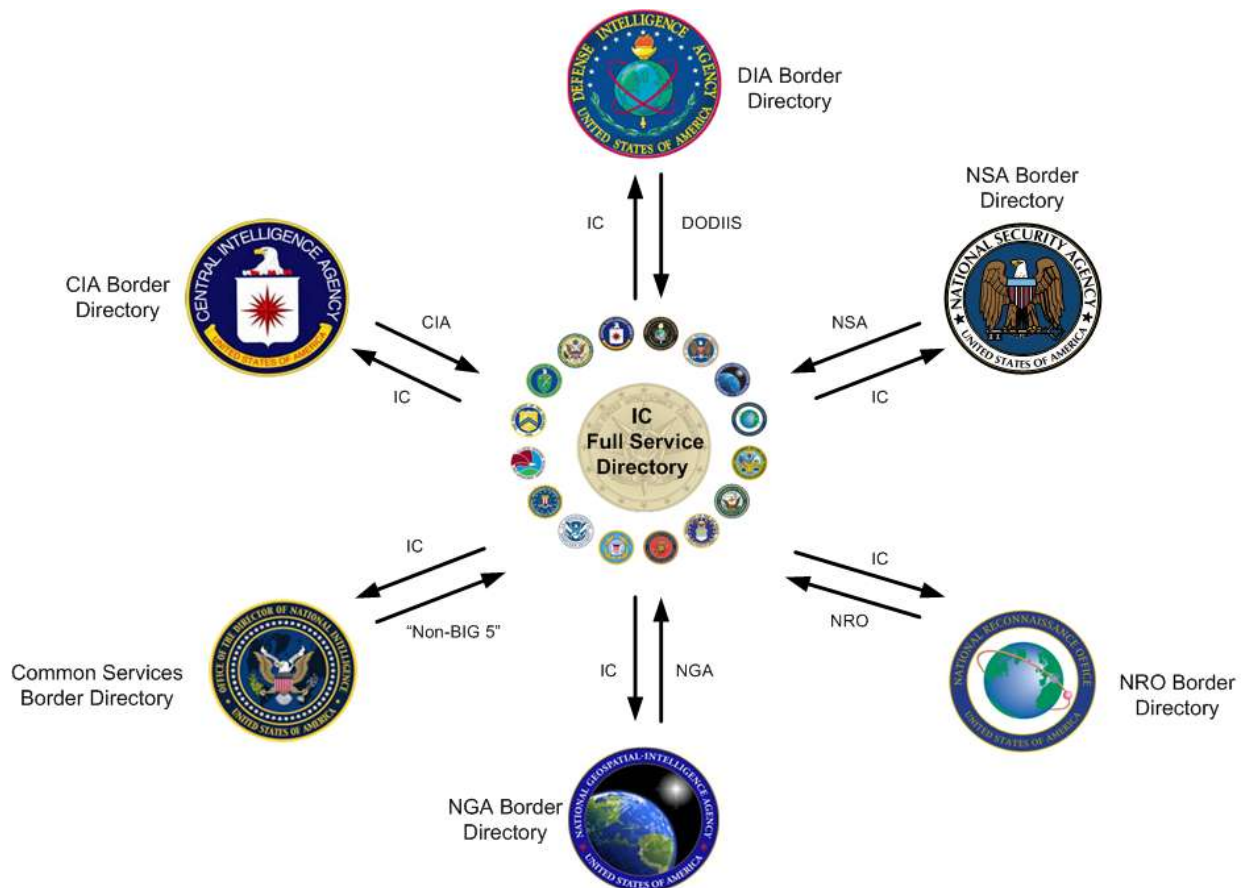


## Chapter 2 - Development Guidance

For information on the structure and content of the specifications, please see the “Specification Overview” chapter in the IC-SF.XML<sup>[10]</sup> framework document. This chapter is intended to expand upon the common information that the framework specifies providing specific development guidance that is specific to the implementation of this specification.

### 2.1 - IC FSD System Description

The IC FSD is based on the X.500 standard for electronic directory services. It is a fully replicated directory framework in which each participating IC element holds a full and accurate copy of the IC FSD content. The architecture is based on a hub and spoke model, with the central IC FSD serving as the master replication hub. IC elements are the authoritative provider of their personnel's directory data. Other sources may provide data only in coordination with the IC element. When a participating IC element adds, deletes, or modifies data in its border directory, the IC FSD detects and replicates the updated content to itself and all other border directories. This full replication scenario strengthens the IC FSD's disaster recovery posture. [Figure 2](#) below depicts the IC FSD replication model.



**Figure 2 : IC FSD Replication**

The IC FSD, acting in its role as the master replication manager, is designed to only communicate with authorized border directories. The IC FSD always initiates communications with the

authorized border directories; no IC Element border directory can initiate communication with the IC FSD.

The IC FSD maintains redundancy through two geographically diverse locations, each with three servers. The first server communicates with authorized border directories (currently Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Geospatial Intelligence Agency (NGA), National Reconnaissance Office (NRO), and National Security Agency (NSA)) retrieving updates and replicating any changes to the other border directories. The second server replicates information to and from the Common Services border directory. The third server provides local redundancy and, in the event of a complete failure of one of the first two servers, can serve as the replication engine for either.

## **2.2 - IC FSD Policy Statements**

### **2.2.1 - Duplicate Entries**

IC elements that replicate information via their IC FSD border directories to the IC FSD shall provide only records that contain IC Email addresses in address spaces that they own, or to which they have been delegated administrative responsibility for populating the IC FSD. IC elements shall not contribute a record to their IC FSD border directory with an IC Email address in an address space that they do not control or manage.

### **2.2.2 - Account Disablement**

The identity and attributes associated with an inactive user shall not be replicated to an agency's border directory for update to the IC FSD White Pages. A user shall be considered inactive when the user has not accessed the account for ninety (90) calendar days unless the agency indicates an exception to the 90 day rule for that user, allowing them to remain active.

## Chapter 3 - Constraints

The normative LDAP schemas are found in [Chapter 5 - IC FSD Schema](#) and [Chapter 8 - IC FSD Schema for PKI Root and Intermediate Certificate Authorities](#). Constraints on attributes are listed in [Chapter 6 - Attribute Status](#)

## **Chapter 4 - Conformance Validation**

An implementation of FSD MUST be conforming to the schema's provided and abide by the cardinality constraints.

## Chapter 5 - IC FSD Schema

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

### 5.1 - IC FSD Schema for IC Person

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

```
objectclass ( 2.5.6.6 NAME 'person' SUP top
    DESC 'RFC4519: Person'
    STRUCTURAL
    MUST ( sn $ cn )
    MAY ( userPassword $ telephoneNumber $ seeAlso $ description )
)
```

```
objectclass ( 2.5.6.7 NAME 'organizationalPerson' SUP person
    DESC 'RFC4519: organizationalPerson'
    STRUCTURAL
    MAY ( title $ x121Address $ registeredAddress $
        destinationIndicator $ preferredDeliveryMethod $
        telexNumber $ teletexTerminalIdentifier $
        telephoneNumber $ internationalISDNNumber $
        facsimileTelephoneNumber $ street $ postOfficeBox $
        postalCode $ postalAddress $ physicalDeliveryOfficeName $
        ou $ st $ l )
)
```

```
objectclass (2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson'
```

```

DESC 'RFC2798: Internet Organizational Person'

SUP organizationalPerson

STRUCTURAL

MUST ( employeeType )

MAY ( audio $ businessCategory $ carLicense $
      departmentNumber $ displayName $
      employeeNumber $ givenName $ homePhone $
      homePostalAddress $ initials $ jpegPhoto $
      labeledURI $ mail $ manager $ mobile $ o $ pager $
      photo $ roomNumber $ secretary $ uid $
      userCertificate $ x500uniqueIdentifier $
      preferredLanguage $ userSMIMECertificate $
      userPKCS12 )
)

```

```

objectclass (2.16.840.1.101.2.2.3.73 NAME 'icOrgPerson'

DESC 'Intelligence Community Person'

SUP inetOrgPerson

STRUCTURAL

MUST ( countryOfAffiliation $ dutyOrganization $
      dn $ adminOrganization $ isICMember $
      icNetworks $ resourceSecurityMark )

MAY ( auditRoutingOrganization $ icEmail $ secureTelephoneNumber $
companyName $
      internetEmail $ niprnetEmail $ siprnetEmail $
      rank $ buildingName $ countryName $
      militaryTelephoneNumber $ preferredName $
      secureFacsimileNumber $ expertCountry $
      expertFunctionalArea $ productionManager $

```

```

        personaUID $ dutySubOrganization $ instantMessageAddress )
    )

```

## 5.2 - IC FSD Schema for IC Non-Person Entity

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

```

objectclass (2.16.840.1.101.2.2.3.74 NAME 'icOrgServer'

    DESC 'Intelligence Community Non-Person Entity'

    SUP <implementation specific>

    STRUCTURAL

    MUST ( cn $ dutyOrganization $

        adminOrganization $ isICMember $ dn $

        ATOSStatus $ lifeCycleStatus $ givenName $

        countryOfAffiliation $ employeeType $

        uid $ userCertificate $ resourceSecurityMark $

        icNetworks $ serverPOC $ userCertificate )

    MAY ( auditRoutingOrganization $ description $ serverURL $
icServerAddress )

)

```

## 5.3 - IC FSD Attribute Definitions

The following section defines a collection of attributes from the **@objectClasses** described in sections 5.1 and 5.2 that participating IC Elements should attempt to support so that the IC FSD can realize its full potential as an IC Enterprise-level directory service. Each attribute is described using the formal attribute definition format as defined in IETF-RFC 4512, *Lightweight Directory Access Protocol (LDAP): Directory Information Models* <sup>[24]</sup>, Section 4.1.2. A tabular format will also be used to provide additional information and a controlled vocabulary (when appropriate) for each attribute.

In terms of IC Element provisioning requirements, this specification organizes attributes about an IC entity into mandatory, policy-based, optional or deprecated categories and is further described in Chapter 6.

This specification establishes three authentication tiers, providing graded authentication for attributes of varying sensitivity and is further described in Chapter 7.

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

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

```
attributetype ( 2.5.4.41 NAME 'name'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

)
```

### 5.3.1 - adminOrganization

This attribute specifies the home or administrative organization affiliation with which the entity (person or non-person) is associated.

The **@adminOrganization** attribute may be used for identifying the home or administrative organization of the entity for audit purposes, but may also be used for access control decisions where relevant to the protected resource provider.

```
attributetype (`OID TBD` NAME `adminOrganization`

    EQUALITY caseignoreMatch

    SUBSTR caseignoreSubstringMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)
```

**Table 3 - adminOrganization**

Attribute Name	adminOrganization
Reference	FSD, ICD 501, <i>Discovery and Dissemination or Retrieval of Information within the Intelligence Community</i> <sup>[12]</sup> , Executive Order (E.O.) 12333, <i>Executive Order 12333 - United States Intelligence Activities, as Amended</i> <sup>[4]</sup> , UIAS.XML <sup>[33]</sup>
Object Class	icOrgPerson / icOrgServer
Friendly Name	Admin Organization
Description	Reflects the home organization of the entity



Attribute Name	adminOrganization
Allowable Values	Summation of two sets: <ul style="list-style-type: none"> <li>Values listed in <i>CVE Encoding Specification for US Agency Acronyms</i> (USAgency.CES<sup>[35]</sup>)</li> <li>Values listed in table <a href="#">Table 4</a></li> </ul>
Example	USA.DIA, USA.FBI, GBR.GCHQ
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

In support of Second Party Integree (2PI), additional values for **@adminOrganization** are needed to identify the entity's top-level foreign government agency and the country of the entity's foreign government agency.

**Table 4 - Foreign Government adminOrganization Countries**

Value	Definition
AUS.[A-Za-z0-9_\-\.\.]{1,36}	Agencies that are operating under the government of Australia (AUS)
CAN.[A-Za-z0-9_\-\.\.]{1,36}	Agencies that are operating under the government of Canada (CAN)
GBR.[A-Za-z0-9_\-\.\.]{1,36}	Agencies that are operating under the government of the United Kingdom (GBR)
NZL.[A-Za-z0-9_\-\.\.]{1,36}	Agencies that are operating under the government of New Zealand (NZL)

The values that appear in the Foreign Government **@adminOrganization** Countries table are Regular Expressions (REGEX), a kind of short-hand description of allowable values for the given field. Allowable values can be interpreted as follows:

- AUS., CAN., GBR., or NZL. indicates the value must begin with one of those sequences.
- {1,36} indicates that 1 to 36 characters can follow the opening sequence.
- [A-Za-z0-9\_\-\.\.] indicates the 1 to 36 characters that follow the opening sequence can be upper or lower case alphabetic characters, any digit from 0 to 9, or underscore ('\_'), dash ('-'), or period ('.') characters.
- Example: New Zealand Government Communications Security Bureau might be represented as NZL.GCSB.

## 5.3.2 - auditRoutingOrganization

This attribute specifies the organization(s) to which Audit records will be routed beyond the entity's **adminOrganization** and **dutyOrganization**. Audit software and services **MUST** always

route audit records to both the **adminOrganization** and **dutyOrganization**. If the entity has values in **auditRoutingOrganization**, then audit software and services MUST also route audit data to the organizations in **auditRoutingOrganization**. Allowable values can be found in “CVENumAuditRoutingOrg”. This attribute is applicable to both Persons and Non-Persons.

```
attributetype (`OID TBD` NAME `auditRoutingOrganization`

    EQUALITY    caseignoreMatch

    SUBSTR      caseignoreSubstringMatch

    SYNTAX      1.3.6.1.4.1.1466.115.121.1.15

    MULTI-VALUE

)
```

**Table 5 - auditRoutingOrganization**

Attribute Name	auditRoutingOrganization
Reference	UIAS.XML <sup>[33]</sup>
Object Class	icOrgPerson / icOrgServer
Friendly Name	Audit Routing Organization
Description	This attribute specifies the organization(s) to which Audit Records should be forwarded in addition to the entity's <b>dutyOrganization</b> and <b>adminOrganization</b> .
Allowable Values	Values listed in USAgency.CES <sup>[35]</sup> from the Controlled Vocabulary Enumeration (CVE) “CVENumAuditRoutingOrg”
Example	USA.CIA, USA.USPACOM, USA.EOP
Provisioning	[0..10]
Authentication	Strong Server
Single/Multi	MULTI-VALUE

### 5.3.3 - ATOSStatus

This attribute indicates the Authority To Operate (ATO) status for the non-person entity. As defined by ICD 503, *Intelligence Community Information Technology Systems Security Risk Management* <sup>[13]</sup>, ATO is approved for operation at a particular level of security in a particular environment, with the established level of risk associated with operating the system. This includes ATOs with waivers, which can be derived based upon the approved necessary conditions of the approving authority.

The **@ATOSStatus** attribute is only applicable for non-person entities.

```
attributetype (`OID TBD` NAME `ATOSStatus`

    EQUALITY    booleanmatch

)
```

```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.7

SINGLE-VALUE

)

```

**Table 6 - ATOSStatus**

Attribute Name	ATOSStatus
Reference	FSD, ICD 501 <sup>[12]</sup> , E.O. 12333 <sup>[4]</sup> , UIAS.XML <sup>[33]</sup>
Object Class	icOrgServer
Friendly Name	Authority to Operate Status
Description	This attribute indicates the ATO status for the Non-Person entity.
Allowable Values	Boolean True/False (false by default)
Example	True
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

### 5.3.4 - buildingName

```

attributetype ( 0.9.2342.19200300.100.1.48 NAME 'buildingName'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256}

)

```

**Table 7 - buildingName**

Attribute Name	buildingName
Reference	IETF-RFC 4524, <i>COSINE LDAP/X.500 Schema</i> <sup>[27]</sup>
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
Examples	LX2 NBP-304
Provisioning	Optional
Authentication	Strong User

Attribute Name	buildingName
Single/Multi	MULTI-VALUE

### 5.3.5 - c, countryName

```

attributetype ( 2.5.4.6 NAME 'c' 'countryName'

    SUP name

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.11

    SINGLE-VALUE

)

```

**Table 8 - c, countryName**

Attribute Name	c, countryName
Reference	IETF-RFC 4519, <i>Lightweight Directory Access Protocol (LDAP): Schema for User Applications</i> <a href="#">[25]</a>
Object Class	icOrgPerson
Friendly Name	Physical Country
Description	Country where IC Person's physical work facility is located
Allowable Values	Two-letter country codes as identified by GENC <a href="#">[5]</a>
Examples	US AU
Provisioning	Optional
Authentication	Strong User
Single/Multi	SINGLE-VALUE

### 5.3.6 - cn, commonName

```

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

```

**Table 9 - cn, commonName**

Attribute Name	cn, commonName
Reference	IETF-RFC 4519 <a href="#">[25]</a>
Object Class	icOrgPerson / icOrgServer
Friendly Name	Common Name

Attribute Name	cn, commonName
Description	This is the X.500 @ <b>commonName</b> attribute, which contains a name of an object. When the object corresponds to an IC Entity, it typically matches the Common Name (CN) component of the entity's Distinguished Name in its/his/her Public Key Infrastructure (PKI) certificate.
Allowable Values	For the IC, the IC PKI Certificate Revocation List (CRL), <i>Intelligence Community Public Key Infrastructure Certificate and Certificate Revocation List Profiles</i> [8] provides the basis for specifying 4523s for both IC Person and Non-Person Entities. Consult Chapter 6 - CERTIFICATE DISTINGUISHED NAME (DN) SCHEMA of the IC PKI CRL [8] for allowable values.
Examples	Smith John A John A Smith webserver.dni.ic.gov
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

### 5.3.7 - companyName

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

```

attributetype ( 2.16.840.1.101.2.2.1.148 NAME 'companyName'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 10 - companyName**

Attribute Name	companyName
Reference	FSD
Object Class	icOrgPerson
Friendly Name	Company Name
Description	Company name of an IC Person with " <b>CTR</b> " @ <b>employeeType</b>
Allowable Values	Legal name of company provided by authoritative source
Example	Company Inc.
Provisioning	Optional

Attribute Name	companyName
Authentication	Strong User
Single/Multi	SINGLE-VALUE

### 5.3.8 - countryOfAffiliation

For Person Entity (PE), this is the identifier of the PE's country or countries of citizenship. In the case of NPEs, this represents the citizenship of the administrator(s) and/or the country of affiliation for the organization(s) in control of the non-person entity.

The **@countryOfAffiliation** attribute is multi valued, since an entity could possibly have multiple citizenships (e.g., "dual citizenship") relevant for access control decisions.

```

attributetype ( `OID TBD` NAME `countryOfAffiliation`

    EQUALITY caseignoreMatch

    SUBSTR caseignoreSubstringMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

)

```

**Table 11 - countryOfAffiliation**

Attribute Name	countryOfAffiliation
Reference	FSD, ICD 501 <sup>[12]</sup> , Executive Order 12333 <sup>[4]</sup> , UIAS.XML <sup>[33]</sup>
Object Class	icOrgPerson / icOrgServer
Friendly Name	Country of Affiliation
Description	Reflects the citizenship or affiliation of the entity
Allowable Values	Includes values listed in <i>CVE Encoding Specification for Geopolitical Entities, Names, and Codes</i> (IC-GENC.CES <sup>[9]</sup> ), in the CVE "CVEnumGENCCountryCode".
Example	USA
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

### 5.3.9 - displayName

```

attributetype ( 2.16.840.1.113730.3.1.241 NAME 'displayName'

    DESC 'preferred name of a person to be used when displaying
entries'

    EQUALITY caseIgnoreMatch

```

```

SUBSTR caseIgnoreSubstringsMatch

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

SINGLE-VALUE

)

```

**Table 12 - displayName**

Attribute Name	displayName
Reference	IETF-RFC 2798, <i>Definition of the inetOrgPerson LDAP Object Class</i> [22], ICS 500-13, <i>Intelligence Community Email Standard Display Name Format</i> [16]
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	<p>Format as defined in ICS 500-13[16]:</p> <p>Last Name&lt;space&gt;First Name&lt;space&gt;Middle Name/ Initial&lt;space&gt;Generation ID&lt;space&gt; Personal Title&lt;space&gt;Duty Organization&lt;space&gt; Duty Sub-Organization&lt;space&gt; Citizenship&lt;space&gt;Employee Type</p> <p>In terms of corresponding directory attribute names:</p> <p>&lt;sn givenName initials generationQualifier personalTitle dutyOrganization dutySubOrganization countryOfAffiliation employeeType&gt;</p> <p>In cases where multiple values are available for @countryOfAffiliation, the value "USA" should be listed last, and the values separated by spaces.</p>
Example	Smith John M Jr Maj DIA PACOM USA MIL
Provisioning	Policy-based
Authentication	Network
Single/Multi	SINGLE-VALUE

### 5.3.10 - dn, distinguishedName

```

attributetype ( 2.5.4.49 NAME 'dn' 'distinguishedName'

    EQUALITY distinguishedNameMatch

```

```
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
```

```
)
```

**Table 13 - dn, distinguishedName**

Attribute Name	dn, distinguishedName
Reference	IETF-RFC 4519 <sup>[25]</sup> , ICS 500-29, <i>Intelligence Community Digital Identifier</i> <sup>[20]</sup>
Object Class	icOrgPerson / icOrgServer
Friendly Name	Distinguished Name
Description	This is the X.500 <b>@distinguishedName</b> attribute, which contains the entity's Distinguished Name from the PKI certificate
Allowable Values	For the IC, the IC PKI CRL <sup>[8]</sup> 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 IC PKI CRL <sup>[8]</sup> for allowable values
Examples	cn=Doe John A jdoe, ou=DNI, o=U.S Government, c=US cn=webserver.dni.ic.gov, ou=DNI, o=U.S. Government, c=US
Provisioning	Mandatory
Authentication	Network
Single/Multi	SINGLE-VALUE

### 5.3.11 - dutyOrganization

This attribute specifies the organization which the entity (person or non-person) is representing.

The **@dutyOrganization** may differ from the **@adminOrganization** in cases where the entity is detailed from his or her home or administrative agency to another agency for a Joint Duty assignment or other rotation, or the NPE is loaned or transferred from its administrative agency to another agency, or operated by another agency.

```
attributetype ( `OID TBD` NAME `dutyOrganization`

    EQUALITY caseignoreMatch

    SUBSTR caseignoreSubstringMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

)
```



**Table 14 - dutyOrganization**

Attribute Name	dutyOrganization
Reference	FSD, ICD 501 <sup>[12]</sup> , Executive Order 12333 <sup>[4]</sup> , UIAS.XML <sup>[33]</sup>
Object Class	icOrgPerson / icOrgServer
Friendly Name	Duty Organization
Description	Reflects the assigned organization of the entity
Allowable Values	Summation of two sets: <ul style="list-style-type: none"> <li>Values listed in <i>CVE Encoding Specification for US Agency Acronyms</i> (USAgency.CES<sup>[35]</sup>)</li> <li>Values listed in table <a href="#">Table 15</a></li> </ul>
Example	USA.DNI, GBR.GCHQ
Provisioning	Mandatory
Authentication	Network
Single/Multi	SINGLE-VALUE

In support of 2PI, the @**dutyOrganization** should represent the US government sponsoring agency.

In support of Second Party Sovereign (2PS), the @**dutyOrganization** should represent the non-US government sponsoring agency.

**Table 15 - Foreign Government dutyOrganization Countries**

Value	Definition
AUS.[A-Za-z0-9_-\.\.]{1,36}	Agencies that are operating under the government of Australia (AUS)
CAN.[A-Za-z0-9_-\.\.]{1,36}	Agencies that are operating under the government of Canada (CAN)
GBR.[A-Za-z0-9_-\.\.]{1,36}	Agencies that are operating under the government of the United Kingdom (GBR)
NZL.[A-Za-z0-9_-\.\.]{1,36}	Agencies that are operating under the government of New Zealand (NZL)

The values that appear in the Foreign Government @**dutyOrganization** Countries table are Regular Expressions (REGEX), a kind of short-hand description of allowable values for the given field. Allowable values can be interpreted as follows:

- AUS., CAN., GBR., or NZL. indicates the value must begin with one of those sequences.
- {1,36} indicates that 1 to 36 characters can follow the opening sequence.

- [A-Za-z0-9\_-\.] indicates the 1 to 36 characters that follow the opening sequence can be upper or lower case alphabetic characters, any digit from 0 to 9, or underscore ('\_'), dash ('-'), or period('.') characters.
- Example: New Zealand Government Communications Security Bureau might be represented as NZL.GCSB.

### 5.3.12 - dutySubOrganization

This attribute specifies the sub-organization which the IC Person is representing.

```
attributetype ( `OID TBD` NAME `dutySubOrganization`

    EQUALITY  caseignoreMatch

    SUBSTR    caseignoreSubstringMatch

    SYNTAX    1.3.6.1.4.1.1466.115.121.1.15

)
```

**Table 16 - dutySubOrganization**

Attribute Name	dutySubOrganization
Reference	FSD, ICS 500-13 <sup>[16]</sup>
Object Class	icOrgPerson
Friendly Name	Duty Sub-Organization
Description	Reflects the assigned sub organization of the entity
Allowable Values	Agency defined authoritative sub-organization of the IC Person's duty organization
Example	PACOM, NCTC
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

### 5.3.13 - employeeType

This attribute indicates the type of the entity (person or non-person), and may be used for access control to protected resources. The value of the attribute will indicate if the type, e.g., if the entity is a person or non-person.

This attribute is consistent with the **@entityType** attribute in UIAS.XML<sup>[33]</sup>

```
attributetype ( 2.16.840.1.113730.3.1.4 NAME `employeeType`

    EQUALITY  caseIgnoreMatch

    SUBSTR    caseIgnoreSubstringsMatch

)
```

```
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
```

**Table 17 - employeeType**

Attribute Name	employeeType
Reference	IETF-RFC 2798 <sup>[22]</sup> , FSD, ICD 501 <sup>[12]</sup> , E.O. 12333 <sup>[4]</sup> , UIAS.XML <sup>[33]</sup>
Object Class	inetOrgPerson / icOrgServer
Friendly Name	Employee Type
Description	Reflects the type of the entity
Allowable Values	Values found in Extensible Markup Language (XML) CVE for Entity Type, "CVEnumUIASEntityType".
Example	GOV
Provisioning	Mandatory
Authentication	Network
Single/Multi	SINGLE-VALUE

Per IETF-RFC 2798<sup>[22]</sup> this LDAP attribute is Multi-Valued, however, the IC FSD implementation is Single-Valued.

Further clarification of NPE attribute definitions are below:

SVR - A hardware or software server system upon which other software systems reside and execute. Such systems typically provide support for and management of those other software systems. Such server systems include, but are not limited to, physical servers, virtual servers or server environments, application servers, and web servers. Note that while similar, end-point devices (DEV) and network devices (NET) are special purpose systems which have been called out separately.

SVC - A software system that performs specific functionality which can be generally viewed as self-encapsulated or decomposed and managed as discrete functional components. The intent is to deliver functional capabilities to systems, users or other software systems. Such software systems can include, but are not limited to, services, widgets, applications, and appliances whose primary functionality is delivery of functional capabilities as opposed to networking capabilities.

DEV - A hardware or software end-point device from which users or other external entities access systems or networks. End-point devices, while typically used to access networks or other key systems directly, can operate as standalone entities if required by mission use and enabled by functional capabilities. End-point devices can include, but are not limited to, workstations, laptops, smart phones, tablets, and sensors.

NET - A hardware or software device directly supportive of networking operations. This does not include those end-point devices and servers which leverage and are dependent upon the networking operations. Networking operation devices include, but are not limited to, firewalls,

bridges, routers, switches, concentrators, Domain Name System (DNS) servers, and appliances whose primary function is the support and management of such operations.

### 5.3.14 - expertCountry

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

```
attributetype ( 2.16.840.1.101.2.2.1.149 NAME 'expertCountry'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)
```

**Table 18 - expertCountry**

Attribute Name	expertCountry
Reference	FSD
Object Class	icOrgPerson
Friendly Name	Expert Country
Description	3-letter country code describing an IC Person's expertise area
Allowable Values	Includes values listed in <i>CVE Encoding Specification for Geopolitical Entities, Names, and Codes</i> (IC-GENC.CES <sup>[9]</sup> ), in the CVE "CVEnumGENCCountryCode".
Example	USA
Provisioning	Optional
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

### 5.3.15 - expertFunctionalArea

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

```
attributetype ( 2.16.840.1.101.2.2.1.150 NAME 'expertFunctionalArea'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)
```

)

**Table 19 - expertFunctionalArea**

Attribute Name	expertFunctionalArea
Reference	FSD
Object Class	icOrgPerson
Friendly Name	Expert Functional Area
Description	IC Person's functional area expertise
Allowable Values	DIA Intelligence Functional Code
Example	IFC1000
Provisioning	Optional
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

### 5.3.16 - facsimileTelephoneNumber

```

attributetype ( 2.5.4.23 NAME 'facsimileTelephoneNumber' 'fax'

                SYNTAX 1.3.6.1.4.1.1466.115.121.1.22

                )

```

**Table 20 - facsimileTelephoneNumber**

Attribute Name	facsimileTelephoneNumber
Reference	IETF-RFC 4519 <sup>[25]</sup>
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

### 5.3.17 - generationQualifier

```

attributetype ( 2.5.4.44 NAME 'generationQualifier' SUP name )

```

**Table 21 - generationQualifier**

Attribute Name	generationQualifier
Reference	IETF-RFC 4519 <sup>[25]</sup>
Object Class	<i>Implementation Dependent</i>
Friendly Name	Generational Qualifier
Description	The <b>@generationQualifier</b> attribute contains the part of the IC Person's name which typically is the suffix
Allowable Values	Any generational qualifier, for example, JR, SR, III, IV, etc.
Examples	JR SR
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

### 5.3.18 - givenName

```
attributetype ( 2.5.4.42 NAME 'givenName' SUP name )
```

**Table 22 - givenName**

Attribute Name	givenName
Reference	IETF-RFC 4519 <sup>[25]</sup>
Object Class	inetOrgPerson / icOrgServer
Friendly Name	First Name
Description	The <b>@givenName</b> attribute is used to hold the part of a person's name which is not his or her surname nor middle name. For NPEs, the <b>@givenName</b> attribute is used for the name of the service.
Allowable Values	For IC Persons, this should reflect a person's legal first name
Examples	Joseph Katherine
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

### 5.3.19 - icEmail

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

```
attributetype ( 2.16.840.1.101.2.2.1.154 NAME 'icEmail'
    EQUALITY caseIgnoreMatch
```

```

SUBSTR caseIgnoreSubstringsMatch

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

SINGLE-VALUE

)

```

**Table 23 - icEmail**

Attribute Name	icEmail
Reference	FSD
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 the email provider
Example	jsmith@intelink.ic.gov
Provisioning	Policy-based
Authentication	Network
Single/Multi	SINGLE-VALUE

### 5.3.20 - icNetworks

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

```

attributetype ( 2.16.840.1.101.2.2.1.160 NAME 'icNetworks'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

)

```

**Table 24 - icNetworks**

Attribute Name	icNetworks
Reference	FSD
Object Class	icOrgPerson / icOrgServer
Friendly Name	IC Networks

Attribute Name	icNetworks
Description	@ <b>icNetworks</b> 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	Values listed in "VIRTCVEnums.pdf" in <i>XML Data Encoding Specification for Virtual Coverage</i> (VIRT.XML <sup>[36]</sup> )
Examples	ACSS NSANET
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	MULTI-VALUE

### 5.3.21 - icServerAddress

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

```

attributetype ( 2.16.840.1.101.2.2.2.200 NAME 'icServerAddress'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 25 - icServerAddress**

Attribute Name	icServerAddress
Reference	FSD
Object Class	icOrgServer
Friendly Name	Internet Protocol (IP) Address
Description	IP Address of IC Non-Person Entity
Allowable Values	Valid IPv4 or IPv6 address
Examples	10.1.2.3 3ffe:1900:4545:3:200:f8ff:fe21:67cf
Provisioning	Optional
Authentication	Strong Server
Single/Multi	SINGLE-VALUE



## 5.3.22 - initials

```
attributetype ( 2.5.4.43 NAME 'initials' SUP name )
```

**Table 26 - initials**

Attribute Name	initials
Reference	IETF-RFC 4519 <sup>[25]</sup>
Object Class	inetOrgPerson
Friendly Name	Middle Initial
Description	IC Person's middle initial(s)
Allowable Values	Single, first letter of the middle name(s) with no periods, if one is available
Examples	K L N, etc.
Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

## 5.3.23 - instantMessageAddress

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

```
attributetype ( 1.3.6.1.5.5.7.8.5 NAME 'instantMessageAddress'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)
```

**Table 27 - instantMessageAddress**

Attribute Name	instantMessageAddress
Reference	FSD
Object Class	icOrgPerson
Friendly Name	Instant Messaging Address
Description	Instand Messaging address of an IC Person

Attribute Name	instantMessageAddress
Allowable Values	Official Instant messaging address of the IC Person as given by the instant messaging provider
Example	im:jsmith@ugov.gov
Provisioning	Policy-Based
Authentication	Network
Single/Multi	SINGLE-VALUE

### 5.3.24 - internetEmail

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

```

attributetype ( 2.16.840.1.101.2.2.1.155 NAME 'internetEmail'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 28 - internetEmail**

Attribute Name	internetEmail
Reference	FSD
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 the email provider
Example	jsmith@ugov.gov
Provisioning	Policy-Based
Authentication	Network
Single/Multi	SINGLE-VALUE

### 5.3.25 - isICMember

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

```

attributetype ( 'OID TBD' NAME 'isICMember'

    EQUALITY booleanMatch

```

```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.7

SINGLE-VALUE

)

```

**Table 29 - isICMember**

Attribute Name	isICMember
Reference	FSD, ICD 501 <sup>[12]</sup> , E.O. 12333 <sup>[4]</sup> , UIAS.XML <sup>[33]</sup>
Object Class	icOrgPerson / icOrgServer
Friendly Name	IC Membership
Description	Value that denotes an individual's IC membership status for ICD 501 <sup>[12]</sup> purposes
Allowable Values	Boolean true/false (false by default)
Example	False
Provisioning	Mandatory
Authentication	Strong User
Single/Multi	SINGLE-VALUE

The **@isICMember** attribute is a flag that reflects whether the persona is a member of the Intelligence Community.

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

Each IC organization will make the determination as to which of its users will have a true value for this attribute. This process will be documented by the organization and approved by the organization's senior leadership and general counsel. The Office of the Director of National Intelligence (ODNI) will then review and approve the process. The following, from E.O. 12333<sup>[4]</sup>, is used as general guidance in making this determination: an IC member is "a person employed by, assigned or detailed to, or acting for an element within the IC".

### 5.3.26 - I, localityName

```

attributetype ( 2.5.4.7 NAME ( 'I' 'localityName' ) SUP name )

```

**Table 30 - I, localityName**

Attribute Name	I, localityName
Reference	IETF-RFC 4519 <sup>[25]</sup>
Object Class	organizationalPerson
Friendly Name	Physical City
Description	IC Person's physical city or location name

Attribute Name	I, localityName
Allowable Values	City or location name
Example	Fairfax
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

### 5.3.27 - languageProficiency

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

This attribute is deprecated and should no longer be used.

```

attributetype ( 2.16.840.1.101.2.2.1.151 NAME 'languageProficiency'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 31 - languageProficiency**

Attribute Name	languageProficiency
Reference	FSD
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
Examples	Reading Level 1 Listening Level 0+
Provisioning	Deprecated
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

## 5.3.28 - lifeCycleStatus

This attribute indicates the life cycle phase in which the entity is operating, and may be used for access control to protected resources. This attribute is only applicable for NPEs.

```
attributetype ( `OID TBD` NAME `lifeCycleStatus`

    EQUALITY caseignoreMatch

    SUBSTR caseignoreSubstringMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)
```

**Table 32 - lifeCycleStatus**

Attribute Name	lifeCycleStatus
Reference	FSD, ICD 501 <sup>[12]</sup> , E.O. 12333 <sup>[4]</sup> , UIAS.XML <sup>[33]</sup>
Object Class	icOrgServer
Friendly Name	Life Cycle Status
Description	Indicates the life cycle phase in which the entity is operating
Allowable Values	Values found in XML CVE for Life Cycle Status, "CValenum-UIASLifeCycleStatus".
Example	DEV
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

## 5.3.29 - mail

```
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

)
```

**Table 33 - mail**

Attribute Name	mail
Reference	IETF-RFC 2798 <sup>[22]</sup>

Attribute Name	mail
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 the email provider
Example	jsmith@intelink.ic.gov
Provisioning	Policy-based
Authentication	Network
Single/Multi	MULTI-VALUE

### 5.3.30 - militaryTelephoneNumber

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

```

attributetype ( 2.16.840.1.101.2.2.1.120 NAME 'militaryTelephoneNumber'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 34 - militaryTelephoneNumber**

Attribute Name	militaryTelephoneNumber
Reference	FSD
Object Class	icOrgPerson
Friendly Name	Defense Switched Network (DSN) Voice Telephone Number
Description	IC Person's 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

### 5.3.31 - nationality-Extended

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

This attribute is deprecated and should no longer be used.

```

attributetype ( 2.16.840.1.101.2.2.1.61 NAME 'nationality-Extended'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 35 - nationality-Extended**

Attribute Name	nationality-Extended
Reference	FSD
Object Class	icOrgPerson
Friendly Name	Citizenship
Description	3-letter country code describing an IC Person's citizenship
Allowable Values	Includes values listed in <i>CVE Encoding Specification for Geopolitical Entities, Names, and Codes</i> (IC-GENC.CES <sup>[9]</sup> ), in the CVE "CVEnumGENCCountryCode".
Examples	USA GBR AUS
Provisioning	Deprecated
Authentication	Network
Single/Multi	SINGLE-VALUE

### 5.3.32 - niprnetEmail

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

```

attributetype ( 2.16.840.1.101.2.2.1.156 NAME 'niprnetEmail'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 36 - niprnetEmail**

Attribute Name	niprnetEmail
Reference	FSD
Object Class	icOrgPerson
Friendly Name	Non-Classified Internet Protocol Router Network (NIPRNet) Email Address
Description	NIPRNet email address of an IC Person
Allowable Values	Official NIPRNet email address of the IC Person as given by the Department of Defense (DoD) email provider
Example	jsmith@af.mil
Provisioning	Policy-Based
Authentication	Network
Single/Multi	SINGLE-VALUE

**5.3.33 - personalTitle**

```

attributetype ( 0.9.2342.19200300.100.1.40 NAME 'personalTitle'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256}

)

```

**Table 37 - personalTitle**

Attribute Name	personalTitle
Reference	IETF-RFC 4524 <sup>[27]</sup>
Object Class	<i>Implementation Dependent</i>
Friendly Name	Personal Title
Description	The <b>@personalTitle</b> attribute contains the personal title of an IC Person
Allowable Values	Any honorific, or form of address, such as Dr, Mr, Ms, Mx, Prof, Gen, Adm, etc.
Examples	Mr Dr Ms Mx Adm
Provisioning	Optional



Attribute Name	personalTitle
Authentication	Network
Single/Multi	MULTI-VALUE

### 5.3.34 - personaUID

```

attributetype ( 2.16.840.1.101.2.2.1.161 NAME 'personaUID'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

)

```

**Table 38 - personaUID**

Attribute Name	personaUID
Reference	FSD
Object Class	icOrgPerson
Friendly Name	Persona Unique Identifier
Description	Unique IC identifier that is persistent for the life of the persona
Allowable Values	[A-Za-z]{2}[0-9]{5}
Examples	AB12345 XY56789
Provisioning	Policy-Based
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

The **@personaUID** attribute is an alternate unique identifier associated with the Distinguished Name (DN) of the PKI Certificate that is used to both support use of identities in systems that cannot technically utilize the DN, and enable management of the relationship between those identifiers.

### 5.3.35 - postalAddress

```

attributetype ( 2.5.4.16 NAME 'postalAddress'

    EQUALITY caseIgnoreListMatch

    SUBSTR caseIgnoreListSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.41

)

```

**Table 39 - postalAddress**

Attribute Name	postalAddress
Reference	IETF-RFC 4519 <sup>[25]</sup>
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

**5.3.36 - postalCode**

```

attributetype ( 2.5.4.17 NAME 'postalCode'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

)

```

**Table 40 - postalCode**

Attribute Name	postalCode
Reference	IETF-RFC 4519 <sup>[25]</sup>
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

**5.3.37 - preferredName**

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

```

attributetype ( 2.16.840.1.101.2.2.2.201 NAME 'preferredName'

    EQUALITY caseIgnoreMatch

```

```

SUBSTR caseIgnoreSubstringsMatch

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

SINGLE-VALUE

)

```

**Table 41 - preferredName**

Attribute Name	preferredName
Reference	FSD
Object Class	icOrgPerson
Friendly Name	Name the user prefers to be used in email communications
Description	Preferred name of an IC Person in email communications
Allowable Values	Preferred name of an IC Person in email communications
Example	Valid name
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

The **@preferredName** attribute is an alternate displayable name (e.g., if the user goes by his/her middle name) for the user rather than **@displayName** or **@givenName**.

### 5.3.38 - productionManager

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

```

attributetype ( 2.16.840.1.101.2.2.1.152 NAME 'productionManager'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 42 - productionManager**

Attribute Name	productionManager
Reference	FSD
Object Class	icOrgPerson

Attribute Name	productionManager
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

### 5.3.39 - rank

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

```

attributetype ( 2.16.840.1.101.2.2.1.133 NAME 'rank'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 43 - rank**

Attribute Name	rank
Reference	FSD
Object Class	icOrgPerson
Friendly Name	Grade/Rank
Description	Individual's Office of Personnel Management (OPM) defined grade level
Allowable Values	OPM defined grades with two digit level required >Schedule<->Level<
Examples	GS-01 O-01 E-09 GG-09
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

### 5.3.40 - resourceSecurityMark

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

```
attributetype ( 2.16.840.1.101.2.2.1.161 NAME 'resourceSecurityMark'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)
```

**Table 44 - resourceSecurityMark**

Attribute Name	resourceSecurityMark
Reference	FSD
Object Class	icOrgPerson / icOrgServer
Friendly Name	Resource Classification
Description	The classification and handling markings for the associated directory object for both IC Person and Non-Person Entities.
Allowable Values	Classification and handling marking banner as described in the latest published version of the IC Markings, <i>Intelligence Community Markings System Register and Manual</i> <a href="#">[6]</a>
Examples	“UNCLASSIFIED” “SECRET//NOFORN”
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

### 5.3.41 - secureFacsimileNumber

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

```
attributetype ( 2.16.840.1.101.2.2.1.127 NAME 'secureFacsimileNumber'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.22

    SINGLE-VALUE

)
```

)

**Table 45 - secureFacsimileNumber**

Attribute Name	secureFacsimileNumber
Reference	FSD
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

**5.3.42 - secureTelephoneNumber**

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

```

attributetype ( 2.16.840.1.101.2.2.1.128 NAME 'secureTelephoneNumber'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 46 - secureTelephoneNumber**

Attribute Name	secureTelephoneNumber
Reference	FSD
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

Attribute Name	secureTelephoneNumber
Single/Multi	SINGLE-VALUE

### 5.3.43 - serverPOC

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

```

attributetype ( 2.16.840.1.101.2.2.2.201 NAME 'serverPOC'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 47 - serverPOC**

Attribute Name	serverPOC
Reference	FSD
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 Point of Contact (POC)
Example	Valid name
Provisioning	Mandatory
Authentication	Strong User
Single/Multi	SINGLE-VALUE

### 5.3.44 - serverURL

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

```

attributetype ( 2.16.840.1.101.2.2.2.202 NAME 'serverURL'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

```

)

**Table 48 - serverURL**

Attribute Name	serverURL
Reference	FSD
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

**5.3.45 - serviceOrAgency**

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

This attribute is deprecated and should no longer be used.

```

attributetype ( 2.16.840.1.101.2.2.1.82 NAME 'serviceOrAgency'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 49 - serviceOrAgency**

Attribute Name	serviceOrAgency
Reference	FSD
Object Class	icOrgPerson / icOrgServer
Friendly Name	Home Organization



Attribute Name	serviceOrAgency
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 his or her contract. IC Non-Person Entity's owning organization.
Allowable Values	Commonly recognized agency acronym or identifier ( CIA, DIA, DNI, NSA, NGA, NRO, Department of Justice (DOJ), U.S. Department of State (DOS), Department of Energy (DOE), Department of Homeland Security (DHS), Department of Transportation (DOT), Digital Object Identifier (DOI), Health and Human Services (HHS), Department of Commerce (DOC), Department of the Treasury (TREA), U.S. Department of Agriculture (USDA), Executive Office of the President (EOP), Nuclear Regulatory Commission (NRC), Federal Reserve Board (FRB), United States Capitol Police (USCP), U.S. Congress, U.S. Agency for International Development (USAID), United States Postal Service (USPS), United States Postal Inspection Service (USPIS), National Aeronautics and Space Administration (NASA), Environmental Protection Agency (EPA), Department of Veterans Affairs (DVA)). DoD values not covered above will be determined and included in a later issuance of the FSD.
Examples	CIA, NSA, NGA, etc.
Provisioning	Deprecated
Authentication	Network
Single/Multi	SINGLE-VALUE

### 5.3.46 - siprnetEmail

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

```

attributetype ( 2.16.840.1.101.2.2.1.157 NAME 'siprnetEmail'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 50 - siprnetEmail**

Attribute Name	siprnetEmail
Reference	FSD
Object Class	icOrgPerson
Friendly Name	Secret Internet Protocol Router Network (SIPRNet) Email Address
Description	SIPRNet email address of an IC Person
Allowable Values	Official SIPRNet email address of the IC Person as given by the email provider
Example	jsmith@intelink.sgov.gov
Provisioning	Policy-Based
Authentication	Network
Single/Multi	SINGLE-VALUE

**5.3.47 - sn, surname**

```
attributetype ( 2.5.4.4 NAME ( 'sn' 'surname' ) SUP name )
```

**Table 51 - sn, surname**

Attribute Name	sn, surname
Reference	IETF-RFC 4519 <sup>[25]</sup>
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
Examples	Smith Jones
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

**5.3.48 - st, stateOrProvinceName**

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

**Table 52 - st, stateOrProvinceName**

Attribute Name	st, stateOrProvinceName
Reference	IETF-RFC 4519 <sup>[25]</sup>

Attribute Name	st, stateOrProvinceName
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

### 5.3.49 - street, streetAddress

```

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

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

)

```

**Table 53 - street, streetAddress**

Attribute Name	street, streetAddress
Reference	IETF-RFC 4519 <sup>[25]</sup>
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

### 5.3.50 - telephoneNumber

```

attributetype ( 2.5.4.20 NAME 'telephoneNumber'

    EQUALITY telephoneNumberMatch

    SUBSTR telephoneNumberSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.50

)

```

**Table 54 - telephoneNumber**

Attribute Name	telephoneNumber
Reference	IETF-RFC 4519 <sup>[25]</sup>
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

### 5.3.51 - title

```
attributetype ( 2.5.4.12 NAME 'title' SUP name )
```

**Table 55 - title**

Attribute Name	title
Reference	IETF-RFC 4519 <sup>[25]</sup>
Object Class	organizationalPerson
Friendly Name	Title
Description	The <b>@title</b> attribute contains the title of an IC Person in the organizational context
Allowable Values	Official title as given by the IC person's organization, such as IC CIO, Vice President, Director, etc.
Examples	IC CIO NSA CDO ISSM Vice President Director
Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

### 5.3.52 - uid

```
attributetype ( 0.9.2342.19200300.100.1.1 NAME ('uid' )
```

```
EQUALITY caseIgnoreMatch
```

```

SUBSTR caseIgnoreSubstringsMatch

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

)

```

**Table 56 - uid**

Attribute Name	uid
Reference	IETF-RFC 2798 <sup>[22]</sup>
Object Class	inetOrgPerson / icOrgServer
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
Examples	jsmith jsmith1234 12345, etc.
Provisioning	Optional, Mandatory for NPE
Authentication	Network
Single/Multi	MULTI-VALUE

### 5.3.53 - userCertificate

**@userCertificate** attributes must be transferred using the binary encoding, by requesting or returning the attributes via '**@usercertificate; binary**'.

```

attributetype ( 2.5.4.36 NAME 'userCertificate'

    DESC 'X.509 user certificate'

    EQUALITY certificateExactMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.8

)

```

**Table 57 - userCertificate**

Attribute Name	userCertificate
Reference	IETF-RFC 4523 <i>Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates</i> <sup>[26]</sup> , IC PKI CRL <sup>[8]</sup>
Object Class	inetOrgPerson / icOrgServer
Friendly Name	PKI Certificate

Attribute Name	userCertificate
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	IC PKI certificate
Provisioning	Policy-based, Mandatory for NPE
Authentication	Network
Single/Multi	MULTI-VALUE

## Chapter 6 - Attribute Status

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

- **Mandatory:** Attributes that IC Elements **MUST** include in FSD records, without which the record will not be added to the IC FSD.
- **Policy-based:** Attributes which IC Elements **MAY** provide, if present in that IC Element’s internal directories.
- **Optional:** Attributes which IC Elements **MAY** provide to the IC FSD, depending on that IC Element’s security requirements and capabilities. Most optional attributes are not populated.
- **Deprecated:** Attributes that are present in the FSD schema, however, they are no longer needed. By policy the attribute is no longer passed between agency borders and the IC FSD.

**Table 58 - IC Person Attributes Mandatory, Policy-Based, Optional or Deprecated**

@Attribute Name	@Mandatory	@Policy-Based	@Optional	@Deprecated
@adminOrganization	X			
@auditRoutingOrganization			X	
@buildingName			X	
@c, @countryName			X	
@cn, @commonName	X			
@companyName			X	
@countryOfAffiliation	X			
@displayName		X		
@dn, @distinguishedName	X			
@dutyOrganization	X			
@dutySubOrganization			X	
@employeeType	X			
@expertCountry			X	
@expertFunctionalArea			X	
@facsimileTelephoneNumber			X	
@generationQualifier			X	
@givenName	X			
@icEmail		X		

@Attribute Name	@Mandatory	@Policy-Based	@Optional	@Deprecated
@icNetworks	X			
@initials			X	
@instandMessagingAddresses		X		
@internetEmail		X		
@isICMember	X			
@l, @localityName			X	
@languageProficiency				X
@mail		X		
@militaryTelephoneNumber			X	
@nationality-Extended				X
@noprnetEmail		X		
@personalTitle			X	
@personaUID		X		
@postalAddress			X	
@postalCode			X	
@preferredName			X	
@productionManager			X	
@rank			X	
@resourceSecurityMark	X			
@secureFacsimileNumber			X	
@secureTelephoneNumber		X		
@serviceOrAgency				X
@soprnetEmail		X		
@sn, @surname	X			
@st, @stateOrProvinceName			X	
@street, @streetAddress			X	
@telephoneNumber		X		
@title			X	
@uid			X	
@userCertificate		X		



**Table 59 - IC Non-Person Entity Attributes Mandatory, Policy-Based, Optional or Deprecated**

@Attribute Name	@Mandatory	@Policy-Based	@Optional	@Deprecated
@adminOrganization	X			
@ATOSStatus	X			
@auditRoutingOrganization			X	
@cn, @commonName	X			
@countryOfAffiliation	X			
@dn, @distinguishedName	X			
@dutyOrganization	X			
@employeeType	X			
@givenName	X			
@icNetworks	X			
@icServerAddress			X	
@isICMember	X			
@lifeCycleStatus	X			
@resourceSecurityMark	X			
@serviceOrAgency				X
@serverPOC	X			
@serverURL			X	
@uid	X			
@userCertificate	X			

**Note:** @givenName is not a mandatory attribute in terms of the @inetOrgPerson @objectClass. Compliance with the mandatory requirement for @givenName is enforced through the replication agreements in place between the master IC FSD and participating IC Element Border directories.

## Chapter 7 - Securing Access to IC FSD Attributes

This technical specification requires three authentication tiers, providing graded authentication for attributes of varying sensitivity. The three tiers are defined as follows:

- Network authentication
  - Permits end user access to content
  - Primarily used to support IC White Pages functionality, for attributes viewable by users through the IC White Pages
  - Relies on PKI authentication for web service access to content
  - Applies to attributes such as **@name**, **@countryOfAffiliation**, and **@employeeType**.
- Strong user authentication
  - Permits end user access to content
  - Used for attributes more sensitive than those above
  - Requires users to present an IC PKI certificate
  - Applies to attributes such as **@isICMember**, **@streetAddress**, and **@companyName**.
- Strong server/application authentication
  - Attributes which end users have no need to view in the IC FSD
  - Attributes used by servers and applications
  - Requires those servers and applications to present an IC PKI certificate
  - Applies to attributes such as **@languageProficiency** and **@certificateRevocationList**.

The IC FSD operator and IC elements are expected to maintain the authentication levels defined for each attribute, in whatever locations IC FSD data resides: border directories, element address books, etc. A reduction from three to two IC FSD authentication tiers is desired (eliminating network authentication and requiring strong user authentication to all user accessible content) if and when requirements are defined *and* supporting technology capabilities exist.

**Table 60 - Securing Access to IC FSD IC Person Attributes**

@Attribute Name	@Network	@Strong User	@Strong Server
@adminOrganization			X
@auditRoutingOrganization			X

@Attribute Name	@Network	@Strong User	@Strong Server
@buildingName		X	
@c, @countryName		X	
@cn, @commonName	X		
@companyName		X	
@countryOfAffiliation	X		
@displayName	X		
@dn, @distinguishedName	X		
@dutyOrganization	X		
@dutySubOrganization	X		
@employeeType	X		
@expertCountry			X
@expertFunctionalArea			X
@facsimileTelephoneNumber	X		
@generationQualifier	X		
@givenName	X		
@icEmail	X		
@icNetworks			X
@initials	X		
@instantMessageAddress	X		
@internetEmail	X		
@isICMember		X	
@languageProficiency			X
@l, @localityName		X	
@mail	X		
@militaryTelephoneNumber	X		
@nationality-Extended	X		
@niprnetEmail	X		
@personaUID			X
@personalTitle	X		
@postalAddress		X	
@postalCode		X	
@preferredName	X		
@productionManager	X		
@rank	X		

@Attribute Name	@Network	@Strong User	@Strong Server
@resourceSecurityMark			X
@secureFacsimileNumber	X		
@secureTelephoneNumber	X		
@serviceOrAgency	X		
@siprnetEmail	X		
@sn, @surname	X		
@st, @stateOrProvinceName		X	
@street, @streetAddress		X	
@telephoneNumber	X		
@title	X		
@uid	X		
@userCertificate	X		

**Table 61 - Securing Access to IC FSD IC Non-Person Entity Attributes**

@Attribute Name	@Network	@Strong User	@Strong Server
@adminOrganization			X
@ATOStatus			X
@auditRoutingOrganization			X
@cn, @commonName	X		
@countryOfAffiliation	X		
@dn, @distinguishedName	X		
@employeeType	X		
@givenName	X		
@icNetworks			X
@icServerAddress			X
@isICMember		X	
@lifeCycleStatus			X
@serverPOC		X	
@serverURL		X	
@uid	X		
@userCertificate	X		

The IC FSD operator and IC elements are expected to perform audit at a minimum as indicated through applicable security controls mandated by ICD 503<sup>[13]</sup> and subordinate policy documents, and as directed by IC-wide audit policies.

## Chapter 8 - IC FSD Schema for PKI Root and Intermediate Certificate Authorities

For those IC Elements providing Certificate Authority (CA) capabilities under the IC PKI, Cryptologic Agencies Domain (CAD) PKI, or other authorized PKIs, the following objectClass and associated attributes should be used as a basis to propagate critical CA information into the IC FSD architecture. This CA information is vital to the proper Private Key (PK)-enablement of services and applications within the IC TS/ SCI enterprise.

```
objectclass ( OID-TBD NAME 'icCertificationAuthority'

    DESC 'Intelligence Community Certification Authority'

    SUP <implementation specific>

    STRUCTURAL

    MUST ( certificateRevocationList $ cACertificate $
        icNetworks $ resourceSecurityMark
    )

    MAY ( crossCertificatePair $ authorityRevocationList )

)
```

**Note:** the **@objectClass** hierarchy in support of **@icCertificationAuthority** may vary depending on the commercial Certificate Authority product implementation. In addition, the **@crossCertificatePair** attribute is not applicable to the IC PKI.

### 8.1 - authorityRevocationList

The use and support of authority revocation lists by the IC PKI is not specifically identified in the IC PKI CP, *Intelligence Community Public Key Infrastructure Certificate Policy* [\[7\]](#) or IC PKI CRL [\[8\]](#). It currently is an optional attribute within the **@icCertificationAuthority @objectClass**.

This attribute SHOULD be stored and MUST be requested in binary form as '**@authorityRevocationList;binary**'.

```
attributetype ( 2.5.4.38 NAME 'authorityRevocationList'

    DESC 'X.509 authority revocation list'

    EQUALITY certificateListExactMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.9

)
```

**Table 62 - authorityRevocationList**

Attribute Name	authorityRevocationList
Reference	IETF-RFC 4523 <sup>[26]</sup>
Object Class	icCertificationAuthority
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 Authority Revocation List (ARL) issued by an authorized PKI Certificate Authority
Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

## 8.2 - certificateRevocationList

This attribute SHOULD be stored and MUST be requested in binary form as '@certificateRevocationList;binary'.

```

attributetype ( 2.5.4.39 NAME 'certificateRevocationList'

    DESC 'X.509 certificate revocation list'

    EQUALITY certificateListExactMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.9

)

```

**Table 63 - certificateRevocationList**

Attribute Name	certificateRevocationList
Reference	IETF-RFC 4523 <sup>[26]</sup> , IETF-RFC 5280, <i>Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile</i> <sup>[28]</sup>
Object Class	icCertificationAuthority
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 IC PKI CP <sup>[7]</sup>
Allowable Values	A valid X.509 V2 CRL as defined in IETF-RFC 5280 <sup>[28]</sup> and the IC PKI CRL <sup>[8]</sup>
Example	Any CRL issued by an authorized PKI Certificate Authority

Attribute Name	certificateRevocationList
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

## 8.3 - cACertificate

This attribute SHOULD be stored and MUST be requested in binary form as '@cACertificate;binary'.

```

attributetype ( 2.5.4.37 NAME 'cACertificate'

    DESC 'X.509 CA certificate'

    EQUALITY certificateExactMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.8

)

```

**Table 64 - cACertificate**

Attribute Name	cACertificate
Reference	IETF-RFC 4523 <sup>[26]</sup> , IETF-RFC 5280 <sup>[28]</sup>
Object Class	icCertificationAuthority
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 IETF-RFC 5280 <sup>[28]</sup> and the IC PKI CRL <sup>[8]</sup>
Example	Any authorized PKI Certificate Authority certificate
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

## 8.4 - icNetworks

```

attributetype ( 2.16.840.1.101.2.2.1.160 NAME 'icNetworks'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

)

```

**Table 65 - icNetworks**

Attribute Name	icNetworks
Reference	FSD
Object Class	icOrgPerson / icOrgServer, icCertificationAuthority
Friendly Name	IC Networks
Description	@ <b>icNetworks</b> 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 and CA.
Allowable Values	Values listed in "VIRTCVEnums.pdf" in VIRT.XML <sup>[36]</sup>
Examples	ACSS NSANET
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	MULTI-VALUE

## 8.5 - resourceSecurityMark

```

attributetype ( 2.16.840.1.101.2.2.1.161 NAME 'resourceSecurityMark'

    EQUALITY caseIgnoreMatch

    SUBSTR caseIgnoreSubstringsMatch

    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

    SINGLE-VALUE

)

```

**Table 66 - resourceSecurityMark**

Attribute Name	resourceSecurityMark
Reference	FSD
Object Class	icOrgPerson / icOrgServer, icCertificationAuthority
Friendly Name	Resource Classification
Description	The classification and handling markings for the associated directory object for both IC Person and Non-Person Entities and CAs.
Allowable Values	Classification and handling marking banner as described in the latest published version of the IC Markings <sup>[6]</sup>



Attribute Name	resourceSecurityMark
Examples	"UNCLASSIFIED" "SECRET//NOFORN"
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

Appendix A Feature Summary

The following table summarizes major features by version for FSD and all dependent specs. The “Required date” is the date when systems should support a feature based on the specified driver. Executive Orders, Information Security Oversight Office (ISOO) notices, ICDs and other policy documents have a variety of effective dates.

Table 67 - Feature Summary Legend

Key	Description
F	Full (able to comply and verified by spec to some degree)
P	Partial (Able to comply but not verifiable)
N	Non-compliance (Can’t comply)
N/A	Not Applicable. Feature is no longer required.
Cell Colors represent the same information as the Key value	

A.1. FSD Feature Summary

A.1.1. Features from V2015-AUG to V2021-NOV

Table 68 - FSD Feature Comparison V2015-AUG to V2021-NOV

Required date	Feature	V2015-AUG	V2016-SEP	V2019-SEP	V2021-NOV
	Add attribute auditRoutingOrganization	N	F	F	F
	Add attribute instantMessageAddress	N	N	F	F
	@countryOfAffiliation, @expertCountry and @nationalityExtended use IC-GENC.CES <sup>[9]</sup>	N	N	F	F
	Change format of UIAS foreign partner organizations to match IC-SEA and 5EE	N	N	N	F

A.1.2. Features from V2 to V2015-AUG

Table 69 - FSD Feature Comparison V2 to V2015-AUG

Required date	Feature	V2	V3	V2014-DEC	V2015-AUG
	Comply with ICS 500-13 Technical Amendment	N	F	F	F
	Added personaUID and distinguishedName (dn)	N	N	F	F
90 Days from Signature	Comply with IC FSD Policy Statements	N	N	F	F
	Update Chapter 6 for ARL, icNetworks, and resourceSecurityMarks	N	N	N	F
	Add attribute preferredName	N	N	N	F
	Replace Object Class certificationAuthority with icCertificationAuthority	N	N	N	F
	Support for other PKI CAs (e.g., CAD)	N	N	N	F

A.1.3. Features from V1 to V2

Table 70 - FSD Feature Comparison V1 to V2

Required date	Feature	V1	V2
	Map to Unified Identity Attribute Set (UIAS)	N	F

## Appendix B Change History

[Table 71](#) summarizes the version identifier history for this Data Encoding Specification.

**Table 71 - Identifier History**

Version	Date	Purpose
1	December 14, 2011	Initial Release. For details of changes, see <a href="#">Section B.8 - V1 Change Summary</a>
2	August 16, 2013	Updated to comply with appropriate attributes from <i>IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3.1</i> . For details of changes, see <a href="#">Section B.7 - V2 Change Summary</a>
3	March 14, 2014	Updated to comply with Technical Amendment to ICS 500-13. For details of changes, see <a href="#">Section B.6 - V3 Change Summary</a>
2014-DEC	December 4, 2014	Added personaUID and distinguishedName (dn). For details of changes, see <a href="#">Section B.5 - V2014-DEC Change Summary</a>
2015-AUG	August 13, 2015	Routine revision to technical specification. For details of changes, see <a href="#">Section B.4 - V2015-AUG Change Summary</a>
2016-SEP	September 9, 2016	Routine revision to technical specification. For details of changes, see <a href="#">Section B.3 - V2016-SEP Change Summary</a>
2019-SEP	September 6, 2019	Routine revision to technical specification. For details of changes, see <a href="#">Section B.2 - V2019-SEP Change Summary</a>
2021-NOV	December 3, 2021	Routine revision to technical specification. For details of changes, see <a href="#">Section B.1 - V2021-NOVChange Summary</a>

### B.1 - V2021-NOVChange Summary

Significant drivers for version 2021-NOV include:

- Community Change Requests

[Table 72](#) summarizes the changes made to this technical specification from version 2019-SEP to version 2021-NOV.

**Table 72 - Data Encoding Specification V2021-NOV Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Change format of UIAS foreign partner organizations to match IC-SEA and 5EE (CR-2019-003)	Documentation	Data generation and ingestion systems for entity attributes need to be updated to accommodate the changes. Identity, Credential, and Access Management (ICAM) systems and software services need to be updated to accommodate the changes.
2	Updated ICD 503 document name. (CR-2019-064)	Documentation	No impact to systems.
3	Modified IC FSD System Description to align with public release. (CR-2019-178)	Documentation	No impact to systems.
4	Modified personalTitle to include the gender neutral title of Mx. (CR-2021-027)	Documentation	No impact to systems.

## B.2 - V2019-SEP Change Summary

Significant drivers for version 2019-SEP include:

- Community Change Requests

[Table 73](#) summarizes the changes made to this technical specification from version 2016-SEP to version 2019-SEP.

**Table 73 - Data Encoding Specification V2019-SEP Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Updated documentation to use the specification framework. Removed the Dependency Over Time table. (CR-2019-028)	Documentation	No impact to systems.
2	Added <code>@instantMessageAddress</code> (CR-2018-134)	Documentation Schema	Added new attribute.
3	Updated <code>auditRoutingOrganization</code> multiplicity and values. (CR-2019-073)	Documentation	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
4	@countryOfAffiliation, @expertCountry and @nationalityExtended use IC-GENC.CES <sup>[9]</sup> (CR-2019-074)	Documentation	No impact to systems.

## B.3 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Community Change Requests

Summarizes the changes made to this technical specification from Version 2015-AUG to Version 2016-SEP.

**Table 74 - Data Encoding Specification V2016-SEP Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Added @auditRoutingOrganization (CR-2016-022)	DES Schema	Added new required attribute
2	Added reference to UIAS CVEs for entityType and lifeCycleStatus. (CR-2015-034, CR-2016-016)	DES Schema	Align with UIAS CVEs
3	Added reference to ISMCAT's Responsible Entity CVE for expertCountry, nationality-extended, and countryOfAffiliation (CR-2015-102)	DES Schema	Align with other specifications designating country names.
4	Added reference to GENC for countryName (CR-2016-044)	DES Schema	Align with other specifications designating country names.
5	Update applicability section to reflect a requirement to comply with Law/Policy (CR-2016-063)	Documentation	Implementers must verify that they are complying with applicable laws and policies.

## B.4 - V2015-AUG Change Summary

Significant drivers for Version 2015-AUG include:

- Community Change Requests

Summarizes the changes made to this technical specification from Version 2014-DEC to Version 2015-AUG.

**Table 75 - Data Encoding Specification V2015-AUG Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Attribute updated.	@icNetworks	Changed from Optional to Mandatory for CA Objects; updated allowed values to reference VIRT.XML <sup>[36]</sup> .
2	Attribute updated.	@resourceSecurityMark	Changed from Optional to Mandatory for CA Objects.
3	Attribute updated.	@authorityRevocationList	Changed from Mandatory to Optional for CA Objects.
4	Deprecated attribute.	@languageProficiency	Deprecated attribute.
5	Attribute added.	@preferredName	Attribute added.
6	Modified text.	FSD Data Encoding Specification (DES) Chapter 4	Added table to separate persons from NPE.
7	Modified text.	FSD DES Chapter 5	Added table to separate persons from NPE.
8	Modified text.	FSD DES Chapter 6	changed certificationAuthority to icCertificationAuthority.
9	Modified text.	FSD DES Chapter 6	changed language to support other PKI Certification Authorities.

## B.5 - V2014-DEC Change Summary

Significant drivers for Version 2014-DEC include:

- Added new attribute for personaUID
- Added policy statements

Summarizes the changes made to this technical specification from Version 3 to Version 2014-DEC.

**Table 76 - Data Encoding Specification V2014-DEC Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Implemented new versioning scheme.	DES	Changed versioning scheme from version number (e.g., V3) to version YYYY-MMM (e.g, 2014-DEC).
2	Attribute updated.	@ipServerAddress	Changed from Mandatory to Optional.

#	Change	Artifacts changed	Compatibility Notes
3	Attribute updated.	@adminOrganization	Added support for 2PI.
4	Added new attribute.	@personaUID	Added new attribute.
5	Added new attribute.	@distinguishedName (dn)	Added attribute to support Common Operating Environment identifier.
6	Added policy statements.	n/a	Added new policy statements.

## B.6 - V3 Change Summary

Significant drivers for Version 3 include:

- Add attribute for @dutySubOrganization

Summarizes the changes made to this technical specification from Version 2 to Version 3.

**Table 77 - Data Encoding Specification V3 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Attribute displayName updated.	@displayName	Updated with new attribute @dutySubOrganization.
2	Added Attribute.	@dutySubOrganization	Added new attribute to be managed and populated by participating IC Elements.
3	Updated CVE.	@icNetworks	Updated CVE.

## B.7 - V2 Change Summary

Significant drivers for Version 2 include:

- Provide alignment to UIAS

Summarizes the changes made to this technical specification from Version 1 to Version 2.

**Table 78 - Data Encoding Specification V2 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	New Attribute	@adminOrganization	New attribute to be managed and populated by participating IC Elements.
2	New Attribute	@ATOSStatus	New attribute to be managed and populated by participating IC Elements.



#	Change	Artifacts changed	Compatibility Notes
3	New Attribute	@countryOfAffiliation	New attribute to be managed and populated by participating IC Elements.
4	New Attribute	@dutyOrganization	New attribute to be managed and populated by participating IC Elements.
5	New Attribute	@lifeCycleStatus	New attribute to be managed and populated by participating IC Elements.
6	Deprecated attribute.	@serviceOrAgency	Deprecated attribute.
7	Deprecated attribute.	@nationality-Extended	Deprecated attribute.
8	Promoted	@isICMember	Promotion to Mandatory attribute.
9	Updated	@employeeType	Added NPE values.
10	Updated	CA objects	Added Resource Security Mark and icNetworks attributes to schema.

## B.8 - V1 Change Summary

Significant drivers for Version 1 include:

- Many of these attributes were already in use in the community. This specification serves to codify an agreed-upon interpretation of these attributes and their meaning.

Summarizes the changes made to this technical specification from prior documentation to Version 1.

### Table 79 - Data Encoding Specification V1 Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	New attribute to be managed and populated by participating IC Elements.	@isICMember	New attribute to be managed and populated by participating IC Elements.
2	New attribute to be managed and populated by participating IC Elements.	@generationQualifier	New attribute to be managed and populated by participating IC Elements.
3	Deprecated attribute.	Community of Interest (COI)	Deprecated attribute due to lack of use.
4	Promotion to Mandatory attribute.	@cn	Promotion to Mandatory attribute.

#	Change	Artifacts changed	Compatibility Notes
5	Promotion to Mandatory attribute.	@employeeType	Promotion to Mandatory attribute.
6	Promotion to Mandatory attribute.	@icNetworks	Promotion to Mandatory attribute.
7	Promotion to Mandatory attribute.	@resourceSecurityMark	Promotion to Mandatory attribute.
8	Controlled Vocabulary defined.	@employeeType	Controlled Vocabulary defined.
9	Controlled Vocabulary defined.	@serviceOrAgency	Controlled Vocabulary defined.
10	Authentication Mechanisms	Various	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 – <i>Securing Access to IC FSD Attributes</i> of this technical specification.

## Appendix C Glossary

This appendix lists terms, definitions and sources of the definitions for terms used in this document.

attribute	<p>A distinct characteristic of an object. In the context of ICAM standards for PE and NPE entities, an attribute captures characteristics of PEs and NPEs.</p> <p>Source: ICS 500-30, <i>Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources</i> <a href="#">[21]</a>.</p>
audit	<ol style="list-style-type: none"> <li>1. Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.</li> </ol> <p>Source: Committee on National Security Systems Instruction (CNSSI) 4009, <i>National Information Assurance (IA) Glossary</i> <a href="#">[2]</a>.</p> <ol style="list-style-type: none"> <li>2. Provides authorized personnel with the ability to review and examine any action that can potentially cause access to, generation of, or affect the release of classified or sensitive information.</li> </ol> <p>Source: Intelligence Community Standard (ICS) 500-27, <i>Intelligence Community Standard for Collection and Sharing of Audit Data</i> <a href="#">[19]</a>.</p>
Entity	<p>An individual (person), organization, device, or process.</p> <p>Source: NIST 800-56Br1, <i>Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Revision 1</i> <a href="#">[30]</a>.</p>
Non-Person Entity (NPE)	<p>Entity related to Information Technology (IT), e.g., hardware objects (physical entities/devices) and software objects (virtual/logical entities).</p> <p>Source: ICS 500-30, <i>Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources</i> <a href="#">[21]</a>.</p>
Person Entity (PE)	<p>A human Entity that is the Owner of a PKI certificate (NIST SP 800-56Br1). A human entity that is the Name or Role Subscriber in a PKI certificate (CNSSI 1300).</p>

Source: NIST SP 800-56Br1, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Revision 1* [\[30\]](#).

Source: CNSSI 1300, *Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy under CNSS Policy No. 25* [\[1\]](#)

## Second Party Integree

Second Party Integree means:

1. A Second Party citizen who is employed by a Second Party Government who works in support of a USG objective at a USG organization, under the supervision and direction of USG personnel within a USG facility or Second Party facility with a co-utilization agreement
2. A Second Party citizen who works under a USG contract, in support of a USG objective at a USG organization, under the supervision and direction of USG personnel within a USG facility or Second Party facility with a co-utilization agreement.

Individuals who act on behalf of a Second Party in a representational capacity are not Second Party Integrees.

Sources:

1. DNI Executive Correspondence 2016-00816, *Second Party Integree Access to the IC Information Environment* [\[3\]](#).

## Appendix D List of Abbreviations

This appendix lists all the acronyms and abbreviations referenced in this encoding specification.

2PI	Second Party Integree
2PS	Second Party Sovereign
ACSS	Allied Collaborative Shared Services
ARL	Authority Revocation List
ATO	Authority To Operate
CA	Certificate Authority
CAD	Cryptologic Agencies Domain
CIA	Central Intelligence Agency
CN	Common Name
COI	Community of Interest
CRL	Certificate Revocation List
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DN	Distinguished Name
DNI	Director of National Intelligence
DNS	Domain Name System
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Digital Object Identifier
DOJ	Department of Justice
DOS	U.S. Department of State
DOT	Department of Transportation

DSN	Defense Switched Network
DVA	Department of Veterans Affairs
E.O.	Executive Order
EOP	Executive Office of the President
EPA	Environmental Protection Agency
ESB	Enterprise Standards Baseline
FRB	Federal Reserve Board
FSD	Full Service Directory
HHS	Health and Human Services
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC ESB	Intelligence Community Enterprise Standards Baseline
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
JWICS	Joint Worldwide Intelligence Communications System
LDAP	Lightweight Directory Access Protocol
NASA	National Aeronautics and Space Administration
NGA	National Geospatial Intelligence Agency
NIPRNet	Non-Classified Internet Protocol Router Network
NPE	Non-Person Entity

NRC	Nuclear Regulatory Commission
NRO	National Reconnaissance Office
NSA	National Security Agency
NSANET	The National Security Agency intranet
ODNI	Office of the Director of National Intelligence
OMG	Object Management Group
OPM	Office of Personnel Management
PE	Person Entity
PK	Private Key
PKI	Public Key Infrastructure
POC	Point of Contact
RFC	Request for Comments
SCI	Sensitive Compartmented Information
SIPRNet	Secret Internet Protocol Router Network
S/MIME	Secure/Media Type
TREA	Department of the Treasury
TS	Top Secret
UAAS	Unified Authorization and Attribute Services
UIAS	Unified Identity Attribute Set
URL	Uniform Resource Locator
US	United States
USAID	U.S. Agency for International Development
USCP	United States Capitol Police
USDA	U.S. Department of Agriculture
USPIS	United States Postal Inspection Service
USPS	United States Postal Service
XML	Extensible Markup Language

XSL	Extensible Stylesheet Language
XSLT	XSL Transformations



## Appendix E Bibliography

[1] CNSSI 1300

Committee on National Security Systems. *Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy under CNSS Policy No. 25*. 1300. December 2014.

Available online at: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

[2] CNSSI 4009

Committee on National Security Systems. *National Information Assurance (IA) Glossary*. 4009. 6 April 2015.

Available online at: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

[3] ES 2016-00816

ODNI. *Second Party Integree Access to the IC Information Environment*. ES 2016-00816. 30 December 2016.

[4] E.O. 12333

The White House. *Executive Order 12333 - United States Intelligence Activities, as Amended*. Federal Register, Vol. 46, No. 235. 4 December 1981.

Available online at: <http://www.archives.gov/federal-register/codification/executive-order/12333.html>

[5] GENC

Country Codes Working Group. *Geopolitical Entities, Names, and Codes*. 3.0.

Available online Intelink-TS at: <https://go.ic.gov/Tuxrlnu> (case sensitive – Tango uniform xray romeo India november uniform )

Available online at: <https://nsgreg.nga.mil/genc/discovery>

[6] IC Markings

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*.

Available online Intelink-TS at: <https://go.ic.gov/tGXkwGO> (case sensitive – tango Golf Xray kilo whiskey Golf Oscar )

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/icmarkings>

[7] IC PKI CP V5.6

Office of the Director of National Intelligence. *Intelligence Community Public Key Infrastructure Certificate Policy*. Version 5.6. 7 Jan 2021.

Available online Intelink-TS at: <https://go.ic.gov/KVNEsXt> (case sensitive – Kilo Victor November Echo sierra Xray tango )

[8] IC PKI CRL

Office of the Director of National Intelligence. *Intelligence Community (IC) Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profiles*. Version 2.9.13 FINAL. 13 April 2021.

Available online Intelink-TS at: <https://go.ic.gov/bEA2UCP> (case sensitive – bravo Echo Alpha 2 Uniform Charlie Papa )

[9] IC-GENC.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Geopolitical Entities, Names, and Codes (IC-GENC.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/Tuxrlnu> (case sensitive – Tango uniform xray romeo India november uniform )

Available online Intelink-U at: <https://w3id.org/ic/standards/IC-GENC>

Available online at: <https://w3id.org/ic/standards/public>

[10] IC-SF.XML

Office of the Director of National Intelligence. *Intelligence Community Specification Framework (IC-SF.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/pNFyuVg> (case sensitive – papa November Foxtrot yankee uniform Victor golf )

Available online Intelink-U at: <https://w3id.org/ic/standards/IC-SF>

Available online at: <https://w3id.org/ic/standards/public>

[11] ICD 500

Office of the Director of National Intelligence. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.

Available online Intelink-TS at: <https://go.ic.gov/U7v6ZRL> (case sensitive – Uniform 7 victor 6 Zulu Romeo Lima )

Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_500.pdf](http://www.dni.gov/files/documents/ICD/ICD_500.pdf)

[12] ICD 501

Office of the Director of National Intelligence. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.

Available online Intelink-TS at: <https://go.ic.gov/fTBM8OS> (case sensitive – foxtrot Tango Bravo Mike 8 Oscar Sierra )

Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_501.pdf](http://www.dni.gov/files/documents/ICD/ICD_501.pdf)

[13] ICD 503

Office of the Director of National Intelligence. *Intelligence Community Information Technology Systems Security Risk Management*. Intelligence Community Directive 503. 21 July 2015.

Available online Intelink-TS at: <https://go.ic.gov/Ru5XGc9> (case sensitive – Romeo uniform 5 Xray Golf charlie 9 )

Available online at: <http://www.dni.gov/files/documents/ICD/ICD503.pdf>

[14] ICPG 500.1

Deputy Director of National Intelligence for Policy, Plans, and Requirements. *Digital Identity*. Intelligence Community Policy Guidance 500.1. 7 May 2010.

Available online Intelink-TS at: <https://go.ic.gov/kEqL6Dh> (case sensitive – kilo Echo quebec Lima 6 Delta hotel )

[15] ICPG 500.2

Assistant Director of National Intelligence for Policy and Strategy. *Attribute-Based Authorization and Access Management*. Intelligence Community Policy Guidance 500.2. 23 November 2010.

Available online Intelink-TS at: <https://go.ic.gov/NUAEWk1> (case sensitive – November Uniform Alpha Echo Whiskey kilo 1 )

Available online at: [http://www.dni.gov/files/documents/ICPG/icpg\\_500\\_2.pdf](http://www.dni.gov/files/documents/ICPG/icpg_500_2.pdf)

[16] ICS 500-13

Director of National Intelligence Chief Information Officer. *Intelligence Community Email Standard Display Name Format*. Intelligence Community Standard 500-13. 2014.

Available online Intelink-TS at: <https://go.ic.gov/jQodYin> (case sensitive – juliet Quebec oscar delta Yankee india november )

[17] ICS 500-15

Director of National Intelligence Chief Information Officer. *Intelligence Community Optimized Network Email Full Service Directory*. Intelligence Community Standard 500-15. 16 October 2008.

Available online Intelink-TS at: <https://go.ic.gov/XsbGMr2> (case sensitive – Xray sierra bravo Golf Mike romeo 2 )

[18] ICS 500-20

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.

Available online Intelink-TS at: <https://go.ic.gov/kh8NMVJ> (case sensitive – kilo hotel 8 November Mike Victor Juliet )

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-20>

[19] ICS 500-27

Director of National Intelligence Chief Information Officer. *Intelligence Community Standard for Collection and Sharing of Audit Data*. Intelligence Community Standard 500-27. 2 June 2011.

Available online Intelink-TS at: <https://go.ic.gov/Jznuy0x> (case sensitive – Juliet zulu november uniform yankee 0 xray )

[20] ICS 500-29

Director of National Intelligence Chief Information Officer. *Intelligence Community Digital Identifier*. Intelligence Community Standard 500-29. 12 July 2012.

Available online Intelink-TS at: <https://go.ic.gov/ObgTCPJ> (case sensitive – Oscar bravo golf Tango Charlie Papa Juliet )

[21] ICS 500-30

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources*. Intelligence Community Standard 500-30. 24 April 2014.

Available online Intelink-TS at: <https://go.ic.gov/lqk775v> (case sensitive – lima quebec kilo 7 7 5 victor )

[22] IETF-RFC 2798

Internet Engineering Task Force. *Definition of the inetOrgPerson LDAP Object Class*. April 2000.

Available online at: <http://www.ietf.org/rfc/rfc2798.txt>

[23] IETF-RFC 4510

OpenLDAP Foundation. *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*. June 2006.

- Available online at: <https://www.ietf.org/rfc/rfc4519.txt>
- [24] IETF-RFC 4512  
OpenLDAP Foundation. *Lightweight Directory Access Protocol (LDAP): Directory Information Models*. June 2006.  
Available online at: <https://www.ietf.org/rfc/rfc4512.txt>
- [25] IETF-RFC 4519  
eB2Bcom. *Lightweight Directory Access Protocol (LDAP): Schema for User Applications*. June 2006.  
Available online at: <https://www.ietf.org/rfc/rfc4519.txt>
- [26] IETF-RFC 4523  
OpenLDAP Foundation. *Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates*. June 2006.  
Available online at: <https://www.ietf.org/rfc/rfc4523.txt>
- [27] IETF-RFC 4524  
OpenLDAP Foundation. *COSINE LDAP/X.500 Schema*. June 2006.  
Available online at: <https://www.ietf.org/rfc/rfc4524.txt>
- [28] IETF-RFC 5280  
Internet Engineering Task Force. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. May 2008.  
Available online at: <http://www.ietf.org/rfc/rfc5280.txt>
- [29] ISO 11179-3  
International Organization for Standardization (ISO). *ISO/IEC 11179, Information Technology -- Metadata registries (MDR), Part 3: Registry metamodel and basic attributes*.  
Available online at: <https://www.iso.org/standard/50340.html>
- [30] NIST 800-56Br1  
National Institute of Standards and Technology. *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*. Revision 1. September 2014.  
Available online at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf>
- [31] Public\_Law\_80-242  
Secretary of the Interior. *Public Law 242-80th Congress*. 1947-07-25.  
Available online at: [https://geonames.usgs.gov/docs/pubs/Public\\_Law\\_242.pdf](https://geonames.usgs.gov/docs/pubs/Public_Law_242.pdf)
- [32] Schematron  
International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron*. ISO/IEC 19757-3:2006.  
ISO Spec Available online at: <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>  
StyleSheets for compiling Available online at: <http://code.google.com/p/schematron/>
- [33] UIAS.XML

Office of the Director of National Intelligence. *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/xQK4AX1> (case sensitive – xray Quebec Kilo 4 Alpha Xray 1 )

Available online Intelink-U at: <https://w3id.org/ic/standards/UIAS>

Available online at: <https://w3id.org/ic/standards/public>

[34] UML

Object Management Group (OMG). *Unified Modeling Language*. 6 December 2017.

Available online at: <https://www.omg.org/spec/UML/2.5.1/PDF/changebar>

[35] USAgency.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/wmyIRCV> (case sensitive – whiskey mike yankee India Romeo Charlie Victor )

Available online Intelink-U at: <https://w3id.org/ic/standards/USAgency>

Available online at: <https://w3id.org/ic/standards/public>

[36] VIRT.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Virtual Coverage (VIRT.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/BljGxq> (case sensitive – Bravo India lima juliet Golf xray quebec )

Available online Intelink-U at: <https://w3id.org/ic/standards/VIRT>

Available online at: <https://w3id.org/ic/standards/public>

[37] XSLT2

World Wide Web Consortium (W3C). *XSL Transformations (XSLT) Version 2.0*. W3C Recommendation 23 January 2007.

Available online at: <http://www.w3.org/TR/xslt20/>

## 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 the following DNI-sponsored web sites.

Public Website: <https://w3id.org/ic/standards/public>

Intelshare: <https://w3id.org/ic/standards/data-specs>

Direct all inquiries about this IC technical specification, IC technical specification collaboration and coordination forums, or IC element representatives involved in those forums, to the IC CIO.

E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov).

## Appendix G IC CIO Approval Memo

An IC CIO Approval Memo should accompany this enterprise technical data specification bearing the signature of the IC CIO or an IC CIO-designated official(s). If an IC CIO Approval Memo is not accompanying this specification's version release package, then refer back to the authoritative web location(s) for this specification to see if a more complete package or a specification update is available.

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

Upon signature of the IC CIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the Intelligence Community Enterprise Standards Baseline (IC ESB) as defined in ICS 500-20<sup>[18]</sup>.