Intelligence Community Technical Specification

IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set

Version 2

Approval Date: 17-JUL-2012

Distribution Notice

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

Table of Contents

List of Tables

Chapter 1 Introduction

1.1 Purpose

This technical specification governs the set of Intelligence Community (IC) enterprise identity attributes and associated values that must be supported by an Attribute Service (AS) participating in the IC's Unified Authorization and Attribute Service (UAAS) capability. The specification is the basis for defining and populating the set of attributes and values that comprise an attribute statement or assertion, e.g., Security Assertion Markup Language (SAML) Attribute Statement as described in the *SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Version 1.0*, *[Encrypted Mode]* (27 March 2008).

1.2 Scope

This specification is applicable to the IC and access to the information produced by, stored within, or shared throughout the IC's TS/SCI information domain as defined in Intelligence Community Policy Guidance (ICPG) 500.1, *Digital Identity*. 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 identity attributes, multiplicity and values defined at the enterprise level for entities, both persons and non-person entities (NPEs) (e.g., machines, servers, services, processes, applications, etc.) within the IC information domain required for UAAS exchange. In the case that the attribute is not applicable to a type of entity, or if the entity does not have any values listed for the particular attribute, then the attribute is not exchanged as part of the attribute assertion.

In addition to enterprise identity attributes, there are other classes of attributes (such as extended and local) that may be used to further protect resources as appropriate, but they are outside the scope of this document. Undocumented attribute exchange is supported by UAAS, as described in the *Department of Defense and Intelligence Community Unified Authorization and Attribute Service, Concept of Operations, December 8, 2008, Version 1.11*. These additional attributes may become enterprise attributes over time, necessitating updates to this document over time.

IC Enterprise Identity Attributes are assigned per persona. A persona is an electronic identity that is unambiguously associated with a single person or 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).

1.3 Background

The IC Chief Information Officer (IC CIO) is leading the IC's enterprise transformation to a flexible, scalable and interoperable architecture for use within and across the IC's environments. Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer*, grants the IC CIO the authority and responsibility to:

- Develop an IC Enterprise Architecture (IC EA)

- Lead the IC's identification, development, and management of IC enterprise standards
- Incorporate technically sound, de-conflicted, interoperable enterprise standards into the IC EA
- Certify IC elements adhere to the architecture and standards.

In the area of enterprise standardization, the IC CIO is called upon to establish common IT standards, protocols, and interfaces; to establish uniform information security standards; and to ensure information technology infrastructure, enterprise architecture, systems, standards, protocols, and interfaces, support the overall information sharing strategies and policies of the IC as established in relevant law, policy, and directives.

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse.

1.4 Enterprise Need

Defining the set of IC enterprise identity attributes and values for sharing through IC UAAS supports the opportunity for consistent and assured information sharing across the enterprise. The IC UAAS supports Attribute-Based Access Control (ABAC) to promote on-demand access to information and other resources by IC users and services, and reduces authorization vulnerabilities by strengthening the access control decision process.

Implementers of IC UAAS-compliant attribute services require coordination of identity attribute definitions. This requires the usage of standardized attribute names and values when exchanging attribute assertions (e.g., SAML protocol messages) between systems participating in IC UAAS.

This technical specification aligns with the Attribute Practice Statement (APS) provided by each IC UAAS Attribute Service provider. The APS describes how each service provider populates the IC enterprise identity attributes provisioned to each persona, and how attribute data is managed and kept current.

1.5 Audience and Applicability

The primary audience for this document is the implementer and/or administrator who must configure an Attribute Service to meet the requirements for participation in the IC UAAS capability. The audience for this document also includes:

- Those responsible for implementing and managing the capabilities that create, provide, modify, store, exchange, search, display, or further process IC enterprise identity attributes
- Data stewards for protected resources, who will use this information to develop policies for access control

This document applies to all IC enterprise identity attributes exchanged amongst UAAS-compliant Attribute Services and capabilities on the IC information domain.

The conditions and applicability for this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*, defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

The IC ESB defines the compliance requirements associated with each version of a technical specification. Each version will be individually registered in the IC ESB. The IC ESB will define, among other things, the location(s) of the relevant artifacts, prescriptive status, and validity period, all of which characterize the version and its utility.

Additional applicability and guidance may be defined in separate IC policy guidance.

1.6 Conventions

Certain technical and presentation conventions were used in the creation of this document in order to ensure technical consistency across this specification and others.

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

Certain typography is used throughout the body of this document to ensure readability and understanding, and to convey certain meanings, in particular:

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

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 1. Multiplicity

Multiplicity	Description
1	Indicates the attribute is mandatory and must contain only one value.
0:1	Indicates the attribute is optional and must 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 may contain one or more values.
0:n	Indicates the attribute is optional and may contain at most n values.
n:m	Indicates the attribute is mandatory having at least n values, and may contain at most m values.

Additionally within this technical specification there is the notation that some attributes are only applicable to person or non-person entities. These conditional multiplicity values are noted as “P” for persons and “NPE” for non-persons.

1.7 Conformance

For an implementation to conform to this specification, it MUST adhere to all normative aspects of the specification. For the purposes of this document, normative and informative are defined as:

Normative: considered to be prescriptive and necessary to conform to the standard.

Informative: serving to instruct, enlighten or inform.

Within this document, class name, attribute names, attribute multiplicity, attribute visibility, and class inheritance are normative for class diagrams. All tables describing the class attributes are normative for descriptions of the attributes and informative for all other aspects of the class. Paragraphs in this document containing a word in ALL CAPS as described in section 1.6 are normative. All other parts of this document are informative.

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

1.8 Dependencies

This technical specification depends on the additional technical specifications or additional documentation listed in Table 2. The documents listed below may or may not be referenced in Chapter 2 or Appendix C, and may or may not be considered normative or informative.

Table 2. Dependencies

Name
Data Encoding Specification for the IC Full Service Directory Schema, Version 1.0 (14 Dec 2011)
Scattered Castles, Version 2
NSA’s Master Data Registry
ISO 3166-1, Country Codes

Chapter 2 IC Enterprise Identity Attributes Specification

2.1 IC Enterprise Identity Attribute Names and Values

The attributes as defined in this specification represent the set of IC enterprise identity attributes and associated values that must be supported by an AS participating in the IC's UAAS capability. UAAS exchange requires using these attributes and values for exchange of attributes for both persons and non-person entities, except where indicated in the definition and multiplicity.

All of these attributes may be required within an attribute assertion sent in response to an attribute query originating from another Attribute Service for entity's attributes. In cases where attribute names and values defined below differ in underlying authoritative sources or agency implementations, they must be transformed or derived to match this specification before passing them via UAAS.

In each of the definitions below, the entity's persona is uniquely identified within the IC information domain (as defined in ICPG 500.1) by the Distinguished Name (DN) in the Public Key Infrastructure (PKI) issued certificate. An entity may have one or more personas for both persons and NPEs (e.g., servers, services, applications, etc.).

To ensure trust, where authoritative sources for Allowed Values are cited for specific attributes, the authoritative source must support and work in conjunction with this technical specification and under guidance from designated community governance authorities by managing and governing the controlled value enumerations (CVE) for the value set.

2.1.1 Admin Organization

Attribute Name	**AdminOrganization**
Definition/Purpose	Reflects the home organization of the entity
Allowed Values	Values listed for serviceOrAgency attribute in *Data Encoding Specification for the IC Full Service Directory Schema,* Version 1.0, (14 Dec 2011)
Multiplicity	[1]
Example	DIA

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

AdminOrganization 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.

2.1.2 Authority Category

Attribute Name	**AuthorityCategory**

Definition/Purpose	This attribute specifies the authority(ies) under which the entity is authorized to access and/or discover protected resources.
Allowed Values	Values listed for the Legal Authority Categories attribute from NSA's Master Data Registry
Multiplicity	[0:*]
Example	ICD503, FISA_B, EO12333_IA, DODD8530_USA

This attribute specifies the authority under which the entity (person or non-person) is authorized to access and/or discover protected resources.

Authority types can include, but are not limited to, legal, policy, training or mission. AuthorityCategory is used for access control decisions to protected resources. If the entity does not have any values listed for the AuthorityCategory attribute, then the attribute is not exchanged as part of the attribute assertion.

2.1.3 Authority to Operate (ATO) Status

Attribute Name	**ATOStatus**
Definition/Purpose	This attribute indicates the Authority to Operate (ATO) status for the Non-Person entity.
Allowed Values	Boolean: True, False

Multiplicity	Conditional:
	P = [0]
	NPE = [1]
	Default=False

Example	True

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, Certification and Accreditation*, 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 ATOStatus attribute is only applicable for non-person entities. If the UAAS exchange is for a person entity, then the ATOStatus attribute is not exchanged as part of the attribute assertion.

2.1.4 Authorized IC Person (AICP)

Attribute Name	**AICP**
Definition/Purpose	Reflects whether or not the entity is an AICP
Allowed Values	Boolean: True, False

Multiplicity	Conditional:
	P = [1]
	NPE = [0]
	Default=False

Example	True

AICP is defined by ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community* as follows:

> *"A U.S. person employed by, assigned to, or acting on behalf of an IC element who, through the course of their duties and employment, has a mission need and an appropriate security clearance for information collected or analysis produced. Authorized IC personnel shall be identified by their IC element head and shall have discovery rights to information collected and analysis produced by all elements of the IC. The term may include contractor personnel."*

This attribute is a flag that reflects whether a person has been identified by their IC element head to act as an AICP. Under ICD 501, only users employed by, assigned to, or acting on behalf of an IC element may be AICPs.

This is a Boolean attribute that is set to False by default. Where this attribute is unpopulated, its value shall be treated as False. AICP will only be set to True if the isICMember attribute is also set to True.

AICP is specific to persons and associated personas, and is not applicable to non-person entities, and is used for access control decisions to protected resources.

If the UAAS exchange is for a non-person entity, then the AICP attribute is not exchanged as part of the attribute assertion.

2.1.5 Clearance

Attribute Name	**Clearance**
Definition/Purpose	Reflects the clearance level of the entity
Allowed Values	U, R, C, S, TS, L, Q, NATO-C, NATO-S, NATO-TS
Multiplicity	[1:*]
Example	TS

This attribute specifies the entity's highest security clearance level for a person entity, or the highest security classification of information that can be handled by an NPE.

It contains values from US Security Controls, Five Eyes Controls, Department of Energy Security Controls, and NATO Security Controls.

Value	**Definition**	**Control System**
U	Unclassified	US Security Controls, Five Eyes Controls
R	Restricted	Five Eyes Controls
C	Confidential	US Security Controls, Five Eyes Controls
S	Secret	US Security Controls, Five Eyes Controls
TS	Top Secret	US Security Controls, Five Eyes Controls
L	"L"	Department of Energy Security Controls
Q	"Q"	Department of Energy Security Controls
NATO-C	NATO Confidential	NATO Security Controls

NATO-S	NATO Secret	NATO Security Controls
NATO-TS	NATO Top Secret	NATO Security Controls

Clearance is used for access control decisions to protected resources.

2.1.6 Country of Affiliation

Attribute Name	**CountryOfAffiliation**
Definition/Purpose	Reflects the citizenship of the entity
Allowed Values	3-letter country code as defined in ISO 3166-1 plus international organizations tetragraphs
Multiplicity	[1:*]
Example	USA

This attribute specifies the entity's association with a country or countries.

In the case of person entities, this is the identifier of the entity's country or countries of citizenship. In the case of non-person entities, this represents the citizenship of the administrator(s) and/or the organization(s) in control of the non-person entity.

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

2.1.7 Digital Identifier

Attribute Name	**DigitalIdentifier**
Definition/Purpose	Reflects the DN from the entity's PKI certificate
Allowed Values	DN from the entity's PKI certificate
Multiplicity	[1]

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

The DigitalIdentifier is the representation that uniquely identifies a person or non-person IC entity's persona. Intelligence Community Standard (ICS) 500-29, *Intelligence Community Digital Identifier*, specifies that the IC Digital Identifier (IC DI) is the Distinguished Name (DN) from the Public Key Infrastructure (PKI) Certificate, and is unique to the persona associated with that certificate.

A DistinguishedName (DN) is a string representation that uniquely identifies a subject within a PKI. An UAAS-compliant Attribute Service must use the DN from an entity's PKI certificate associated with that particular persona as the means for specifying the subject identity in attribute assertion being exchanged between partners in the federation. The DN is treated as an opaque key to retrieve the associated persona's attributes.

The DN entry is single valued, but an entity could possibly have multiple DNs, with a unique persona per DN as defined by IC Standard 500-29, *Intelligence Community Digital Identifier*.

2.1.8 Duty Organization

Attribute Name	**DutyOrganization**
Definition/Purpose	Reflects the assigned organization of the entity
Allowed Values	Values listed for serviceOrAgency attribute in *Data Encoding Specification for the IC Full Service Directory Schema,* Version 1.0, (14 Dec 2011)
Multiplicity	[1]
Example	DNI

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 their home or administrative agency to another agency for a Joint Duty assignment or other rotation.

2.1.9 Entity Type

Attribute Name	**EntityType**
Definition/Purpose	Reflects the type of the entity
Allowed Values	GOV, CTR, MIL, SVR, SVC, DEV, NET
Multiplicity	[1]
Example	GOV

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.

Value	**Definition**	**Applicable Entity**
MIL	Military service member	Person
CTR	Contractor	Person
GOV	U.S. federal government civilian employee	Person
SVR	Server	Non-Person
SVC	Service, Widget, Application, Software, etc	Non-Person
DEV	End-point device	Non-Person
NET	Network device	Non-Person

2.1.10 Fine Access Controls

Attribute Name	**FineAccessControls**
Definition/Purpose	Reflects the fine grain access control systems, e.g., compartments, and SAPs of the entity
Allowed Values	Values listed for the AccessValue attribute from Scattered Castles Version 2.

Multiplicity	[1:*]
Examples	HCS, SI, TK

This attribute includes but is not limited to SCI Control Systems and Compartments, Special Access Programs/Special Access Restrictions, Atomic Energy Act, DoD's Critical Nuclear Weapons Design Information (CNWDI) and Department of Energy compartments which an entity (person or non-person) is authorized to access or process. It also includes the caveats associated with the clearances, where appropriate.

Note: The schema does NOT indicate that an entity holds an "interim" Sensitive Compartment Information (SCI) control.

2.1.11 Is IC Member

Attribute Name	**isICMember**
Definition/Purpose	Reflects whether or not the entity is a member of the Intelligence Community
Allowed Values	Boolean: True, False
Multiplicity	[1]
Example	True

This attribute is a flag that reflects whether the entity (person or non-person) is a member of the IC as defined by Executive Order (EO) 12333.

This is a Boolean attribute that will be set to False by default. Where this attribute is unpopulated, its value shall be treated as False.

Each organization will make the determination as to which of its personas 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 following Executive Order 12333, where an IC member is "a person employed by, assigned or detailed to, or acting for an element within the IC".

An isICMember attribute value of True is a prerequisite for determining an entity's AICP value to be True.

The isICMember attribute is used for access control decisions to protected resources for both persons and non-persons.

2.1.12 Life Cycle Status

Attribute Name	**LifeCycleStatus**
Definition/Purpose	Indicates the life cycle phase in which the entity is operating
Allowed Values	DEV, TEST, PROD, SUNSET

Multiplicity	Conditional:
	P=[0]
	NPE=[1]

Example	DEV

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.

Value	**Definition**
DEV	Development
TEST	Test
PROD	Production
SUNSET	Sunset/Retired

If the UAAS exchange is for a person entity, then the LifeCycleStatus attribute is not exchanged as part of the attribute assertion.

2.1.13 Region

Attribute Name	**Region**
Definition/Purpose	Indicates the individual countries or larger sub-regions such as geographical areas of combatant command Areas of Responsibility (AORs), Areas of Interest (AOIs), or State and Non-State Actor(s)
Allowed Values	Values listed for the ICCIO4 Subregion attribute from Scattered Castles Version 2
Multiplicity	[0:*]
Example	AFce, AFea, ASea, EUce

This attribute specifies the entity's (person or non-person) need-to-know for access to protected resources, such as individual countries or larger sub-regions such as geographical areas of combatant command, Areas of Responsibility (AORs), Areas of Interest (AOIs), or State and Non-State Actor(s).

Region is used for access control decisions to protected resources. If the entity does not have any values listed for the Region attribute, then the attribute is not exchanged as part of the assertion.

2.1.14 Role

Attribute Name	**Role**
Definition/Purpose	Indicates the position, job or area of responsibility that ties membership to the function that the entity needs to perform the expected task
Allowed Values	Values listed for the Extended Functional Role attribute from Scattered Castles Version 2
Multiplicity	[0:*]
Example	Proxy, Direct, Content Provider, Bulk

This attribute characterizes the entity's (person or non-person) authorized position, job or area of responsibility that ties membership to the function that the entity needs to perform the expected task.

Role is used for access control decisions to protected resources. If the entity does not have any values listed for the Role attribute, then the attribute is not exchanged as part of the attribute assertion.

2.1.15 Topic

Attribute Name	**Topic**
Definition/Purpose	Indicates the particular intelligence subject area
Allowed Values	Values listed for the ICCIO4 Issue attribute from Scattered Castles Version 2
Multiplicity	[0:*]
Example	HREL, HLTH, CN, DI, IC

This attribute specifies the entity's (person or non-person) need-to-know for access to protected resources, such as particular intelligence subject area.

Topic is used for access control decisions to protected resources. If the entity does not have any values listed for the Topic attribute, then the attribute is not exchanged as part of the attribute assertion.

Appendix A Change History

Table 3 summarizes the version identifier history for this technical specification.

Table 3. ICTS Version History

Version	Date	Purpose
1	14 DEC 2011	Initial Release
2	12 JUL 2012	Updated to incorporate required attributes for Non-Person Entities and IC Smart Data in support of the IC IT Enterprise (IC ITE).

Table 4 summarizes the changes made to this technical specification from to Version 1 to Version 2.

Table 4. Change History

Attribute Change	Change History Notes
AdminOrganization	New
AICP	No change.
ATOStatus	New
AuthorityCategory	New
Clearance	Updated definition to include NPEs, NATO and DoE clearances.
CountryOfAffiliation	Updated attribute name and definition to apply to NPEs
DigitialIdentifier	Updated DistinguishedName attribute name and definition to apply to NPEs
DutyOrganization	Updated Organization attribute name and definition to apply to NPEs
EntityType	Updated Employee Type attribute name and definition to apply to NPEs
FineAccessControls	Updated sciControls attribute name and definition to apply to NPEs
isICMember	Updated definition to include NPEs
LifeCycleStatus	New
Region	New
Role	New
Topic	New

Appendix B Acronyms

Table 5 summarizes the acronyms used in this technical specification.

Table 5. Acronyms

Name	Description
ABAC	Attribute Based Access Control
AICP	Authorized IC Person
AOI	Area of Interest
AOR	Area of Responsibility
APS	Attribute Practice Statement
AS	Attribute Service
ATO	Authority to Operate
CIO	Chief Information Officer
CNWDI	Critical Nuclear Weapons Design Information
CVE	Controlled Vocabulary Enumeration
DI	Digital Identifier
DoD	Department of Defense
DoE	Department of Energy
DN	Distinguished Name
DNI	Director of National Intelligence
EA	Enterprise Architecture
EO	Executive Order
ESB	Enterprise Standards Baseline
FSD	Full Service Directory
FY	Fiscal Year
HTTP	Hyper Text Transport Protocol
IC	Intelligence Community
ICD	Intelligence Community Directive
ICPG	Intelligence Community Policy Guidance
ICS	Intelligence Community Standard
ICTS	Intelligence Community Technical Specification
IC ITE	Intelligence Community Information Technology Enterprise
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ITE	Information Technology Enterprise
LDAP	Lightweight Directory Access Protocol
NATO	North Atlantic Treaty Organization

NPE	Non-Person Entity
NIST	National Institute of Standards and Technology
OCIO	Office of the Intelligence Community Chief Information Officer
PKI	Public Key Infrastructure
RFC	Request For Comments
SAML	Security Assertion Markup Language
SCI	Sensitive Compartment Information
TS	Top Secret
UAAS	Unified Authorization and Attribute Services
US	United States
X.509	X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

Appendix C Bibliography

This appendix lists all the sources referenced in this Technical Specification and lists other sources that may have been used in other Technical Specifications. This appendix is a shared resource across multiple documents so in any given Technical Specification there are likely sources that are not referenced in that particular Technical Specification.

(ICD 500)

Director of National Intelligence Chief Information Officer. Intelligence Community Directive Number 500. 7 August 2008. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_500.pdf.

(ICD 501)

Discovery and Dissemination or Retrieval of Information within the Intelligence Community, Intelligence Community Directive Number 501. 21 January 2009. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_501.pdf

(ICD 503)

Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation, 15 September, 2008. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_503.pdf

(ICPG 500.1)

Digital Identity, Intelligence Community Policy Guidance Number 500.1. 7 May 2010. Office of the Director of National Intelligence. http://www.intelink.ic.gov/sites/ppr/policyHome/ICPG/default.aspx

(ICPG 500.2)

Attribute–Based Authorization and Access Management, Intelligence Community Policy Guidance Number 500.2. 23 November 2010. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICPG_500_2.pdf.

(ICS 500-20)

Intelligence Community Enterprise Standards Compliance. Intelligence Community Standard 500-20. 16 December 2010. Office of the Director of National Intelligence. http://www.intelink.ic.gov/sites/ppr/policyHome/ICS/default.aspx

(ICS 500-21)

Tagging of Intelligence and Intelligence Related Information. Intelligence Community Standard 500-21. 28 January 2011. Office of the Director of National Intelligence. http://www.intelink.ic.gov/sites/ppr/policyHome/ICS/default.aspx

(ICS 500-29)

Intelligence Community Digital Identifier, Intelligence Community Standard 500-29. 12 July 2012. Office of the Director of National Intelligence. http://www.intelink.ic.gov/sites/cps/policystrategy/policy/Pages/default.aspx

(ICS 500-30)
Enterprise Authorization Attributes: Assignment, Authoritative Sources, And Use For Attribute-Based Access Control Of Resources, Intelligence Community Standard 500-30. DRAFT. Office of the Director of National Intelligence.

(EO 12333)
Goals, Direction, Duties, and Responsibilities with Respect to the National Intelligence Effort, Executive Order 12333, The White House.
http://it.ojp.gov/default.aspx?area=privacy&page=1261

(ISO 3166-1)
Codes for the representation of names of countries and their subdivisions – Part 1: Country Codes. International Organization for Standardization.
Alpha-3 character codes are available for purchase at
http://www.iso.org/iso/country_codes/iso_3166_databases.htm

(SCv2)
Scattered Castles Version 2
https://sites.share.ic.gov/sites/ScatteredCastles/default.aspx

(NSA's Master Data Registry)
NSA's Master Data Registry
https://
registries.mws.coi.nsa.ic.gov/rs/registry/ui/ECI_Markings#legal_authority_categories

(IC FSD)
Data Encoding Specification for the IC Full Service Directory Schema, Version 1.0, 14 December 2011. Office of the Director of National Intelligence.

(SAML V2.0)
SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Version 1.0, *[Encrypted Mode]* (27 March 2008)

(RFC 2119)
Key words for use in RFCs to Indicate Requirement Levels
http://www.ietf.org/rfc/rfc2119.txt

(RFC 5280)
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
http://www.ietf.org/rfc/rfc5280.txt

(ITU-T X.509)
X.509: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks
http://www.itu.int/rec/T-REC-X.509/en

(AATT CONOPS)
Department of Defense and Intelligence Community Unified Authorization and Attribute Service, Concept of Operations, December 8, 2008, Version 1.11

Appendix D Points of Contact

The 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 DNI-sponsored web sites. Direct all inquiries about this IC technical specification to the IC CIO Identity and Access Management Program.

Appendix E IC CIO Approval Memo

An Office of the Intelligence Community Chief Information Officer (OCIO) Approval Memo should accompany this enterprise technical data specification bearing the signature of the Intelligence Community Chief Information Officer (IC CIO) or an IC CIO-designated official(s). If an OCIO 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 OCIO staffing and coordination process leading to signature of the OCIO Approval Memo. The signature date of the OCIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the OCIO 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 IC Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.