Intelligence Community Technical Specification

IC Enterprise Authorization Attribute Exchange Between IC Attribute Services

Authorization Attribute Set

Version 1.0

Date of Release: 14 DEC 2011

Table of Contents

List of Tables

Chapter 1 Introduction

1.1 Purpose

This technical specification governs the mandatory minimum set of IC enterprise authorization attributes and associated values that must be supported by an Attribute Service participating in the IC's Unified Authorization and Attribute Service (UAAS) Federation. The specification is the basis for defining and populating the set of attributes and values that comprise a 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*, (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*. Authorization 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 authorization attributes defined at the enterprise level for entities, both person and non-person (e.g., machines, servers, services, processes, applications, etc.) within the IC information domain. UAAS exchange requires using these attributes and values for exchange of persons' attributes, but does not yet require exchanging attributes for non-person entities (NPEs). During FY11 the IC began assessing NPE attribute requirements, the results of which will affect this and related documents over time. Until those requirements are defined, UAAS exchange of NPE attributes is not required but may occur, if it uses the allowed values in this document, and with the knowledge that IC NPE attribute definitions and values are not yet formally established.

In addition to enterprise authorization 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. These additional attributes may become enterprise attributes over time, necessitating updates to this document over time.

IC Enterprise Authorization Attributes are assigned per 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 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 an "interoperable federated architecture." 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 mandatory minimum set of IC enterprise authorization attributes and values for sharing through the IC UAAS federation 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 authorization attribute definitions. This requires the usage of standardized attribute names and values when exchanging SAML protocol messages between systems participating in the IC UAAS federation.

This technical specification aligns with the Attribute Practice Statement (APS) provided by each IC UAAS federation service provider. The APS describes how each service provider populates the IC enterprise authorization attributes provisioned to each user persona or NPE, 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 federation. 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 authorization attributes. This document applies to all IC enterprise authorization attributes exchanged amongst UAAS-compliant Attribute Services 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.
- **Bold** – A variable, element, or attribute name.

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 1. 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 1. Dependencies

Name
Data Encoding Specification for Information Security Marking, Version 7.0, (9 Aug 2011)
Data Encoding Specification for the IC Full Service Directory Schema, Version 1.0 (14 Dec 2011)
SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Version 1.0, (27 March 2008)

Chapter 2 IC Enterprise Authorization Attributes Specification

2.1 IC Enterprise Authorization Attribute Names and Values

The attributes as defined in this specification represent the mandatory set of enterprise authorization attributes about persons and personas that must be exchanged between Attribute Services participating in the IC UAAS federation. UAAS exchange requires using these attributes and values for exchange of persons' attributes, but does not yet require exchanging attributes for non-person entities (NPEs). See Section1.2 for additional information.

All of these attributes must be included within a SAML Response message sent in response to an attribute query originating from another Attribute Service for persons' attributes. In cases where attribute names and values defined below differ in underlying authoritative sources, they must be transformed to match this specification before passing them via UAAS, as in section 2.1.7.

In each of the definitions below, the IC entity is uniquely identified within the IC information domain (as defined in ICPG 500.1) by the Distinguished Name (DN) in its IC PKI issued certificate. "Entity" includes both IC persons and personas, and NPEs such as servers, services, applications, etc. As described in the Intelligence Community Public Key Infrastructure documents, all IC PKI certificates and the DNs contained within them follow the specifications as defined in [ITU-T X.509] and [RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile].

2.1.1 Authorized IC Person (AICP)

Attribute Name	**AICP**
Definition/Purpose	Reflects whether or not the IC Entity is an AICP
Allowed Values	True, False
Single/Multi	Single
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.

Note: Although the current definition of an AICP is specific to persons and personas, it may eventually apply to non-person entities.

2.1.2 Clearance

Attribute Name	**Clearance**
Definition/Purpose	Reflects the clearance level of the IC entity
Allowed Values	Values listed for ClassificationUS in the XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML), Version 7 (9 Aug 2011)
Single/Multi	Single
Example	TS

This attribute specifies the IC entity's highest security clearance level, or in the case of an NPE, the highest security classification of information it can process.

ISM.XML is approved as an IC technical data specification suitable for use by IC elements with electronic information security marking requirements and is deemed technically sound and supportive of IC mission objectives. ISM.XML leverages the CAPCO Register and Implementation Manual as the authoritative sources for controlled values, marking relationships, and presentation formats.

2.1.3 CountryOfCitizenship

Attribute Name	**CountryOfCitizenship**
Definition/Purpose	Reflects the citizenship of the IC entity
Allowed Values	3-letter country code as defined in ISO 3166-1
Single/Multi	Multi
Example	USA

This attribute contains the identifier of the IC entity's country of citizenship.

CountryOfCitizenship is multi valued, since an entity could possibly have multiple citizenships (i.e. "dual citizenship").

In light of the ongoing NPE attribute requirements analysis mentioned above in Scope, this version 1.0 will defer discussing what country of citizenship means for NPEs.

2.1.4 DistinguishedName

Attribute Name	**DistinguishedName**
Definition/Purpose	Reflects the DN from the IC entity's IC PKI certificate
Allowed Values	DN from the entity's IC PKI certificate
Single/Multi	Single
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

A DistinguishedName (DN) is a string representation that uniquely identifies a subject within a Public Key Infrastructure. An IC UAAS-compliant Attribute Service must use the DN from an entity's IC PKI certificate associated with that particular persona as the means for specifying the subject identity in SAML protocol messages being exchanged between partners in the federation. The DN entry is single valued, but an IC entity could possibly have multiple DNs, with a unique persona per DN as defined by IC Standard 500-29, *Intelligence Community Digital Identifier*-DRAFT.

2.1.5 EmployeeType

Attribute Name	**EmployeeType**
Definition/Purpose	Reflects the employment affiliation of the IC entity
Allowed Values	MIL, CTR, or GOV
Single/Multi	Single
Example	GOV

This attribute is used to indicate whether the entity is operating as a military service member, contractor, or U.S. federal government civil employee.

2.1.6 isICMember

Attribute Name	**isICMember**
Definition/Purpose	Reflects whether or not the IC entity is a member of the Intelligence Community
Allowed Values	True, False
Single/Multi	Single
Example	True

The isICMember attribute is a flag that reflects whether the entity is a member of the IC as defined by Executive Order 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.

Note: Although the current definition of isICMember is specific to persons, it may apply to non-person entities.

2.1.7 OrganizationName

Attribute Name	**OrganizationName**
Definition/Purpose	Reflects the assigned organization of the IC 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)
Single/Multi	Single
Example	DNI

The purpose of the OrganizationName attribute is to specify the organizational affiliation with which an entity is associated, since protected resources may be limited to organization unique audiences.

2.1.8 SCI Control Systems and Compartments (SCIcontrols)

Attribute Name	**SCIcontrols**
Definition/Purpose	Reflects the SCI control systems and compartments of the IC entity
Allowed Values	SCIcontrols as described in the latest version of the XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML), Version 7 (9 Aug 2011)
Single/Multi	Multi
Examples	HCS, SI, TK

The SCIcontrols attribute specifies the SCI Control Systems and Compartments for which an entity is authorized to access or process.

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

ISM.XML is approved as an IC technical data specification suitable for use by IC elements with electronic information security marking requirements and is deemed technically sound and supportive of IC mission objectives. It is also important to note that ISM.XML relies on the CAPCO Register and Implementation Manual as the authoritative sources for controlled values, marking relationships, and presentation formats.

While CAPCO oversees hierarchical compartments and subcompartments, SCIcontrols are not hierarchical, either in syntax or semantics. Subcompartments do not confer access to parent compartments nor do compartments confer access to any subcompartments.

Appendix A Change History

Table 2 summarizes the version identifier history for this ICTS.

Table 2. ICTS Version History

Version	Date	Purpose
1.0	14 Dec 2011	Initial Release

Table 3 summarizes the changes made this ICTS from to Version 1.0 to Version X.

Table 3. Change History

Change	Artifacts Changed	Compatibility Notes

Appendix B Acronyms

Table 4 summarizes the acronyms used in this Technical Specification.

Table 4. Acronyms

Name	Description
ABAC	Attribute Based Access Control
AICP	Authorized IC Person
CAPCO	Controlled Access Program and Coordination Office
CIO	Chief Information Officer
DN	Distinguished Name
DNI	Director of National Intelligence
EA	Enterprise Architecture
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
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISM	Information Security Marking
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
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
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

(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. DRAFT. Office of the Director of National Intelligence.

(CAPCO)
CAPCO Authorized Classification and Control Markings Register, Version 4.2, 31 May 2011. Office of the Director of National Intelligence. https://www.intelink.gov/sites/ssc/divisions/capco/default.aspx

(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

(ISM.XML)
Data Encoding Specification for Information Security Marking Metadata, Version 7.0, 9 August 2011. Office of the Director of National Intelligence. *https://www.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/ism/default.aspx*

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

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 Attribute Sharing Profile for X.509 Authentication-Based Systems, Version 1.0, (27 March 2008)

(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

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.