Intelligence Community Technical Specification

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

Version 2016-SEPr2017-JUL

July 21, 2017

Table of Contents

List of Figures

List of Tables

List of Examples

Chapter 1 - Introduction

1.1 - Purpose

This technical specification governs the set of Intelligence Community (IC) enterprise Unified Identity Attribute Set (UIAS) and associated values that must be supported by an Attribute Service (AS) participating in the IC's Unified Authorization 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).[22]

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) 500.2, *Attribute-based Authorization and Access Management.* [12] 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 direct support of IC Standard (ICS) 500-30, *Enterprise Authorization Attributes: Assignment, Authoritative Sources, And Use For Attribute-Based Access Control Of Resources.* [18] 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. This document also lists environmental identity attributes, multiplicity and values defined at the enterprise for entities, that may or may not be part of the UAAS exchange.

This document identifies the operational usage for each of the identity attributes. These include, but are not limited to ingest, discovery, access, and audit.

Table 1 - Operational Usage

Operational Usage	Definition
Ingest	Enables high-quality data to be brought into the processing environment
Discovery	Enables searching and rapid location of useful data
Access	Enables rule-based access decisions based on law, policy, and mission constraints
Audit	Enables understanding and ability to audit person and non-person participation in key events

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. Those extended and local attributes or attribute values MUST NOT conflict with the attributes and values described in 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.* [1] These additional attributes may become enterprise attributes over time, necessitating updates to this document.

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 Intelligence Community 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,* [8] grants the IC CIO the authority and responsibility to:

- Develop an Intelligence Community 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 the IC Unified Authorization Attribute Service (UAAS) supports the opportunity for consistent and assured information sharing across the enterprise. The IC UAAS supports ICS 500-30, *Enterprise Authorization Attributes: Assignment, Authoritative Sources, And Use For Attribute-Based Access Control Of Resources* [18] 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 UIAS-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 the IC UIAS.

This technical specification relates to the Attribute Practice Compliance Statement (APCS) used by all agencies and system owners who write the Attribute Practice Statements (APS) required for each AAS and AS of an IC element and comply with ICS 500-30,[18] as well as operators and resource owners that rely on attributes for authorization decisions. The APCS, published by the IC CIO, contains a compliance statement for each attribute identified in the UIAS.XML[23] technical specification for both PEs and NPEs that are US owned, controlled, and vetted.

Enterprise needs and requirements for this specification can be found in the following Office of the Director of National Intelligence (ODNI) policies and implementation guidance:

- IC Information Technology Enterprise (IC ITE):
  - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan[5]
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer[8]
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[9]
  - Intelligence Community Policy Guidance (ICPG) 500.1, Digital Identity[11]
  - Intelligence Community Policy Guidance (ICPG) 500.2, Attribute-based Authorization and Access Management[12]
  - Intelligence Community Standard (ICS) 500-27, Collection and Sharing of Audit Data[16]
  - Intelligence Community Standard (ICS) 500-29, IC Digital Identifier[17]
  - Intelligence Community Standard (ICS) 500-30, Enterprise Authorization Attributes: Assignment, Authoritative Sources, and Use for Attribute-Based Access Control of Resources[18]
- 700 Series:
  - Intelligence Community Policy Guidance (ICPG) ICPG 704.5, Intelligence Community Security Database Scattered Castles[13]

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 UIAS 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.
- Those responsible for provisioning and maintaining Authoritative Attribute Sources (AAS).

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

The governance of this specification and the data it describes, including any requirement to use this specification or prohibition thereof, is explicitly outside the scope of this specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance,* [15] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element. *Department of Defense Instruction (DODI) 8310.01, Information Technology Standards in the DoD*,[2] requires DoD elements to use the DoD IT Standards Registry (DISR).

Use of this specification must be consistent with applicable Federal statutes, Executive Orders, Presidential Directives, Attorney General approved guidelines, IC Policy, IC element policies, established concepts of operation, agreements, contractual obligations, etc. However, the determination of any such requirements or restrictions is the sole responsibility of each implementing entity. Implementers may wish to consult the Office of General Counsel for their cognizant agency to determine existing requirements and restrictions for the use of this DES and to determine if new agreements or policy changes are required related to the use of this DES.

1.6 - Conventions

Certain technical and presentation conventions were used in the creation of this document to ensure readability and understanding.

1.6.1 - Language

When appearing in all capital letters in this technical specification, the keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in IETF RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels.” [19] When these words appear in regular case, they are meant in their natural-language sense.

1.6.2 - Typography

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

- *Italics* – A title of a referenced work or a specialized or emphasized term
- Underscore – An abstract data element
- **Bold** – An XML element or attribute

1.6.3 - Terminology

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.

1.6.4 - XML Namespaces

Namespaces referenced in this document and the prefixes used to represent them are listed in the following table. The namespace prefix of any XML Qualified Name used in any example in this document should be interpreted using the information below.

Table 2 - XML Namepaces

Prefix	URI
uias	urn:us:gov:ic:uias

1.6.5 - 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 3 - Definitions of Multiplicities

Multiplicity	Description
1	Indicates the attribute is mandatory and must contain 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.
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 - Dependencies

1.7.1 - Types of Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. Dependencies play an important role in functionality or provide informational relationships between the various artifacts. The following terms are defined to help assist with understanding how the various artifacts work together:

Dependency	Directly or transitively influenced by. Examples: 1. A is influenced by B therefore B is a dependency of A. 2. A is influenced by B and B is influenced by C; therefore C is a dependency of A.
Direct Dependency	Explicit influence. Example: A influences B.
Inverse Dependency	Directly or transitively influences. Example: B influences A.

1.7.2 - Specification Dependencies

This technical specification directly depends on the technical specifications, documentation, and implementations listed in Table 4. 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 IC CIO specifications related to this specification. The graphic depicts direct dependencies (see Direct Dependency). 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 specifications listed in Table 4 will be shown in Figure 1; however not all specifications listed in Figure 1 may appear in Table 4. Figure 1 is to aid users in gaining a general understanding of all direct dependencies.

Table 4 - Dependencies

Name	Dependency Description
CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES.V2016-SEP+)[20]	This specification does not depend on a specific version of ISM Country Codes and Tetragraphs (ISMCAT.CES); ISMCAT.CES versions later than version 2016-SEP MAY be used. The minimum version was based on program choice; Community decision to move to version 2016-SEP.
CVE Encoding Specification for Mission Need (MN.CES.V2015-AUG+)[21]	This specification does not depend on a specific version of Mission Need (MN.CES); MN.CES versions later than version 2015-AUG MAY be used. The minimum version was based on the earliest non-retired version; ESB 17-1 was used for determining the version.

Name	Dependency Description
CVE Encoding Specification for US Agency Acronyms (USAgency.CES.V2016-SEP+)[24]	This specification does not depend on a specific version of US Agency (USAgency.CES); USAgency.CES versions later than version 2016-SEP MAY be used. The minimum version was based on a technical dependency; The use of the USAgency AuditRoutingOrg CVE.
XML Data Encoding Specification for Virtual Coverage (VIRT.XML.V1+)[25]	This specification does not depend on a specific version of Virtual Coverage (VIRT.XML); VIRT.XML versions later than version 1 MAY be used. The minimum version was based on the earliest non-retired version; ESB 17-1 was used for determining the version.
Intelligence Community Markings System Register and Manual[6]	Policy and guidance for marking of classified information.
Security Assertion Markup Language (SAML) Version 2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Version 1.0, [Encrypted Mode] (27 March 2008) [22]	Specification for attribute sharing.

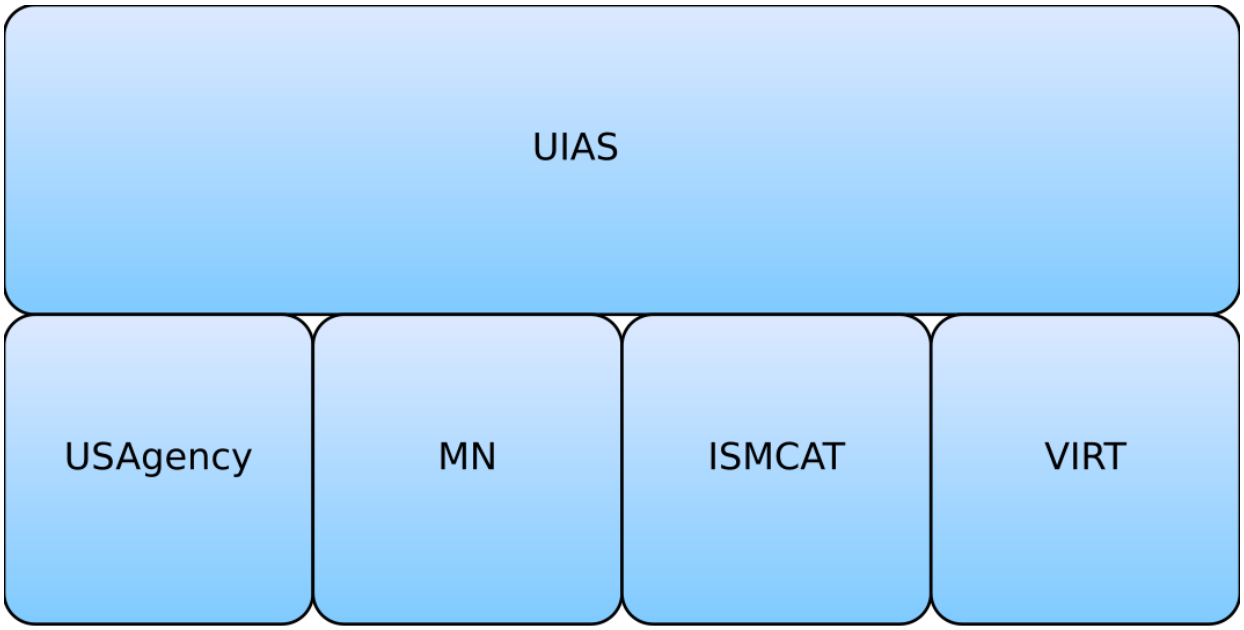

Figure 1 : Related Specifications

1.7.3 - Standalone and Convenience Packages

The standalone package of this specification does not include the specifications that it is dependent on since there may be more recent versions of those specifications available. There is a

convenience package of the specification that includes the most recent versions of all direct dependent (see Direct Dependency) specifications at the time the package is generated. It is anticipated that this convenience package will be updated when any of the dependent specifications change; however, it will not be signed as a formal package. In order to obtain all the necessary standalone packages, this specification's dependencies and their dependencies will have to be traversed and obtained. These packages will have to be downloaded and copied into the appropriate directories for paths to the schema and controlled vocabulary enumerations (CVEs) to validate and operate as intended.

Convenience packages convey all dependencies pre-packaged together and are tested as interoperable. When trying to mix and match versions that have not been pre-packaged together, there may be risk that a particular combination may not be compatible, especially when mixing with versions of specifications that were not available at the time of a specification's release.

1.7.4 - Inverse Dependencies

Generally, it is only necessary to think of the *direct dependencies* (see Direct Dependency) in the dependency tree. However, with the specification versions being decoupled, it is also important to consider the *inverse dependencies* (see Inverse Dependency), 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.

Since this specification is one such specification that is used by other specifications released by the IC CIO, the Figure 2 has been included to assist readers in understanding all of the dependency relationships and how changes in a specification may impact others. This diagram is representative of dependencies at the time of the release of this specification, but are subject to change over time.

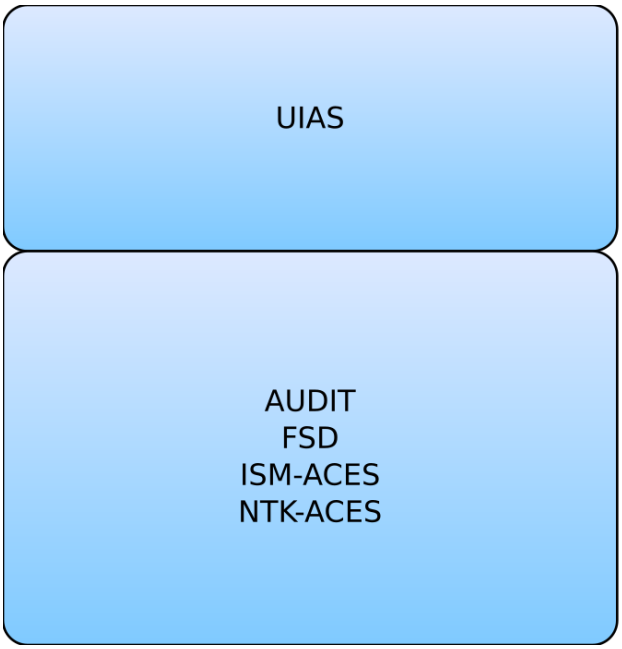

Figure 2 : Inverse Dependency Specifications

1.8 - Conformance

Within this document, attribute names, attribute multiplicity, and allowed values are considered normative, unless explicitly labeled “informative”. All explanatory text associated with each attribute is considered informative, unless explicitly labeled “normative”.

As of v2016-SEP this specification includes an XSD schema and associated Schematron rules.

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.

1.9 - Version Policies

The version numbering for this specification is defined by a year-month structure (e.g., YYYY-MMM) with an optional revision (e.g., rYYYY-MMM). This provides a temporal representation of when the specification was released.

Chapter 2 - Development Guidance

2.1 - Understanding Access Control

Technical specifications or information guidance documents are used to make access control decisions. Control decisions are based upon three components (data attributes, user attributes, and access control policies) and are held together by the context in which the access control decision is made. The context itself includes various elements, such as the environment, temporal state, and method of access, that together provide the Where, When, and How details of the access request. The context, together with the user making the request and the data/repository/ application being requested (the Who and What respectively), make up the framework that supports an access control decision. Access Policy SHOULD be constrained to use data attributes, user attributes, and context information. A Policy Decision Point (PDP) uses this framework to make a grant or deny access decision. An entity MUST meet all criteria in the framework to be granted access. The concept of the access control decision framework is depicted in Figure 3.

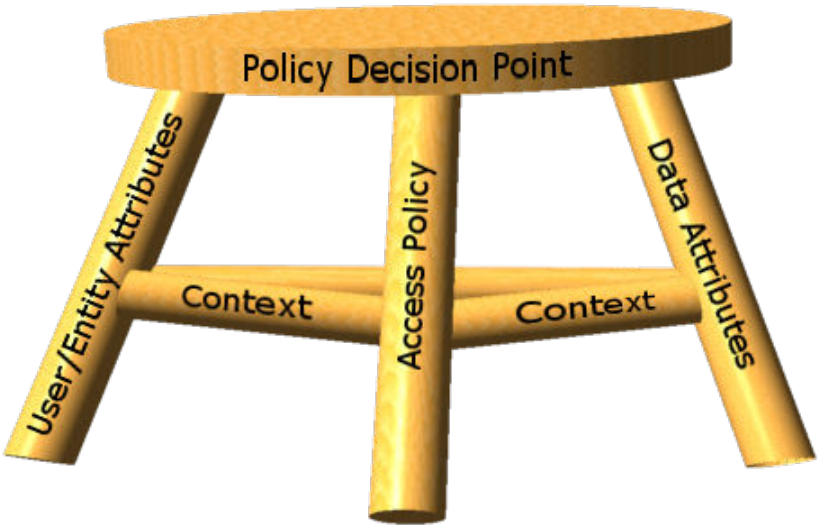

Figure 3 : Three-legged Stool of Access Decisions

All of these parts come together to create a tri-legged stool of access control. When a stool is missing one of the components of its frame, it is unable to function properly. The same is true of access control. Without each component of the framework, access control falls apart. Each component is crucial to make accurate, reliable, and automated access control decisions. Each IC CIO document will address a piece of the framework of access control decisions.

This specification falls into the user attributes leg of the access control framework. User attribute specifications include:

- Full Service Directory (FSD)[4]
- Unified Identity Attribute Set (UIAS.XML)[23]

2.2 - IC UAAS Federation

The IC Unified Authorization and Attribute Service (UAAS) is a federation of agency-based attribute service providers that exchange attributes in order to support systems employing an attribute-based access control (ABAC) model. The UAAS federation contains seven providers, i.e. Central Intelligence Agency (CEAC), Defense Intelligence Agency (DIAS), National Reconnaissance Office (IAMS), National Geospatial-Intelligence Agency (GEOAxIS), National Security Agency (CASPORT), Identity, Authentication and Authorization Service Provider (IAA Service Provider AccessIT!), and National Security Agency Intelligence Community Service Operations Group (ICSOG) (Common Services). DIAS supports all military IC elements, e.g., Army, whereas ICSOG (Common Services) support all other IC elements, e.g., Treasury Department. Lastly, IAA AccessIT! supports ABAC for cloud-based (IC ITE) systems.

The UAAS provides an attribute service and most systems employing ABAC leverage the UAAS federation for UIAS attribute retrieval. The UAAS in turn obtains these UIAS attributes from Authoritative Attribute Sources (AASs), such as the providers' agency-based Security and HR based systems, or shared repositories of common concern, for example the IC Full Service Directory (FSD) for HR-related attributes and Scattered Castles (as defined by [13], *Intelligence Community Security Database Scattered Castles*) for security-related attributes. The UAAS service provider nodes may also provide an authorization service, i.e. a full range of access control rule sets and policy decision points for any system that is configured to offload (outsource) this function. There is a great variety of configurations for systems across the IC that leverage the UAAS for attributes.

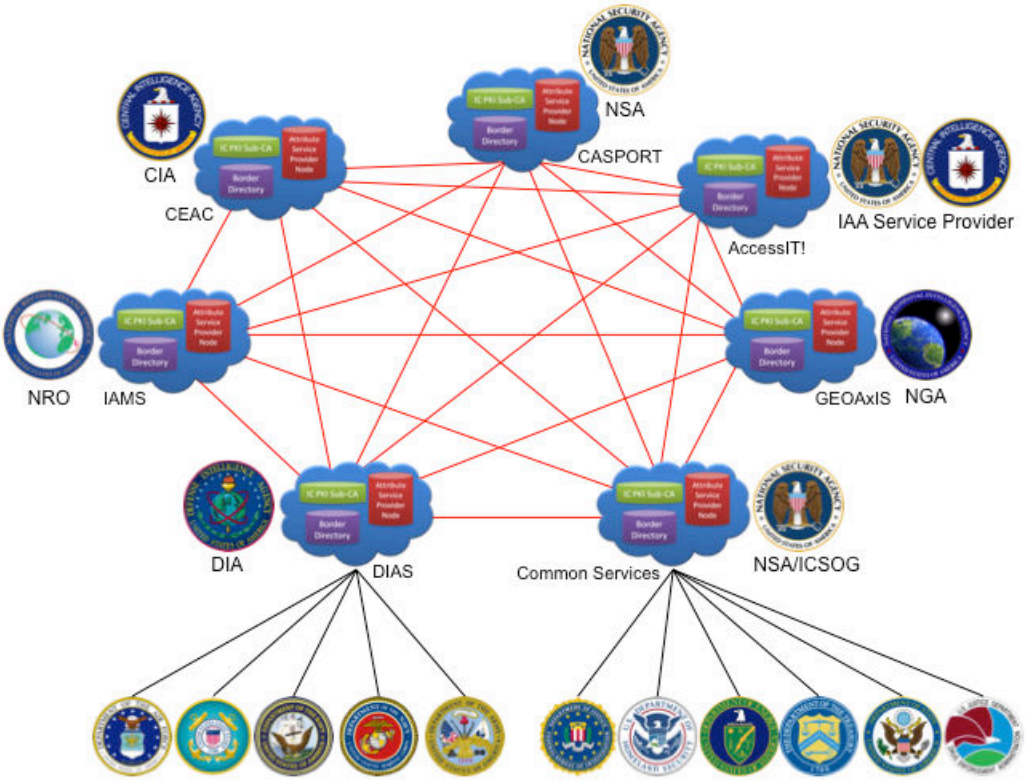

Figure 4 : UAAS Federation

2.3 - 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 the 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)[11] by the Distinguished Name (DN) in the Public Key Infrastructure (PKI) issued certificate. Persons or non-person entities (e.g., servers, services, applications, etc.) may have one or more persona.

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 vocabulary enumerations (CVEs) for the value set.

2.3.1 - Admin Organization

Table 5 - Admin Organization

Attribute Name	adminOrganization
Definition/Purpose	Reflects the home organization of the entity
Allowed Values	Summation of two sets: • Values listed in *XML CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*[24] • Values listed in table Table 6
Multiplicity	[1]
Example	DIA
Operational Usage	Access
Attribute Identifier	urn:us:gov:ic:uias:adminOrganization

This attribute specifies the home or administrative organization affiliation with which the entity (person or non-person) is associated. For persons, the administrative organization is the one that maintains their personnel records. For non-person entities, the administrative organization is the one that controls the administration of the NPE when in use.

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

Authoritative sources can apply specific internal policies for use of this attribute.

In support of Second Party Integrees (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 6 - 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 follows 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.

2.3.2 - Audit Routing Organization

Table 7 - AuditRoutingOrganization

Attribute Name	auditRoutingOrganization
Definition/Purpose	This attribute specifies the organization(s) to which Audit Records should be forwarded.
Allowed Values	Values found in XML CVE for Audit Routing Organization, CVEnumAuditRoutingOrg.xml.
Multiplicity	[1:2]
Examples	CIA, USPACOM, EOP
Operational Usage	Audit
Attribute Identifier	urn:us:gov:ic:uias:auditRoutingOrganization

This attribute specifies the organization(s) to which Audit records will be routed.

2.3.3 - Authority Category

Table 8 - AuthorityCategory

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	Includes values listed in XML CVE for Authority Category CVEnumUIASAuthorityCategory.xml
Multiplicity	[0:*]
Examples	ICD503, FISA_B, EO12333_IA, DODD8530_USA
Operational Usage	Access, Discovery

Attribute Name	authorityCategory
Attribute Identifier	urn:us:gov:ic:uias:authorityCategory

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.

It is the responsibility of the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed values to the enterprise.

2.3.4 - Authority to Operate Status

Table 9 - 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
Operational Usage	Access, Discovery, Ingest
Attribute Identifier	urn:us:gov:ic:uias:ATOStatus

This attribute indicates the ATO status for the non-person entity. As defined by ICD 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation,* [10] 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 (e.g., if an Interim Authority to Test has been granted). A value of “True” indicates that an ATO has been granted. A value of “False” indicates an ATO has not been granted.

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

The **ATOStatus** attribute should be used in conjunction with the **lifeCycleStatus** attribute to determine the actual status of the NPE.

2.3.5 - Authorized IC Person

Table 10 - 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
Operational Usage	Access, Discovery
Attribute Identifier	urn:us:gov:ic:uias:aICP

Authorized IC Person (AICP) is defined by ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community* [9] 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[9], 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 by the receiving system. **aICP** will only be set to True if the **isICMember** attribute is also set to True.

The **aICP** attribute is specific to only U.S. persons and associated personas, and is not applicable to non-person entities, and is used for access control decisions to protected resources. The **aICP** attribute is not applicable to Second Party Integrees.

If the UIAS is for a non-person entity, then the **aICP** attribute is not exchanged as part of the attribute assertion.

2.3.6 - Clearance

Table 11 - Clearance

Attribute Name	clearance
Definition/Purpose	Reflects the clearance or classification level of the entity

Attribute Name	clearance
Allowed Values	Values found in XML CVE for Clearance, CVEnumUIASClearance.xml.
Multiplicity	[1:*]
Examples	TS, Q
Operational Usage	Access, Ingest
Attribute Identifier	urn:us:gov:ic:uias:clearance

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

It contains values from US National Security Information and the Department of Energy. If an entity has a clearance in more than one of these classification or protection marking systems, the highest security clearance/authorization from each must be listed.

Note: The schema does NOT indicate that an entity holds an "interim" clearance.

The **clearance** attribute is used for access control decisions to protected resources.

2.3.7 - Country of Affiliation

Table 12 - Country of Affiliation

Attribute Name	countryOfAffiliation
Definition/Purpose	Reflects the citizenship(s) or affiliation(s) of the entity
Allowed Values	Values listed in *XML CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES)*[20] from the CVE CVEnumISMCATResponsibleEntity.xml excluding "NATO"
Multiplicity	[1:*]
Examples	GBR, USA
Operational Usage	Access, Audit
Attribute Identifier	urn:us:gov:ic:uias:countryOfAffiliation

In the case of person entities, this is the identifier of the person 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.

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

2.3.8 - Digital Identifier

Table 13 - 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
Operational Usage	Access, Audit
Attribute Identifier	urn:us:gov:ic:uias:digitalIdentifier

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,* [17] specifies that the IC Digital Identifier (IC DI) is the Distinguished Name (DN) from the PKI Certificate, and is unique to the persona associated with that certificate.

A *DN* is a string representation that uniquely identifies a subject within a PKI. An UIAS-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 PKI Certificate is not the authoritative source for attributes and parsing the certificate should not be used for granting access. 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.* [17]

2.3.9 - Duty Organization

Table 14 - Duty Organization

Attribute Name	dutyOrganization
Definition/Purpose	Reflects the assigned organization of the entity
Allowed Values	Values listed in *XML CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*[24] from the CVE CVEnum-USAgency.xml
Multiplicity	[1]
Example	DNI
Operational Usage	Access
Attribute Identifier	urn:us:gov:ic:uias:dutyOrganization

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

The **dutyOrganization** attribute may differ from **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.

In support of Second Party Integrees, the **dutyOrganization** should represent the US government sponsoring agency.

2.3.10 - Duty Organization Unit

Table 15 - Duty Organization Unit

Attribute Name	dutyOrganizationUnit
Definition/Purpose	Reflects the assigned organization unit structure of the entity
Allowed Values	Agency defined authoritative organization unit structure of the entity's duty organization separated by colons
Multiplicity	[0:1]
Example	CIA:CIO:APPS:EASPO
Operational Usage	Access
Attribute Identifier	urn:us:gov:ic:uias:dutyOrganizationUnit

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

2.3.11 - Entity Security Mark

Table 16 - Entity Security Mark

Attribute Name	entitySecurityMark
Definition/Purpose	Classification and handling of the entity's digital identifier
Allowed Values	Classification banner as defined by the IC Markings System Register and Manual[6]
Multiplicity	[0:1]
Example	SECRET//REL TO USA, AUS, CAN, GBR, NZL
Operational Usage	Access, Audit
Attribute Identifier	urn:us:gov:ic:uias:entitySecurityMark

This attribute specifies the classification and handling for the entity's (person or non-person) digital identity, and is used for determining if the entity's digital identity can be transmitted to another network or domain. An **entitySecurityMark** does not specify the classification and handling of the

entity's assertion as a whole, and does not presuppose which UIAS attribute values may be transmitted to other networks or domains without additional filtering.

If there is a value in **entitySecurityMark**, the **entitySecurityMark** attribute should be used in conjunction with **icNetworks** attribute to determine if an entity's digital identity and approved subset of attributes should be transmitted to another network or domain.

If no value for **entitySecurityMark** is present, the attribute is not exchanged as part of the attribute assertion, and the entity's digital identity and approved subset of attributes will not be transmitted to another network or domain.

2.3.12 - Entity Type

Table 17 - Entity Type

Attribute Name	entityType
Definition/Purpose	Reflects the type of the entity
Allowed Values	Values found in XML CVE for Entity Type, CVEnumUIASEntityType.xml.
Multiplicity	[1]
Example	GOV
Operational Usage	Access
Attribute Identifier	urn:us:gov:ic:uias:entityType

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 entity is a person or non-person.

Further clarification of attribute values and their definitions can be found in the CVE.

2.3.13 - Fine Access Controls

Table 18 - Fine Access Controls

Attribute Name	fineAccessControls
Definition/Purpose	Reflects the fine grain access aspects of control systems
Allowed Values	Includes values listed in XML CVE for Fine Access Control, CVEnum-UIASFineAccessControl.xml Developers of systems processing SCI or SAP from the unpublished register will need to contact the POC listed in Appendix E - Points of Contact for guidance as those values may have been omitted from the CVE.

Attribute Name	fineAccessControls
Multiplicity	[1:*]
Examples	HCS, SI, TK
Operational Usage	Access, Discovery, Ingest
Attribute Identifier	urn:us:gov:ic:uias:fineAccessControl

This attribute includes but is not limited to the values listed under SCI Control Systems and Compartments, Special Access Programs/Special Access Restrictions, Atomic Energy Act, DoD Critical Nuclear Weapons Design Information (CNWDI), North Atlantic Treaty Organization (NATO) read-ons, and Department of Energy compartments which an entity (person or non-person) is authorized to access or process. It also includes the caveats [1] associated with the clearances, where appropriate. The values in CVEnumUIASFineAccessControl.xml do not represent all allowed values. For example, there are some allowed Unpublished SCI compartments and sub-compartments not included in these resources. Use of these special values requires coordination outside of the UIAS specification.

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

It is the responsibility of the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed values to the enterprise.

2.3.14 - Group

Table 19 - Group

Attribute Name	group
Definition/Purpose	Indicates the group memberships associated with the entity.
Allowed Values	Values governed by the Identity, Authentication and Authorization (IAA) Service Provider Entitlement Management Service
Multiplicity	[0:*]
Examples	TBD
Operational Usage	Access, Discovery, Ingest, Audit
Attribute Identifier	urn:us:gov:ic:uias:group

This attribute characterizes the entity’s (person or non-person) authorized group membership that the entity needs to perform an expected task.

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

[1] See IC Markings System Register and Manual[6] for more information.

It is the responsibility of the Identity, Authentication and Authorization (IAA) Service Provider to govern allowed values and the IAA Service Provider Entitlement Management Service to manage and expose the values to the enterprise.

2.3.15 - Handling Controls

Table 20 - Handling Controls

Attribute Name	handlingControls
Definition/Purpose	Indicates the set of handling controls that an NPE is authorized to have.
Allowed Values	Values found in XML CVE for Handling Controls, CVEnumUIASHandlingControls.xml.
Multiplicity	Conditional: P = [0] NPE = [0:*]
Examples	OC, NF
Operational Usage	Ingest, Audit
Attribute Identifier	urn:us:gov:ic:uias:handlingControls

This attribute characterizes the set of handling controls that an NPE is authorized to have.

If the UIAS assertion is for a person entity, then the **handlingControls** attribute is not exchanged as part of the attribute assertion.

2.3.16 - IC Networks

Table 21 - IC Networks

Attribute Name	icNetworks
Definition/Purpose	List of other IC networks or domains to which an entity's digital identifier may be transmitted
Allowed Values	Includes values listed in XML *Data Encoding Specification for Virtual Coverage*[25] *(VIRT.XML)* from the CVE CVEnum-VIRTNetworkName.xml
Multiplicity	[0:*]
Example	ACSS
Operational Usage	Access, Audit
Attribute Identifier	urn:us:gov:ic:uias:icNetworks

This attribute specifies the list of available networks or domains that an entity's (person or non-person) digital identity may be transmitted to. An **icNetwork** value does not presuppose which UIAS attribute values may be transmitted to other networks or domains without additional filtering.

The **icNetworks** should be used in conjunction with the **entitySecurityMark** attribute to determine if an entity's digital identity and approved subset of attributes should be transmitted to another network or domain.

If no values for **icNetworks** are present, the attribute is not exchanged as part of the attribute assertion, and the entity's digital identity and approved subset of attributes will not be transmitted to another network or domain.

2.3.17 - Is IC Member

Table 22 - 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
Operational Usage	Access
Attribute Identifier	urn:us:gov:ic:uias:isICMember

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 (E.O.) 12333.[3]

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,[3] where an IC member is "a person employed by, assigned or detailed to, or acting for an element within the IC." This includes non-person entities owned 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.

2.3.18 - Life Cycle Status

Table 23 - Life Cycle Status

Attribute Name	lifeCycleStatus
Definition/Purpose	Indicates the life cycle phase in which the entity is operating
Allowed Values	Values found in XML CVE for Life Cycle Status CVEnumUIASLifeCycleStatus.xml.
Multiplicity	Conditional: P = [0] NPE = [1]
Example	DEV
Operational Usage	Access, Audit, Ingest
Attribute Identifier	urn:us:gov:ic:uias: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.

The **lifeCycleStatus** attribute should be used in conjunction with the **ATOStatus** attribute to determine the actual status of the NPE.

If the UIAS assertion is for a person entity, then the **lifeCycleStatus** attribute is not exchanged as part of the attribute assertion.

2.3.19 - Region

Table 24 - 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	Includes values listed in *XML CVE Encoding Specification for Mission Need (MN.CES)*[21] from the CVE CVEnumMNRegion.xml
Multiplicity	[0:*]
Examples	AFce, AFea, ASea, EUce
Operational Usage	Access, Discovery, Ingest
Attribute Identifier	urn:us:gov:ic:uias:region

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).

The **region** attribute 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.

It is the responsibility of the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed values to the enterprise.

2.3.20 - Role

Table 25 - Role

Attribute Name	role
Definition/Purpose	Indicates the position, job or area of responsibility associated with the entity
Allowed Values	The allowed values follow the Namespace Taxonomies listed below.
Multiplicity	[0:*]
Examples	C2S-CIA-Ent-CIO-NETADMIN, C2S-NSA-Msn-MissionA-READONLY, Nebula-CIA-Proxy
Operational Usage	Access, Discovery, Ingest
Attribute Identifier	urn:us:gov:ic:uias:role

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.

The **role** attribute 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.

It is the responsibility of the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed values to the enterprise.

The following Role Taxonomy describes the generic format and lexicon for the **role** attribute. This format and lexicon is used to create specific taxonomies for a given namespace and are included in ensuing subsections. While this specification is useful in and of itself, the intended use is to be incorporated into other specifications, in particular, UIAS.XML[23]. For this purpose, **role** is defined by the use of ABNF. The following ABNF rules explicitly define the content of ABNF and are used to provide a formal description independent of any particular technology.

It is important to note that ABNF strings are case-insensitive, therefore all components of the **role** attribute are case-insensitive. ALPHA is defined to be A-Z / a-z.

Role-Template Format

```
[1]  Role-Template  ::= Namespace 1*10 Concept-Template
[2]  Namespace      ::= 1*255(ALPHA / DIGIT / "_" )
[3]  Concept-Template ::= "-" 1*255(ALPHA / DIGIT / "_" )
```

Role Lexicon

The following vocabulary helps explain the meaning of terms used in Role-Template documentation.

A new namespace has to define all of the following terms:

Role-Template (Canonical Role)	A globally unique attribute used to define an entity's allowed actions in an IC system. The **role** attribute is composed of a namespace and one or more concepts. There is no theoretical size limit (length) of the value for a **role,** but maximum lengths have been established for each component of the CVE to avoid practical issues with software implementation and to support interoperability needs.
Namespace	Namespace is the highest level of the taxonomy and identifies the environment for which the **role** attribute value set is created. Valid values for namespace can be found in the CVE, CVEnumUIASRoleNamespace.xml, included in this specification package. All **role** values SHOULD be UNCLASSIFIED. Each namespace will have an ABNF for the particular pattern that is appropriate for that namespace.
Concept-Template	Concept-Template is a template for the concepts of **role** within a namespace. Each concept MAY have a CVE associated with it. The namespace owner MAY create a taxonomy consisting of up to 10 concepts.

2.3.20.1 - C2S Namespace Taxonomy

This section describes the format and lexicon for the **roles** of the Commercial Cloud Services (C2S) namespace.

C2S Format

```
[4]  C2S          ::= "C2S" "-" RoleOrg "-" RoleScope "-" RoleName "-"
                      RoleFunction
[5]  RoleOrg      ::= 1*255(ALPHA / DIGIT / "_" )
[6]  RoleScope    ::= 1*255(ALPHA / DIGIT / "_" )
[7]  RoleName     ::= 1*255(ALPHA / DIGIT / "_" )
[8]  RoleFunction ::= 1*64(UPALPHA / DIGIT / "_" )
[9]  UPALPHA      ::= %x41-5A ; any US-ASCII uppercase letter "A".."Z"
```

Role Lexicon

The following vocabulary helps explain the meaning of terms used in the C2S **role** value documentation, and it may further constrain the set of allowable values:

C2S (Canonical C2S Role)	The C2S Role is a globally unique attribute used to define an entity's allowed actions in the C2S system. The value string is composed of the namespace C2S and four concepts: a RoleOrg, a RoleScope, a RoleName and a RoleFunction. Each of these concepts of the taxonomy are separated by a dash (“-”) character.
RoleOrg	The RoleOrg concept of the C2S **role** taxonomy represents the organization or agency for which the **role** is valid. The RoleOrg concept of the C2S **role** taxonomy MUST contain one of the valid values found in the CVE, CVEnumUSAgencyAcronym.xml[24].
RoleScope	The RoleScope concept of the C2S **role** taxonomy defines the context for which the given **role** is valid. The RoleScope could be global or limited to a sub-portion of the IC IT infrastructure. The RoleScope concept of the C2S **role** taxonomy MUST contain one of the valid values found in the CVE, CVEnumUIASC2SScope.xml, included in this specification package.
RoleName	The RoleName concept of the C2S **role** taxonomy contains the context for the **role** attribute. Some possible contexts include a mission name, project name, group name, etc. While there are no controlled values for RoleName, the name MUST NOT contain the dash (“-”) character and MUST conform to the ABNF above.
RoleFunction	The RoleFunction concept of the C2S **role** taxonomy indicates the specific function. It is important to note that the C2S RoleFunction concept can contain values described by a regular expression as show in the C2SFormat table above, including the constraint that all alphabetic characters must be upper case. The RoleFunction concept of the C2S **role** taxonomy MUST contain one of the valid values found in the CVE, CVEnumUIASC2SFunction.xml, however, service providers can create custom role functions and begin using them immediately.

Example 2.1. Examples of Role for C2S Namespace

- C2S-CIA-Ent-CLZ-S3ONLY
- C2S-CIA-Ent-CIO-NETADMIN

- C2S-NSA-Msn-MissionA-READONLY

2.3.20.2 - Nebula Namespace Taxonomy

This section describes the format and lexicon for the **roles** of Nebula namespace.

Nebula Format

```
[10] Nebula ::= "Nebula-CIA-" NamedRole
[11] NamedRole ::= 1*255(ALPHA / DIGIT / "_" )
```

Role Lexicon

The following vocabulary helps explain the meaning of terms used in Nebula **role** value documentation, and it may further constrain the set of allowable values:

Nebula (Canonical Nebula Role)	The Nebula Role is a globally unique attribute used to define an Non-Person Entity's allowed actions in the Nebula system. The value string is composed of the namespace Nebula and 1 concept: a NamedRole. Each element in the Nebula namespace is separated by a dash ("-") character.
NamedRole	The NamedRole concept of the Nebula **role** taxonomy MUST contain one of the valid values found in the CVE, CVEnumUIASNebulaNamedRole.xml, included in this specification package.

Example 2.2. Examples of Role for Nebula Namespace

- Nebula-CIA-Proxy
- Nebula-CIA-Bulk

2.3.20.3 - PAAS Namespace Taxonomy

This section describes the format and lexicon for the **roles** of the Platform as a Service (PAAS) namespace.

PAAS Format

```
[12] PAAS ::= "PAAS" "-" RoleOrg "-" RoleScope "-" RoleName "-"
                RoleFunction
[13] RoleOrg ::= 1*255(ALPHA / DIGIT / "_" )
[14] RoleScope ::= 1*255(ALPHA / DIGIT / "_" )
```

```
[15]  RoleName : := 1*255(ALPHA / DIGIT / "_" )
[16]  RoleFunction : := 1*64(UPALPHA / DIGIT / "_" )
[17]  UPALPHA : := %x41-5A ; any US-ASCII uppercase letter "A".."Z"
```

Role Lexicon

The following vocabulary helps explain the meaning of terms used in the PAAS **role** value documentation, and it may further constrain the set of allowable values:

PAAS (Canonical PAAS Role)	The PAAS Role is a globally unique attribute used to define an entity's allowed actions in the PAAS system. The value string is composed of the namespace PAAS and four concepts: a RoleOrg, a RoleScope, a RoleName and a RoleFunction. Each of these concepts of the taxonomy are separated by a dash (“-”) character.
RoleOrg	The RoleOrg concept of the PAAS **role** taxonomy represents the organization or agency for which the **role** is valid. The RoleOrg concept of the PAAS **role** taxonomy MUST contain one of the valid values found in the CVE, CVEnumUSAgencyAcronym.xml[24].
RoleScope	The RoleScope concept of the PAAS **role** taxonomy defines the context for which the given **role** is valid. The RoleScope could be global or limited to a sub-portion of the IC IT infrastructure. The RoleScope concept of the PAAS **role** taxonomy MUST contain one of the valid values found in the CVE, CVEnumUIASPAASScope.xml, included in this specification package.
RoleName	The RoleName concept of the PAAS **role** taxonomy contains the context for the **role** attribute. Some possible contexts include a mission name, project name, group name, etc. While there are no controlled values for RoleName, the name MUST NOT contain the dash (“-”) character and MUST conform to the ABNF above.
RoleFunction	The RoleFunction concept of the PAAS **role** taxonomy indicates the specific function. It is important to note that the PAAS RoleFunction concept can contain values described by a regular expression as show in the PAASFormat table above, including the constraint that all alphabetic characters must be upper case. The RoleFunction concept of the PAAS **role** taxonomy MUST contain one of the valid values found in the CVE, CVEnumUIASPAASFunction.xml, however, service providers can create custom role functions and begin using them immediately.

Example 2.3. Examples of Role for PAAS Namespace

- PAAS-CIA-Ent-CLZ-S3ONLY
- PAAS-CIA-Ent-CIO-NETADMIN
- PAAS-NSA-Msn-MissionA-READONLY

2.3.21 - Topic

Table 26 - Topic

Attribute Name	topic
Definition/Purpose	Indicates the particular intelligence subject area
Allowed Values	Values listed in *XML CVE Encoding Specification for Mission Need (MN.CES).* [21] from the CVE CVEnumMNIssue.xml
Multiplicity	[0:*]
Examples	HREL, HLTH, CN, DI, IC
Operational Usage	Access, Discovery, Ingest
Attribute Identifier	urn:us:gov:ic:uias:topic

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

The **topic** attribute 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.

It is the responsibility of the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed values to the enterprise.

2.4 - IC Enterprise Environment Attribute Names and Values

The attributes, as defined in this section, represent the set of IC enterprise environment attributes and associated values that may or may not be supported by an AS participating in the IC's UAAS capability. These attributes may be derived at runtime, and not stored by an AS.

2.4.1 - Certificate Authority

Table 27 - Certificate Authority

Attribute Name	certificateAuthority
Definition/Purpose	Reflects the issuing PKI certificate authority for the entity

Attribute Name	certificateAuthority
Allowed Values	ICPKI, CADPKI, ACSSPKI These values are also listed in the XML CVE for Certificate Authority CVEnum-UIASCertificateAuthority.xml
Multiplicity	[0:1]
Example	ICPKI, CADPKI
Operational Usage	Access, Audit
Attribute Identifier	urn:us:gov:ic:uias:certificateAuthority

This provides broader and more explicit support for entities (persons and non-persons) of different CAs including the support of policies requiring discrimination of 2PI (or US operating under 2PI constraints) and US users. By allowing Allied Collaborative Shared Services (ACSS) and Cryptologic Agencies Domain (CAD) PKI entities (persons and non-persons) access to IC ITE resources on JWICS, information resources need to recognize this certificate authority distinctly to enforce the appropriate access controls. This will become more important as the use of trust chains broadens to give more system components support beyond IC PKI.

2.4.2 - Originating Network

Table 28 - Originating Network

Attribute Name	originatingNetwork
Definition/Purpose	Reflects the network or domain that the entity's identity originates from
Allowed Values	Includes values listed in XML *Data Encoding Specification for Virtual Coverage* [25] from the CVE CVEnumVIRTNetworkName.xml
Multiplicity	[0:1]
Examples	NSANET
Operational Usage	Access, Audit, Discovery
Attribute Identifier	urn:us:gov:ic:uias:originatingNetwork

This attribute indicates which network an entity (person and non-person) originates from. Security protections and accreditations vary across environments, especially with regard to foreign nationals and 2PIs sitting within those environments. By allowing 2PIs to access resources on JWICS information resources need to recognize the originating network to enforce the appropriate access controls.

Appendix A Feature Summary

The following table shows the version dependencies for UIAS on other specifications. Direct dependencies are marked with an asterisk.

Table 29 - UIAS Dependency over Time

Dependent Specification	V2016-SEP	V2016-SEPr2017-JUL
ARH	V3+	V3+
NTK	V10+	V10+
USAgency*	V2016-SEP+	V2016-SEP+
ISMCAT*	V2016-SEP+	V2016-SEP+
MN*	V2015-AUG+	V2015-AUG+
LIC	V2015-AUG+	V2015-AUG+
VIRT*	V1+	V1+
ISM	V2016-SEP+	V2016-SEP+

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

Table 30 - 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. UIAS Feature Comparison

Table 31 - UIAS Feature Comparison

UIAS Feature Comparison										
Required date	Feature	V1	V2	V2.1	V3	V3.1	V2014-DEC	V2015-AUG	V2016-SEP	V2016-SEPr2017-JUL
	Non-Person Entities	N	F	F	F	F	F	F	F	F
	IAA	N	N	F	F	F	F	F	F	F
Dec 2013	5EE Safeguarding Initiatives	N	N	N	F	F	F	F	F	F

UIAS Feature Comparison										
Required date	**Feature**	**V1**	**V2**	**V2.1**	**V3**	**V3.1**	**V2014-DEC**	**V2015-AUG**	**V2016-SEP**	**V2016-SEPr2017-JUL**
	Reference **authorityCategory** and **fineAccessControl**	N	N	N	N	F	F	F	F	F
	Reference **role**	N	N	N	N	N	F	F	F	F
	Second-party Integree	N	N	N	N	N	F	F	F	F
	Clarified definition of GOV in support of SLT	N	N	N	N	N	F	F	F	F
	Environment Attributes	N	N	N	N	N	F	F	F	F
	Support for **Group**	N	N	N	N	N	N	F	F	F
	Support for Attribute IDs (URN)	N	N	N	N	N	N	F	F	F
	Updated allowed value reference for **region**	N	N	N	N	N	N	F	F	F
	Updated allowed value reference for **topic**	N	N	N	N	N	N	F	F	F
	originatingNetwork uses **VIRT**	N	N	N	N	N	N	F	F	F
	icNetworks uses **VIRT**	N	N	N	N	N	N	F	F	F
	countryOfAffiliation uses **ISMCAT.CES**	N	N	N	N	N	N	N	F	F
	Support for **dutyOrganizationUnit**	N	N	N	N	N	N	N	F	F
	Support for **handlingControls**	N	N	N	N	N	N	N	F	F
	Schematron Rules	N	N	N	N	N	N	N	F	F
	XSD Schema	N	N	N	N	N	N	N	F	F
	Support for **auditRoutingOrganization**	N	N	N	N	N	N	N	F	F
	Use ISMCAT for country codes and tetragraphs	N	N	N	N	N	N	N	F	F
Dec 2017	Align with 2016-DEC IC Marking System Register and Manual.	N	N	N	N	N	N	N	N	F

UIAS Feature Comparison										
Required date	**Feature**	**V1**	**V2**	**V2.1**	**V3**	**V3.1**	**V2014-DEC**	**V2015-AUG**	**V2016-SEP**	**V2016-SEPr2017-JUL**
	CSV and JSON CVE formats	N	N	N	N	N	N	N	N	F

Appendix B Change History

Table 32 summarizes the version identifier history for this technical specification.

Table 32 - Identifier History

Version	Date	Purpose
1	14 Dec 2011	Initial Release
2	17 Jul 2012	Updated to incorporate required attributes for Non-Person Entities and IC Smart Data in support of the IC IT Enterprise (IC ITE)
2.1	16 August 2013	Updated controlled vocabularies and definitions in support of the IC ITE Identity, Authentication and Authorization (IAA) Service Provider
3	3 September 2013	Updated to include **entitySecurityMark** and **icNetworks** in support of 5EE Safeguarding Initiatives
3.1	14 March 2014	Updated controlled vocabulary pointers for **authorityCategory** and **fineAccessControl**; clarified operational usage
2014-DEC	22 December 2014	Updated controlled vocabulary pointers for **role**; reassigned NATO from **clearance** to **fineAccessControl**; Support 2PI; Remove 'US federal' from GOV definition in **entityType**; added two new attributes: **certificateAuthority**, **originatingNetwork**
2015-AUG	13 August 2015	Routine revision to technical specification. For details of changes, see Section B.3 - V2015-AUG Change Summary
2016-SEP	9 September 2016	Routine revision to technical specification. For details of changes, see Section B.2 - V2016-SEP Change Summary
2016-SEPr2017-JUL	21 July 2017	Routine revision to technical specification. For details of changes, see Section B.1 - V2016-SEPr2017-JUL Change Summary

B.1 - V2016-SEPr2017-JUL Change Summary

Significant drivers for Version 2016-SEPr2017-JUL include:

- Community Change Requests
- Alignment with December 2016 IC Marking System Register and Manual[7]

Table 33 summarizes the changes made to this technical specification from Version 2016-SEP to Version 2016-SEPr2017-JUL.

Table 33 - V2016-SEPr2017-JUL Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Moving ECRU and NONBOOK as sub-compartments under SI and handling the removal of ENDSEAL (CR-2015-097)	CVEs CVEUIASFineAccessControl.xml modified CVEnum-sUIASFineAccessControl.xml modified	Data generation and ingestion systems need to be updated to accommodate the changes to SCI controls.
2	Added inverse dependency section and definitions for Dependencies and Inverse Dependencies. (CR-2017-125)	Documentation	No impact to systems.
3	Create JSON version of CVEs in ISM (CR-2017-068)	CVEs	No impact to systems.
4	Create CSV version of CVEs in ISM (CR-2017-046)	CVEs	No impact to systems.
5	Added @id and @role to all sch:rule elements, in support of commercial tools warnings and errors and to support open source unit testing frameworks. (CR-2017-216)	All non-abstract Schematron rules modified	No impact to existing systems. Additional capabilities.
6	Update the version numbering prose to reflect the existence of Revisions. (CR-2017-237)	Documentation	No impact to systems.
7	Remove UIAS orphan abstract rule file, TypeConstraintPatterns.sch, since it is not referenced by any rules. (CR-2017-261)	Schematron TypeConstraintPatterns removed.	No impact to systems.
8	Modified cardinality rendering. (CR-2016-078)	CVEs	No impact to existing systems, documentation rendering change only.

B.2 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Community Change Requests

Table 34 summarizes the changes made to this technical specification from Version 2015-AUG to Version 2016-SEP.

Table 34 - V2016-SEP Change History

Change	Artifacts Changed	Compatibility Notes
Updated **countryOfAffiliation** (CR-2015-102)	DES Schema Schematron UIAS-ID-00065 added.	CVE updated to reference ISMCAT[20] *CVEnum-ISMCATResponsibleEntity*
Added **dutyOrganizationUnit** (CR-2015-071)	DES Schema	Added new attribute
Added **handlingControls** (CR-2015-037)	CVE CVEnum-UIASHandlingControls Schema DES	Added new attribute

Change	Artifacts Changed	Compatibility Notes
Added Schematron rules (CR-2015-034)	Schematron added UIAS-ID-00001 added. UIAS-ID-00004 added. UIAS-ID-00005 added. UIAS-ID-00006 added. UIAS-ID-00007 added. UIAS-ID-00008 added. UIAS-ID-00009 added. UIAS-ID-00011 added. UIAS-ID-00012 added. UIAS-ID-00014 added. UIAS-ID-00016 added. UIAS-ID-00019 added. UIAS-ID-00021 added. UIAS-ID-00022 added. UIAS-ID-00023 added. UIAS-ID-00024 added. UIAS-ID-00025 added. UIAS-ID-00026 added. UIAS-ID-00028 added. UIAS-ID-00030 added. UIAS-ID-00036 added. UIAS-ID-00047 added. UIAS-ID-00050 added. UIAS-ID-00051 added. UIAS-ID-00052 added.	Systems implementing UIAS MUST exchange information valid to the Schematron.

Change	Artifacts Changed	Compatibility Notes
	UIAS-ID-00053 added. UIAS-ID-00056 added. UIAS-ID-00057 added. UIAS-ID-00065 added. UIAS-ID-00066 added.	
Added schema (CR-2015-034, CR-2016-016)	UIAS XSD Schema added	Systems implementing UIAS MUST exchange information valid to the schema.
Added PAAS to CVEnum-UIASRoleNamespace and created CVENumUIASPAASScope, CVENumUIASPAASFunction (CR-2015-110)	CVE CVEnum-UIASRoleNamespace updated. CVENumUIASPAASScope added. CVENumUIASPAASFunction added.	CVE value added and new CVEs created.
Added **auditRoutingOrganization** (CR-2016-001, CR-2016-014)	DES Schema	Added new required attribute
Incorporated ROLE and AUTHCAT CVEs into UIAS (CR-2016-013)	CVE CVEnum-UIASAuthorityCategory added CVEnum-UIASRoleNamespace added	CVEs are now internal to UIAS

Change	Artifacts Changed	Compatibility Notes
Added Clearance, CertificateAuthority, EntityType, Non-Person EntityType, FineAccessControls, and LifeCycleStatus CVEs into UIAS (CR-2015-015, CR-2015-016, CR-2015-034)	CVE CVEnum-UIASCertificateAuthority added CVEnumUIASClearance added CVEnumUIASEntityType-added CVEnum-UIASFineAccessControl added CVEnum-UIASLifeCycleStatus added CVEnum-UIASNonPersonEntity-Type added CVEnum-UIASPersonEntityType-added	CVEs internal to UIAS now control corresponding attribute values.
Updated schema to make all Elements begin with capital letters to be consistent with Naming and Design Rules (CR-2015-034, CR-2016-016)	Schema	Systems need to be updated to accommodate this change.
Updated CVE to reflect removal of KDK and the moving of its subcompartments under TK (CR-2016-024)	CVE CVEnum-UIASFineAccessControl updated	Systems need to be updated to accommodate this change.
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.3 - V2015-AUG Change Summary

Significant drivers for Version 2015-AUG include:

- Community Change Requests

- Alignment with standalone CVE specifications

Table 35 summarizes the changes made to this technical specification from Version 2014-DEC to Version 2015-AUG.

Table 35 - V2015-AUG Change History

Change	Artifacts Changed	Compatibility Notes
Added **group**	**group**	Added new attribute
Added attribute ID	*DES*	Added Attribute ID (URN) for all attributes
Updated **region**	**region**	CVE updated to reference MN.CES.[21] CVEnumMNRegion
Updated **topic**	**topic**	CVE updated to reference MN.CES.[21] CVEnumMNIssue
Updated **originatingNetwork**	**originatingNetwork**	CVE updated to reference VIRT.XML.[25]
Updated **icNetworks**	**icNetworks**	CVE updated to reference VIRT.XML.[25]

B.4 - V2014-DEC Change Summary

Significant drivers for Version 2014-DEC include:

- Clarified definition of GOV in support of SLT
- Add CVE for **role**
- Move NATO to CVE FAC
- Add support for 2PI
- Added Authoritative Attribute Source for specific attributes

Table 36 summarizes the changes made to this technical specification from Version 3.1 to Version 2014-DEC.

Table 36 - V2014-DEC Change History

Change	Artifacts Changed	Compatibility Notes
Implemented new versioning scheme.	DES	Changed versioning scheme from version number (e.g., V3) to version YYYY-MMM (e.g, 2014-DEC).
Updated **role**.	**role**	CVE for **role** values added.

Change	Artifacts Changed	Compatibility Notes
Updated attribute **clearance**.	**clearance**	Remove NATO from attribute **clearance** .
Updated **adminOrganization**.	**adminOrganization**	Added support for 2PI.
Updated **entityType**.	**entityType**	Removed 'US federal' in definition of GOV in entityType.
Added new attribute **certificateAuthority**.	**certificateAuthority**	Added new environment attribute.
Added new attribute **originatingNetwork**.	**originatingNetwork**	Added new environment attribute.

B.5 - V3.1 Change Summary

Significant drivers for Version 3.1 include:

- Add CVEs for **authorityCategory** and **fineAccessControl**

Table 37 summarizes the changes made to this technical specification from Version 3 to Version 3.1.

Table 37 - V3.1 Change History

Change	Artifacts Changed	Compatibility Notes
Updated **authorityCategory**.	**authorityCategory**	Updated CVE.
Updated **clearance**.	**clearance**	Clarified definition.
Updated **fineAccessControl**.	**fineAccessControl**	Updated CVE.
Updated **icNetworks**.	**icNetworks**	Updated CVE.

B.6 - V3 Change Summary

Significant drivers for Version 3 include:

- Provide for safeguards

Table 38 summarizes the changes made to this technical specification from Version 2.1 to Version 3.

Table 38 - V3 Change History

Change	Artifacts Changed	Compatibility Notes
Added new attribute.	**entitySecurityMark**	Added new attribute.
Added new attribute.	**icNetworks**	Added new attribute.

B.7 - V2.1 Change Summary

Significant drivers for Version 2.1 include:

- Provide updated CVEs for **adminOrganization** and **dutyOrganization**

Table 39 summarizes the changes made to this technical specification from Version 2 to Version 2.1.

Table 39 - V2.1 Change History

Change	Artifacts Changed	Compatibility Notes
Updated**adminOrganization**.	**adminOrganization**	Updated CVE and clarified definition.
Updated **authorityCategory**.	**authorityCategory**	Clarified definition.
Updated **ATOStatus**.	**ATOStatus**	Clarified definition.
Updated **clearance**.	**clearance**	Clarified definition.
Updated **dutyOrganization**.	**dutyOrganization**	Updated CVE and clarified definition.
Updated **entityType**.	**entityType**	Clarified definition.
Updated **lifeCycleStatus**.	**lifeCycleStatus**	Clarified definition.
Updated **region**.	**region**	Clarified definition.
Updated **role**.	**role**	Clarified definition.
Updated **topic**.	**topic**	Clarified definition.

B.8 - V2 Change Summary

Significant drivers for Version 2 include:

- The addition of attributes to provide Fine-Grain Access Control

Table 40 summarizes the changes made to this technical specification from to Version 1 to Version 2.

Table 40 - V2 Change History

Change	Artifacts Changed	Compatibility Notes
Added new attribute.	**adminOrganization**	Added new attribute.
None	**aICP**	No change.
Added new attribute.	**ATOStatus**	Added new attribute.
Added new attribute.	**authorityCategory**	Added new attribute.
Updated **clearance**.	**clearance**	Updated definition to include NPEs, NATO and DoE clearances.
Updated **countryOfAffiliation**.	**countryOfAffiliation**	Updated attribute name and definition to apply to NPEs.

Change	Artifacts Changed	Compatibility Notes
Updated **digitialIdentifier**.	**digitialIdentifier**	Updated DistinguishedName attribute name and definition to apply to NPEs.
Updated **dutyOrganization**.	**dutyOrganization**	Updated Organization attribute name and definition to apply to NPEs.
Updated **entityType**.	**entityType**	Updated Employee Type attribute name and definition to apply to NPEs.
Updated **fineAccessControls**.	**fineAccessControls**	Updated sciControls attribute name and definition to apply to NPEs.
Updated **isICMember**.	**isICMember**	Updated definition to include NPEs.
Added new attribute.	**lifeCycleStatus**	Added new attribute.
Added new attribute.	**region**	Added new attribute.
Added new attribute.	**role**	Added new attribute.
Added new attribute.	**topic**	Added new attribute.

Appendix C List of Abbreviations

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

2PI	Second Party Integree
5EE	Five-Eyes Enterprise
AAS	Authoritative Attribute Source
ABAC	Attribute Based Access Control
ABNF	Augmented Backus-Naur Form
ACSS	Allied Collaborative Shared Services
AICP	Authorized IC Person
AOI	Area of Interest
AOR	Area of Responsibility
APCS	Attribute Practice Compliance Statement
APS	Attribute Practice Statement
ARH	Access Rights and Handling
AS	Attribute Service
ATO	Authority To Operate
C2S	Commercial Cloud Services
CA	Certification Authority
CAD	Cryptologic Agencies Domain
CEAC	CIA Enterprise Access Control
CIO	Chief Information Officer
CN	Common Name
CNWDI	Critical Nuclear Weapons Design Information
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DI	Digital Identifier
DIA	Defense Intelligence Agency

DIAS	DoDIIS Identity and Authorization Services
DN	Distinguished Name
DNI	Director of National Intelligence
DOD	Department of Defense
E.O.	Executive Order
ESB	Enterprise Standards Baseline
FAC	Fine Access Control
FSD	Full Service Directory
IAA	Identity, Authentication and Authorization
IAMS	Identity Access Management Service
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IETF	Internet Engineering Task Force
ISM	Information Security Markings
ICSOG	Intelligence Community Service Operations Group
ISMCAT	Information Security Marking Country Codes and Tetragraphs
ISOO	Information Security Oversight Office
IT	Information Technology
JWICS	Joint Worldwide Intelligence Communications System
LIC	License
MN	Mission Need Profile

NATO	North Atlantic Treaty Organization
NPE	Non-Person Entity
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PAAS	Platform as a Service
PDP	Policy Decision Point
PE	Person Entity
PKI	Public Key Infrastructure
POC	Point of Contact
RFC	Request for Comments
SAML	Security Assertion Markup Language
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SI	Special Intelligence
SLT	State, Local, and Tribal Governments
TBD	To Be Determined
TK	Talent-Keyhole
TS	Top Secret
UAAS	Unified Authorization and Attribute Services
UIAS	Unified Identity Attribute Set
USAGENCY	Controlled Vocabulary Enumeration Encoding Specification for US Agencies
URN	Uniform Resource Name
US	United States
VIRT	Virtual Coverage
X.509	ITU-T standard for public key infrastructures

XML	Extensible Markup Language
XSL	Extensible Stylesheet Language

Appendix D Bibliography

Bibliography

[1] AATT CONOPS
Department of Defense / Intelligence Community. *Unified Authorization and Attribute Service, Concept of Operations*. Version 1.11. 8 December 2008.
Available online Intelink-TS at: http://go.ic.gov/19Vvzzm

[2] DoD Instruction 8310.01
DoD CIO. *Information Technology Standards in the DoD*. 8310.01. 2 February 2015.
Available online at: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/831001p.pdf

[3] 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

[4] FSD
Office of the Director of National Intelligence. *Data Encoding Specification for IC Full Service Directory Schema (FSD)*.
Available online Intelink-TS at: http://go.ic.gov/iZiePDW
Available online Intelink-U at: https://w3id.org/ic/standards/FSD
Available online at: https://w3id.org/ic/standards/public

[5] IC ITE INC1 IMPL
Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.
Available online Intelink-TS at: http://go.ic.gov/4X6TOc1

[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: http://go.ic.gov/5DjqqWz
Available online Intelink-U at: https://w3id.org/ic/standards/policy/icmarkings [https://w3id.org/ic/standards/policy/icmarkings]

[7] IC Markings DEC 2016
Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 31 Dec 2016.
Available online Intelink-U at: https://w3id.org/ic/standards/policy/icmarkings [https://w3id.org/ic/standards/policy/icmarkings]

[8] 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: http://go.ic.gov/5Ot5sbK

Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[9] 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: http://go.ic.gov/GG61roi
Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[10] ICD 503
Office of the Director of National Intelligence. *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*. Intelligence Community Directive 503. 15 September 2008.
Available online Intelink-TS at: http://go.ic.gov/W0oErK2
Available online at: http://www.dni.gov/files/documents/ICD/ICD_503.pdf

[11] 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: http://go.ic.gov/qY6rM4s

[12] 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: http://go.ic.gov/ha2FxyZ
Available online at: http://www.dni.gov/files/documents/ICPG/icpg_500_2.pdf

[13] ICPG 704.5
Deputy Directory of National Intelligence for Policy, Plans and Requirements . *Intelligence Community Security Database Scattered Castles*. Intelligence Community Policy Guidance 704.5. 02 October 2008.
Available online Intelink-TS at: http://go.ic.gov/3JbG1OH
Available online at: http://www.dni.gov/files/documents/ICPG/icpg_704_5.pdf

[14] ICPG 710.1
Director of National Intelligence. *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.
Available online Intelink-TS at: http://go.ic.gov/0d147Ee
Available online at: http://www.dni.gov/files/documents/ICPG/ICPG710.1.pdf

[15] 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: http://go.ic.gov/sLKNq3N
Available online Intelink-U at: https://w3id.org/ic/standards/policy/ICS500-20

[16] 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: http://go.ic.gov/3czwVuQ

[17] 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: http://go.ic.gov/zdD89EN

[18] 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: http://go.ic.gov/EwKUJ2f

[19] IETF-RFC 2119
Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997.
Available online at: http://tools.ietf.org/html/rfc2119

[20] ISMCAT.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES)*.
Available online Intelink-TS at: http://go.ic.gov/xhPfIl3
Available online Intelink-U at: https://w3id.org/ic/standards/ISMCAT
Available online at: https://w3id.org/ic/standards/public

[21] MN.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for Mission-Need (MN.CES)*.
Available online Intelink-U at: https://w3id.org/ic/standards/MN
Available online at: https://w3id.org/ic/standards/public

[22] SAML 2.0 Attribute Sharing
OASIS Security Services Technical Committee. *SAML 2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Version 1.0, [Encrypted Mode]* . 27 March 2008.
Available online at: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd.html

[23] 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: http://go.ic.gov/H8RwEw8
Available online Intelink-U at: https://w3id.org/ic/standards/UIAS
Available online at: https://w3id.org/ic/standards/public

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

Available online Intelink-TS at: http://go.ic.gov/MmBEpFU
Available online Intelink-U at: https://w3id.org/ic/standards/USAgency
Available online at: https://w3id.org/ic/standards/public

[25] VIRT.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Virtual Coverage (VIRT.XML)*.
Available online Intelink-TS at: http://go.ic.gov/HGb1l2P
Available online Intelink-U at: https://w3id.org/ic/standards/VIRT
Available online at: https://w3id.org/ic/standards/public

Appendix E 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@iarpa.gov.

Appendix F 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.[15]