Intelligence Community Technical Specification

Access Control Encoding Specification for Need-To-Know

Version 2016-SEP

September 9, 2016

This document has been approved for Public Release by the Office of the Director of National Intelligence. See Distribution Notice for details.

Distribution Notice:

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

This document has been approved for Public Release by the Office of the Director of National Intelligence. See Distribution Notice for details.

Table of Contents

List of Figures

List of Tables

Chapter 1 - Introduction

1.1 - Purpose

This *Access Control Encoding Specification for Need-To-Know* (NTK.ACES) defines implementation requirements for providing access to resources protected with NTK metadata. This Access Control Encoding Specification (ACES) defines the combinational logic between data tags and user/entity attributes. The logic defined in this ACES MUST be used in the access control decision process for resources protected with NTK metadata.

1.2 - Scope

This ACES combines guidance previously provided in separate NTK profiles including ICO-ACES, OC-NTK-ACES, and PROPIN-NTK-ACES. The existing, separate NTK profiles are NOT immediately retired upon signature of this specification. Instead, the existing, separate profiles, including all related ACES, will sunset together in 2016. Systems that implement versions of NTK prior to 2015-AUG must refer to the separate profile ACES that existed immediately prior to this version of NTK. This ACES is for use only with 2015-AUG NTK metadata.

This specification applies to the Intelligence Community (IC) and information produced by, stored, or shared within the IC. This ACES may have relevance outside the scope of intelligence. However, prior to application outside of this defined scope, the ACES should be closely scrutinized and differences separately documented and assessed for applicability.

1.3 - Background

The Intelligence Community 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* [6] grants the IC CIO the authority and responsibility to:

- Develop an Intelligence Community Enterprise Architecture (IC EA).
- Lead the IC's identification, selection, development, and management of IC enterprise standards.
- Incorporate technically sound, de-conflicted, interoperable enterprise standards into the IC EA.
- Certify that IC elements adhere to the architecture and standards.

In the area of enterprise standardization, the IC CIO is called upon for the following: to establish common Information Technology (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. As detailed in Intelligence Community Standard (ICS) 500-21, *Tagging of Intelligence and Intelligence-Related Information* [12] the extensive and consistent use of XML within data encoding specifications allows for improved data exchanges and processing of information, thereby facilitating achievement of the IC’s data discovery, data sharing, and interoperability goals.

An Access Control Encoding Specification (ACES) furthers those goals by codifying mappings and combinational logic between data attributes and user/entity attributes to facilitate consistent enterprise-wide boolean access decisions. Historically, access control decisions have been made in local environments based on local interpretations of agreements and policies that have resulted in decisions that are not uniform across the entire enterprise. ACES hope to reduce the need for such local interpretations and further the goal of improving data exchanges and processing of information by documenting and encoding the enterprise interpretation.

ACES provide both abstract and concrete guidance for making access control decisions. The generic abstract guidance is intended to be used in various contexts for making informed access decision logic, but it is the goal of ACES to also provide concrete guidance in appendices or separate annexes for certain contexts.

1.4 - Enterprise Need

Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, within the enterprise may be marked with a variety of Need to Know markings using the NTK.XML specification. Persons or Non-Person Entities (NPEs) wishing to access or distribute such information must first be granted the ability to do so by the originator or data steward of the information. Access control systems must be able to determine the meaning of the asserted NTK values on information as well as the relation between those attributes and the attributes that belong to entities in order to make informed and accurate dissemination decisions.

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[2]
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer[6]
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[7]
  - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information[12]
- 200 Series:
  - Intelligence Community Directive (ICD) 208, Write for Maximum Utility[4]
  - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination[5]
  - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community’s Responsibility to Provide[10]
- 700 Series:
  - Intelligence Community Directive (ICD) 710, Classification and Control Markings System[8]

- Intelligence Community Policy Guidance (ICPG) 710.1, Application of Dissemination Controls: Originator Control[9]

1.5 - Audience and Applicability

ACESs are primarily intended to be used by those developing tools and services to perform access control decisions.

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,* [11] 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*,[1] 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.” [13] 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
- <u>Underscore</u> – 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 1 - XML Namepaces

Prefix	**URI**
ism	urn:us:gov:ic:ism
ntk	urn:us:gov:ic:ntk

1.7 - Dependencies

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

Table 2 - Dependencies

Name	**Dependency Description**
CVE Encoding Specification for License [15]	This ACES depends on the current version of License (LIC.CES).
CVE Encoding Specification for Mission Need [16]	This ACES depends on the current version of Mission Need (MN.CES).
XML Data Encoding Specification for Need-To-Know Metadata [18]	This ACES depends on the current version of Need-To-Know (NTK.XML).
XML Data Encoding Specification for Unified Identity Attribute Set [19]	This ACES depends on the current version of Unified Identity Attribute Set (UIAS.XML).
CVE Encoding Specification for US Agency Acronyms [20]	This ACES depends on the current version of US Agency (USAgency.CES).

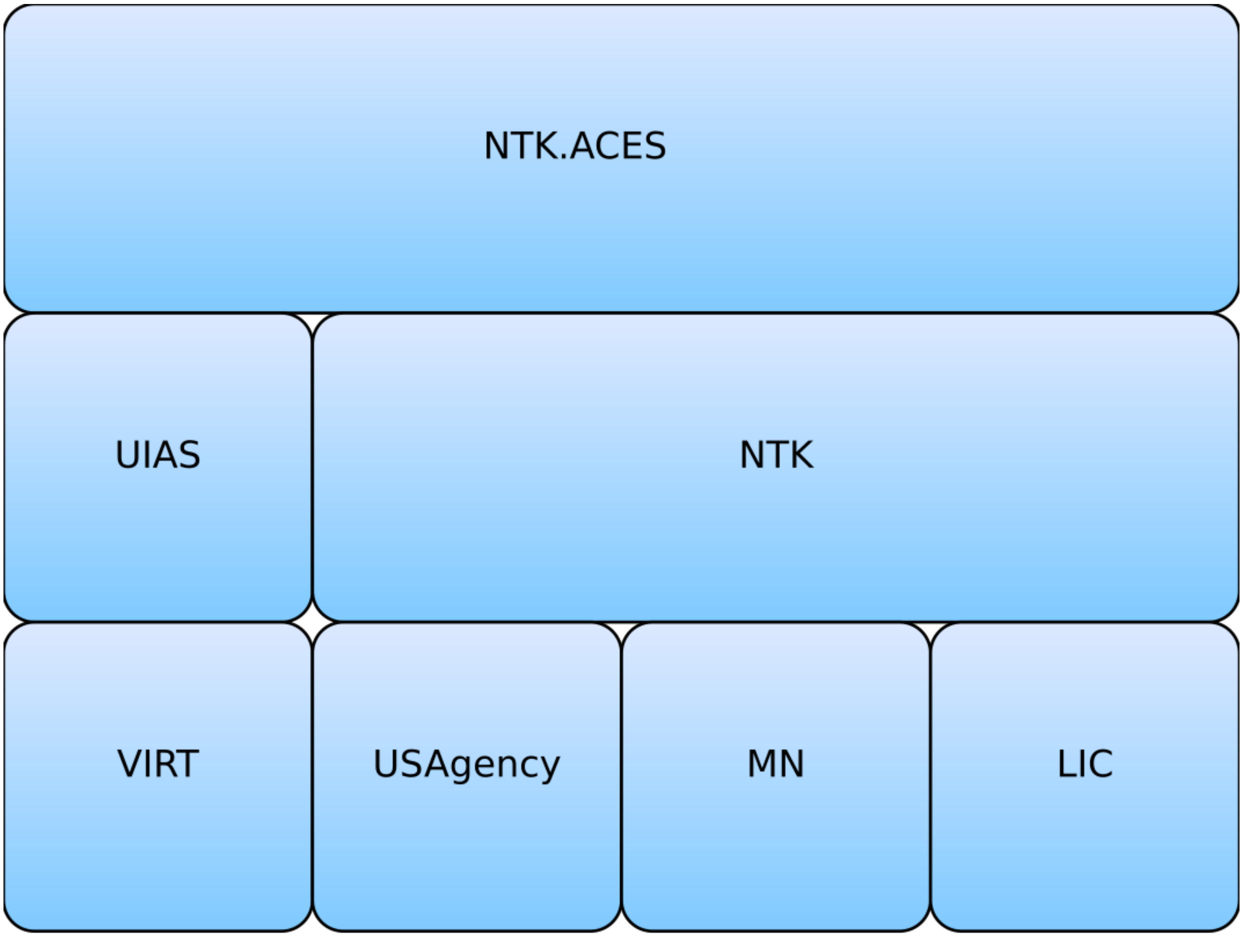

Figure 1 : Related Specifications

1.8 - 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.

Concrete mappings of one set of attributes to another as defined within an ACES are normative.

Additional guidance that is either classified or has handling controls can be found in separate annexes, which are 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). This provides a temporal representation of when the specification was released. ACES are specifically designed such that changes to the specification are retroactive and apply to all data previously marked with the ACES. Changes to the specification in which that is not the desired behavior would require a new ACES to be created. Due to this feature, data marked with an ACES do NOT capture the version number in the instance document like other types of encoding specifications. ACES therefore have no equivalent to the **@DESVersion** or **@CESVersion** attributes, and if an ACES is directly referenced in data, it is done so only by its URI with no version number.

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 2.

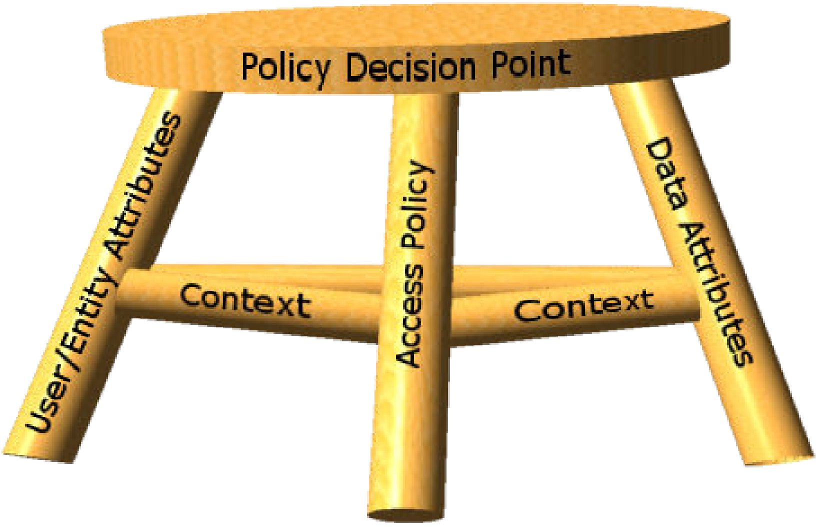

Figure 2 : Three-legged Stool of Access Decisions

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 access policy leg of the access control framework, helping to define mapping conditions between the other two legs. Access policy specifications include: ISM.ACES[14] and NTK.ACES.[17]

2.2 - Additional Guidance

This section provides additional guidance for encoding data in specific situations. In particular, situations for which there is no clear or single method of encoding the data are documented here. The content of this section will evolve over time as additional situations are identified. Implementers are encouraged to contact the maintainers of this specification for further guidance if necessary.

2.2.1 - Required Conditions for Access

Every condition MUST be met prior to access being granted. For example, access to a TS//SI/TK//REL TO USA, CAN/RELIDO resource would require passing the TS, SI, TK, and REL conditions.

2.2.2 - Handling Prior CVE Versions

An ACES maps controlled vocabulary values to user attributes for the purpose of access control; all access control-relevant values in all current Controlled Vocabulary Enumerations (CVEs) Encoding Specifications (CESs) are explicitly mapped by an ACES in the IC ESB. When a new version of a CES is entered into the IC ESB, it immediately replaces all previous versions, so there is only one version of each vocabulary mandated in the IC ESB at a given time. Enterprise systems SHOULD produce and share information tagged using current CESs in accordance with the IC ESB.

The ACES directly supports access decisions based on current CES values. However, existing resources are not necessarily remarked when vocabularies are replaced, and production systems may lag behind the IC ESB. Systems may encounter legacy metadata when making access control decisions.

The Office of the IC CIO provides upgrade transforms each time a CES is replaced. Legacy metadata SHOULD be upgraded to current CES values before an access control decision is made. Relevant ACES will explicitly handle current values. Note that it may be necessary to apply a series of upgrade transforms. If the metadata is not upgraded the ACES MAY not provide an accurate access decision.

Chapter 3 - Definitions, Interfaces, and Constraints

3.1 - NTK Metadata Validity

The NTK.ACES only works for valid NTK marked data. Granting access based on invalid NTK metadata (that is, metadata that does not pass both schema and Schematron validation) poses a significant risk of spilling information.

Chapter 4 - Conformance Validation

An access decision is considered conformant with this specification if it grants or denies access based on the normative mappings. The following steps do not dictate how this validation strategy is implemented.

4.1 - Business Rule Validation

The only necessary compliance validation step is to ensure that an access control decision complies with the business rules (normative mappings) expressed in Chapter 3 - Definitions, Interfaces, and Constraints of this specification. It should be noted that while the business rules for this specification are expressed in English, the English is informative but the constraints they express are normative. As such, any languages or tools may be used to perform the validation as long as the results are consistent with results of the English included in this specification and its dependencies.

Chapter 5 - Access Control

Each section in this chapter is identified by a URN. When used as the value of an **ntk:AccessPolicy** element in an NTK assertion, the URN specifies that the protected resource is subject to the access controls encoded in the corresponding section of this chapter and contextually relevant annexes of this document. This document provides access control encoding for NTK access profiles listed in Table 3. For information about each NTK Access Profile, see the NTK DES. [18]

Table 3 - NTK Access Policies

Access Policy URN	Associated Access Profile
`urn:us:gov:ic:aces:ntk:xd`	Exclusive Distribution
`urn:us:gov:ic:aces:ntk:ico`	Intelligence Community Only
`urn:us:gov:ic:aces:ntk:license`	Licensing Agreements
`urn:us:gov:ic:aces:ntk:mn`	Mission Need
`urn:us:gov:ic:aces:ntk:nd`	No Distribution
`urn:us:gov:ic:aces:ntk:oc`	Originator Controlled
`urn:us:gov:ic:aces:ntk:permissive`	Permissive Groups and Individuals
`urn:us:gov:ic:aces:ntk:propin:1`	Proprietary Information for All Government Employees
`urn:us:gov:ic:aces:ntk:propin:2`	Proprietary Information for Specified Members Only
`urn:us:gov:ic:aces:ntk:restrictive`	Restrictive Groups

The access control encodings in this document rely solely on information in (1) an NTK Access Profile and (2) related controls expressed in Information Security Markings (ISM) attributes. For the evaluation of an access decision for a particular NTK assertion, a policy decision point must have the entire related NTK access profile, all ISM attributes associated with the resource, and an entity's attributes. The access determination for any particular NTK access profile may be part of a larger access control decision.

The guidance in this section is abstract and maps NTK metadata to abstract entity concepts. However, part of an access control decision is the context in which it is made, and any associated concrete mappings can be found in the appendices. The associated concrete mappings are normative and MUST be used when applicable. In the absence of an appropriate concrete mapping, the following abstract mapping MAY be used to make an access determination.

Note

Some NTK Access Profiles support requirements of the *IC Marking System Register and Manual*. Other NTK Access Profiles support policy in ICPG 710.1.[9] Some NTK Access Profiles are provided to meet a mission need and are not based on a specific policy.

5.1 - Exclusive Distribution

The Exclusive Distribution (EXDIS) Access Policy is identified by the URN `urn:us:gov:ic:aces:ntk:xd`.

For the UIAS attributes that implement the abstract entity requirements in the table below, see Section C.2 - Mapping EXDIS to UIAS.

Note

- In the following table, the '[ORIG_AGENCY]' and '[DISSEM_AGENCY]' tokens are placeholders for actual agency acronyms.

Table 4 - EXDIS Access List

NTK Access Profile	Entity Attribute
ntk:AccessPolicy contains the EXDIS URN	The person or NPE MUST meet *at least one* of these criteria: 1. The person or NPE's duty organization matches [ORIG_AGENCY] 2. The person or NPE's duty organization matches one of [DISSEM_AGENCY]
ntk:ProfileDes contains the Agency Dissem URN	
exactly one originator agency	
zero to many dissemto agencies	

```
<ntk:AccessPolicy>
     urn:us:gov:ic:aces:ntk:xd
</ntk:AccessPolicy>
```

```
<ntk:ProfileDes>
     urn:us:gov:ic:ntk:profile:agencydissem
</ntk:ProfileDes>
```

```
<ntk:AccessProfileValue
   ntk:qualifier="originator"
   ntk:vocabulary="organization:usa-agency"
     >[ORIG_AGENCY]</ntk:AccessProfileValue>
```

```
<ntk:AccessProfileValue
   ntk:qualifier="dissemto"
   ntk:vocabulary="organization:usa-agency"
     >[DISSEM_AGENCY]</ntk:AccessProfileValue>
```

5.2 - Intelligence Community Only

The Intelligence Community Only (ICO) Access Policy is identified by the URN `urn:us:gov:ic:aces:ntk:ico`.

For the UIAS attributes that implement the abstract entity requirements in the table below, see Section C.3 - Mapping ICO to UIAS.

Table 5 - Restriction to IC Members

NTK Access Profile	Abstract Person Attributes
ntk:AccessPolicy contains the ICO URN	The person or NPE MUST be a member of the Intelligence Community.

```
<ntk:AccessProfile ism:classification="U"
ism:ownerProfile="USA">
     <ntk:AccessPolicy>
          urn:us:gov:ic:aces:ntk:ico
     </ntk:AccessPolicy>
</ntk:AccessProfile>
```

5.3 - License

The License Access Policy is identified by the URN `urn:us:gov:ic:aces:ntk:license`.

For the UIAS attributes that implement the abstract entity requirements in the table below, see Section C.4 - Mapping LICENSE to UIAS.

Table 6 - LICENSE-NTK Access List

NTK Access Profile	Person or NPE Attributes
ntk:AccessPolicy contains the License URN **ntk:ProfileDes** contains the Data Sphere URN one to many licenses	The person or NPE MUST meet all of these criteria: 1. If [OSC-CommercialOpenSource1] is one of the [LICENSE] values, the person or NPE MUST be a member of the Intelligence Community. 2. The person or NPE MUST meet the requirements for all other license agreements as indicated by the set of [LICENSE] values.

ntk:AccessPolicy contains the License URN

```
<ntk:AccessPolicy>
     urn:us:gov:ic:aces:ntk:license
</ntk:AccessPolicy>
```

ntk:ProfileDes contains the Data Sphere URN

```
<ntk:ProfileDes>
     urn:us:gov:ic:ntk:profile:datasphere
</ntk:ProfileDes>
```

one to many licenses

```
<ntk:AccessProfileValue
   ntk:vocabulary="datasphere:license"
     >[LICENSE]</ntk:AccessProfileValue>
```

5.4 - Mission Need

The Mission Need (MN) Access Policy is identified by the URN `urn:us:gov:ic:aces:ntk:mn`.

For the UIAS attributes that implement the abstract entity requirements in the table below, see Section C.5 - Mapping MN to UIAS.

Table 7 - MN-NTK Access List

NTK Access Profile	Person or NPE Attributes

ntk:AccessPolicy contains the MN URN
`<ntk:AccessPolicy>`
`     urn:us:gov:ic:aces:ntk:mn`
`</ntk:AccessPolicy>`
ntk:ProfileDes contains the Data Sphere URN
`<ntk:ProfileDes>`
`     urn:us:gov:ic:ntk:profile:datasphere`
`</ntk:ProfileDes>`
zero to many MN issues
`<ntk:AccessProfileValue`
`   ntk:vocabulary="datasphere:mn:issue"`
`     >[ISSUE]</ntk:AccessProfileValue>`
zero to many MN regions
`<ntk:AccessProfileValue`
`   ntk:vocabulary="datasphere:mn:region"`
`     >[REGION]</ntk:AccessProfileValue>`
	The person or NPE MUST meet *both* the issue and region criteria:
	Issue Criteria. If MN issues are listed in the NTK Access Profile, the user or NPE MUST have an association with at least one of the listed [ISSUE] values.
	Note
	If no MN issues are listed in NTK, there is no issue restriction.
	Region Criteria. If MN regions are listed in the NTK Access Profile, the user or NPE MUST have an association with at least one of the listed [REGION] values.
	Note
	If no MN regions are listed in NTK, there is no region restriction.

5.5 - No Distribution

The No Distribution (NODIS) Access Policy is identified by the URN `urn:us:gov:ic:aces:ntk:nd`.

For the UIAS attributes that implement the abstract entity requirements in the table below, see Section C.6 - Mapping NODIS to UIAS.

Table 8 - ND-NTK Access List

NTK Access Profile	Person or NPE Attributes

ntk:AccessPolicy contains the NODIS URN
`<ntk:AccessPolicy>`
`    urn:us:gov:ic:aces:ntk:nd`
`</ntk:AccessPolicy>`
ntk:ProfileDes contains the Group & Individual URN
`<ntk:ProfileDes>`
`    urn:us:gov:ic:ntk:profile:grp-ind`
`</ntk:ProfileDes>`
zero to many groups
`<ntk:AccessProfileValue`
`  ntk:vocabulary="group:[GRP_VOCAB]"`
`    >[GRP_VALUE]</ntk:AccessProfileValue>`
zero to many individuals
`<ntk:AccessProfileValue`
`  ntk:vocabulary="individual:[IND_VOCAB]"`
`    >[IND_VALUE]</ntk:AccessProfileValue>`
	The user or NPE MUST meet *at least one* of these criteria:
	1. One or more groups are listed in the NTK Access Profile and the person or NPE has an association with at least one [GRP_VALUE] from the appropriate system identified by group:[GRP_VOCAB].
	2. One or more individuals are listed in the NTK Access Profile and the person matches the [IND_VALUE] from the appropriate system identified by individual:[IND_VOCAB].

5.6 - Originator Controlled

The ORCON Access Policy is identified by the URN `urn:us:gov:ic:aces:ntk:oc`.

For the UIAS attributes that implement the abstract entity requirements in the table below, see Section C.7 - Mapping ORCON to UIAS.

Note

- The NTK-ACES ORCON access rule does not apply in a Secure Community of Interest (SCOI) and SCOI policies should be used instead. In a SCOI, the ORCON-NTK in a document should not be used for automated access decisions and instead use the list of authorized members of the SCOI.

Table 9 - ORCON Access Control Mapping

NTK Access Profile	Entity Attribute
ntk:AccessPolicy contains the ORCON URN **ntk:ProfileDes** contains the Agency Dissem URN exactly one originator agency zero to many dissemto agencies	The user or NPE MUST meet *at least one* of these criteria: 1. The person or NPE's duty organization matches [ORIG_AGENCY]. 2. The person or NPE's duty organization matches one of [DISSEM_AGENCY].

```
<ntk:AccessPolicy>
     urn:us:gov:ic:aces:ntk:oc
</ntk:AccessPolicy>
```

```
<ntk:ProfileDes>
     urn:us:gov:ic:ntk:profile:agencydissem
</ntk:ProfileDes>
```

```
<ntk:AccessProfileValue
   ntk:qualifier="originator"
   ntk:vocabulary="organization:usa-agency"
     >[ORIG_AGENCY]</ntk:AccessProfileValue>
```

```
<ntk:AccessProfileValue
   ntk:qualifier="dissemto"
   ntk:vocabulary="organization:usa-agency"
     >[DISSEM_AGENCY]</ntk:AccessProfileValue>
```

5.7 - Permissive

The Permissive Access Policy is identified by the URN `urn:us:gov:ic:aces:ntk:permissive`.

For the UIAS attributes that implement the abstract entity requirements in the table below, see Section C.8 - Mapping Permissive to UIAS.

Table 10 - Permissive Access Control Mapping

NTK Access Profile	Entity Attribute
ntk:AccessPolicy contains the Permissive URN **ntk:ProfileDes** contains the Group & Individual URN zero to many groups zero to many individuals	The user or NPE MUST meet *at least one* of these criteria: 1. One or more groups are listed in the NTK Access Profile and the person or NPE has an association with at least one [GRP_VALUE] from the appropriate system identified by group:[GRP_VOCAB]. 2. One or more individuals are listed in the NTK Access Profile and the person matches the [IND_VALUE] from the appropriate system identified by individual:[IND_VOCAB].

ntk:AccessPolicy contains the Permissive URN

```
<ntk:AccessPolicy>
     urn:us:gov:ic:aces:ntk:permissive
</ntk:AccessPolicy>
```

ntk:ProfileDes contains the Group & Individual URN

```
<ntk:ProfileDes>
     urn:us:gov:ic:ntk:profile:grp-ind
</ntk:ProfileDes>
```

zero to many groups

```
<ntk:AccessProfileValue
   ntk:vocabulary="group:[GRP_VOCAB]"
     >[GRP_VALUE]</ntk:AccessProfileValue>
```

zero to many individuals

```
<ntk:AccessProfileValue
   ntk:vocabulary="individual:[IND_VOCAB]"
     >[IND_VALUE]</ntk:AccessProfileValue>
```

5.8 - Proprietary Information for All US Government Employees

The All US Government Employees Proprietary Information (PROPIN) Access Policy is identified by the URN `urn:us:gov:ic:aces:ntk:propin:1`.

For the UIAS attributes that implement the abstract entity requirements in the table below, see Section C.9 - Mapping PROPIN to UIAS.

Table 11 - All US Government Employee PROPIN Access List

NTK Access Profile	Person or NPE Attributes
ntk:AccessPolicy contains the All USG PROPIN URN	The person or NPE MUST be a US Government employee or member of the US military.

```
<ntk:AccessProfile
   ism:classification="U"
   ism:ownerProducer="USA">
     <ntk:AccessPolicy
          >urn:us:gov:ic:aces:ntk:propin:1
     </ntk:AccessPolicy>
</ntk:AccessProfile>
```

<table>
<tr><th>NTK Access Profile</th><th>Person or NPE Attributes</th></tr>
<tr><td>

ntk:AccessPolicy contains the All USG PROPIN URN

```
<ntk:AccessPolicy>
     urn:us:gov:ic:aces:ntk:propin:1
</ntk:AccessPolicy>
```

ntk:ProfileDes containing the Group & Individual URN

```
<ntk:ProfileDes>
     urn:us:gov:ic:ntk:profile:grp-ind
</ntk:ProfileDes>
```

zero or more groups

```
<ntk:AccessProfileValue
   ntk:vocabulary="group:[GRP_VOCAB]"
     >[GRP_VALUE]</ntk:AccessProfileValue>
```

zero or more individuals

```
<ntk:AccessProfileValue
   ntk:vocabulary="individual:[IND_VOCAB]"
     >[IND_VALUE]</ntk:AccessProfileValue>
```

</td><td>

The Person or NPE MUST meet *at least one* of the following criteria:

1. The person or NPE is a US Government employee or member of the US military.
2. One or more groups are listed in the NTK Access Profile and the person or NPE has an association with at least one [GRP_VALUE] from the appropriate system identified by group:[GRP_VOCAB].
3. One or more individuals are listed in the NTK Access Profile and the person matches the [IND_VALUE] from the appropriate system identified by individual:[IND_VOCAB].

</td></tr>
</table>

5.9 - Proprietary Information for Specified Members Only

The Specified Members Only PROPIN Access Policy is identified by the URN `urn:us:gov:ic:aces:ntk:propin:2`

For the UIAS attributes that implement the abstract entity requirements in the table below, see Section C.9 - Mapping PROPIN to UIAS.

Table 12 - Group PROPIN Access List

NTK Access Profile	Person or NPE Attributes

ntk:AccessPolicy contains the Specified Members Only PROPIN URN
`<ntk:AccessPolicy>`
`     urn:us:gov:ic:aces:ntk:propin:2`
`</ntk:AccessPolicy>`
ntk:ProfileDes containing the Group & Individual URN
`<ntk:ProfileDes>`
`      urn:us:gov:ic:ntk:profile:grp-ind`
`</ntk:ProfileDes>`
zero or more groups
`<ntk:AccessProfileValue`
`   ntk:vocabulary="group:[GRP_VOCAB]"`
`     >[GRP_VALUE]</ntk:AccessProfileValue>`
zero or more individuals
`<ntk:AccessProfileValue`
`   ntk:vocabulary="individual:[IND_VOCAB]"`
`     >[IND_VALUE]</ntk:AccessProfileValue>`
	The Person or NPE MUST meet *at least one* of the following criteria:
	1. One or more groups are listed in the NTK Access Profile and the person or NPE has an association with at least one [GRP_VALUE] from the appropriate system identified by group:[GRP_VOCAB].
	2. One or more individuals are listed in the NTK Access Profile and the person matches the [IND_VALUE] from the appropriate system identified by individual:[IND_VOCAB].

5.10 - Custom Profiles for PROPIN

When existing PROPIN profiles are insufficient for protecting PROPIN information, it is expected that a custom profile will be created. There are some restrictions to custom profiles that MUST be adhered to in order to comply with enterprise standards:

- The **ntk:AccessPolicy** URN MUST start with: `urn:us:gov:ic:aces:ntk:propin:`.
- The characters following the predefined beginning of the PROPIN-NTK.ACES URI are used to uniquely identify the custom profile and MUST NOT be purely numeric unless previously coordinated with the IC CIO Technical Specifications team. Numeric entries are restricted to enterprise PROPIN-NTK.ACES profiles to prevent collisions with custom profiles. Combinations of numbers and letters are allowed as long as the extension starts with at least one alphabetic character.

5.11 - Restrictive

The Restrictive Access Policy is identified by the URN `urn:us:gov:ic:aces:ntk:restrictive`

For the UIAS attributes that implement the abstract entity requirements in the table below, see Section C.10 - Mapping Restrictive to UIAS.

Table 13 - Restrictive Access Control Mapping

NTK Access Profile	Entity Attribute
ntk:AccessPolicy contains the Restrictive URN **ntk:ProfileDes** contains the Group & Individual URN zero to many groups	The Person or NPE MUST have an association with *all* groups specified in **ntk:AccessProfileValue**s such that they are a member of the group [GRP_VALUE] from the system identified by group:[GRP_VOCAB].

```
<ntk:AccessPolicy>
     urn:us:gov:ic:aces:ntk:restrictive
</ntk:AccessPolicy>
```

```
<ntk:ProfileDes>
     urn:us:gov:ic:ntk:profile:grp-ind
</ntk:ProfileDes>
```

```
<ntk:AccessProfileValue
   ntk:vocabulary="group:[GRP_VOCAB]"
     >[GRP_VALUE]</ntk:AccessProfileValue>
```

Appendix A Feature Summary

Table 14 - Feature Comparison

NTK ACES Feature Comparison			
Driver	**Feature**	**V2015-AUG**	**V2016-SEP**
IC Marking System Register and Manual 31 December 2013[3]	Specify originating agency for ORCON	F	F
IC Marking System Register and Manual 31 December 2013[3]	Specify agencies approved for dissemination	F	F
	Support for PROPIN access control	F	F
	Support for License-based access control	F	F
	Support for Mission-Need access control	F	F
	Support for EXDIS access control	F	F
	Support for NODIS access control	F	F
	Support for ICO access control	F	F
	Support for Group Restrictive access control	F	F
	Support for Group and Individual Permissive List access control	F	F
	Support for the handlingControl attribute in UIAS	N	F

Appendix B Change History

The following table summarizes the version identifier history for this ACES.

Table 15 - DES Version Identifier History

Version	Date	Purpose
2015-AUG	13 August 2015	Initial Release
2016-SEP	9 September 2016	Routine revision to technical specification. For details of changes, see Section B.1 - 2016-SEP Change Summary

B.1 - 2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Updates to UIAS

The following table summarizes the changes made to v2015-AUG in developing 2016-SEP.

Table 16 - Data Encoding Specification 2016-SEP Change Summary

Change	Artifacts Changed	Compatibility Notes
Updated UIAS Annex to deal with the new handlingControls attribute for non-person entities. (CR-2015-037)	Documentation	Systems making access control decisions will need to be updated to support the new access/handling logic.
Removed ARH from related specifications diagram.	Documentation	No impact to systems.
Updated to account for Secure Community of Interest (SCOI) as defined in ICPG 710.1[9] (CR-2016-004)	Documentation	Systems in SCOIs should follow the new guidance that is in alignment with ICPG 710.1 [9]
Removed USGovAgency from dependencies, USGovAgency[21] was incorporated into USAgency[20]. (CR-2016-012)	Documentation	Systems handling ORCON-USGOV will need to look at USAgency[20] for the list of pre-approved values.
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.

Appendix C Mapping to UIAS

C.1 - Introduction

This appendix discusses the relationship of NTK Access Profiles on data objects to the entity attributes expressed in UIAS for the purpose of access control. In the Access section, a document with the markings in the NTK column must have all of the corresponding UIAS Attributes for access to be granted. Specifically, it gives an exact value-to-value mapping between the two specifications. This mapping is used for both Access (AC-3) and Flow (AC-4) control purposes. For Access, the entity being evaluated is the *final* consumer, specifically the *user* who initiated a request. For Flow control purposes, the entity being evaluated would be the network or system in the *chain* between the final consumer and the user. Different architectures MAY require the immediate adjacent node to be the flow control or MAY require every node to be accounted for.

C.2 - Mapping EXDIS to UIAS

This section discusses the relationship of EXDIS markings on data objects to the entity attributes expressed in UIAS. The ISM **ism:nonICmarkings** value of ‘XD’ requires an EXDIS access policy be present.

The following table provides a mapping from specific EXDIS NTK elements to concrete UIAS attributes. The ‘[ORIG_AGENCY]’ and ‘[DISSEM_AGENCY]’ tokens are placeholder values; these placeholders stand for actual agency acronyms used in an EXDIS NTK assertion. There may be multiple **ntk:AccessProfileValue** elements listing agencies authorized for dissemination.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see Section 5.1 - Exclusive Distribution.

Table 17 - EXDIS Access Control Mapping

ntk:AccessProfile	UIAS Attribute
ntk:AccessPolicy contains the EXDIS URN	The person or NPE MUST meet *at least one* of these criteria: 1. The person or NPE UIAS attribute **dutyOrganization** matches [ORIG_AGENCY] 2. The person or NPE UIAS attribute **dutyOrganization** matches one of [DISSEM_AGENCY] AND If NPE, MUST have UIAS attribute **handlingControls** containing [XD]
ntk:ProfileDes contains the Agency Dissem URN	
exactly one originator agency	
zero to many dissemto agencies	

ntk:AccessPolicy contains the EXDIS URN

```
<ntk:AccessPolicy>
     urn:us:gov:ic:aces:ntk:xd
</ntk:AccessPolicy>
```

ntk:ProfileDes contains the Agency Dissem URN

```
<ntk:ProfileDes>
     urn:us:gov:ic:ntk:profile:agencydissem
</ntk:ProfileDes>
```

exactly one originator agency

```
<ntk:AccessProfileValue
   ntk:qualifier="originator"
   ntk:vocabulary="organization:usa-agency"
     >[ORIG_AGENCY]</ntk:AccessProfileValue>
```

zero to many dissemto agencies

```
<ntk:AccessProfileValue
   ntk:qualifier="dissemto"
   ntk:vocabulary="organization:usa-agency"
     >[DISSEM_AGENCY]</ntk:AccessProfileValue>
```

C.3 - Mapping ICO to UIAS

This section discusses the relationship of ICO constraint on data objects to the entity attributes expressed in the UIAS specification. The following Access Control Mapping table provides a mapping from specific ICO elements to concrete UIAS attributes.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see Section 5.2 - Intelligence Community Only.

Table 18 - Restriction to IC Members

ntk:AccessProfile	UIAS Attributes
ntk:AccessPolicy contains the ICO URN	The person or NPE UIAS attribute **isICMember** MUST be [TRUE].

```
<ntk:AccessProfile
   ism:classification="U"
   ism:ownerProfile="USA">
     <ntk:AccessPolicy>
          urn:us:gov:ic:aces:ntk:ico
     </ntk:AccessPolicy>
<ntk:AccessProfile>
```

C.4 - Mapping LICENSE to UIAS

This section discusses the relationship of LICENSE constraints on data objects to the entity attributes expressed in the UIAS specification.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see Section 5.3 - License.

Table 19 - LICENSE-NTK Access List

LICENSE-NTK	UIAS Attributes
ntk:AccessPolicy contains the License URN **ntk:ProfileDes** contains the Data Sphere URN one to many licenses	The person or NPE MUST meet *all* of these criteria: 1. If [osc1] is one of the [LICENSE] values, the entity's UIAS attribute **isICMember** must be [TRUE]. 2. The person or NPE MUST meet the requirements for *all* other license agreements as indicated by the set of [LICENSE] values.

ntk:AccessPolicy contains the License URN

```
<ntk:AccessPolicy>
     urn:us:gov:ic:aces:ntk:license
</ntk:AccessPolicy>
```

ntk:ProfileDes contains the Data Sphere URN

```
<ntk:ProfileDes>
     urn:us:gov:ic:ntk:profile:datasphere
</ntk:ProfileDes>
```

one to many licenses

```
<ntk:AccessProfileValue
   ntk:vocabulary="datasphere:license"
     >[LICENSE]</ntk:AccessProfileValue>
```

C.5 - Mapping MN to UIAS

This section discusses the relationship of MN constraints on data objects to the entity attributes expressed in the UIAS specification. The following Access Control Mapping table provides a mapping from specific MN elements to concrete UIAS attributes. The '[ISSUE]' and '[REGION]' tokens are placeholder values; these placeholders stand for actual issues and regions used in an MN NTK assertion.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see Section 5.4 - Mission Need.

Table 20 - MN-NTK Access List

MN-NTK	UIAS Attributes
ntk:AccessPolicy contains the MN URN **ntk:ProfileDes** contains the Data Sphere URN zero to many MN issues zero to many MN regions	The person or NPE MUST meet *both* the issue and region criteria: **Issue Criteria.** If MN issues are listed in the NTK Access Profile, the UIAS attribute **topic** MUST contain at least one of the listed [ISSUE] values. **Note** If no MN issues are listed in NTK, there is no issue restriction. **Region Criteria.** If MN regions are listed in the NTK Access Profile, the UIAS attribute **region** MUST contain at least one of the listed [REGION] values. **Note** If no MN regions are listed in NTK, there is no region restriction.

```
<ntk:AccessPolicy>
     urn:us:gov:ic:aces:ntk:mn
</ntk:AccessPolicy>
```

```
<ntk:ProfileDes>
     urn:us:gov:ic:ntk:profile:datasphere
</ntk:ProfileDes>
```

```
<ntk:AccessProfileValue
   ntk:vocabulary="datasphere:mn:issue"
     >[ISSUE]</ntk:AccessProfileValue>
```

```
<ntk:AccessProfileValue
   ntk:vocabulary="datasphere:mn:region"
     >[REGION]</ntk:AccessProfileValue>
```

C.6 - Mapping NODIS to UIAS

This section discusses the relationship of NODIS markings on data objects to the entity attributes expressed in UIAS with the focus on the agency dissemination **ntk:ProfileDes** for data markings. The ISM **ism:nonICmarkings** value of ‘ND’ requires an NODIS access policy be present.

The following Access Control Mapping table provides a mapping from specific NODIS NTK elements to concrete UIAS attributes. The use of [TYPES] below is the notional place holder for actual vocabulary types defined in NTK. [18] There may be multiple **ntk:AccessProfileValue** elements listing groups or individuals authorized for dissemination.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see Section 5.5 - No Distribution.

Table 21 - ND-NTK Access List

<table>
<tr><th>ND-NTK</th><th>UIAS Attributes</th></tr>
<tr>
<td>

ntk:AccessPolicy contains the NODIS URN

```xml
<ntk:AccessPolicy>
     urn:us:gov:ic:aces:ntk:nd
</ntk:AccessPolicy>
```

ntk:ProfileDes contains the Group & Individual URN

```xml
<ntk:ProfileDes>
     urn:us:gov:ic:ntk:profile:grp-ind
</ntk:ProfileDes>
```

zero to many groups

```xml
<ntk:AccessProfileValue
   ntk:vocabulary="group:[GRP_VOCAB]"
     >[GRP_VALUE]</ntk:AccessProfileValue>
```

zero to many individuals

```xml
<ntk:AccessProfileValue
   ntk:vocabulary="individual:[IND_VOCAB]"
     >[IND_VALUE]</ntk:AccessProfileValue>
```

</td>
<td>

The user or NPE MUST meet *at least one* of these criteria:

1. One or more IAA Service Provider Entitlement Management Service groups are listed in the NTK Access Profile and the entity's UIAS **group** attribute contains at least one [GRP_VALUE] from the Entitlement Management Service.
2. One or more individuals are listed in the NTK Access Profile and the person's UIAS **digitalIdentifier** attribute matches the [IND_VALUE] from the appropriate system identified by individual: [IND_VOCAB]
    a. When [IND_VOCAB] = 'icpki' the entity has the UIAS attribute **certificateAuthority** = 'ICPKI' and **digitalIdentifier** = [IND_VALUE]
    b. When [IND_VOCAB] = 'acsspki' the entity has the UIAS attribute **certificateAuthority** = 'ACSSPKI' and **digitalIdentifier** = [IND_VALUE]
    c. When [IND_VOCAB] = 'cadpki' the entity has the UIAS attribute **certificateAuthority** = 'CADPKI' and **digitalIdentifier** = [IND_VALUE]

</td>
</tr>
</table>

ND-NTK	UIAS Attributes
	AND If NPE, MUST have UIAS attribute **handlingControls** containing [ND]

C.7 - Mapping ORCON to UIAS

This section discusses the relationship of OC markings on data objects to the entity attributes expressed in UIAS with the focus on the agency dissemination **ntk:ProfileDes** for data markings. The ISM **ism:disseminationControls** value of 'OC' requires an ORCON access policy be present. For resources marked with 'OC-USGOV', distribution MAY be expanded beyond the implied distribution list through the use of NTK. The basic access rules and mapping of UIAS to OC-USGOV are found in ISM.ACES. If an OC-USGOV document includes NTK that expands the list of authorized dissemination agencies beyond those automatically approved for OC-USGOV, then the access rules in this appendix apply.

The following Access Control Mapping table provides a mapping from specific OC-NTK elements to concrete UIAS attributes. The '[ORIG_AGENCY]' and '[DISSEM_AGENCY]' tokens are placeholder values; these placeholders stand for actual agency acronyms used in an EXDIS NTK assertion. There may be multiple **ntk:AccessProfileValue** elements listing agencies authorized for dissemination.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see Section 5.6 - Originator Controlled.

Note

- The NTK-ACES ORCON access rule does not apply in a Secure Community of Interest (SCOI) and SCOI policies should be used instead. In a SCOI, the ORCON-NTK in a document should not be used for automated access decisions and instead use the list of authorized members of the SCOI.

Table 22 - ORCON Access Control Mapping

<table>
<tr><th>ntk:AccessProfile</th><th>UIAS Attributes</th></tr>
<tr><td>

ntk:AccessPolicy contains the ORCON URN

```
<ntk:AccessPolicy>
     urn:us:gov:ic:aces:ntk:oc
</ntk:AccessPolicy>
```

ntk:ProfileDes contains the Agency Dissemination URN

```
<ntk:ProfileDes>
     urn:us:gov:ic:ntk:profile:agencydissem
</ntk:ProfileDes>
```

exactly one originator agency

```
<ntk:AccessProfileValue
   ntk:qualifier="originator"
   ntk:vocabulary="organization:usa-agency"
     >[ORIG_AGENCY]</ntk:AccessProfileValue>
```

zero to many dissemto agencies

```
<ntk:AccessProfileValue
   ntk:qualifier="dissemto"
   ntk:vocabulary="organization:usa-agency"
     >[DISSEM_AGENCY]</ntk:AccessProfileValue>
```

</td><td>

The person or NPE MUST meet *at least one* of these criteria:

1. The person or NPE UIAS **dutyOrganization** matches [ORIG_AGENCY]
2. The person or NPE UIAS **dutyOrganization** matches one of [DISSEM_AGENCY]

AND

If NPE, MUST have UIAS attribute **handlingControls** containing [OC]

</td></tr>
</table>

C.8 - Mapping Permissive to UIAS

This section discusses the relationship of Restrictive constraints on data objects to the entity attributes expressed in the UIAS specification.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see Section 5.7 - Permissive.

Table 23 - Permissive Access Control Mapping

ntk:AccessProfile	UIAS Attribute

ntk:AccessPolicy contains the Permissive URN
`<ntk:AccessPolicy>`
`urn:us:gov:ic:aces:ntk:permissive`
`</ntk:AccessPolicy>`
ntk:ProfileDes contains the Group & Individual URN
`<ntk:ProfileDes>`
`urn:us:gov:ic:ntk:profile:grp-ind`
`</ntk:ProfileDes>`
zero to many group vocabularies:
`<ntk:AccessProfileValue`
`ntk:vocabulary="group:[GRP_VOCAB]"`
`>[GRP_VALUE]</`
`ntk:AccessProfileValue>`
and zero to many individual vocabularies:
`<ntk:AccessProfileValue`
`ntk:vocabulary="individual:[IND_VOCAB]"`
`>[IND_VALUE]</ntk:AccessProfileValue>`
	The user or NPE MUST meet *at least one* of these criteria:
	1. One or more IAA Service Provider Entitlement Management Service groups are listed in the NTK Access Profile and the entity's UIAS **group** attribute contains at least one [GRP_VALUE] from the Entitlement Management Service.
	2. One or more individuals are listed in the NTK Access Profile and the person's UIAS **digitalIdentifier** attribute matches the [IND_VALUE] from the appropriate system identified by individual: [IND_VOCAB]
	a. When [IND_VOCAB] = 'icpki' the entity has the UIAS attribute **certificateAuthority** = 'ICPKI' and **digitalIdentifier** = [IND_VALUE]
	b. When [IND_VOCAB] = 'acsspki' the entity has the UIAS attribute **certificateAuthority** = 'ACSSPKI' and **digitalIdentifier** = [IND_VALUE]
	c. When [IND_VOCAB] = 'cadpki' the entity has the UIAS attribute **certificateAuthority** = 'CADPKI' and **digitalIdentifier** = [IND_VALUE]

C.9 - Mapping PROPIN to UIAS

C.9.1 - All US Government Employee PROPIN to UIAS Mapping

This section discusses the relationship of PROPIN markings on data objects to the entity attributes expressed in UIAS. This section covers PROPIN access policy `urn:us:gov:ic:aces:ntk:propin:1`, which automatically permits dissemination to all employees of the United States Government. The ISM **ism:disseminationControls** value of ‘PROPIN’ requires a PROPIN access policy be present.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see Section 5.8 - Proprietary Information for All US Government Employees.

For the purposes of this section, the expression "[USAgencyList]" refers to the list of organizations in the USAgency[20] Agency Acronym List with namespace urn:us:gov:ic:cvenum:usagency:agencyacronym.

Table 24 - All US Government Employee PROPIN Access List

ntk:AccessProfile	UIAS Attributes
ntk:AccessPolicy contains the All USG PROPIN URN	The Person or NPE MUST meet *all* of the following: 1. Have the **entityType** UIAS attribute with a value of [MIL] or [GOV]. 2. Have the **adminOrganization** UIAS attribute exists in [USAgencyList]. AND If NPE, MUST have UIAS attribute handlingControls containing [PR]

```
<ntk:AccessProfile
   ism:classification="U"
   ism:ownerProducer="USA">
     <ntk:AccessPolicy>
          urn:us:gov:ic:aces:ntk:propin:1
     </ntk:AccessPolicy>
</ntk:AccessProfile>
```

ntk:AccessProfile	UIAS Attributes

ntk:AccessPolicy contains the All USG PROPIN URN
`<ntk:AccessPolicy>`
`urn:us:gov:ic:aces:ntk:propin:1`
`</ntk:AccessPolicy>`
ntk:ProfileDes containing the Group & Individual URN
`<ntk:ProfileDes>`
`urn:us:gov:ic:ntk:profile:grp-ind`
`</ntk:ProfileDes>`
zero or more groups
`<ntk:AccessProfileValue`
`ntk:vocabulary="group:[GRP_VOCAB]"`
`>[GRP_VALUE]</ntk:AccessProfileValue>`
zero or more individuals
`<ntk:AccessProfileValue`
`ntk:vocabulary="individual:[IND_VOCAB]"`
`>[IND_VALUE]</ntk:AccessProfileValue>`
	The Person or NPE MUST meet *at least one* of the following:
	1. The Person or NPE meets *both* A and B:
	A. Have the **entityType** UIAS attribute with a value of [MIL] or [GOV].
	B. Have the **adminOrganization** UIAS attribute exists in [USAgencyList].
	2. The person or NPE meets A or B:
	A. One or more IAA Service Provider Entitlement Management Service groups are listed in the NTK Access Profile and the entity's UIAS **group** attribute contains at least one [GRP_VALUE] from the Entitlement Management Service.
	B. One or more individuals are listed in the NTK Access Profile and the person's UIAS **digitalIdentifier** attribute matches the [IND_VALUE] from the appropriate system identified by individual: [IND_VOCAB]
	I. When [IND_VOCAB] = 'icpki' the entity has the UIAS attribute **certificateAuthority** = 'ICPKI' and

ntk:AccessProfile	UIAS Attributes
	digitalIdentifier = [IND_VALUE] II. When [IND_VOCAB] = 'acsspki' the entity has the UIAS attribute **certificateAuthority** = 'ACSSPKI' and **digitalIdentifier** = [IND_VALUE] III. When [IND_VOCAB] = 'cadpki' the entity has the UIAS attribute **certificateAuthority** = 'CADPKI' and **digitalIdentifier** = [IND_VALUE] AND If NPE, MUST have UIAS attribute **handlingControls** containing [PR]

C.9.2 - PROPIN for Specified Members to UIAS Mapping

This section discusses the relationship of PROPIN markings on data objects to the entity attributes expressed in UIAS. This section covers PROPIN access policy `urn:us:gov:ic:aces:ntk:propin:2`. This policy requires all authorized recipients to be explicitly listed in the PROPIN NTK access profile. That is, dissemination to employees of the US Government is NOT automatically authorized. The ISM **ism:disseminationControls** value of 'PROPIN' requires a PROPIN access policy be present.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see Section 5.9 - Proprietary Information for Specified Members Only.

Table 25 - Group PROPIN Access List

ntk:AccessProfile	UIAS Attributes

ntk:AccessPolicy contains the Specified Members Only PROPIN URN
`<ntk:AccessPolicy>`
`urn:us:gov:ic:aces:ntk:propin:2`
`</ntk:AccessPolicy>`
ntk:ProfileDes containing the Group & Individual URN
`<ntk:ProfileDes>`
`urn:us:gov:ic:ntk:profile:grp-ind`
`</ntk:ProfileDes>`
zero or more groups
`<ntk:AccessProfileValue`
`ntk:vocabulary="group:[GRP_VOCAB]"`
`>[GRP_VALUE]</ntk:AccessProfileValue>`
zero or more individuals
`<ntk:AccessProfileValue`
`ntk:vocabulary="individual:[IND_VOCAB]"`
`>[IND_VALUE]</ntk:AccessProfileValue>`
	The person or NPE MUST meet *at least one* of the following:
	1. One or more IAA Service Provider Entitlement Management Service groups are listed in the NTK Access Profile and the entity's UIAS **group** attribute contains at least one [GRP_VALUE] from the Entitlement Management Service.
	2. One or more individuals are listed in the NTK Access Profile and the person's UIAS **digitalIdentifier** attribute matches the [IND_VALUE] from the appropriate system identified by individual: [IND_VOCAB]
	a. When [IND_VOCAB] = 'icpki' the entity has the UIAS attribute **certificateAuthority** = 'ICPKI' and **digitalIdentifier** = [IND_VALUE]
	b. When [IND_VOCAB] = 'acsspki' the entity has the UIAS attribute **certificateAuthority** = 'ACSSPKI' and **digitalIdentifier** = [IND_VALUE]
	c. When [IND_VOCAB] = 'cadpki' the entity has the UIAS attribute **certificateAuthority** = 'CADPKI' and **digitalIdentifier** = [IND_VALUE]

ntk:AccessProfile	UIAS Attributes
	AND If NPE, MUST have UIAS attribute **handlingControls** containing [PR]

C.10 - Mapping Restrictive to UIAS

This section discusses the relationship of Restrictive constraints on data objects to the entity attributes expressed in the UIAS specification.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see Section 5.11 - Restrictive.

Table 26 - Restrictive Access Control Mapping

ntk:AccessProfile	UIAS Attribute

ntk:AccessPolicy contains the Restrictive URN
`<ntk:AccessPolicy>`
`    urn:us:gov:ic:aces:ntk:restrictive`
`</ntk:AccessPolicy>`
ntk:ProfileDes contains the Group & Individual URN
`<ntk:ProfileDes>`
`    urn:us:gov:ic:ntk:profile:grp-ind`
`</ntk:ProfileDes>`
one or more groups
`<ntk:AccessProfileValue`
`   ntk:vocabulary="group:[GRP_VOCAB]"`
`    >[GRP_VALUE]</ntk:AccessProfileValue>`
	The Person or NPE MUST meet *all* of the following:
	1. One or more IAA Service Provider Entitlement Management Service groups are listed in the NTK Access Profile and the entity's UIAS **group** attribute contains ALL of the [GRP_VALUE] values.
	Warning
	If any **ntk:vocabulary** attributes contain a group: [GRP_VOCAB] that is unknown to the system making the access control decision, then access must be denied.

Appendix D List of Abbreviations

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

AC-3	NIST 800-53r4:ACCESS ENFORCEMENT
AC-4	NIST 800-53r4:INFORMATION FLOW ENFORCEMENT
ACES	Access Control Encoding Specification
CES	Controlled Vocabulary Enumeration Encoding Specification
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
EXDIS	Exclusive Distribution
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
ICO	Intelligence Community Only
ICPG	Intelligence Community Program Guidance
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IETF	Internet Engineering Task Force
ISM	Information Security Markings
IT	Information Technology
MN	Mission Need Profile
No Distribution	Data Encoding Specification for No Distribution Need-To-Know
NPE	Non-Person Entity
NTK	Need-To-Know Metadata

OC	Originator Controlled
OCIO	Office of the Intelligence Community Chief Information Officer
OC-NTK	Originator Controlled Need-to-Know
OC-USGOV	An Originator Control marking with implied distribution to a pre-determined list of United States Government agencies.
ODNI	Office of the Director of National Intelligence
ORCON	See OC.
PDP	Policy Decision Point
PROPIN	Proprietary Information
RFC	Request for Comments
SCOI	Secure Community of Interest
UIAS	Unified Identity Attribute Set
URI	Uniform Resource Identifier
URN	Uniform Resource Name
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language

Appendix E Bibliography

Bibliography

[1] DoD Instruction 8310.01

DoD CIO. *Information Technology Standards in the DoD*. 8310.01. 2 February 2015.
Available online at: http://www.dtic.mil/whs/directives/corres/pdf/831001p.pdf

[2] 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

[3] 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]

[4] ICD 208

Office of the Director of National Intelligence. *Write For Maximum Utility*. Intelligence Community Directive 208. 17 December 2008.
Available online at: http://www.dni.gov/files/documents/ICD/icd_208.pdf

[5] ICD 209

Office of the Director of National Intelligence. *Tearline Production and Dissemination*. Intelligence Community Directive 209. 6 September 2012.
Available online at: http://www.dni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf

[6] 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

[7] 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

[8] ICD 710

Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.
Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[9] 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

[10] ICPM 2007-200-2
Office of the Director of National Intelligence. *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide*. Intelligence Community Policy Memorandum 2007-200-2 . 11 December 2007.
Available online at: http://www.dni.gov/files/documents/IC%20Policy%20Memos/ICPM%202007-200-2%20Responsibility%20to%20Provide.pdf

[11] 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

[12] ICS 500-21
Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.
Available online Intelink-TS at: http://go.ic.gov/cWyv9nw
Available online Intelink-U at: https://w3id.org/ic/standards/policy/ICS500-21

[13] 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

[14] ISM.ACES
Office of the Director of National Intelligence. *Access Control Encoding Specification for Information Security Markings (ISM.ACES)*.
Available online Intelink-TS at: http://go.ic.gov/F72Qp5x
Available online Intelink-U at: https://w3id.org/ic/standards/ISM.ACES
Available online at: https://w3id.org/ic/standards/public

[15] LIC.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for License (LIC.CES)*.
Available online Intelink-TS at: http://go.ic.gov/mssZ6bc
Available online Intelink-U at: https://w3id.org/ic/standards/LIC
Available online at: https://w3id.org/ic/standards/public

[16] 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

[17] NTK.ACES
Office of the Director of National Intelligence. *Access Control Encoding Specification for Need-To-Know (NTK.ACES)*.
Available online Intelink-TS at: http://go.ic.gov/grsUpTK
Available online Intelink-U at: https://w3id.org/ic/standards/NTK.ACES
Available online at: https://w3id.org/ic/standards/public

[18] NTK.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML)*.
Available online Intelink-TS at: http://go.ic.gov/YLXsYUX
Available online Intelink-U at: https://w3id.org/ic/standards/NTK
Available online at: https://w3id.org/ic/standards/public

[19] 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

[20] 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

[21] USGOVAgency.XML
Office of the Director of National Intelligence. *XML CVE Encoding Specification for US Government Agency Acronyms (USGOVAgency.XML)*.
Available online Intelink-TS at: http://go.ic.gov/tnYcElX
Available online Intelink-U at: https://w3id.org/ic/standards/USGOVAgency
Available online at: https://w3id.org/ic/standards/public

Appendix F Points of Contact

The Intelligence Community Chief Information Officer (IC CIO) facilitates one or more collaboration and coordination forums charged with the adoption, modification, development, and governance of IC technical specifications of common concern. This technical specification was produced by the IC CIO and coordinated with these forums, approved by the IC CIO or a designated representative, and made available at the following DNI-sponsored web sites.

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

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

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

E-mail: ic-standards-support@iarpa.gov.

Appendix G 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.[11]