



# **Intelligence Community Technical Specification**

---

## **XML Data Encoding Specification for Multi Audience Collections**

**Version 2016-SEP**

September 9, 2016

Distribution Notice:

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

# Table of Contents

Chapter 1 - Introduction .....	1
1.1 - Purpose .....	1
1.2 - Scope .....	1
1.3 - Background .....	1
1.4 - Enterprise Need .....	2
1.5 - Audience and Applicability .....	2
1.6 - Conventions .....	3
1.6.1 - Language .....	3
1.6.2 - Typography .....	3
1.6.3 - Terminology .....	3
1.6.4 - XML Namespaces .....	3
1.7 - Dependencies .....	4
1.7.1 - Standalone and Convenience Packages .....	6
1.8 - Conformance .....	7
Chapter 2 - Development Guidance .....	8
2.1 - Relationship to Abstract Data Definition and other encodings .....	8
2.2 - Additional Guidance .....	8
2.2.1 - Multi Audience Collection Usage .....	8
2.2.2 - Multi Audience Collection Elements .....	8
2.2.2.1 - MultiAudience Element .....	8
2.2.2.2 - MultiAudienceObject Element .....	9
Chapter 3 - Definitions, Interfaces, and Constraints .....	10
3.1 - Constraint Rule Types .....	10
3.2 - "Living" Constraint Rules .....	10
3.3 - Classified or Controlled Constraint Rules .....	10
3.4 - Constraint Terminology .....	10
3.5 - Errors and Warnings .....	11
3.6 - Rule Identifiers .....	11
3.7 - Data Validation Constraint Rules .....	11
3.7.1 - Purpose .....	11
3.7.2 - Schematron .....	12
3.7.3 - Non-null Constraints .....	12
3.7.4 - Inherited Constraints .....	12
3.7.5 - Value Enumeration Constraints .....	13
3.7.6 - Additional Constraints .....	13
3.7.6.1 - DES Constraints .....	13
3.7.7 - Constraint Rules .....	13
3.8 - Data Rendering Constraint Rules .....	13
3.8.1 - Purpose .....	13
3.8.2 - Rendering Constraint Rules .....	13
Chapter 4 - Conformance Validation .....	15
4.1 - Schema Validation .....	15
4.2 - Business Rule Validation .....	15
Chapter 5 - Generated Guides .....	16
5.1 - Schema Guide .....	16
5.2 - Schematron Guide .....	17

Appendix A - Feature Summary .....	18
A.1 - MAC Feature Summary .....	18
Appendix B - Change History .....	20
B.1 - V2016-SEP Change Summary .....	20
Appendix C - List of Abbreviations .....	21
Appendix D - Bibliography .....	23
Appendix E - Points of Contact .....	26
Appendix F - IC CIO Approval Memo .....	27

## List of Figures

Figure 1 - Related Specifications .....	6
---	---

## List of Tables

Table 1 - XML Namepaces .....	3
Table 2 - Dependencies .....	4
Table 3 - Relationships .....	6
Table 4 - Numerical Rule Identifier Ranges .....	11
Table 5 - Constraint Rules .....	14
Table 6 - MAC Dependency over time .....	18
Table 7 - Feature Summary Legend .....	18
Table 8 - MAC Feature Comparison .....	18
Table 9 - DES Version Identifier History .....	20
Table 10 - Data Encoding Specification V2016-SEP Change Summary .....	20

## Chapter 1 - Introduction

### 1.1 - Purpose

This *XML Data Encoding Specification for Multi Audience Collections* (MAC.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode MAC data. This Data Encoding Specification (DES) defines the XML elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing MAC data concepts using XML. This DES defines how to properly structure a valid instance of Trusted Data Format (TDF) that would conform with this specification. Use of TDF is required for compliance with this DES. A TDF may conform with multiple DES simultaneously assuming none of the criteria are in conflict.

### 1.2 - Scope

This specification is applicable to the Intelligence Community (IC) and information produced by, stored, or shared within the IC. This DES may have relevance outside the scope of intelligence; however, prior to applying outside of this defined scope, the DES 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* [\[8\]](#) 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 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* [\[13\]](#) the extensive and consistent use of Extensible Markup Language (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 encoding specification defines a concrete implementation – a file format for example – for concepts in the *IC Abstract Data Definition* <sup>[1]</sup>. Many IC encoding specifications are based on XML, but other technologies are possible. For example, IC-ID<sup>[4]</sup> defines a plain-text format for IC Identifiers as well as an associated XML structure.

## 1.4 - Enterprise Need

Broad information sharing within the national intelligence enterprise is facilitated by the creation and identification of variants of information resources to serve different audiences. The creation of variants at lower classifications or in different formats allows for wider distribution of essential intelligence, protects classified information, protects information sources and methods, and provides a mechanism to connect variants thus diminishing one possible source of circular intelligence reporting. The Office of the Director of National Intelligence (ODNI) has called out a need to write for tailored reuse and emphasized the minimization of post-production manipulation, thereby facilitating sanitation and the production of tearlines. This specification supports this need by providing the ability to tearline without any post-production changes through simple extraction of the desired rendition.

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<sup>[3]</sup>
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer<sup>[8]</sup>
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC<sup>[9]</sup>
  - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information<sup>[13]</sup>
- 200 Series:
  - Intelligence Community Directive (ICD) 208, Write for Maximum Utility<sup>[6]</sup>
  - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination<sup>[7]</sup>
  - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide<sup>[11]</sup>

## 1.5 - Audience and Applicability

This is a data encoding specification. It defines the structure and related business rules for encoding the described data type. A DES is intended for those developing tools and services that create, modify, store, exchange, search, display, or further process the type of data being described.

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*, <sup>[12]</sup> 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*,<sup>[2]</sup> 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.” [\[14\]](#) 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 1 - XML Namespaces**

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

Prefix	URI
mac	urn:us:gov:ic:mac
mime	urn:us:gov:ic:mime
xsd	http://www.w3.org/2001/XMLSchema

## 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.

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 and transitive dependencies. However, the representations may not match an exact schema import tree or dependency diagram that an analysis of the Schema, Schematron or other documents would yield. For example, the graphic only shows a given specification once even though it may actually be imported by many specifications or be a direct dependency. All specifications listed in [Table 2](#) will be shown in [Figure 1](#); however not all specifications listed in [Figure 1](#) may appear in [Table 2](#). [Figure 1](#) is to aid users in gaining a general understanding of all transitive dependencies.

**Table 2 - Dependencies**

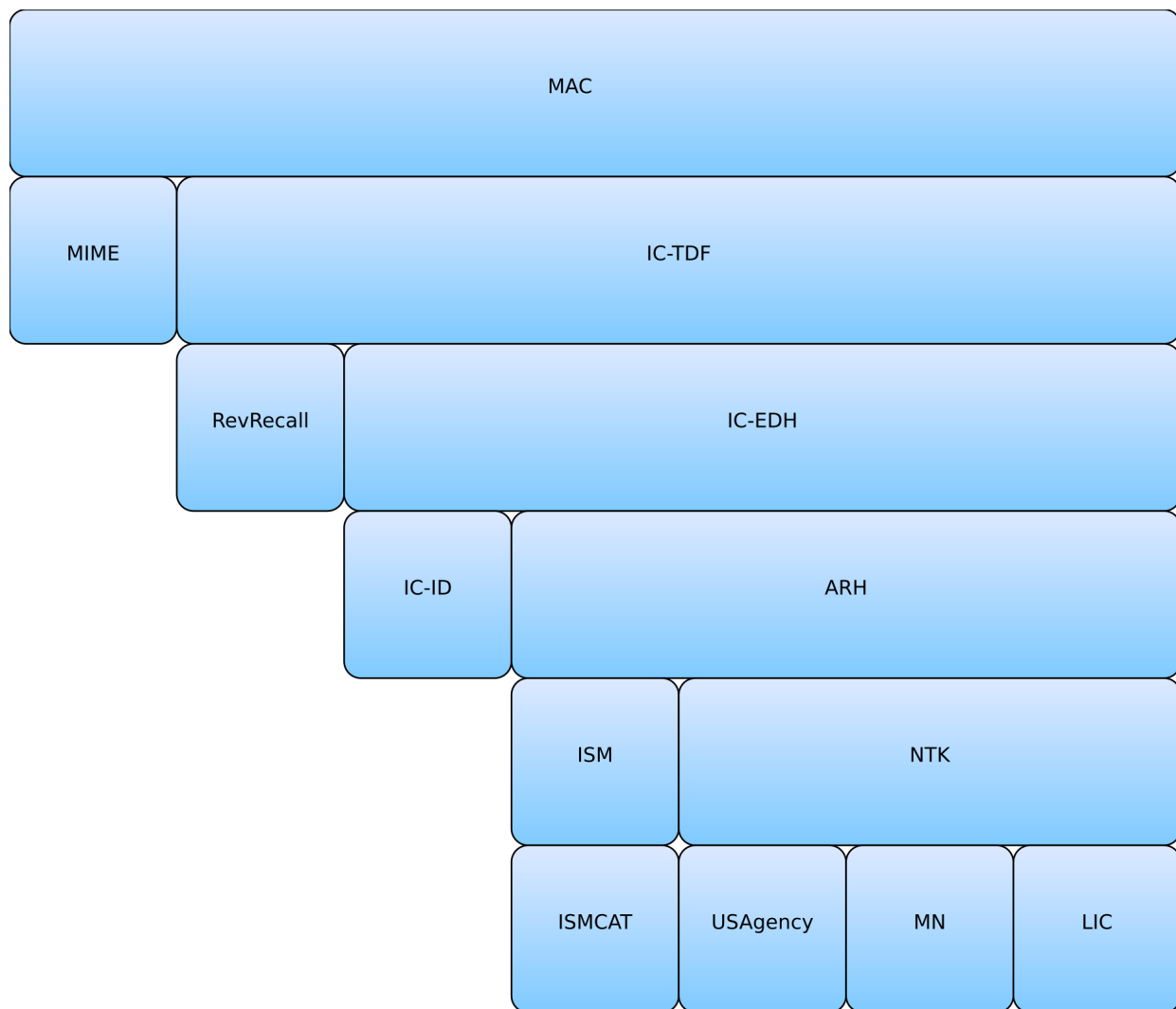
Name	Dependency Description
<i>XML Data Encoding Specification for Trusted Data Format (IC-TDF.XML.V3+)</i> <sup>[5]</sup>	MAC elements are used in conjunction with TDF collections as structured assertions that indicate how objects in a trusted data collection are related. The dependence of MAC on IC-TDF.XML is normative. This specification does not depend on a specific version of Trusted Data Format (IC-TDF.XML); IC-TDF.XML versions later than version 3 MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
<i>CVE Encoding Specification for Media Type (MIME.CES.V2016-SEP+)</i> <sup>[16]</sup>	This specification does not depend on a specific version of Media Type (MIME.CES); MIME.CES versions later than version 2016-SEP MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.

Name	Dependency Description
Schematron <sup>[19]</sup>	<p>Schematron — ISO/IEC 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative.</p> <p>The Schematron rules are normative in the sense that they convey criteria that a document <b>MUST</b> adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers <b>MAY</b> use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification.</p> <p>Note: The Schematron rules in this specification use XSLT 2.0<sup>[23]</sup> query binding.</p>
<p>XSLT 2.0<sup>[23]</sup> implementation of Schematron<sup>[19]</sup> by Rick Jelliffe (2010-04-14)</p> <p>Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following URL: <a href="http://code.google.com/p/schematron/">http://code.google.com/p/schematron/</a>.</p>	<p>The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative.</p> <p>Implementers <b>MAY</b> use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator <b>MUST</b> find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.</p>
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this DES.	Specification uses CVEs to encode controlled vocabularies. The use of the MAC CVEs is normative.

This technical specification can be used in conjunction with the additional technical specifications or additional documentation listed in the following table. The documents listed below may or may not be referenced in this Data Encoding Specification, and may or may not be considered normative or informative.

**Table 3 - Relationships**

Related Specification	Relationship Description
<i>XML Data Encoding Specification for Intelligence Publications (PUBS.XML.V*)</i> <sup>[18]</sup>	MAC elements as Trusted Data Object (TDO) assertions may be used in conjunction with PUBS.XML to describe the relationship between multiple PUBS.XML TDO payloads in a Trusted Data Collection (TDC).

**Figure 1 : Related Specifications**

### 1.7.1 - 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 transitive dependent 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.

## 1.8 - Conformance

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and any Schematron<sup>[19]</sup> rules are normative for this specification. The rest of this document and the rest of this package, including the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and PDF CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119<sup>[14]</sup> is considered normative within the scope of the sentence. All other parts of this document are informative.

The XML schemas provided may import other specifications. The versions of dependency specifications imported are not normative in that to import a different version of a component specification you could modify the import or substitute a different version of the component using the existing import path. This could be done by changing the schema file or by using XML Catalogs.<sup>[21]</sup> For example, a schema could be changed to incorporate a different version of a dependency like ISM by changing the attribute declaration of **@ism:DESVersion='9'** to **@ism:DESVersion='10'** in the `xsd:schema` statement. The ability to specify which version of a dependent specification to import enables the configuration change control of parent specifications (such as PUBS and TDF) to be "decoupled" from the configuration change control of dependent specifications (such as ISM CVE updates). This "decoupling" method has not been in place for all versions of these parent specifications; therefore, please verify with the dependency table to ensure use of allowed dependency versions.

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.

## Chapter 2 - Development Guidance

### 2.1 - Relationship to Abstract Data Definition and other encodings

The relationship of the XML structures defined in this encoding specification to the abstract terms defined in the ADD are described using a mapping table in the ADD. The mapping tables generally show the mapping to the encoding specification where a structure is defined, not where it is used. These mappings are provided for reference only. The complete set of encoding specification artifacts, both normative and informative, should be consulted in order to gain a complete understanding of this encoding specification.

The mappings in the ADD provide a starting point for the development of automated transformations between formats defined by the encoding specifications. However, it should be noted that when these transformations are used between formats with different levels of detail there might be some data loss.

### 2.2 - Additional Guidance

This section provides additional guidance for encoding data in specific situations. In particular, situations for which there is not clearly a single method of encoding the data are documented here. The content of this section will evolve over time as additional situations are identified. Implementers of this DES are encouraged to contact the maintainers of this DES for further guidance when necessary.

#### 2.2.1 - Multi Audience Collection Usage

MAC.XML is used in conjunction with TDF collections as structured assertions that indicate how objects in a trusted data collection are related. A Trusted Data Collection conforms to the MAC.XML specification when it contains:

- A structured assertion of scope TDC with a MultiAudience element
- Optional: A structured assertion of scope PAYL in a TrustedDataObject element may also appear to provide additional information about each object in the collection regarding its relationship to the larger collection. In this way, MAC.XML can be used to describe a set of tearlined assets, or other related data sets as needed.

#### 2.2.2 - Multi Audience Collection Elements

MAC.XML consists of two elements, MultiAudience and MultiAudienceObject, which are used in conjunction with a Trusted Data Collection to indicate the relationship between objects within the collection.

##### 2.2.2.1 - MultiAudience Element

The MultiAudience element is used with a Trusted Data Collection (TDC) as a structured assertion with scope TDC. In this context, the instance should be representative of the entire package

including all variants. The DESVersion attribute indicates the MAC.XML version, and the multiAudienceType attribute indicates the type of collection. Common multiAudienceType types may be "Tearline" and "Format." A multiAudienceType of "Tearline" indicates that the collection consists of variants of an original asset which have been modified for audiences of different clearance levels. A multiAudienceType of "Format" indicates that the collection consists of the same asset in different formats, such as PDF, DOC, and DOCX.

Example:

```
<Assertion tdf:scope="TDC">
  <StatementMetadata>
    <Security xmlns="urn:us:gov:ic:arh"
      ism:classification="U"
      ism:ownerProducer="USA" />
  </StatementMetadata>
  <StructuredStatement>
    <mac:MultiAudience
      mac:DESVersion="1"
      mac:multiAudienceType="Tearline" />
  </StructuredStatement>
</Assertion>
```

## 2.2.2.2 - MultiAudienceObject Element

The MultiAudienceObject element is intended to be used with a Trusted Data Collection (TDC) as a structured assertion with scope TDO. In this context, the element should be representative of aspects of the object that are important to know in order to understand how it relates to the rest of the collection. The @mac:original attribute indicates which object is the original in a collection of variants. For example, if the @mac:multiAudienceType="Format" in a TDC that contained TDOs, one with a Docx and one with a PDF and the TDO with the Docx had the @mac:original="true" it would indicate that the PDF is derived from the original Docx. The @mime:mimeType element indicates the underlying format of the object, in the case where the collection consists of variants of the same asset in different formats.

Example:

```
<Assertion tdf:scope="TDO">
  <StatementMetadata>
    <Security xmlns="urn:us:gov:ic:arh"
      ism:classification="U"
      ism:ownerProducer="USA" />
  </StatementMetadata>
  <StructuredStatement>
    <mac:MultiAudienceObject
      mac:original="true" />
  </StructuredStatement>
</Assertion>
```

## Chapter 3 - Definitions, Interfaces, and Constraints

### 3.1 - Constraint Rule Types

Data constraint rules fall into two categories - validation and rendering constraints. Data validation constraints explicitly define policy validation constraints, describing how data should be structured and encoded in order to comply with IC policy. Validation constraint rules are implemented as a combination of basic XML Schema constraints and supplemental constraints for more complex rules. Complex constraint rules contain technical rule descriptions, Schematron rule implementations, and *Human Readable* descriptions. The human readable text describes the intent and meaning behind the more technical rule description. The semantics of the constraint rules are normative, whereas the use of the Schematron implementation is informative. Implementers developing alternative validation code should follow the technical rule descriptions and Schematron logic. Should there be a perception of conflict, implementers should bring it to the attention of the appropriate configuration control body for resolution. Rendering constraint rules define constraints on the display and rendering of documents. While expressed in a similar manner to the data validation constraint rules, there is no expectation that evaluation of these rules can be automated; rather these rules should inform the evaluation of a system's capabilities and functionality.

### 3.2 - "Living" Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a valid starter set and do not attempt to address the full scope of business rules addressed by authoritative guidance. These rules will be expanded and modified as the model matures, and as applicable security marking policies change.

Since these constraint rules are only a subset of the entire rule base, an XML document that is compliant with these rules may still not be fully compliant with all of the business rules defined in the authoritative guidance. An XML document that is not compliant with these rules is not compliant with the authoritative guidance.

### 3.3 - Classified or Controlled Constraint Rules

Additional rules that are either classified or have handling controls can be found in separate annexes closely associated with the encoding specification artifacts wherever they are located.

### 3.4 - Constraint Terminology

For the purposes of this document, the following statements apply:

- The term "is specified" indicates that an attribute is applied to an element and the attribute has a non-null value.
- The term "must be specified" indicates that an attribute **MUST** be applied to an element and the attribute **MUST** have a non-null value.
- The term "is not specified" indicates that an attribute is not applied to an element, or an attribute is applied to an element and the attribute has a null value.



- The term “must not be specified” indicates that an attribute **MUST NOT** be applied to an element.

## 3.5 - Errors and Warnings

The severity of a constraint rule violation is categorized as either an “Error” or a “Warning.” An “Error” is more severe and is indicative of a clear violation of a constraint rule, which would be likely to have a significant impact on the quality of a document. A “Warning” is less severe although noteworthy, and may not necessarily have any impact on the quality of a document. The severity of a constraint rule violation is indicated in brackets preceding each constraint rule description.

Each system responsible for processing a document (e.g., create, modify, transform, or exchange) **MUST** make a mission-appropriate decision about using a document with errors or warnings based on mission needs.

## 3.6 - Rule Identifiers

Each constraint rule has an assigned rule identifier, indicated in brackets preceding the constraint rule description. MAC.XML data validation constraint rule identifiers are prefixed with “MAC-ID-” and followed by a 5 digit unique number, assigned from pre-defined ranges to group rules by classification. The numerical ranges are described in [Section 3.6 - Rule Identifiers \[11\]](#). As the constraint rules are managed over time, IDs from deleted rules will not be reused.

**Table 4 - Numerical Rule Identifier Ranges**

Rule Identifier Range		Description
Start	End	
00001	09999	Reserved for Unclassified constraint rules
10001	19999	Reserved for Unclassified but For Official Use Only (FOUO) constraint rules
20001	20999	Reserved for constraint rules classified at the “Secret//REL USA, FVEY” level
21001	21999	Reserved for constraint rules classified at the “Secret//NF” level
22001	29999	Reserved for constraint rules classified at the “Secret//TBD” level
30001 and above		Reserved for constraint rules classified with other classifications

## 3.7 - Data Validation Constraint Rules

### 3.7.1 - Purpose

The MAC.XML schema defines the data elements, attributes, cardinalities and parent-child relationships for which XML instances must comply. Validation of these syntax aspects is an important first step in the validation process. An additional level of validation is needed to ensure that the content complies with the constraints as specified in applicable IC policy guidance and codified in these constraint rules. Traditional schema languages are generally unable to effectively represent these additional constraints.

## 3.7.2 - Schematron

Schematron<sup>[19]</sup> is the formal language used in this specification to encode normative data validation constraints. The Schematron rules are normative in the sense that they convey criteria a document **MUST** meet, exactly as English may be used to convey normative criteria.

It is not necessary for implementers to use the specific Schematron encoding in this specification, and implementers **MAY** use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator **MUST** find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

For better understanding, the Schematron<sup>[19]</sup> rules for this specification may be executed in *Oxygen*<sup>[17]</sup> or with an XSLT 2.0-compliant processor using the XSLT 2.0<sup>[23]</sup> transforms in the Schematron implementation from Rick Jelliffe (see [XSLT 2.0 implementation of Schematron by Rick Jelliffe](#) in the Dependency table).

The constraint rules for this specification are dependent on XPath 2.0<sup>[22]</sup> and XSLT 2.0<sup>[23]</sup> features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:<sup>[15]</sup>

By default, Schematron uses the XPath language as used in XSLT 1.0, and is typically implemented by converting the schema into an XSLT 1.0 script which is run against the document being validated. However, ISO Schematron also allows XSLT 2.0 to be used, and this is becoming an increasingly popular choice because of the extra expressive convenience of XPath 2.0: a different skeleton is available for this.



### Note

For convenience, the specification package provides the XSLT 2.0<sup>[23]</sup> implementation of Schematron<sup>[19]</sup> along with a compiled version of the rules.

## 3.7.3 - Non-null Constraints

XML syntax allows all elements with content declared to be of data type “string” to have zero or more characters of content, meaning elements can be empty or null. According to this specification, all required elements (and certain conditional elements) **MUST** have content, other than white space.<sup>1</sup> Elements, which are allowed to only have text content, **MUST** have text content specified.

## 3.7.4 - Inherited Constraints

In an instance of MAC.XML, the use of attributes and elements from supplementary data encoding specifications must be fully conformant with the constraint rules defined in those specifications. For a full list of supplementary specifications, see [Section 1.7 - Dependencies](#).

<sup>1</sup>“White space” is defined in XML 1.0<sup>[20]</sup> as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

## 3.7.5 - Value Enumeration Constraints

Several elements and attributes of the MAC.XML model use Controlled Vocabulary Enumerations (CVEs) to define the data allowed in the element or attribute. In some cases the specific CVE is specified via an attribute, which may include a default CVE. Further, in some of the cases where the CVE can be specified, the attribute may restrict the list of CVEs allowed and some may allow for the author to specify their own CVE. For each of these, the value must be in the specified external CVE or the default CVE.

Some CVEs are not available on all networks. A subset CVE will be provided for use on networks not approved for the entire list. If the processing will occur on a network where the entire CVE is not available, the subset CVE may be substituted in the constraint rules since the excluded values would be excluded from use on the lower network.

As noted in the specific rules, a failure of validation against a CVE will generate an Error.

## 3.7.6 - Additional Constraints

### 3.7.6.1 - DES Constraints

The DES version is specified through attributes on the root element. The schema constrains the values of these attributes. The **DESVersion** attribute enables systems processing an instance document to be certain which set of constraint rules, schema, CVEs and business rules are intended by the author to be used.

## 3.7.7 - Constraint Rules

The detailed constraint rules for the MAC.XML schema can be found in a separate document inside the SchematronGuide directory, in the MAC\_Rules.pdf file. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron. Obsolete rule numbers are listed in the SchematronGuide.

## 3.8 - Data Rendering Constraint Rules

### 3.8.1 - Purpose

Rendering rules define constraints on the rendering and display of MAC.XML documents. The intent is to inform the development of systems capable of rendering or displaying MAC.XML data for use by individuals not familiar with the details of the MAC.XML markup. While expressed in a similar manner to the data validation constraint rules above, there is no expectation that evaluation of these rules can be automated; rather these rules should inform the evaluation of a system's capabilities and functionality.

### 3.8.2 - Rendering Constraint Rules

The following table contains the information for the MAC.XML data rendering constraint rules.

**Table 5 - Constraint Rules**

Rule Number	Severity	Description	Human Readable Description
There are no Data Rendering Constraint rules at this time.			

## Chapter 4 - Conformance Validation

An instance document conforms with this specification if it conforms to all normative guidance of this specification and this specification's dependencies and it passes all of the following validation steps. This specification does not dictate how this validation strategy is implemented.

### 4.1 - Schema Validation

An instance document **MUST** comply with the schemas for this specification and this specification's dependencies, and schema validation **SHOULD** occur prior to other validation steps. If schema validation fails, results from later steps may be indeterminate.

### 4.2 - Business Rule Validation

An instance document **MUST** comply with the business rules expressed in this specification and those expressed in this specification's dependencies. The business rules in this specification are expressed in Schematron, but it is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers **MAY** use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator **MUST** find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

## Chapter 5 - Generated Guides

### 5.1 - Schema Guide

The detailed description and reference documentation for the MAC.XML schema can be found as a collection of HTML files inside the SchemaGuide directory. These files comprise a guide that serves as an interactive presentation of the MAC.XML schema as well as an implementation-specific data element dictionary.

The guide was generated with a commercially available product named *oXygen®*, produced by SyncRO Soft.

The guide provides an interactive index to:

- Global Elements and Attributes
- Local Elements and Attributes
- Simple and Complex Types
- Groups and Attribute Groups
- Referenced Schemas

Where applicable, the guide provides:

- Diagram
- Namespace
- Type
- Children (Child Elements)
- Used by
- Properties
- Patterns
- Enumerations
- Attributes
- Annotations
- Source Code

The guide is published in a folder consisting of the master HTML file *SchemaGuide.html* with supporting graphics.

## 5.2 - Schematron Guide

The detailed description and reference documentation for the MAC.XML Schematron rules can be found in a separate document named *MAC\_Rules.pdf*, which is located inside the SchematronGuide directory. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron.

Appendix A Feature Summary

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

Table 6 - MAC Dependency over time

Dependent Specification	V1	V2016-SEP
IC-TDF*	V1+	V3+
ISM	V9+	V13+
NTK	V7+	V10+
ARH	V1+	V3+
IC-EDH	V1+	V4+
MIME*	V1+	V2016-SEP+
ISMCAT	V1+	V2015-MAY+
USAgency	V1+	V2015-FEB+
MN	V1+	V2015-FEB+
LIC	V1+	V2015-FEB+
IC-ID	V1+	V1+
RevRecall	V1+	V1+

The following table summarizes major features by version for this MAC and all dependent specs.

Table 7 - 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. MAC Feature Summary

Table 8 - MAC Feature Comparison

MAC Feature Comparison			
Required date	Feature	V1	v2016-SEP
	Collection of Tearline	F	F
	Collection of Formats	F	F
	Declaration of Original Object	F	F



MAC Feature Comparison			
Required date	Feature	V1	v2016-SEP
	Version decoupling, allowing import of any version of ISM and other dependent specifications at or above ISM v9+, NTKv7+, ARHv1+, TDFv1+, and EDHv1+	F	F
	MimeTypes controlled by the MIME CES	N	F

## Appendix B Change History

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

**Table 9 - DES Version Identifier History**

Version	Date	Purpose
1	14 January 2013	Initial Release
2016-SEP	9 September 2016	Routine revision to technical specification. For details of changes, see <a href="#">Section B.1 - V2016-SEP Change Summary</a>

### B.1 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Changes to use MIME.CES

The following table summarizes the changes made to V1 in developing V2016-SEP.

**Table 10 - Data Encoding Specification V2016-SEP Change Summary**

Change	Artifacts changed	Compatibility Notes
Refactored schema to use MIME.CES <sup>[16]</sup> (CR-2015-107)	Schema	Systems need to be updated to accommodate this change including the new mimeType attribute from MIME.CES.
Added Schematron rule to enforce minimum version of TDF.	Added rule 00003.	Systems need to be updated to accommodate this change.
The schema change logs will no longer be maintained as of the 2016-SEP release. The existing change logs will only serve as legacy information. For changes to schema as of and after 2016-SEP, reference the change history in the DES.	Schema	No impact to systems.
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 List of Abbreviations

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

ADD	Abstract Data Definition
ARH	Access Rights and Handling
CES	Controlled Vocabulary Enumeration Encoding Specification
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
EDH	Enterprise Data Header
ESB	Enterprise Standards Baseline
FOUO	For Official Use Only
HTML	HyperText Markup Language
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
IC-ID	IC Identifier
ICD	Intelligence Community Directive
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISM	Information Security Markings
ISMCAT	Information Security Marking Country Codes and Tetragraphs
ISO	International Organization for Standardization
IT	Information Technology

LIC	License
MAC	Multi Audience Collection
MIME	Multipurpose Internet Mail Extensions
MN	Mission Need Profile
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PUBS	Intelligence Publications
RFC	Request for Comments
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
USAGENCY	Controlled Vocabulary Enumeration Encoding Specification for US Agencies
URL	Uniform Resource Locator
XML	Extensible Markup Language
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

## Appendix D Bibliography

### Bibliography

[1] ADD

Office of the Director of National Intelligence. *Intelligence Community Abstract Data Definition (IC-ADD.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/soSC6M8>

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

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

[2] 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>

[3] 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>

[4] IC-ID.XML

Office of the Director of National Intelligence. *Text and XML Data Encoding Specification for Intelligence Community Identifier (IC-ID.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/mQ4IUDk>

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

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

[5] IC-TDF.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Trusted Data Format (TDF.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/sonBSai>

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

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

[6] 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](http://www.dni.gov/files/documents/ICD/icd_208.pdf)

[7] 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>

[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](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](http://www.dni.gov/files/documents/ICD/ICD_501.pdf)
- [10] 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>
- [11] 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>
- [12] 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>
- [13] 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>
- [14] 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>
- [15] Jelliffe  
Richard Alan Jelliffe. *FAQ. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?*.  
Available online at: <http://www.schematron.com>
- [16] MIME.CES  
Office of the Director of National Intelligence. *XML CVE Encoding Specification for Media Type (MIME.CES)*.
- [17] Oxygen  
SyncRO Soft. *<oXygen/> XML Editor*.

Available online at: <http://www.oxygenxml.com/>

[18] PUBS.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Intelligence Publications (PUBS.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/0rezXle>

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

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

[19] Schematron

International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron*. ISO/IEC 19757-3:2006.

ISO Spec Available online at: <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

StyleSheets for compiling Available online at: <http://code.google.com/p/schematron/>

[20] XML 1.0

World Wide Web Consortium (W3C). *Extensible Markup Language (XML) 1.0, Second Edition*. W3C, 6 October 2000.

Available online at: <http://www.w3.org/TR/2000/REC-xml-20001006>

[21] XML Catalogs

The Organization for the Advancement of Structured Information Standards [OASIS]. *XML Catalogs*. Committee Specification 06 Aug 2001.

Available online at: <https://www.oasis-open.org/committees/entity/spec-2001-08-06.html>

[22] XPath2

World Wide Web Consortium (W3C). *XML Path Language (XPath) 2.0 (Second Edition)*. W3C Recommendation 14 December 2010 (Link errors corrected 3 January 2011).

Available online at: <http://www.w3.org/TR/xpath20/>

[23] XSLT2

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

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

## Appendix 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](mailto: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.<sup>[12]</sup>