Intelligence Community Technical Specification

XML Data Encoding Specification for Trusted Data Format

Version 1

17 July 2012

Table of Contents

List of Tables

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for Trusted Data Format* (IC-TDF.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode IC-TDF 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 trusted data format data concepts using XML.

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 IC Chief Information Officer (IC CIO) is leading the IC's enterprise transformation to an “interoperable federated architecture.” Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer* [6] grants the IC CIO the authority and responsibility to:

- Develop an IC Enterprise Architecture (IC EA).
- Lead the IC's identification, development, and management of IC enterprise standards.
- Incorporate technically sound, deconflicted, 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 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 ICS 500-21,[9] the extensive and consistent use of Extensible Markup Language (XML) within data encoding specifications allows for improved data exchanges and processing of information, thereby achieving the IC's data discovery, data sharing, and interoperability goals.

A DES specifies how to implement the abstract data elements in the IC.ADD in a particular physical encoding (e.g., data or file format). For example:

- DESs for textual markup formats, such as Extensible Markup Language (XML) and HyperText Markup Language (HTML), define markup elements and attributes, their relationships, cardinalities, processing requirements, and use.

- DESs for display formats, such as text and Adobe Portable Document Format (PDF), define text and typographic conventions, cardinalities, processing requirements, and use.

- DESs for application-specific formats, for e.g. Microsoft Word, define document properties; styles; fields; cardinalities; processing requirements; and use.

1.4 - Enterprise Need

Information sharing within the national intelligence enterprise will increasingly rely on information assurance metadata (including enterprise data headers) to allow interagency access control, automated exchanges, and appropriate protection of shared intelligence. A structured, verifiable representation of security metadata bound to the intelligence data is required in order for the enterprise to become inherently "smarter" about the information flowing in and around it. Such a representation, when implemented with other data formats, improved user interfaces, and data processing utilities, can provide part of a larger, robust information assurance infrastructure capable of automating some of the management and exchange decisions today being performed by human beings.

The Intelligence Community (IC) has standardized the various classification and control markings established for information sharing within the Information Security Markings (ISM), Need-To-Know (NTK), Information Resource Metadata (IRM), Enterprise Data Header (EDH), and Access Rights and Handling (ARH) XML specifications of the Intelligence Community Enterprise Architecture (ICEA) Data Standards. The IC Trusted Data Format XML specification further expands on this body of work, adapting and extending it as necessary for TDF to function as the IC submission format for binding assertion metadata with data resource(s). This TDF functionality supports the IC way ahead strategy of implementing secure cloud-based information exchange and discovery on the IC Enterprise.

1.5 - Audience and Applicability

DESs are primarily intended to be used by those developing tools and services to create, modify, store, exchange, search, display, or further process the type of data being described.

The conditions of use and applicability of this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*,[8] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

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

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

1.6 - Conventions

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

The keywords "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" in this technical specification are to be interpreted as described in the IETF RFC 2119.[10] These implementation indicator keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

Certain typography is used throughout the body of this document to 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

1.7 - Conformance

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

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

Informative: serving to instruct or enlighten or inform.

The XML schemas, CVE values from the XML CVE files, and the Schematron[20] code version of the constraint rules are normative for this DES. 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 HTML CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119[10] is considered normative within the scope of the sentence. All other parts of this document are informative.

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.

1.8 - Dependencies

This technical specification depends on 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 1 - Dependencies

Name
XML Data Encoding Specification for Information Security Marking (ISM.XML.V9)[12]
XML Data Encoding Specification for Information Resource Metadata (IRM.XML.V8)[11]
XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML.V7)[16]
XML Data Encoding Specification for Enterprise Data Header (EDH.XML.V1)[EDH.XML]
XML Data Encoding Specification for Access Rights and Handling (ARH.XML.V1)[ARH.XML]
Department of Defense Discovery Metadata Specification [1] (DDMS 4.1)
ISO Schematron [20]implementation by Rick Jelliffe (2010-04-14)
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this DES.

Chapter 2 - Development Guidance

2.1 - Relationship to Abstract Data Definition and other encodings

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

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

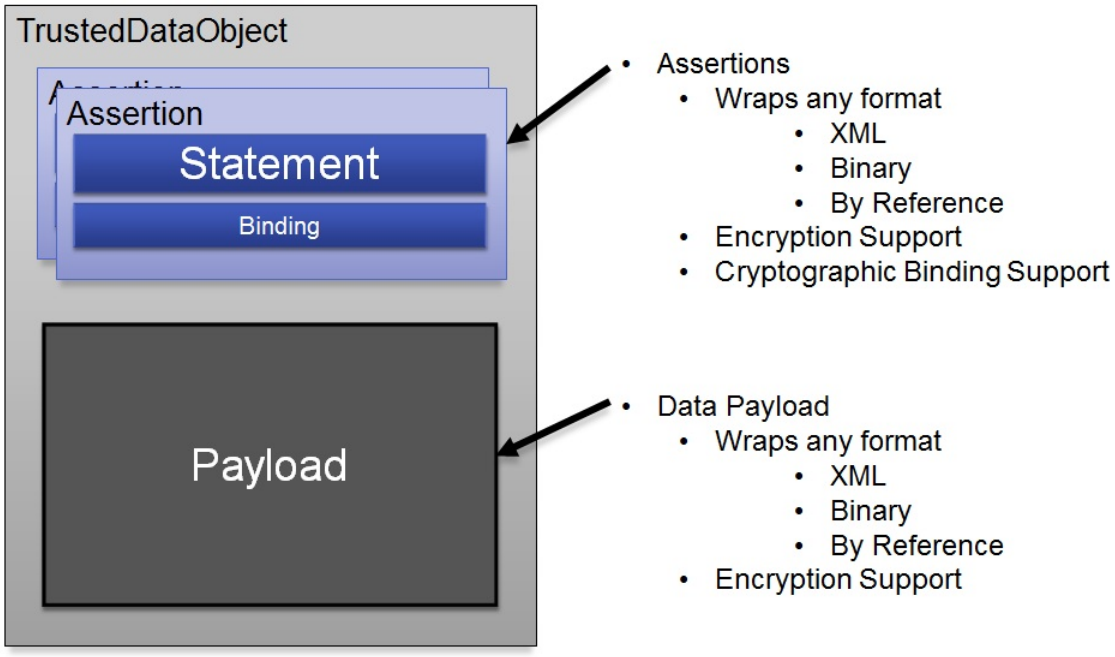
2.2 - Additional Guidance

Developer guidance for using particular sections of the specification to securely wrap data for IC Cloud ingest.

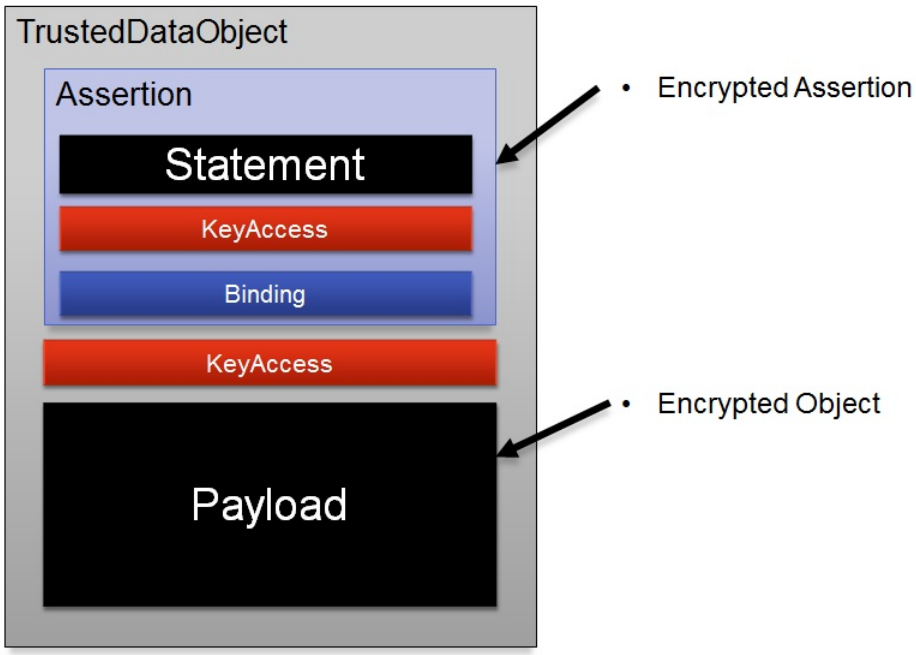
2.2.1 - TDF Structure

The TDF.XML specification has a consistent and simple concept of Assertions and Payloads. There are two options for root elements: TrustedDataObject (TDO) and TrustedDataColleciton (TDC). A TDO contains some data (the payload) and some statements about that data (the assertions). In the context of TDF, an 'assertion' is defined as a statement providing handling, discovery, or mission metadata describing a payload, TDO, or TDC, depending on the scope of the assertion. Each TDO must contain at least one handling assertion, which provides the minimum information needed to protect the data. Additional discovery and mission assertions may also be provided. A TDC contains a list of TDOs (the payload) and some statements about those TDOs (the assertions).

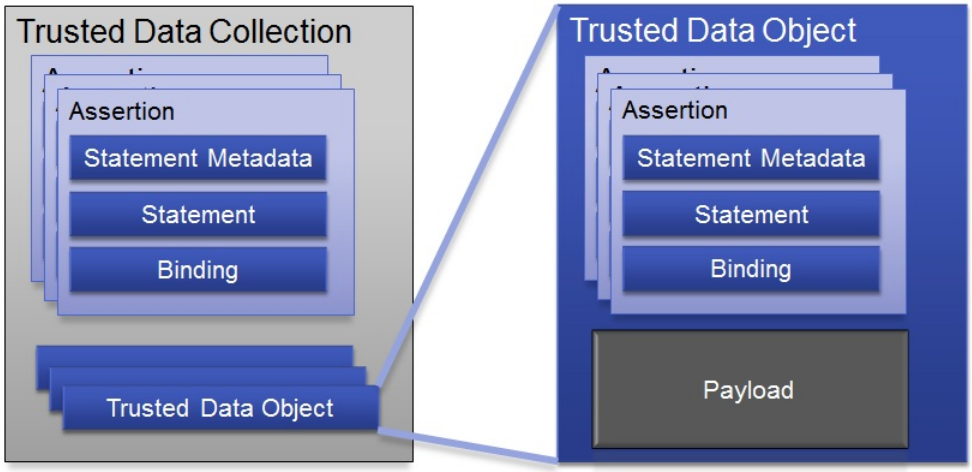
Each trusted data object consists of one or more assertions and a payload. At minimum, a handling assertion is required. Assertions may optionally be cryptographically bound to the payload to provide assurance over the integrity of the assertion, the payload, and the relationship between the assertion and payload.



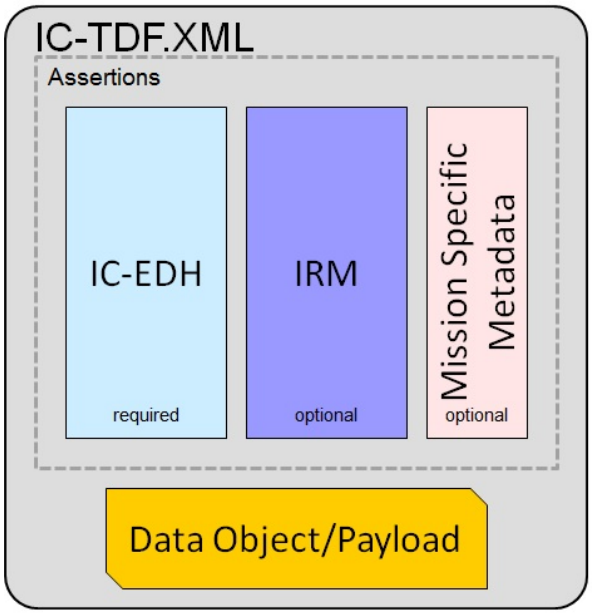
In a scenario where encryption is required, the TDO assertion statements and/or TDO payload may be optionally encrypted:



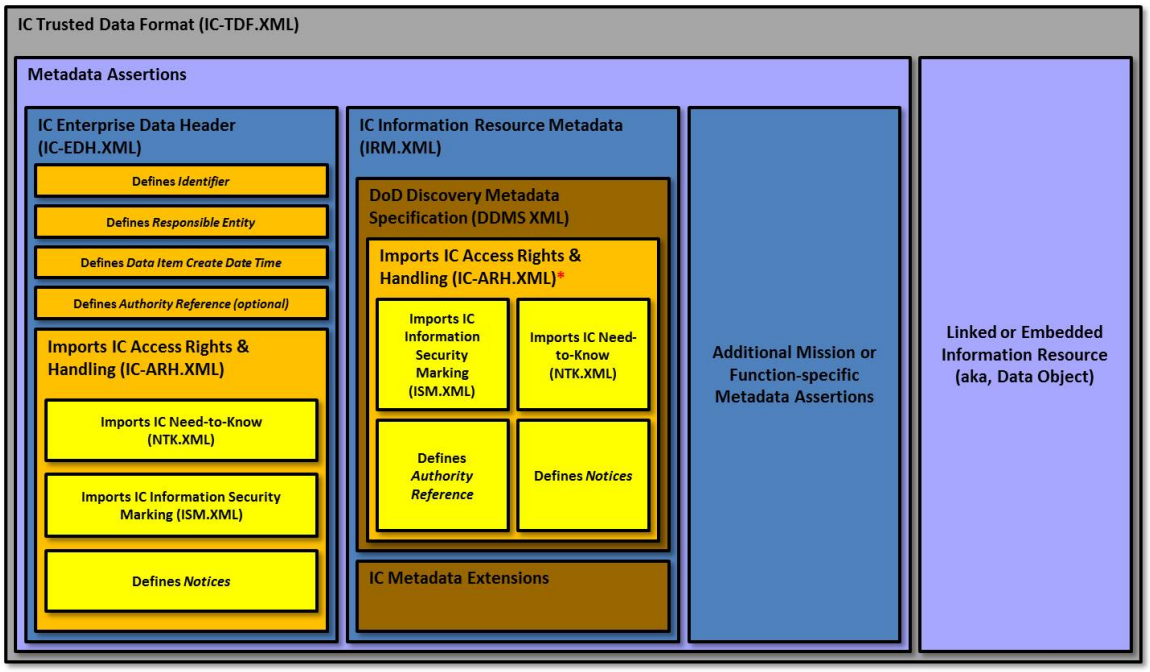
Trusted Data Collection consists of a collection of trusted data objects. It is expected but not required that the TDOs in a TDC are in some way related, with relationships encoded in the TDC assertions. For example, in a biometric use case, a TDC might correspond to a biometric identity, with TDOs corresponding to biometric modalities, such as finger prints, iris scans, and facial images. In this biometric use case the TDC assertions would describe the entire identity, while the TDO assertions would describe the individual modalities.



Each TDO requires at least one handling assertion, optional discovery and mission assertions, and a payload. The handling assertion must consist of a structured IC-EDH block. A common discovery assertion might be a structured IRM block. Mission specific metadata may consist of a a structured block (XML) or unstructured data (binary). The payload may be structured XML, unstructured data, or a reference.



The diagram below shows expected use of IC specifications within a Trusted Data Object. The use of the IC-EDH handling assertion and payload are required, where the discovery and mission specific assertions are optional.



2.2.2 - Assertions

2.2.2.1 - Handling Assertions

To facilitate handling and access control decisions, each TDO must contain at least one HandlingAssertion. A HandlingAssertion is a special type of structured assertion that contains the IC Enterprise Data Header for the TDO or payload, providing the attributes needed for policy decisions regarding access control and how the data must be handled. ISM and NTK markings are contained in Handling Assertions, as part of the Access Rights and Handling block.

2.2.2.2 - Assertion Scope

Assertions can be scoped to apply either to the entire Trusted Data Object, the payload only, or both. In the case of handling assertions, generally, two handling assertions are expected, one scoped to the entire TDO, and the other scoped to the payload only. This allows for separate access control decisions to be made for the discovery metadata versus the payload. To avoid redundancy, a single assertion may be scoped to apply to both the payload and TDO if and only if there are no other assertions present. In future versions, the concept of scope will be extended to support a flexible, explicit list of bound elements.The scope of assertions in various scenarios can be observed in the table below.

Table 2 - Assertion Scope

Scenario	Assertion Level	Scope Tokens	Applies To	TDO Payload	TDO Assertions	TDO	TDC Assertions
1	TDO	PAYL	To TDO Payload	X			
2	TDO	TDO	To TDO Payload and each Assertion (other than self) within TDO	X	X		
3	TDC	PAYL	To a list of TDOs			X	
4	TDC	TDC	To a list of TDOs and each Assertion (other than self) within TDC			X	X
5	TDO	TDO PAYL	To TDO Payload when there are no other assertions present	X	N/A	X	
6	*TDO or TDC*	*EXPLICIT*	*Anything contained in the bound value list*				

Note

Scope of EXPLICIT is not yet supported, and will require either reference list or a bound value list. In either case the "scope" of an EXPLICIT assertion is solely determined by the values in the reference list or bound value list.

2.2.2.3 - Mission-Specific Metadata Assertions

Missions may create their own unique set of assertions, no understanding by the enterprise beyond access control is assured. The Assertion @type is intended to provide additional context, allowing various systems to pre-determine relevance of assertions without parsing or

reading all of the assertions. Assertion @type might include categorizations such as 'discovery,' 'mission,' or 'task order' to allow various systems to determine which assertions are relevant for them to parse.

2.2.2.4 - Assertions and Data State

If a TDO payload or assertion statement is encrypted, there are in fact two potentially different markings needed for decision making, analysis and querying, one describing the handling required for the encrypted blob, and the other for the handling required for the unencrypted (and in effect external) state. In cases where statements and/or payloads are encrypted, allow handling assertions and statement metadata elements to indicate whether their marks apply to the encypted blob state vs. actual data by using an attribute “appliesToState.” This attribute may be leveraged in use cases such as:

- A user or system knows that they are not allowed to have/process data with NTK systemXYZ, and the user/system wants to query a large IC cloud repo and filter out results that require systemXYZ handling. For results with encrypted payloads, if the handling assertion only reflects the encypted blob handling (say Confidential) the user/system could get back thousands of encrypted results they can’t decrypt, shouldn’t see, and don’t want to sort through.

- Agency X publishes data to the IC cloud with encrypted payloads. In a decrypted state, the payload requires NTK markings that IC cloud cannot yet handle access-wise. In this case, when the markings in an assertion apply to state 'encrypted,' they should be part of rollup and used for the handling of the TDO. When the markings in an assertion apply to state 'unencrypted' they should be excluded from rollup, and used for search filtering, or access and processing decisions in systems that are able to decrypt the payload.

2.2.3 - IRM as a TDO Assertion

An entire IRM.XML record may be placed in an assertion. If the IRM record described a TDO payload it would be contained in the StructuredStatement element of an Assertion within a TDO with the scope attribute of the Assertion set to PAYL.

2.2.4 - Binding and BindingInfo

A key concept in the TDF specification is the ability to cryptographically assure the relationship among portions of the document. This assurance is represented by the optional **Binding** element available on each Assertion and HandlingAssertion.

The **Binding** element includes information about the key used to calculate the signature, the **SignatureValue**, and an optional **BoundValueList**. To simplify initial usage of Binding in IC-TDF version 1, the BoundValueList is currently not allowed in the IC-TDF, but will be supported in future versions to provide more granular binding functionality. A **BoundValueList** is a container of bound value references that point to the elements that are included in a cryptographic binding. The **idref** attribute of **BoundValue** or **Reference** element is the internal instance reference to the element being bound.The intent of the **BoundValueList** is to allow granular control over the scope of the binding signature. In the future, when BoundValueList is present , the **SignatureValue** will be calculated over the normalized value of the

BoundValueList using the normalization method denoted in the **Binding/SignatureValue/ @normalizationMethod** attribute.

In IC-TDFv1, where the **BoundValueList** is never present, the **SignatureValue** is always calculated over a concatenation of the normalized portions of the document in the same order they appear in the document described by the Assertion.

The normalization method expressed in **Binding/SignatureValue/@normalizationMethod** and **Binding/BoundValueList/BoundValue/@normalizationMethod** is a URI that provides guidance on how to format the included values such as whitespace, attributes, and child nodes in a universally consistent manner. The normalization method is essential to prevent formatting such as whitespace and order from interfering with the validation of the cryptographic integrity of data. For example, XML canonicalization is one form of normalization that might be utilized. More information on XML canonicalization is available online at: W3C Canonical XML [http://www.w3.org/TR/xml-c14n]. To use XML canonicalization as a normalization method, provide the URI to the form of XML canonicalization you are using, such as http://www.w3.org/TR/2001/REC-xml-c14n-20010315 [http://www.w3.org/TR/2001/REC-xml-c14n-20010315] as the value for the **Binding/SignatureValue/@normalizationMethod**.This example URL is the URL defined in XML-SEC Rec for inclusive c14n without comments.

The expected portions of the document that each scope MUST include in the **SignatureValue** are detailed in the table below. (Note: this table assumes that **BoundValueList** is not utilized to provide granular integrity across the portions, further guidance on the use of **BoundValueList** is coming soon).

Table 3 - Binding Contents

XPath	Included in Binding

TrustedDataObject/ Assertion[@scope='PAYL']	• Required
	  • Assertion/Statement
	  • TrustedDataObject/Payload
	• Optional
	  • Assertion/StatementMetadata; if Binding/ SignatureValue/ @includesStatementMetadata='true'

XPath	Included in Binding

TrustedDataObject/ Assertion[@scope='TDO']	• Required
	  • TrustedDataObject//HandlingAssertion/ HandlingStatement
	  • TrustedDataObject//Assertion/Statement
	  • TrustedDataObject/Payload
	• Optional
	  • TrustedDataObject//Assertion/ StatementMetadata; if Binding/ SignatureValue/ @includesStatementMetadata='true'

TrustedDataObject/ HandlingAssertion[@scope='PAYL']	• Required
	  • HandlingAssertion/HandlingStatement
	  • TrustedDataObject/Payload

TrustedDataObject/ HandlingAssertion[@scope='TDO']	• Required
	  • TrustedDataObject//HandlingAssertion/ HandlingStatement
	  • TrustedDataObject//Assertion/Statement
	  • TrustedDataObject/Payload
	• Optional
	  • TrustedDataObject//Assertion/ StatementMetadata; if Binding/ SignatureValue/ @includesStatementMetadata='true'

TrustedDataCollection/ Assertion[@scope='PAYL']	• Required
	  • Assertion/Statement
	  • TrustedDataCollection//TrustedDataObject
	• Optional
	  • Assertion/StatementMetadata; if Binding/ SignatureValue/ @includesStatementMetadata='true'

XPath	Included in Binding

TrustedDataCollection/ Assertion[@scope='TDC']	• Required
	  • TrustedDataCollection//HandlingAssertion/ HandlingStatement
	  • TrustedDataCollection//Assertion/ Statement
	  • TrustedDataCollection//TrustedDataObject
	• Optional
	  • TrustedDataCollection//Assertion/ StatementMetadata; if Binding/ SignatureValue/ @includesStatementMetadata='true'

TrustedDataCollection/ HandlingAssertion['PAYL']	• Required
	  • HandlingAssertion/HandlingStatement
	  • TrustedDataCollection//TrustedDataObject
	• Optional
	  • Assertion/StatementMetadata; if Binding/ SignatureValue/ @includesStatementMetadata='true'

TrustedDataCollection/ HandlingAssertion[@scope='TDC']	• Required
	  • TrustedDataCollection//HandlingAssertion/ HandlingStatement
	  • TrustedDataCollection//Assertion/ Statement
	  • TrustedDataCollection//TrustedDataObject
	• Optional
	  • TrustedDataCollection//Assertion/ StatementMetadata; if Binding/ SignatureValue/ @includesStatementMetadata='true'

2.2.5 - Normalization Method

The normalization method expressed in Binding/SignatureValue/@normalizationMethod and Binding/BoundValueList/BoundValue/@normalizationMethod is a URI that provides guidance on how to format the included values such as whitespace, attributes, and child nodes in a

universally consistent manner. The normalization method is essential to prevent formatting such as whitespace and order from interfering with the validation of the cryptographic integrity of data. For example, XML canonicalization is one form of normalization that might be utilized. The table below lists several XML canonicalization URLs.

Table 4 - Sample URLs for XML Canonicalization Normalization Methods

Sample NormalizationMethod URL	Description
http://www.w3.org/TR/2001/REC-xml-c14n-20010315	The URL defined in XML-SEC Rec for inclusive c14n without comments.
http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments	The URL defined in XML-SEC Rec for inclusive c14n with comments.
http://www.w3.org/2001/10/xml-exc-c14n#	The URL defined in XML-SEC Rec for exclusive c14n without comments..
http://www.w3.org/2001/10/xml-exc-c14n#WithComments	The URL defined in XML-SEC Rec for exclusive c14n without comments..
http://www.w3.org/2006/12/xml-c14n11	The URI for inclusive c14n 1.1 without comments..
http://www.w3.org/2006/12/xml-c14n11#WithComments	The URI for inclusive c14n 1.1 with comments..

2.2.6 - Encryption and EncryptionInfo

A key concept in the TDF specification is the ability to encrypt payloads, assertions, and keys. Whenever content is encrypted, encryption information must be provided. Encryption information can contain either KeyAccess or EncryptionMethod information, providing the information necessary for decryption or key retrieval. Onion or layered encryption is also supported. In this case, there will be multiple KeyAccess and/or EncryptionMethod elements within one EncryptionInformation element. Encryption information is required to be provided in a first-in-last-out order, where the first KeyAccess or EncryptionMethod element corresponds to the outermost layer of encryption. For example, this layered or onion encryption may be required in a use case where both a system and a user must provide certificates before information can be decrypted. Encryption Method allows key size, algorithm, and Optimal Asymmetric Encryption Padding Scheme (OAEP)[17] information.

2.2.7 - Linked or Embedded Data Objects

Linked objects classification does NOT impact the classification of the TDO. Embedded objects classification does impact the classification of the TDO.

2.2.8 - MIME type

The Multipurpose Internet Mail Extensions (MIME) type for a IC-TDF.XML document is application/dni-tdf+xml. This is a convention for our community. This type has NOT been registered with the Internet Assigned Numbers Authority (IANA). Should there be a conflict in

the future it will be addressed at that time. Systems can use this MIME type to facilitate communications and address business needs within the community.

Chapter 3 - Data Validation Constraint Rules

Constraint Rules explicitly define the validation constraints for IC-TDF.XML. They provide additional restrictions (i.e., constraints) on how the data should be structured and encoded, especially for criteria that exceed the constraints implemented in the XML Schema. These rules are written in plain English phrases; however, knowledge of the IC-TDF.XML schemas is required to understand the rules. Complex constraint rules may be followed by text labeled *Human Readable*. This text is intended to inform the intent of the more formal language above it. Implementers are intended to implement the formal language, and should there be a perception of conflict, bring it to the attention of the appropriate configuration control body to be resolved.

3.1 - Basics

The IC-TDF.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.

3.1.1 - Schematron

Schematron[20] was selected as the language in which to encode these additional rules. The provided Schematron[20] is used to define the constraint rules; it is NOT a required implementation. Implementers can use any tools at their disposal as long as the data complies with the rules expressed. To facilitate testing and understanding of the rules they are executable in either *oXygen*® [19] or the XSLT 2.0[24] implementation of ISO Schematron[20] provided by Rick Jelliffe at http://schematron.com/ [http://schematron.com/]. Constraint rules are dependent on XPath 2.0[23] and XSLT 2.0[24] features. According to Mr. Jelliffe, the editor of Schematron[20] for ISO:

> "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."

Included in the package are the ISO Schematron[20] implementation and XSLT 2.0[24] files provided as a convenience along with a compiled version of the rules.

3.1.2 - “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 logic that may be required. These rules will be expanded and modified as the model matures, and as policy is issued constraining the use of TDF.

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.

3.1.3 - 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 DES artifacts wherever they are located.

3.1.4 - 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.

3.1.5 - Rule Identifiers

Each constraint rule has an assigned rule ID, indicated in brackets preceding the constraint rule description. The rule IDs from 00001 to 10000 are unclassified and 10001 to 20000 are “for official use only” (FOUO). IDs from 20001 to 30000 are reserved for “Secret” rules and 30001 and above for more classified rules. IC-TDF.XML data validation constraint rule IDs are prefixed with “IC-TDF-ID-”.

As the constraint rules are managed over time, IDs from deleted rules will not be reused.

3.1.6 - 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.

3.2 - 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 — which allows for empty (or null) content. According to this specification, all required elements (and certain conditional elements) must have content, other than white space. [1] Elements, which are allowed to only have text content, must have text content specified.

3.3 - Inherited Constraints

In an instance of IC-TDF.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 1.8 - Dependencies .

3.4 - Value Enumeration Constraints

Several elements and attributes of the IC-TDF.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.

3.5 - Additional Constraints

3.5.1 - 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.

3.6 - Constraint Rules

The detailed constraint rules for the IC-TDF.XML schema can be found in a separate document inside the SchematronGuide directory, in the IC-TDF_Rules.pdf file. This document is generated from the individual Schematron files to provide a single searchable document for all of the

[1] "white space" is defined in XML 1.0[22] as "(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs."

constraint rules encoded in Schematron. Obsolete rule numbers are listed in the SchematronGuide.

Chapter 4 - Data Rendering Constraint Rules

The constraint rules in this chapter define constraints on the rendering of IC-TDF.XML documents. The intent is to inform the development of systems capable of rendering or displaying IC-TDF.XML data for use by individuals not familiar with the details of the IC-TDF.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.

4.1 - Basics

4.1.1 - "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 TDF rendering issues. These rules will be expanded and modified as the model matures, and as policy is issued regarding TDF rendering.

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.

4.1.2 - 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 DES artifacts wherever they are located.

4.1.3 - Rule Identifiers

Each constraint rule has an assigned rule ID, indicated in brackets preceding the constraint rule description. The rule IDs from 00001 to 10000 are unclassified and10001 to 20000 are “for official use only” (FOUO). IDs from 20001 to 30000 are reserved for Secret rules and 30001 and above for more classified rules. IC-TDF.XML data rendering constrain rule IDs are prefixed with “IC-TDF-RENDER-”.

As the constraint rules are managed over time, IDs from deleted rules will not be reused.

4.1.4 - Errors and Warnings

The severity of a constraint rule violation is categorized as either an “Error” or a “Warning” and is indicated in brackets preceding each constraint rule description. 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 system. A “Warning” is less severe although noteworthy, and may not necessarily have any impact on the quality of a system.

Each system responsible for rendering documents must be evaluated based on its use. Those evaluating the system must make a mission-appropriate decision about the system's suitability for use.

4.2 - Constraint Rules

The following table contains the information for the IC-TDF.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 5 - Generated Guides

5.1 - Schema Guide

The detailed description and reference documentation for the IC-TDF.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 IC-TDF.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
- 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 IC-TDF.XML Schematron rules can be found in a separate document named *IC-TDF_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 TDF on other DES.

Table 6 - TDF Dependency over time

Dependent DES	V1
ISM	V9
IRM	V8
IC-EDH	V1
NTK	V7
ARH	V1

The following table summarizes major features by version for this TDF 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)
Cell Colors represent the same information as the Key value	

A.1. IC-TDF Feature Summary

Table 8 - IC-TDF Feature comparison

IC-TDF Feature Comparison		
Required date	Feature	V1
	Mime Types	F

A.2. ISM Feature Summary

Table 9 - ISM Feature comparison

ISM Feature Comparison										
Driver Required date	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9
CAPCO Register and Manual 2.1 January 22, 2009 (1 year after 2008 memo)	Declass Removed from Banner	N	F	F	F	F	F	F	F	F

ISM Feature Comparison										
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
E.O. 13526[5] December 29, 2009	Compilation Reason	N	F	F	F	F	F	F	F	F
CAPCO Register and Manual 3.1 May 7, 2010	LES	P	N	F	F	F	F	F	F	F
CAPCO Register and Manual 3.1 May 7, 2010	LES-NF	P	N	F	F	F	F	F	F	F
CAPCO Register and Manual All versions Pre 2008	Require Notices	N	N	F	F	F	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2010	KDK	N	N	F	F	F	F	F	F	F
ICD 710[7] September 11, 2009	710 Foreign Release	P	P	F	F	F	F	F	F	F
E.O. 13526[5] December 29, 2009	DeclassReasons/Dates	P	P	F	F	F	F	F	F	F
IC-CIO enhance data quality See IC ESB	schema validation of CVE values	N	N	N	F	F	F	F	F	F
DoD Directive 5230.24[3] March 18, 1987	DoD Distro Statements	N	N	N	F	F	F	F	F	F
DoD Directive 5240.01[4] August 27, 2007	US Person Notice	P	P	P	P	F	F	F	F	F
CAPCO Register and Manual 2.2 September 25, 2010 (1 Year after 2.2)	Remove SAMI	P	P	P	P	F	F	F	F	F
ISOO Marking Booklet 2010[14] / ISOO Notice 2009-13[15] December 2010	Remove exempted source	P	P	P	P	F	F	F	F	F

ISM Feature Comparison										
Driver Required date	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9
E.O. 13526[5] December 29, 2009	derivativelyClassifiedBy	P	P	P	P	F	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	Atomic Energy New banner location	N	N	N	N	F	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	Display Only	N	N	N	N	F	F	F	F	F
IC-CIO enhance data quality See IC ESB	Schematron[20] Implementation of rules	N	N	N	N	F	F	F	F	F
E.O. 13526[5] December 29, 2009	50X1-Hum 50X2-WMD	N	N	N	N	F	F	F	F	F
DoD Directive 5200.1-R[2] January 1997	DoD ACCM Markings	N	N	N	N	N	F	F	F	F
CAPCO Register and Manual 4.2 May 31, 2011	SSI	N	N	N	N	N	F	F	F	F
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)[13] June 28, 2010	TFNI	N	N	N	N	N	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2010	HCS SubCompartments	N	N	N	N	N	F	F	F	N
CAPCO Register and Manual 4.1 November 16, 2010 (date disestablished)	MCFI Remove	P	P	P	P	P	F	F	F	F
CAPCO Register and Manual 4.2 May 31, 2011	MIFH, EUDA and EFOR removed	P	P	P	P	P	P	F	F	F

ISM Feature Comparison										
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)[13] June 28, 2010	Multivalue declassException	F	N	N	N	N	N	F	F	F
IC-CIO enhance data quality See IC ESB	SouthSudan	N	N	N	N	N	N	F	F	F
ICD 710[7] September 11, 2009	710 POC	N	N	N	N	N	N	F	F	F
DNI ORCON Memo [18] March 11, 2011	ORCON POC	N	N	N	N	N	N	F	F	F
ISOO Marking Booklet[14] December 2010	Allow 50X1-HUM and 50X2-WMD to not have a date/event	N	N	N	N	N	N	F	F	F
IC-CIO enhance data quality See IC ESB	RD, FRD, and Sigma rolldown enforced	N	N	N	N	N	N	N	F	F
December 30, 2012	Unclassified REL, RELIDO, NF, and DISPLAYONLY	N	N	N	N	N	N	N	F	F
IC-CIO enhance data quality See IC ESB	@ism:excludeFromRollup=true() allowed to not have an ICD-710 foreign release indicator	N	N	N	N	N	N	N	F	F
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	SINFO Remove	P	P	P	P	P	P	P	F	F
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	SC Remove	P	P	P	P	P	P	P	F	F
CAPCO Register and Manual 5.1 December 30, 2011	RSV	N	N	N	N	N	N	N	F	F
CAPCO Register and Manual 5.1 December 30, 2011	Require using 50X1-HUM instead of 25X1-human	N	N	N	N	P	P	P	F	F

ISM Feature Comparison										
Driver Required date	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9
CAPCO Register and Manual 5.1 December 30, 2011	Allow use of KDK SubCompartments and Sub-SubCompartments	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 5.1 December 30, 2011	Allow use of SI SubCompartments and Sub-SubCompartments	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 5.1 Annex A	Allow use of OSTY Open Skies	N	N	N	N	N	N	N	N	F
IC-CIO enhance data quality	External Notice	N	N	N	N	N	N	N	N	F
DoD Directive 5200.1-R[2] February 2012	COMSEC Notice	N	N	N	N	N	N	N	N	F
DoD Directive 5200.1-R[2] February 2012	Support for NNPI	N	N	N	N	N	N	N	N	F

A.3. NTK Feature Summary

Table 10 - NTK Feature comparison

NTK Feature Comparison								
Required date	Feature	V1	V2	V3	V4	V5	V6	V7
	Schematron[20] Implementation of rules	N	N	F	F	F	F	F
	Portion Level NTK	N	N	N	N	N	N	F

A.4. IRM Feature Summary

Table 11 - IRM Feature comparison

IRM Feature Comparison									
Required date	Feature	V1	V2	V3	V4	V5	V6	V7	V8
	Mime Types	N	F	F	F	F	F	F	F
	Schematron[20] Implementation of rules	N	N	F	F	F	F	F	F
	ORCON Memo[18] support	P	P	P	P	F	F	F	F
	XLink 1.1[21]	N	N	N	N	F	F	F	F
	Allow more than 3 decimal places on times	N	N	N	N	N	N	F	F

IRM Feature Comparison									
Required date	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**
	MinDiscoverable and MinAccessible modes	N	N	N	N	N	N	N	F

Appendix B Change History

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

Table 12 - DES Version Identifier History

Version	Date	Purpose
1	17 July 2012	Initial Release

Appendix C Acronyms

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

Table 13 - Acronyms

Name	Definition
ATO	Authority To Operate
BNF	Backus-Naur Form
CAPCO	Controlled Access Program Coordination Office
CVE	Controlled Vocabulary Enumeration
DAA	Designated Approval Agent
DCMI	Dublin Core Metadata Initiative
DC MES	Dublin Core Metadata Element Set
DES	Data Encoding Specification
DOI	Digital Object Identifier
DN	Distinguished Name
DNI	Director of National Intelligence
E.O.	Executive Order
ES&IS	Enterprise Search & Integration Services
GNS	Geographic Names Server
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
I2	Information Integration
IC	Intelligence Community
IC.ADD	Intelligence Community Abstract Data Definition
IC CIO	Intelligence Community Chief Information Officer
IC ESB	Intelligence Community Enterprise Standards Baseline
ICD	Intelligence Community Directive
ICEA	Intelligence Community Enterprise Architecture
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IETF	Internet Engineering Task Force
ISBN	International Standard Book Number
ISM	Information Security Marking
ISO	International Organization for Standardization

Name	Definition
ISOO	Information Security Oversight Office
KA	Knowledge Assertion
KOS	Knowledge Organization System
MIME	Multipurpose Internet Mail Extensions
NARA	National Archives and Records Administration
NGA	National Geospatial Intelligence Agency
NGT	Next Generation Trident
NSI	National Security Information
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PK	Private Key
RDBMS	Relational Database Management System
REST	REpresentational State Transfer
RFC	Request for Comments
SSD	Special Security Directorate
SSL	Secure Socket Layer
SOAP	Simple Object Access Protocol
TGN	Thesaurus of Geographic Names
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
W3CDTF	World Wide Web Consortium Date Time Format
XML	Extensible Markup Language

Appendix D Bibliography

Bibliography

[1] DDMS
Department of Defense. *DoD Discovery Metadata Specification*. 4.0.1.
Available online at: http://metadata.dod.mil/mdr/irs/DDMS/

[2] DoD Directive 5200.1
Under Secretary of Defence for Intelligence. *DoD Information Security Program:*. 5200.1. February 24, 2012.
Vol 1 Available online at: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf
Vol 2 Available online at: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf
Vol 3 Available online at: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf
Vol 4 Available online at: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf

[3] DoD Directive 5230.24
Secretary of Defense. *Distribution Statements on Technical Documents*. 5230.24. 18 March 1987.
Available online at: http://www.dtic.mil/dtic/pdf/submit/523024p.pdf

[4] DoD Directive 5240.01
Secretary of Defense. *DoD Intelligence Activities*. 5240.01. August 2007.
Available online at: http://www.dtic.mil/dtic/pdf/submit/5240.01.pdf

[5] E.O. 13526
The White House. *Executive Order 13526 – Classified National Security Information*. 29 December 2009.
Available online at: http://www.archives.gov/isoo/pdf/cnsi-eo.pdf

[6] ICD 500
Director of National Intelligence Chief Information Officer. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.
Available online at: http://www.dni.gov/electronic_reading_room/ICD_500.pdf

[7] ICD 710
Director of National Intelligence Chief Information Officer. *Classification and Control Markings System*. Intelligence Community Directive 710. 11 September 2009.
Available online at: http://www.dni.gov/electronic_reading_room/ICD_710.pdf

[8] 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 at: https://www.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS-500-21.aspx

[9] 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 at: https://www.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS-500-21.aspx

[10] 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

[11] IRM.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Resource Metadata (IRM.XML)*.
Available online IntelLinkU at: http://purl.org/IC/Standards/IRM
Available online IntelLinkU at: http://purl.org/IC/Standards/public

[12] ISM.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML)*.
Available online IntelLinkU at: http://purl.org/IC/Standards/ISM
Available online at: http://purl.org/IC/Standards/public

[13] ISOO 32 CFR Parts 2001 and 2003
Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *Classified National Security Information; Final Rule*. 32 CFR Parts 2001 and 2003. Federal Register, Vol. 75, No. 123. 28 June 2010.
Available online at: http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.pdf

[14] ISOO Marking Booklet
Information Security Oversight Office. *Marking Classified National Security Information*. December 2010.
Available online at: http://www.archives.gov/isoo/training/marking-booklet.pdf

[15] ISOO Notice 2009-13
Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *ISOO Notice 2009-13: Prohibited Use of X1-X8 Markings*.
Available online at: http://www.archives.gov/isoo/notices/notice-2009-13.pdf

[16] NTK.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML)*.
Available online IntelLinkU at: http://purl.org/IC/Standards/NTK
Available online at: http://purl.org/IC/Standards/public

[17] OAEP
Mihir Bellare. Phillip Rogaway. *Optimal Asymmetric Encryption Padding Scheme (OAEP)*.
Available for purchase at: http://dx.doi.org/10.1007/BFb0053428

Conference online at: http://www.informatik.uni-trier.de/~ley/db/conf/eurocrypt/eurocrypt94.html

[18] ORCON Memo
Director of National Intelligence. *Guiding Principles for Use of the ORCON Marking and for Sharing Classified National Intelligence with U.S. Entities*. 29 March 2011.
Available online at: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/Guiding%20Principles%20for%20Use%20of%20the%20ORCON%20Markings_ES%2000045.pdf
Attachment A: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20A.doc.pdf
Attachment B: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20B.pdf
Attachment C: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20C.pdf

[19] Oxygen
SyncRO Soft. *<oXygen/> XML Editor*. version 13.2.
Available online at: http://www.oxygenxml.com/

[20] Schematron
International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron*. ISO/IEC 19757-3:2006.
Available online at: http://www.schematron.com/

[21] XLink
World Wide Web Consortium (W3C) . *XML Linking Language (XLink) Version 1.1*. W3C Recommendation 06 May 2010.
Available online at: http://www.w3.org/TR/2010/REC-xlink11-20100506/

[22] 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/

[23] 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/

[24] 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 DNI-sponsored web sites. Direct all inquiries about this IC technical specification to the IC CIO, an IC technical specification collaboration and coordination forum, or IC element representatives involved in those forums.

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.[8]