Intelligence Community Technical Specification

XML Data Encoding Specification for Trusted Data Format

Version 2

14 January 2013

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

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

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

Table of Contents

List of 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* [10] 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,[16] 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.

Enterprise needs and requirements for this specification can be found in the following ODNI policies and implementation guidance.

- IC Information Technology Enterprise (IC ITE)

  - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan[7]

- 500 Series:

  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[11]

  - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information[16]

- 200 Series:

- Intelligence Community Directive (ICD) 208, Write for Maximum Utility[8]
- Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination[9]
- Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide[14]

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*, [15] 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.[17] 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 - Dependencies

This technical specification depends on the additional technical specifications or additional documentation listed in the following table. The documents listed below are referenced in this

Data Encoding Specification, and are normative or informative as indicated in the dependencies table.

Table 1 - Dependencies

Name	Dependency Description
XML Data Encoding Specification for Information Security Marking (ISM.XML.V9+) [18]	Depends on Information Security Markings (ISM). Starting with ISM v9, the version of ISM imported is no longer normative, so any ISM version 9 or above may be used.
XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML.V7+)[23]	Depends on Need To Know (NTK) markings. Starting with NTK v7, the version of NTK imported is no longer normative, so any NTK version 7 or above may be used.
XML Data Encoding Specification for Enterprise Data Header (IC-EDH.XML.V1+)[5]	Depends on Enterprise Data Header (EDH) Specification. Starting with EDH v1, the version of EDH imported is no longer normative, so any EDH version 1 or above may be used.
XML Data Encoding Specification for Access Rights and Handling (ARH.XML.V1+)[1]	Depends on Access Rights and Handling(ARH) Specification. Starting with ARH v1, the version of ARH imported is no longer normative, so any ARH version 1 or above may be used.
ISO Schematron [27]implementation by Rick Jelliffe (2010-04-14)	Specification uses Schematron to encode IC business rules. Conformance to the logic of the business rules is normative, whereas use of the schematron language to encode them is informative.
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 IC-TDF CVEs is normative.

1.8 - Conformance

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

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

Informative: serving to instruct or enlighten or inform.

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and the Schematron[27] 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[17] 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 [29]. 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 import different versions of dependent specifications decouples parent specifications like PUBS and TDF from changes to dependency specifications, such as ISM CVE updates. The decoupling of dependency versions is not retroactive, see the dependency table for allowed dependency versions.

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.

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 - 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 TrustedDataCollection (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. To facilitate handling and access control decisions, each TDO and TDC 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. 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). A TDC may also be a collection of collections, and contain other TDCs.

Each TDO consists of one or more assertions and a payload. 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.

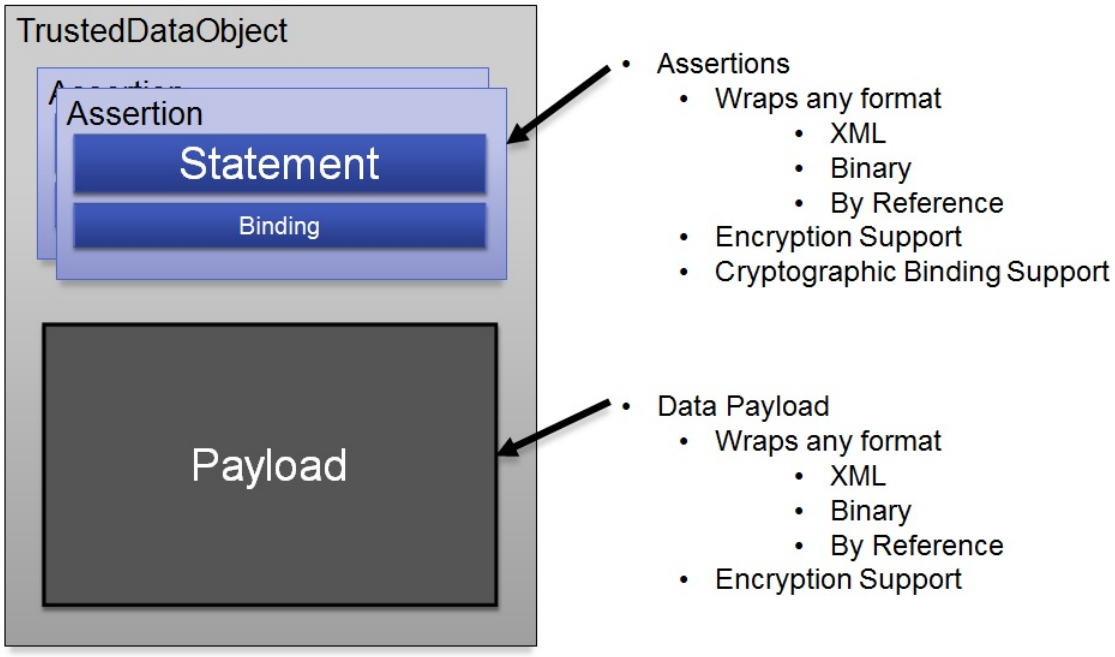

Figure 2 - Simple TDO

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

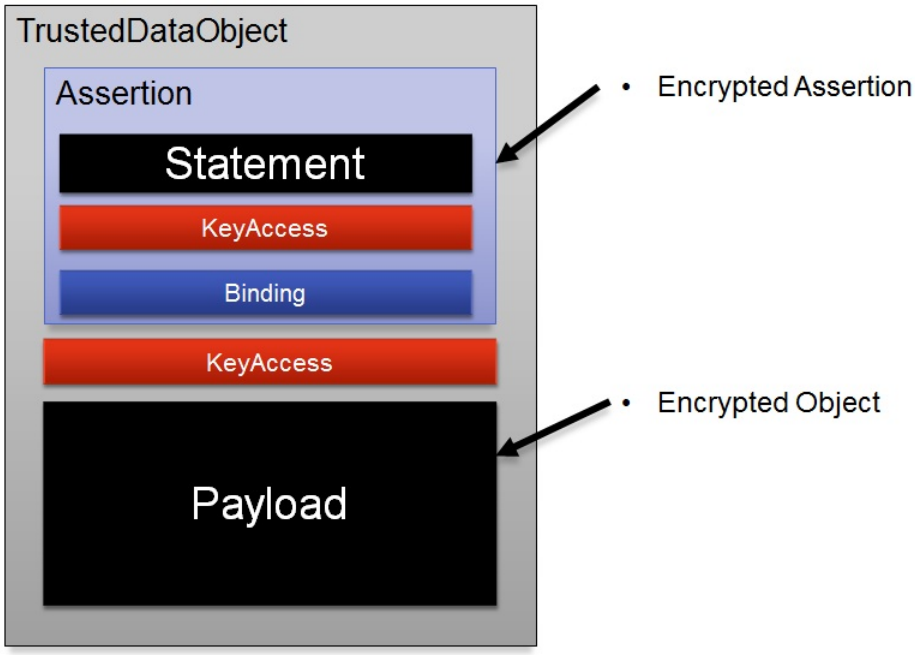

Figure 3 - TDO with Encryption

Each IC-TDF 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 structured block (XML) or unstructured data (binary). The payload may be structured XML, unstructured data, or a reference.

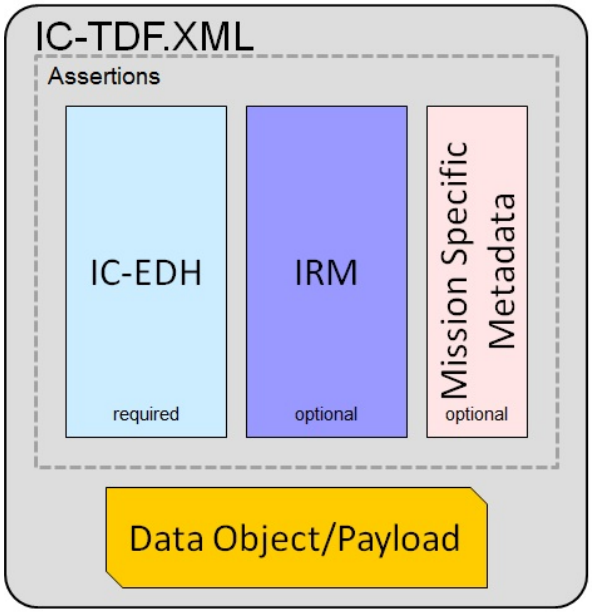

Figure 4 - TDF Structure

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

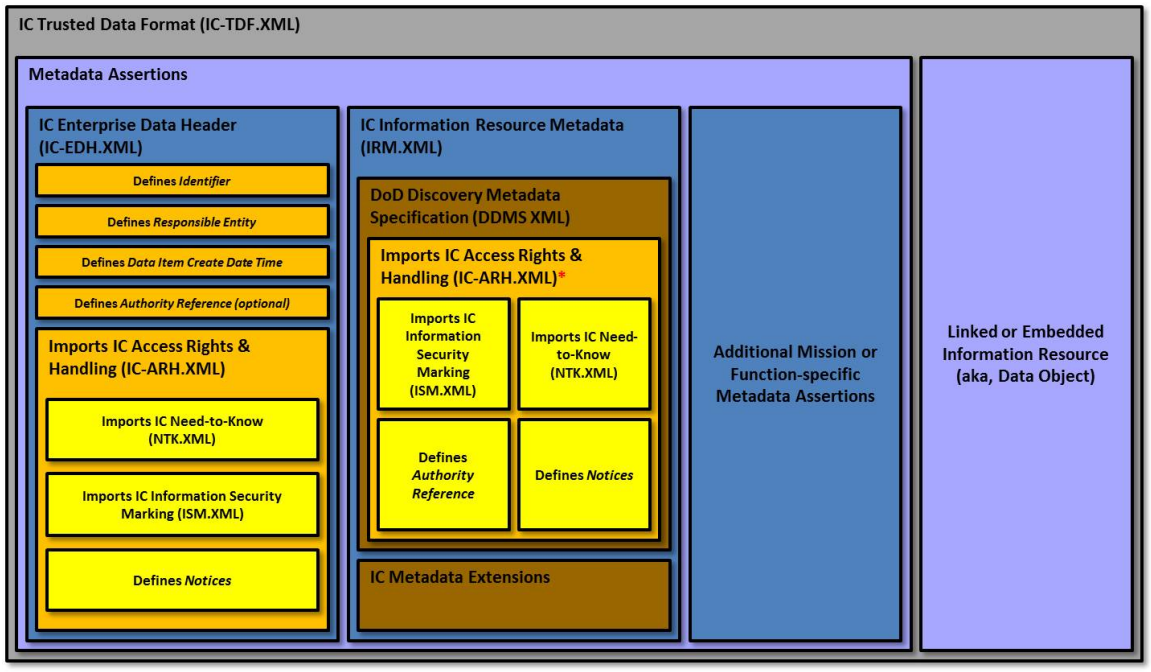

Figure 5 - TDF Detailed Structure

A TDC consists of a collection of TDOs or TDCs. It is expected but not required that the child TDOs and TDCs within 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 child TDOs corresponding to biometric modalities, such as finger prints, iris scans, and facial images. In this biometric use case the root TDC assertions would describe the entire identity, while the child TDO assertions would describe the individual modalities.

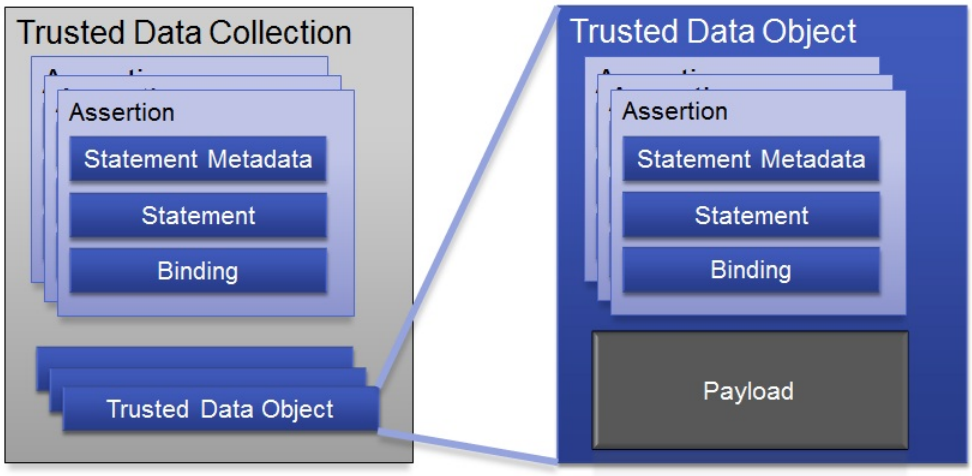

Figure 6 - Trusted Data Collection (TDC)

2.3 - Assertions

2.3.1 - Assertion Scopes

Assertions can be scoped to apply to different portions of an IC-TDF instance. Several assertion scopes imply certain meaning and processing instructions. The following sections explain the valid assertion scopes for use within TDOs and TDCs and any additional processing requirements they imply.

2.3.1.1 - Assertion Scopes Within TDO

Assertions within a TDO can be scoped to apply to either to the entire TDO, the payload only, or both. The following tokens are used to specify the scope of assertions within a TDO:

1. [PAYL] means this assertion applies only to the payload within this TDO.

2. [TDO] means this assertion applies to every element within the TDO other than itself (includes peer HandlingAssertions, Assertions, and the Payload). This scope essentially means "the entire TDO".

2.3.1.2 - Assertion Scopes Within TDC

Assertions within a TDC can be scoped to apply to several different portions of a TDC instance. [Definition: The child TDOs and TDCs contained within a TDC are referred to as the *collection members*.]

[Definition: An assertion with a *transitive scope* recursively applies to specific portions of each collection member within this TDC and MAY be inherited by a collection member if that collection member is extracted from this TDC.] Each transitive scope defines exactly which portions of the collection members the assertion applies to and how the assertion must be inherited when a collection member is extracted. Transitive scopes help reduce the need for duplicate assertions within collection members. For example, instead of making an identical assertion in each collection member individually, a single assertion with a transitive scope at the TDC level may have the same intent with much less overhead.

[Definition: An assertion with a *non-transitive* scope does not recursively apply to each collection member within this TDC and MUST NOT get inherited by a collection member if that collection member is extracted from this TDC.] Each non-transitive scope defines exactly which portion of this TDC the assertion applies to. Non-transitive scopes are used for assertions which only have meaning when considered in the scope of the TDC.

Whenever any change is made to the TDC, the intent of an assertion may no longer logically apply depending upon the assertion's scope and the change that was made. If a collection member is removed from the TDC, then the intent of an assertion with a transitive scope still logically applies to the remaining subset of collection members. However, any other change made to the collection members within the TDC may logically invalidate an assertion with a transitive scope (e.g., a new collection item is added or an existing collection member is modified). The intent of an assertion with a non-transitive scope may no longer logically apply if any modification is made to the portions of the TDC to which the assertion applies. Users modifying the TDC should understand the intent of each existing assertion in order to correctly preserve their intent or make some corrective modification after changes have been made. Section 2.4 - Binding and BindingInfo outlines how to cryptographically bind an assertion to the portions of the document to which it applies.

The following list defines the tokens used to specify the scope of assertions within TDCs:

1. [TDC] is a non-transitive scope and means this assertion applies to all TDC elements collectively (other than itself). This includes peer HandlingAssertions, Assertions, TrustedDataObjects, and TrustedDataCollections. This scope essentially means "the entire TDC".

2. [DESC_TDO] (short for descendant TDO) is a transitive scope and means this assertion applies to every TDO contained within this TDC.

   When a collection member is extracted from this TDC it MAY inherit assertions with scope [DESC_TDO] from its ancestor TDCs in the following ways:

   If the collection member being extracted is a TDO, then any assertion with scope [DESC_TDO] in an ancestor TDC becomes an assertion with scope [TDO] in the extracted TDO.

If the collection member being extracted is a TDC, then any assertion with scope [DESC_TDO] in an ancestor TDC becomes an assertion with scope [DESC_TDO] in the extracted TDC.

3. [DESC_PAYL] (short for descendant payload) is a transitive scope and means this assertion applies to every Payload within this TDC. This scope is similar to [DESC_TDO], but this scope applies ONLY to the Payloads within descendent TDOs and does NOT include any assertions or handling assertion of those TDOs.

   When a collection member is extracted from this TDC it MAY inherit assertions with scope [DESC_PAYL] from its ancestor TDCs in the following ways:

   If the collection member being extracted is a TDO, then any assertion with scope [DESC_PAYL] in an ancestor TDC becomes an assertion with scope [PAYL] in the extracted TDO.
   If the collection member being extracted is a TDC, then any assertion with scope [DESC_PAYL] in an ancestor TDC becomes an assertion with scope [DESC_PAYL] in the extracted TDC.

4. [TDC_MEMBER] is a non-transitive scope and means this assertion applies to all collection members within this TDC. Unlike scope [TDC], this scope does not apply to peer HandlingAssertions and Assertions.

   This scope is useful for making an assertion about the "current state" of the collection members within the TDC. For example, one might use the [TDC_MEMBER] scope to make an assertion that all members of the TDC contain biometric modalities for an certain individual. However, as soon as any modification is made to the collection members, then the assertion may no longer apply to the new state of the collection members (a collection member is added to the TDC, a collection member is removed from the TDC, any modification is made to any existing collection member).

2.3.1.3 - HandlingAssertion scopes within TDO

A TDO generally has two HandlingAssertions, a TDO handling assertion and a payload handling assertion . This allows for separate access control decisions to be made for the payload versus the entire TDO (which includes the payload metadata). A minimal case TDO has a single handling assertion to reduce redundancy. The HandlingAssertion for this minimal case MUST use scope [TDO PAYL], in that specific order, because the IC-TDF business rules require both tokens to be present within the instance.

2.3.1.4 - HandlingAssertion scopes within TDC

A TDC can only have a single HandlingAssertion and its scope must be [TDC].

2.3.2 - 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.

2.3.3 - Assertions and Data State

If an assertion statement or a payload is encrypted, then there are in fact two (potentially different) markings needed for decision making, analysis and querying. One describing the handling required for the ciphertext, and the other for the handling required for the unencrypted (and in effect external) state. In cases where statements and/or payloads are encrypted, handling assertions and statement metadata elements indicate whether their marks apply to the ciphertext vs. plaintext by using the attribute @tdf: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 repository and filter out results that require systemXYZ handling. For results with encrypted payloads, if the handling assertion only reflects the ciphertext handling (say Confidential) the user/system could get back thousands of encrypted results they cannot 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.

The attribute @tdf:appliesToState can be used with tdf:Assertion/tdf:StatementMetadata or with tdf:HandlingAssertion. The appliesToState attribute can only be used when content is encrypted, as indicated by the attribute @tdf:isEncrypted. When payload content is encrypted (@tdf:isEncrypted='true'), it must be marked with two HandlingAssertion blocks, one indicating the classification and handling required for the cyphertext payload (with @appliesToState='encrypted'), and the other indicating the classification and handling required for the plaintext payload after decryption (with appliesToState='unencrypted'). In this case, the HandlingAssertion that applies to the plaintext state is considered external to rollup, since the plain text content is not included in the instance. The appliesToState attribute should only be used with HandlingAssertions scoped to the payload. When Assertion statement content is encrypted (@tdf:isEncrypted='true') it must be marked with two StatementMetadata blocks, one indicating the classification and handling required to protect the cyphertext statement (with @tdf:appliesToState='encrypted'), and the other indicating the classification and handling required to protect the plaintext statement after decryption (with @tdf:appliesToState='unencrypted). In this case, the StatementMetadata describing the plaintext statement is considered external to rollup, since the plain text content is not included in the instance.

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**

In the current version of IC-TDF 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** 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 white-space 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 tables below. The abbreviation IFF stands for "if and only if". The pseudo XPaths in the tables below are not syntactically valid and use some abbreviations to save space and improve readability:

Assume each element and attribute is in the IC-TDF namespace
Payload refers to the *TDF extension points* tdf:StringPayload, tdf:StructuredPayload, tdf:ReferenceValuePayload, and tdf:Base64BinaryPayload
AssertionStatement refers to the *TDF extension points* tdf:StringStatement, tdf:StructuredStatement, tdf:ReferenceStatement, and tdf:Base64BinaryStatement
HandlingStatement refers to an IC-EDH instance (Edh or ExternalEdh)

Table 2 - TDO Binding Contents

XPath	Required to include in binding
TrustedDataObject/ Assertion[@scope='PAYL']	1. ./AssertionStatement 2. ./StatementMetadata IFF ./Binding/ SignatureValue/ @includesStatementMetadata='true' 3. ../Payload
TrustedDataObject/ HandlingAssertion[@scope='PAYL']	1. ./HandlingStatement 2. ../Payload

XPath	Required to include in binding
TrustedDataObject/ Assertion[@scope='TDO'] or **TrustedDataObject/ HandlingAssertion[@scope='TDO']** or **TrustedDataObject/ Assertion[@scope='TDO PAYL']** or **TrustedDataObject/ HandlingAssertion[@scope='TDO PAYL']**	1. ../HandlingAssertion/HandlingStatement 2. ../Assertion/AssertionStatement 3. ../Assertion/StatementMetadata IFF ./ Binding/SignatureValue/ @includesStatementMetadata='true' 4. ../Payload

Table 3 - TDC Binding Contents

XPath	Required to include in binding
TrustedDataCollection/ Assertion[@scope='TDC'] or **TrustedDataCollection/ HandlingAssertion[@scope='TDC']**	1. ../HandlingAssertion/HandlingStatement 2. ../Assertion/AssertionStatement 3. ../Assertion/StatementMetadata IFF ./ Binding/SignatureValue/ @includesStatementMetadata='true' 4. ..//TrustedDataObject/HandlingAssertion/ HandlingStatement 5. ..//TrustedDataObject/Assertion/ AssertionStatement 6. ..//TrustedDataObject/Assertion/ StatementMetadata IFF ./Binding/ SignatureValue/ @includesStatementMetadata='true' 7. ..//TrustedDataObject/Payload 8. ..//TrustedDataCollection/ HandlingAssertion/HandlingStatement 9. ..//TrustedDataCollection/Assertion/ AssertionStatement 10. ..//TrustedDataCollection/Assertion/ StatementMetadata IFF ./Binding/ SignatureValue/ @includesStatementMetadata='true'

XPath	Required to include in binding
TrustedDataCollection/ Assertion[@scope='DESC_TDO'] or **TrustedDataCollection/ Assertion[@scope='TDC_MEMBER']**	1. ./AssertionStatement 2. ./StatementMetadata IFF ./Binding/ SignatureValue/ @includesStatementMetadata='true' 3. ..//TrustedDataObject/HandlingAssertion/ HandlingStatement 4. ..//TrustedDataObject/Assertion/ AssertionStatement 5. ..//TrustedDataObject/Assertion/ StatementMetadata IFF ./Binding/ SignatureValue/ @includesStatementMetadata='true' 6. ..//TrustedDataObject/Payload 7. ..//TrustedDataCollection/ HandlingAssertion/HandlingStatement 8. ..//TrustedDataCollection/Assertion/ AssertionStatement 9. ..//TrustedDataCollection/Assertion/ StatementMetadata IFF ./Binding/ SignatureValue/ @includesStatementMetadata='true'
TrustedDataCollection/ Assertion[@scope='DESC_PAYL]	1. ./AssertionStatement 2. ./StatementMetadata IFF ./Binding/ SignatureValue/ @includesStatementMetadata='true' 3. ..//TrustedDataObject/Payload

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..

2.6 - 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)[24] information.

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.

2.8 - 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 Constraint Rules

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 to be resolved. 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 DES artifacts wherever they are located.

3.4 - 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.

3.5 - 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 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.

3.7 - Data Validation Constraint Rules

3.7.1 - Purpose

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.

3.7.2 - Schematron

Schematron[27] was selected as the language in which to encode these additional rules. The provided Schematron[27] 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*® [26] or the XSLT 2.0[31] implementation of ISO Schematron[27] provided by Rick Jelliffe at http://schematron.com/ [http://schematron.com/]. Constraint rules are dependent on XPath 2.0[30] and XSLT 2.0[31] features. According to Mr. Jelliffe, the editor of Schematron[27] 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[27] implementation and XSLT 2.0[31] files provided as a convenience 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 — 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.

3.7.4 - 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 1.7 - Dependencies .

3.7.5 - 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.

3.7.6 - 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.

[1] "white space" is defined in XML 1.0[28] as "(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs."

3.7.7 - 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 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 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.

3.8.2 - Rendering 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 4 - Conformance Validation

An instance is considered conformant with the IC-TDF specification if it passes all of the following normative validation steps. The following steps do not dictate how this validation strategy is implemented.

4.1 - Definitions

Terms are defined the first time they are used. Definitions are cumulative, meaning that a term used in any given step may be defined in a previous step. The following definitions are global concepts, so they are defined in this section instead of in-line.

[Definition: A *TDF extension point*is an element within the IC-TDF specification whose purpose is to hold multiple forms of user content in-line.] There are six extension points within IC-TDF

1. tdf:StringStatement
2. tdf:Base64BinaryStatement
3. tdf:StructuredStatement
4. tdf:StringPayload
5. tdf:Base64BinaryPayload
6. tdf:StructuredPayload

Note that tdf:ReferenceStatement and tdf:ReferenceValuePayload are not considered extension points because they only convey a link to content and do not hold content in-line.

[Definition: The content contained within elements tdf:Base64BinaryStatement and tdf:Base64BinaryPayload is referred to as *binary content*.]

[Definition: The content contained within elements tdf:StringStatement and tdf:StringPayload is referred to as *string content*.]

[Definition: The content contained within elements tdf:StructuredStatement and tdf:StructuredPayload is referred to as *structured content*.]

[Definition: The term *TDO structure* refers to all elements within an IC-TDF instance excluding the content of any TDF extension point].

4.2 - Why a verbose validation strategy is required

The IC-TDF specification is designed to be extremely flexible by allowing users to include several formats of in-line content in several extension points (see figure 1). These *TDF extension points* require IC-TDF instances to use a more verbose validation strategy for several reasons:

1. IC-TDF schema defines the extension points tdf:StructuredStatement and tdf:StructuredPayload as <xs:any processContents="skip"/>, which skips all schema validation for the content contained within those extension points.

2. *Structured content* within the IC-TDF instance can contain data which can conflict with the data contained within the elements declared as part of the IC-TDF specification.

   For example, the IC-TDF specification uses Information Security Markings (ISM) for conveying classification markings. The Publication Metadata (PUBS) specification also uses ISM. Suppose the payload contained an old PUBS document, which used a different version of ISM than defined in the IC-TDF specification. Applying the version of ISM business rules defined in IC-TDF to this instance document could easily fail because the older version ISM markings in the PUBS document could contain different attributes, removed tokens, among other changes.

3. For *binary content* and *string content*, XSD schema validation and XML business rules are not applicable and custom validation logic is required to validate that content.

Figure 1 - TDF extension points

4.3 - How to determine the ISM version within structured content

The version of ISM markings used within *structured content* is determined by the first occurrence of attribute @ism:DESVersion in document order contained in the structured content. If the structured content does not specify attribute @ism:DESVersion, then the ISM version is defined to be the same as the ISM markings used within the parent IC-TDF structure (TDO or TDC).

4.4 - Required Order of HandlingAssertions

Before any validation takes place on a TDO, a validation implementation MUST ensure that the tdo handling assertion is the first handling assertion in document order.

[Definition: The tdf:HandlingAssertion element which specifies attribute @tdf:scope with a value containing “TDC” is referred to as the *tdc handling assertion*.]

Before any validation takes place on a TDC, a validation implementation MUST ensure that the tdc handling assertion is the first handling assertion in document order.

[Definition: The ISM business rules define the first element in document order which specifies attribute @ism:resourceElement="true" to be the *resource element*.] The resource element contains the banner level ISM markings for the entire instance (i.e., the "roll-up").

The banner level markings within an IC-TDF instance are contained within a tdf:HandlingAssertion element and an instance may have multiple tdf:HandlingAssertion elements, each specifying a different scope. It is required that the first tdf:HandlingAssertion element in document order contain the banner level markings intended for the entire IC-TDF instance.

[Definition: The tdf:HandlingAssertion element which specifies attribute @tdf:scope with a value containing “PAYL” is referred to as the *payload handling assertion*]. [Definition: The tdf:HandlingAssertion element which specifies attribute @tdf:scope with a value containing “TDO” is referred to as the *tdo handling assertion*]. [Definition: A TDO instance is considered to be a *minimal case TDO* if the tdo handling assertion and the payload handling assertion are the same element.] A TDO instance can only be a minimal case TDO if it meets the following criteria:

TDO contains zero Assertion elements
payload is not encrypted
TDO contains a single HandlingAssertion element which specifies attribute @tdf:scope with a value of [TDO PAYL]
the handling assertion itself contains no classified data (i.e., no ISM markings which contribute to rollup other than @ism:classification="U" and @ism:ownerProducer="USA")

4.5 - TDO Validation Steps

This section outlines the required steps to fully validate a TrustedDataObject (TDO).

4.5.1 - Step 1 - TDO aware and cross assertion constraints

This step is intended to support validation which requires knowledge of the TDO structure.

IC-TDF validation, to include schema and business rules, should be run during this step.

ISM and NTK validation MUST NOT be run in this step because, as explained in the justification above, a *TDF extension point* could contain *structured content* which contains ISM or NTK markings from a different version of ISM/NTK than the TDO structure is using, which could fail validation. ISM and NTK validation is performed in Section 4.5.3 - Step 3 – TDO structure constraints . ARH and IC-EDH validation SHOULD NOT be performed at this step as it may be problematic when dealing with extension points that utilize different versions of these specifications from those used in the TDO.

TDO aware validation MAY be performed during this step. For example, one might want to run business rules specific to a certain domain or system. Some examples of custom validation could include::

If this TDO contains an Assertion with child element X, then it must also contain a peer Assertion with child element Y.
Verify that this TDO instance contains a custom assertion specific to a certain domain.
Verify all bindings within this TDO.
If the payload is encrypted, attempt to decrypt it and run additional custom validation on the decrypted content.

4.5.2 - Step 2 – Extension point constraints

This step is intended to support validation for the content of all *TDF extension points* contained within the TDO.

The child content of any *TDF extension point* MAY be validated. Any content validated in this step MUST be validated independently and in isolation. Determining which *TDF extension points* are validated in this step is implementation specific. For example, an implementation might choose to only validate *structured content* while ignoring *binary content* and *string content* completely. Or, an implementation might define a configuration which only validates *structured content* whose root element is in a certain namespace or set of namespaces.

If the content being validated is *structured content*, then the ISM business rules MUST NOT be applied unless the content is a *standalone ISM document*.[Definition: A *standalone ISM document* is an XML document which specifies the ISM attributes @ism:resourceElement and @ism:DESVersion]. Any NTK, ARH, or IC-EDH validation SHOULD be performed during this step for the *structured content* if the appropriate DESVersion attributes are specified.

Several examples of validation which could occur in this step include:

Schema and business rules for IC specifications from the 2012-Charlie release and earlier, including Publication Metadata (PUBS.XML) and Information Resource Metadata (IRM.XML)
Schema and business rules for mission specific assertion statements.
Custom validation for an audio/video file contained within a binary payload.

4.5.3 - Step 3 – TDO structure constraints

This step is intended to verify that ISM markings within the *TDO structure* are consistent. By treating *structured content* within *TDF extension points* as black boxes, only the ISM markings within the *TDO structure* will be validated. This includes ISM markings within HandlingAssertions and StatementMetadata. It does not include ISM markings within the payload and assertion extension points, which are considered 'black box' extensions in this step. This is also the time when any NTK, ARH, and IC-EDH validation that is specific to the *TDO structure* itself SHOULD be performed.

If IC-TDF rules were not run in Step 1

[Definition: A *placeholder element* is an XML element whose localname is “PlaceHolderContent”, namespace is “urn:placeholder”, and contains no text content or child elements].

[Definition: A *TDF skeleton* is an IC-TDF instance in which the structured content contained within all TDF extension points has been replaced by a placeholder element]. Whether *string content* and *binary content* is preserved when converting an IC-TDF instance to a TDF skeleton is implementation specific. Replacing string content and binary content with default values may yield performance improvements during validation if that content is large in size and is not intended to be validated.

[Definition: A TDF skeleton whose root element is tdf:TrustedDataObject is referred to as a *TDO skeleton*].

The tdf:TrustedDataObject element MUST be converted into a *TDO skeleton*, which MUST be validated in isolation against the normative portions of the ISM specification version in use by the TDO. Additional validation MAY be performed during this step.

4.5.4 - Step 4 – ISM consistency constraints

This step is intended to verify that ISM markings contained within *structured content* matches the corresponding ISM markings within the *TDO structure*. This step has several sub-steps because assertions and payloads require slightly different processing depending upon certain criteria.

4.5.4.1 - Step 4a – Consistency constraints for Assertions with resource level portion markings

[Definition: An *assertion fragment* is a tdf:Assertion element containing at least one tdf:StatementMetadata element and a TDF extension point]. Whether an assertion fragment contains any other child elements (tdf:Binding, tdf:ReferenceList, etc) is implementation specific.

[Definition: A *structured assertion fragment* is an assertion fragment whose TDF extension point is tdf:StructuredStatement].

Structured assertion fragments meeting the following criteria MUST be validated in isolation against the normative portions of the ISM specification version in use by the TDO:

1. The *structured content* contains ISM markings.

2. The ISM markings contained in the *structured content* are from the same version of the ISM specification as the ISM markings within the *TDO structure*. See Section 4.3 - How to determine the ISM version within structured content .

3. One of the tdf:StatementMetadata child elements specifies attribute @ism:resourceElement="true".

Validation of a *structured assertion fragment* verifies that the ISM markings contained within the *structured content* and the ISM markings contained within the tdf:StatementMetadata element are consistent. The ISM business rules use the tdf:StatementMetadata ISM markings as the resource level ("banner level") markings and treat the ISM markings in the *structured content* as portion markings. Constraint #3 above ensures that a tdf:StatementMetadata element can provide the resource level markings required for the ISM business rules.

For example, if the tdf:StatementMetadata contained @ism:classification="U" and the TDF extension point content contained @ism:classification="TS", then the ISM business rules would throw an error saying that unclassified documents must not contain TS portions.

4.5.4.2 - Step 4b – Consistency constraints for Payloads with resource level portion marking

[Definition: A *payload fragment* is a tdf:TrustedDataObject element containing a single tdf:HandlingAssertion element which is the payload handling assertion and a child TDF extension point]. Whether a payload fragment contains any other child elements (tdf:Assertion, etc) is implementation specific.

[Definition: A *structured payload fragment* is a payload fragment whose TDF extension point is tdf:StructuredPayload].

Structured payload fragments meeting the following criteria MUST be validated in isolation against the normative portions of the ISM specification version in use by the TDO:

1. The *structured content* contains ISM markings.

2. The ISM markings contained in the *structured content* are from the same version of the ISM specification as the ISM markings within the *TDO structure*. See Section 4.3 - How to determine the ISM version within structured content .

3. The *payload handling assertion* specifies attribute @ism:resourceElement="true".

Validation of the structured payload fragment verifies that the ISM markings contained within the *structured content* are consistent with the ISM markings in the payload handling assertion. The ISM business rules use the *payload handling assertion* as the resource level ("banner level") markings and treats the ISM markings in the *structured content* as portion markings. Constraint #3 above ensures that the *payload handling assertion* can provide the resource level markings required for the ISM business rules.

For example, if the *payload handling assertion* contained @ism:classification="U" and the *structured content* contained @ism:classification="TS", then the ISM business rules would throw an error saying that unclassified documents must not contain TS portions.

4.5.4.3 - Step 4c – Consistency constraints for Assertions and Payloads with non-resource level markings

This step is intended to check the consistency of ISM markings within assertions and payloads which do not have corresponding resource level ISM portion markings in the TDO structure (assertions and payloads not checked in step 4a or 4b).

The tdf:TrustedDataObject element MUST be modified to replace *structured content* meeting the following criteria with a *placeholder element*:

1. The *structured content* contains ISM markings.

2. The ISM markings contained within the *structured content* are from a *different version* of the ISM specification as the ISM markings within the *TDO structure*. See Section 4.3 - How to determine the ISM version within structured content .

The modified tdf:TrustedDataObject element MUST be validated in isolation against the normative portions of the ISM specification version in use by the TDO.

Replacing all of the *structured content* containing ISM markings from different versions allows the ISM business rules for the version used within the TDO structure to run correctly. The ISM business rules will use the tdo handling assertion as the resource level ("banner level") markings and treat the ISM markings in the rest of the TDO as portion markings. This step is very similar to Section 4.5.3 - Step 3 – TDO structure constraints , but step 3 replaces all *structured content* with a *placeholder element* whereas this step leaves *structured content* in-line if is uses the same ISM version as the ISM markings within the TDO structure.

For example, if the *tdo handling assertion* contained @ism:classification="U" and the *structured content* of an assertion not checked in step 4a or 4b (using the same ISM version) contained @ism:classification="TS", then the ISM business rules would throw an error saying that unclassified documents must not contain TS portions.

4.6 - TDC Validation Steps

This section outlines the required steps to fully validate a TrustedDataCollection (TDC).

4.6.1 - Step 1 – TDC aware and cross assertion constraints

This step is intended to support validation which requires knowledge of the TDC structure.

IC-TDF validation to include schema and business rules should be run during this step.

ISM validation MUST NOT be run in this step because, as explained in the justification above, a *TDF extension point* could contain *structured content* which contains ISM markings from a different version of ISM than the TDC structure is using, which could fail validation. ISM validation is performed in Section 4.6.3 - Step 3 – TDC structure constraints . NTK, ARH, and

IC-EDH validation at this step may also be problematic when dealing with extension points that utilize versions of these specifications used in the TDO.

Additional validation may be performed during this step. For example, one might want to run business rules specific to a certain domain or system. Some examples of custom validation could include:

Test if this TDC contains an Assertion with child element X, then it must also contain a peer Assertion with child element Y.
Test if this TDC must contain a a certain assertion type, such as a Multi-Audience Collection (MAC) assertion.

4.6.2 - Step 2 – Extension point constraints

This step is intended to support validation for the TDF extension point content contained within child tdf:Assertion elements of the TDC. The rules outlined in Section 4.5.2 - Step 2 – Extension point constraints should be applied to each child tdf:Assertion element of the tdf:TrustedDataCollection element.

4.6.3 - Step 3 – TDC structure constraints

This step is intended to verify that ISM markings within the TDC structure are consistent. By treating *structured content* within *TDF extension points* as black boxes, only the ISM markings within the TDC structure will be validated. This includes ISM markings within HandlingAssertions and StatementMetadata. This is also the place to perform any NTK, ARH, and IC-EDH validation that is specific to the TDC structure itself.

[Definition: A TDF skeleton whose root element is tdf:TrustedDataCollection is referred to as a *TDC skeleton*].

The tdf:TrustedDataCollection element MUST be converted into a *TDC skeleton*, which MUST be validated in isolation against the normative portions of the ISM specification version in use by the TDC. Additional validation MAY be performed during this step.

4.6.4 - Step 4 – ISM consistency constraints

This step is intended to verify that ISM markings contained within *structured content* match the corresponding ISM markings within the TDC structure. This step has several sub-steps because assertions with resource level ("banner level") ISM markings require slightly different processing than non-resource level ISM markings.

4.6.4.1 - Step 4a – Consistency constraints for Assertions with resource level portion markings

This step is intended to verify the consistency of ISM markings contained within child tdf:Assertion elements of the tdf:TrustedDataCollection element. The rules outlined in Section 4.5.4.1 - Step 4a – Consistency constraints for Assertions with resource level portion markings should be applied to each child tdf:Assertion element within the TDC.

4.6.4.2 - Step 4b – Consistency constraints for Assertions with non-resource level markings

This step is intended to check the consistency of ISM markings within child tdf:Assertion elements which do not have corresponding resource level ISM portion markings in the TDC structure (assertions not checked in step 4a).

The tdf:TrustedDataCollection element MUST be modified to replace *structured content* meeting the following criteria with a *placeholder element*:

1. The *structured content* contains ISM markings.

2. The ISM markings contained within the *structured content* are from a different version of the ISM specification as the ISM markings within the TDC structure. See Section 4.3 - How to determine the ISM version within structured content.

The modified tdf:TrustedDataCollection element MUST be validated in isolation against the normative portions of the ISM specification version in use by the TDC.

Replacing all of the *structured content* containing ISM markings from different versions allows the ISM business rules for the version used within the TDC structure to run correctly. The ISM business rules will use the tdc handling assertion as the resource level (“banner level”) markings and treat the ISM markings in the rest of the TDC as portion markings.

For example, if the tdc handling assertion contained @ism:classification=”U” and the structured content of an assertion not checked in step 4a (using the same ISM version) contained @ism:classification=”TS”, then the ISM business rules would throw an error saying that unclassified documents must not contain TS portions.

4.6.5 - Step 5 - Recursive Validation

A tdf:TrustedDataCollection element supports recursion by allowing child tdf:TrustedDataObject and tdf:TrustedDataCollection elements. Each tdf:TrustedDataObject element must be validated according to the steps outlined in Section 4.5 - TDO Validation Steps. Each tdf:TrustedDataCollection element must be validated according to the steps outlined in Section 4.6 - TDC Validation Steps.

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 (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 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.

Chapter 6 - Future Features

6.1 - Explicit Scope

In future versions, the concept of scope will be extended to support a flexible, explicit list of elements. The token [EXPLICIT] is expected to be used to indicate this granularity. An assertion using explicit scope will require either a ReferenceList or a BoundValueList and the elements to which it "applies" will be determined by the values in the ReferenceList or BoundValueList.

6.2 - BoundValueList

A key concept in the TDF specification is the ability to cryptographically assure the relationship among portions of the document. Future versions of TDF will make Cryptographic Binding more flexible and granular thorugh the introduction of an optional Bound Value List as a child of the **Binding** element. 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-TDF, where the **BoundValueList** is not 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 white-space 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.

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	V2
ISM	V9	V9+
IC-EDH	V1	V1+
NTK	V7	V7+
ARH	V1	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)
N/A	Not Applicable. Feature is no longer required.
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**	**V2**
	Mime Types	F	F
	Support for multiple versions of ISM.XML (V9 - Current)	N	F
	Support for multiple versions of NTK.XML (V7 - Current)	N	F
	Support for multiple versions of ARH.XML (V1 - Current)	N	F
	Support for multiple versions of IC-EDH.XML (V1 - Current)	N	F
	Support for TDC scope [PAYL]	F	N/A
	Support for TDC scopes [DESC_TDO], [DESC_PAYL], and [TDC_MEMBER]	N	F
	Support for multiple bindings in Assertions and HandlingAssertions	N	F
	Version decoupling, allowing import of any version of ISM and other dependent specifications at or above ISM v9+, NTKv7+, ARHv1+, and EDHv1+.	N	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**	**V10**
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	F
E.O. 13526[6] December 29, 2009	Compilation Reason	N	F	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	F
CAPCO Register and Manual 3.1 May 7, 2010	LES-NF	P	N	F	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	F
CAPCO Register and Manual 4.1 December 10, 2010	KDK	N	N	F	F	F	F	F	F	F	F
ICD 710[12] September 11, 2009	710 Foreign Disclosure or Release	P	P	F	F	F	F	F	F	F	F
E.O. 13526[6] December 29, 2009	DeclassReasons/Dates	P	P	F	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	F
DoD Instruction 5230.24[3] March 18, 1987	DoD Distro Statements	N	N	N	F	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	F

ISM Feature Comparison											
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**	**V10**
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	F
ISOO Marking Booklet 2010[20] / ISOO Notice 2009-13[21] December 2010	Remove exempted source	P	P	P	P	F	F	F	F	F	F
E.O. 13526[6] December 29, 2009	derivativelyClassifiedBy	P	P	P	P	F	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	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	F
IC-CIO enhance data quality See IC ESB	Schematron[27] Implementation of rules	N	N	N	N	F	F	F	F	F	F
E.O. 13526[6] December 29, 2009	50X1-Hum 50X2-WMD	N	N	N	N	F	F	F	F	F	F
DoD Manual 5200.1[2] January 1997	DoD ACCM Markings	N	N	N	N	N	F	F	F	F	F
CAPCO Register and Manual 4.2 May 31, 2011	SSI	N	N	N	N	N	F	F	F	F	F
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)[19] June 28, 2010	TFNI	N	N	N	N	N	F	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2010	HCS SubCompartments	N	N	N	N	N	F	F	F	N	N

ISM Feature Comparison											
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**	**V10**
CAPCO Register and Manual 4.1 November 16, 2010 (date disestablished)	MCFI Remove	P	P	P	P	P	F	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	F
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)[19] June 28, 2010	Multivalue declassException	F	N	N	N	N	N	F	F	F	N/A
IC-CIO enhance data quality See IC ESB	SouthSudan	N	N	N	N	N	N	F	F	F	F
ICD 710[12] September 11, 2009	710 POC	N	N	N	N	N	N	F	F	F	F
DNI ORCON Memo [25] March 11, 2011	ORCON POC	N	N	N	N	N	N	F	F	F	N/A
ISOO Marking Booklet[20] December 2010	Allow 50X1-HUM and 50X2-WMD to not have a date/event	N	N	N	N	N	N	F	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	F
December 30, 2012	Unclassified REL, RELIDO, NF, and DISPLAYONLY	N	N	N	N	N	N	N	F	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	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	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	F

ISM Feature Comparison											
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**	**V10**
CAPCO Register and Manual 5.1 December 30, 2011	RSV	N	N	N	N	N	N	N	F	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	F
CAPCO Register and Manual 5.1 December 30, 2011	Allow use of KDK compartments and sub-compartments	N	N	N	N	N	N	N	N	F	F
CAPCO Register and Manual 5.1 December 30, 2011	Allow use of SI compartments and sub-compartments	N	N	N	N	N	N	N	N	F	F
CAPCO Register and Manual 5.1 Annex A	Allow use of OSTY Open Skies	N	N	N	N	N	N	N	N	F	F
IC-CIO enhance data quality	External Notice	N	N	N	N	N	N	N	N	F	F
DoD Manual 5200.1-R[2] February 2012	COMSEC Notice	N	N	N	N	N	N	N	N	F	F
DoD Manual 5200.1-R[2] February 2012	Support for NNPI	N	N	N	N	N	N	N	N	F	F
Decouple ISM from the Schema January 2013	Schema is Informative, Schematron and CVEs are Normative.	N	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 5.1 December 2012	Add ENDSEAL system with compartments ECRU and NONBOOK	N	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 5.1 December 2013	Limit KDK system compartments to BLUEFISH, IDITAROD and KANDIK.	N	N	N	N	N	N	N	N	P	F
ISOO Notice 2013-01[22]. November 2012	Support NATO exemptions to declass date.	N	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**	**V8**
	Schematron[27] Implementation of rules	N	N	F	F	F	F	F	F
	Portion Level NTK	N	N	N	N	N	N	F	F
	Support multiple verions of ISM.XML (V9 - Current)	N	N	N	N	N	N	N	F

A.4. ARH Feature Summary

Table 11 - ARH Feature comparison

ARH Feature Comparison			
Required date	**Feature**	**V1**	**V2**
	Supports multiple versions of ISM.XML (V9 - Current) and NTK.XML (V7 - Current)	N	F

A.5. IC-EDH Feature Summary

Table 12 - IC-EDH Feature comparison

IC-EDH Feature Comparison			
Required date	**Feature**	**V1**	**V2**
	Supports multiple versions of ISM.XML (V9 - Current), NTK.XML (V7 - Current), and ARH.XML (V1 - Current)	N	F

Appendix B Change History

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

Table 13 - DES Version Identifier History

Version	Date	Purpose
1	17 July 2012	Initial Release
2	21 January 2013	Routine revision to technical specification. For details of changes, see Section B.1 - V2 Change Summary

B.1 - V2 Change Summary

Significant drivers for Version 2 include:

- See ISM V10 drivers
- See EDH V2 drivers

The following table summarizes the changes made to V1 in developing V2.

Table 14 - Data Encoding Specification V2 Change Summary

Change	Artifacts changed	Compatibility Notes
Added Schematron rules to require the specification of the **issuer** attribute and either the **subject** or **serial** attribute for the **tdf:Signer** element.	Schematron IC-TDF_ID_00038.sch	Data generation and ingestion systems need to be updated enforce the new rules.
Added Schematron rules to ensure that the versions of the imported specs meet the minimum allowed versions.	Schematron IC-TDF-ID-00036 Added IC-TDF-ID-00037 Added	Data generation and ingestion systems need to be updated enforce the new rules.
Updated the GUIDE id in the example files to comply with the updated regex in IC-EDH-ID-00007. The updated rule ensures there are no additional characters before or after the id.	Examples	Data generation and ingest systems complying with the GUIDE id rules do not need to be updated. Systems that were allowing invalid GUIDE ids will need to be updated to comply with the constraint rule.

Change	Artifacts changed	Compatibility Notes
Added validation strategy to the DES Version.	DES	Systems performing validation of the TDF should follow the appropriate validation strategy to ensure thorough and complete validation.
Added requirements for References to have external security markings.	IC-TDF-ID-00033 added IC-TDF-ID-00034 added	Data generation and ingest systems will be required to comply with the new rules.
Added scopes [DESC_TDO], [DESC_PAYL], and [TDC_MEMBER] for use within TDC Assertions to disambiguate trusted data collection scope meaning.	Schema IC-TDF-ID-00007 modified IC-TDF-ID-00035 added	Data generation and ingest systems will be required to comply with the new rules.
Deprecated scope [PAYL] for use within TDC Assertions.	IC-TDF-ID-00007 modified	Data generation and ingest systems will be required to comply with the new rules.
Added support for multiple bindings within Assertions and HandlingAssertions	Schema DES	Data generation and ingest systems need to be updated to support the new schema structure.
Version decoupling, allowing import of any version of ISM and other dependent specifications at or above ISM v9+, NTKv7+, ARHv1+, and EDHv1+.	DES	Data ingestion systems need to be aware of this change and ensure they check appropriate dependent spec versions for validation.
Updated Schema to ISMv10	Schema	Updated the Schema itself to use ism:DESVersion to 10 to mark the xsd schema instance with classification markings.
Added rule to only allow HandlingAssertions with scope of payload to use of the appliesToState attribute because only the payload can have encrypted or unencrypted states.	Schematron IC-TDF-ID-00039 added	Data generation and ingest systems will be required to comply with the new rules, however this rule should prevent systems from having to deal with a nonsensical case.

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 15 - Acronyms

Name	Definition
A&A	Access Rights and Handling
ABAC	Attribute Based Access Control
ARH	Access Rights and Handling
AS	Attribute Service
ATO	Authority To Operate
BNF	Backus-Naur Form
CAPCO	Controlled Access Program Coordination Office
CMS	Cryptographic Message Syntax
CVE	Controlled Vocabulary Enumeration
DAA	Designated Approval Agent
DCMI	Dublin Core Metadata Initiative
DC MES	Dublin Core Metadata Element Set
DES	Data Encoding Specification
DDMS	Department of Defense Discovery Metadata Specification
DOI	Digital Object Identifier
DN	Distinguished Name
DNI	Director of National Intelligence
EDH	Enterprise Data Header
E.O.	Executive Order
ES&IS	Enterprise Search & Integration Services
GIS	Geospatial Information System
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 EA	IC Enterprise Architecture

Name	Definition
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	IC Information Technology Enterprise
ICD	Intelligence Community Directive
ICEA	Intelligence Community Enterprise Architecture
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IETF	Internet Engineering Task Force
IRM	Information Resource Metadata
ISBN	International Standard Book Number
ISM	Information Security Marking
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWT	JSON Web Token
KA	Knowledge Assertion
KOS	Knowledge Organization System
MAC	Multi Audience Collection
MIME	Multipurpose Internet Mail Extensions
NARA	National Archives and Records Administration
NGA	National Geospatial Intelligence Agency
NGT	Next Generation Trident
NPE	Non-Person Entity
NSI	National Security Information
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
OCSP	Online Certificate Status Protocol
ODNI	Office of the Director of National Intelligence
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PK	Private Key
PKI	Public Key Infrastructure
RDBMS	Relational Database Management System
REST	REpresentational State Transfer

Name	Definition
RFC	Request for Comments
RR-ID	REST Security Encoding Specification for End-to-End Identity Propagation
SAML	Security Assertion Markup Language
SSD	Special Security Directorate
SSL	Secure Sockets Layer
SOAP	Simple Object Access Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
TGN	Thesaurus of Geographic Names
TLS	Transport Layer Security
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VIRT	Virtual Coverage
W3CDTF	World Wide Web Consortium Date Time Format
WSDL	Web Service Definition Language
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language

Appendix D Bibliography

Bibliography

[1] ARH.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Access Rights and Handling (ARH.XML)*.
Available online IntelLinkU at: http://purl.org/IC/Standards/ARH
Available online at: http://purl.org/IC/Standards/public

[2] DoD Manual 5200.1
Under Secretary of Defence for Intelligence. *DoD Information Security Program (Vol 1-4):*. 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 Instruction 5230.24
Secretary of Defense. *Distribution Statements on Technical Documents*. 5230.24. 23 August 2012.

23 August 2012 edition replaced the March 18, 1987.
Available online at: http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf

[4] DoD Directive 5240.01
Secretary of Defense. *DoD Intelligence Activities*. 5240.01. August 2007.
Available online at: http://www.dtic.mil/whs/directives/corres/pdf/524001p.pdf

[5] IC-EDH.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Enterprise Data Header (EDH.XML)*.
Available online IntelLinkU at: http://purl.org/IC/Standards/EDH
Available online at: http://purl.org/IC/Standards/public

[6] 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

[7] 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 at: http://go.ic.gov/HvBHBmY

[8] 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

[9] 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 209 Tearline Production and Dissemination.pdf

[10] 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/files/documents/ICD/ICD_500.pdf

[11] ICD 501
Director of National Intelligence Chief Information Officer. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.
Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[12] 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/files/documents/ICD/ICD_710.pdf

[13] ICPG 710.1
Assistant Director of National Intelligence for . *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.
Available online at: http://go.ic.gov/fU3HML

[14] ICPM 2007-200-2
Assistant Director of National Intelligence for . *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

[15] ICS 500-20
Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.
Available online at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500_20_signed_16DEC2010.pdf

[16] 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://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS_500-21_SIGNED_20110128.pdf

[17] 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

[18] 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

[19] 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

[20] 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

[21] 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

[22] ISOO Notice 2013-01
Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *ISOO Notice 2013-01: Further Marking Guidance on Commingling North Atlantic Treaty Organization (NATO) and Classified National Security Information (NSI)*.
Available online at: www.archives.gov/isoo/notices/notice-2013-01.pdf

[23] 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

[24] 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

[25] 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.

ICPG 710.1 signed July 2012[13], rescinded the ORCON Memo.
Available online at: https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/Guiding%20Principles%20for%20Use%20of%20the%20ORCON%20Markings_ES%2000045.pdf
Attachment A: https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20A.doc.pdf
Attachment B: https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20B.pdf
Attachment C: https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20C.pdf

[26] Oxygen
SyncRO Soft. *<oXygen/> XML Editor*. version 14.1.
Available online at: http://www.oxygenxml.com/

[27] 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/

[28] 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

[29] 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

[30] 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/

[31] 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.[15]