



Intelligence Community Technical Specification

XML Data Encoding Specification for DigitalHazMat TDF

Version 2021-NOV

December 1, 2022

Distribution Notice:

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

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.3 - Enterprise Need	1
1.4 - Conventions	1
1.4.1 - XML Namespaces	2
1.5 - Dependencies	2
1.5.1 - Specification Dependencies	2
1.5.2 - Inverse Dependencies	5
Chapter 2 - Development Guidance	7
2.1 - TDF Structure	7
2.2 - Assertions	7
2.2.1 - Assertion Scopes	7
2.2.2 - Handling Assertion Scopes	7
2.2.3 - Mission-Specific Metadata Assertions	7
2.2.4 - Assertions and Data State	8
2.3 - Binding and BindingInfo	8
2.4 - Normalization Methods	8
2.5 - Encryption and EncryptionInfo	8
2.6 - Linked or Embedded Data Objects	8
2.7 - MIME type	8
2.8 - BASE-TDF Schematron Rules	8
Chapter 3 - Constraints	9
3.1 - Data Validation Constraint Rules	9
3.1.1 - Purpose	9
3.1.2 - Inherited Constraints	9
3.1.3 - Value Enumeration Constraints	9
3.1.4 - Additional Constraints	9
3.1.4.1 - DES Constraints	9
3.1.5 - Constraint Rules	9
3.2 - Data Rendering Constraint Rules	9
3.2.1 - Purpose	9
3.2.2 - Rendering Constraint Rules	10
Chapter 4 - Conformance Validation	11
4.1 - Definitions	11
4.2 - Why a verbose validation strategy is required	11
4.3 - How to determine the ISM version within structured content	12
4.4 - Required Order of Handling Assertions	12
4.5 - TDO Validation Steps	12
4.5.1 - Step 1 - TDO aware and cross Assertion constraints	12
4.5.2 - Step 2 - Extension point constraints	12
4.5.3 - Step 3 - TDO structure constraints	13
4.5.4 - Step 4 - ISM consistency constraints	13
4.6 - TDC Validation Steps	13
Appendix A - Feature Summary	14
A.1 - DHZM-TDF Feature Summary	14

Appendix B - Change History	15
B.1 - V2021-NOV Initial Release Summary	15
Appendix C - Glossary	16
Appendix D - List of Abbreviations	17
Appendix E - Bibliography	19
Appendix F - Points of Contact	22
Appendix G - IC CIO Approval Memo	23

List of Figures

Figure 1 - Related Specifications	5
Figure 2 - Inverse Dependency Specifications	6

List of Tables

Table 1 - XML Namepaces	2
Table 2 - Dependencies	3
Table 3 - Constraint Rules	10
Table 4 - Feature Summary Legend	14
Table 5 - DHZM-TDF Feature comparison	14
Table 6 - DES Version Identifier History	15
Table 7 - Data Encoding Specification V2021-NOV Initial Release Summary	15

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for DigitalHazMat TDF* (DHZM-TDF.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode DHZM-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 within the use of a Trusted Data Format (TDF) Object. It is a profile of *XML Data Encoding Specification for Trusted Data Format* IC-TDF.XML^[7] that is suitable for use by commercial entities in an unclassified uncaveated environment while maintaining the ability to become a full IC-TDF.XML^[7] TDF on networks that require it.

1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML^[6]) defines the basic conceptual structure and outlines the core philosophy of Intelligence Community (IC) technical specifications. For convenience, a copy of this framework is included in every package.

This specification is applicable to the 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 - Enterprise Need

This DES is designed to fulfill a number of requirements in support of the transformational efforts of the IC. These requirements include:

- The need for a minimized profile of TDF for commercial entity use in unclassified uncaveated environments.
- The need to provide non-repudiation, obfuscation, and secure cross domain transfer of digital hazmat across the various domains in the enterprise for provenance and analysis.

Both enterprise needs and requirements for this specification can be found in the following policies and implementation guidance:

- 500 Series:
 - Intelligence Community Directive (ICD) 500, *Director Of National Intelligence Chief Information Officer*^[8]
 - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC*^[9]
 - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance*^[12]

1.4 - Conventions

Certain technical and presentation conventions are used in the creation of the IC technical specifications to ensure readability and understanding. For details, please see the "Specification Conventions" chapter in the IC-SF.XML^[6].

1.4.1 - XML Namespaces

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

Table 1 - XML Namespaces

Prefix	URI
anlys	urn:us:gov:ic:anlysassert
dhzm	urn:us:gov:ic:digitalhazmat
sfhashv	urn:us:gov:ic:sf:hashverification
ism	urn:us:gov:ic:ism
tdf	urn:us:gov:ic:tdf

1.5 - Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. For specific definitions of dependency terminology used throughout this section, please see the “Dependency Definitions” chapter in the IC-SF.XML^[6].

DHZM-TDF.XML is dependent on many specifications; all MUST be consulted in conjunction with this document. For example DHZM-TDF.XML depends on *XML Data Encoding Specification for Trusted Data Format - Base* (BASE-TDF.XML^[2]) for some Controlled Vocabulary Enumeration (CVE)s an several Schematron rules.

1.5.1 - Specification Dependencies

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

The subsequent figure, [Figure 1](#), is an informative graphical representation of all of the Intelligence Community Chief Information Officer (IC CIO) specifications related to this specification. The graphic depicts dependencies. However, the representations may not match an exact schema import tree or dependency diagram that an analysis of the Schema, Schematron or other documents would yield. For example, the graphic only shows a given specification once even though it may actually be imported by many specifications or be a direct dependency. All IC CIO specifications listed in [Table 2](#) will be shown in [Figure 1](#); however not all IC CIO specifications listed in [Figure 1](#) may appear in [Table 2](#). [Figure 1](#) is to aid users in gaining a general understanding of all dependencies whether direct or transitive.

Table 2 - Dependencies

Name	Dependency Description
<i>XML Data Encoding Specification for Information Security Marking Metadata</i> (ISM.XML.V2021-NOVr2022-NOV+ ^[13])	This specification depends on the LATEST technically sound, approved version of ISM.XML ^[13] . The minimum version was based on compliance with the authoritative source, which is ICD-710 ^[10] . Per ICD-710, all security markings MUST be updated within 365 days of a release of the Register and Manual. As of this release, the latest version of ISM.XML is 2021-NOVr2022-NOV which is based on the Register and Manual released in August, 2019.
<i>XML Data Encoding Specification for Enterprise Data Header</i> (IC-EDH.XML.V2019-MAR+ ^[5])	This specification does not depend on a specific version of IC-EDH.XML ^[5] ; versions later than version 2019-MAR MAY be used. The minimum version was based on a technical dependency; The merging of ARH into ISM.
<i>XML Data Encoding Specification for Revision Recall</i> (REVRECALL.XML.V2021-NOV ^[15])	This specification depends on the LATEST technically sound, approved version of REVRECALL.XML ^[15] . The minimum version was based on compliance with the authoritative source, which is ICPM 200-01 ^[11] . Per ICPM 200-01, there is one new value of FISA_COMPLIANCE_RECALL in CVEnum-RevRecallType, and there is a policy-driven redefinition of the meaning and usage of the RevRecallType ADMINISTRATIVE_RECALL that adds the new text "(but is not used for a FISA-compliance recall)."
<i>XML Data Encoding Specification for DigitalHazMat Assertion</i> (DHZM.XML.V2021-NOV+ ^[14])	This specification does not depend on a specific version of DHZM.XML ^[14] ; versions later than version 2021-NOV MAY be used. The minimum version was based on a technical dependency; Reference to DHZM Assertion.
<i>XML Data Encoding Specification for Analysis Assertion</i> (ANLYS.XML.V2021-NOV+ ^[1])	This specification does not depend on a specific version of ANLYS.XML ^[1] ; versions later than version 2021-NOV MAY be used. The minimum version was based on a technical dependency; Reference to ANLYS Assertion.

Name	Dependency Description
<i>XML Data Encoding Specification for Trusted Data Format - Base</i> (BASE-TDF.XML.V2021-NOV+ ^[2])	This specification does not depend on a specific version of BASE-TDF.XML ^[2] ; versions later than version 2021-NOV MAY be used. The minimum version was based on a technical dependency; Multiple schema updates including a bug fix for chunking in ReferenceValuePayload.
<i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ ^[6])	This specification does not depend on a specific version of IC-SF.XML ^[6] ; versions later than version 2021-NOV MAY be used, however, the newest version of IC-SF.XML SHOULD be used as IC-SF.XML is expected to always replace its preceding version. The minimum version was based on technical dependencies on IC-SF.XML; IC-SF.XML is the basic structure of and philosophy behind intelligence community technical specifications.
Schematron ^[16]	<p>Schematron — International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative.</p> <p>The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification.</p> <p>Note: The Schematron rules in this specification use Transformations (XSLT) 2.0^[17] query binding.</p>

Name	Dependency Description
XSLT 2.0 ^[17] implementation of Schematron ^[16] by Rick Jelliffe (2010-04-14) Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following Uniform Resource Locator (URL): http://code.google.com/p/schematron/ .	The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

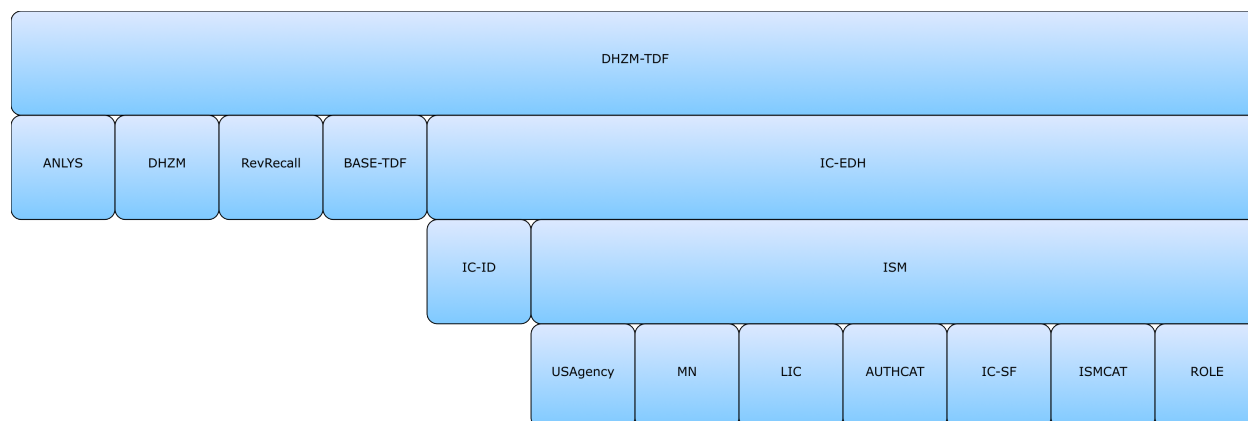


Figure 1 : Related Specifications

1.5.2 - Inverse Dependencies

Generally, it is only necessary to think of the *dependencies* in the dependency tree. However, with the specification versions being decoupled, it is also important to consider the *inverse dependencies*, for compatibility with newer versions of a given specification. The changes introduced to a given specification can sometimes make it incompatible with current versions of its inverse dependencies (specifications that uses the given specification).

Since this specification is one such specification that is used by other specifications released by the IC CIO, the [Figure 2](#) has been included to assist readers in understanding all of the inverse dependency relationships and how changes in this given specification may impact others specifications. This diagram is representative of direct and transitive inverse dependencies at the time of the release of this specification, but are subject to change over time and is presented in a list format that is different than [Figure 1](#).

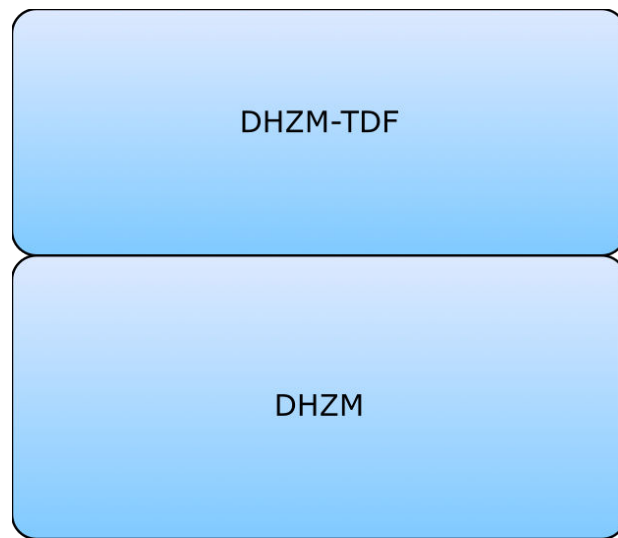


Figure 2 : Inverse Dependency Specifications

Chapter 2 - Development Guidance

For information on the structure and content of the specifications, please see the “Specification Overview” chapter in the IC-SF.XML^[6] framework document. This chapter is intended to expand upon the common information that the framework specifies providing specific development guidance that is specific to the implementation of this specification.

2.1 - TDF Structure

DHZM-TDF.XML is derived from *XML Data Encoding Specification for Trusted Data Format - Base* (BASE-TDF.XML^[2]). It is a profile of IC-TDF.XML^[7] with the following differences:

- Optional Enterprise Data Header (EDH) and Access Rights and Handling (ARH)
- Requires encryption
- Restricts TDF payload to only be by reference or base64 encoded

If any of the removed capabilities above are needed, then it is recommended that the full IC-TDF.XML^[7] be used. For more information on the TDF structure, please see the “Development Guidance” chapter in the BASE-TDF.XML^[2] specification.

2.2 - Assertions

2.2.1 - Assertion Scopes

For information on assertion scopes, please see the “Assertion Scopes” section of the “Development Guidance” chapter in BASE-TDF.XML^[2].

2.2.2 - Handling Assertion Scopes

For information on handling assertion scopes, please see the “Handling Assertion Scopes” section of the “Development Guidance” chapter in BASE-TDF.XML^[2].

2.2.3 - Mission-Specific Metadata Assertions

Although missions may create their own unique set of Assertions, no understanding by the enterprise beyond access control is assured. The only mission-specific metadata assertions allowed in DHZM-TDF.XML are:

1. Only 1 Digital Hazardous Material (DHZM) (dhzm:DigitalHazMatAssertion) assertion which must be the first mission assertion.
2. 0 to many DHZM (dhzm:ProvenanceAssertion) assertions.
3. 0 to many Analysis Assertion (ANLYS) (anlys:AnalysisAssertion) assertions.

2.2.4 - Assertions and Data State

For information on assertions and data state, please see the “Assertions and Data State” section of the “Development Guidance” chapter in BASE-TDF.XML^[2].

2.3 - Binding and BindingInfo

For information on cryptographically assuring the relationship among portions of the document, please see the “Binding and BindingInfo” section of the “Development Guidance” chapter in BASE-TDF.XML^[2].

2.4 - Normalization Methods

For information on normalization methods, please see the “Normalization Methods” section of the “Development Guidance” chapter in BASE-TDF.XML^[2].

2.5 - Encryption and EncryptionInfo

A key concept in the TDF specification is the ability to encrypt Payloads, Assertions, and keys. For information on encryption, please see the “Encryption and EncryptionInfo” section of the “Development Guidance” chapter in BASE-TDF.XML^[2].

2.6 - Linked or Embedded Data Objects

For information on linked or embedded data objects, please see the “Linked or Embedded Data Objects” section of the “Development Guidance” chapter in BASE-TDF.XML^[2].

2.7 - MIME type

For information on Media Type (MIME) type, please see the “MIME type” section of the “Development Guidance” chapter in BASE-TDF.XML^[2].

2.8 - BASE-TDF Schematron Rules

BASE-TDF schematron rules should be used for validation in derived child TDF instances (i.e. a DHZM-TDF.XML instance should be validated against BASE-TDF and DHZM-TDF.XML schematron rules).

Chapter 3 - Constraints

3.1 - Data Validation Constraint Rules

3.1.1 - Purpose

The DHZM-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. For more information, please see the “Data Validation Constraint Rules” chapter in the IC-SF.XML^[6] framework document.

3.1.2 - Inherited Constraints

In an instance of DHZM-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 1.5 - Dependencies](#).

3.1.3 - Value Enumeration Constraints

DHZM-TDF.XML currently does not contain any CVEs.

3.1.4 - Additional Constraints

3.1.4.1 - DES Constraints

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

3.1.5 - Constraint Rules

The detailed constraint rules for the DHZM-TDF.XML schema can be found in a separate document inside the Documents/DHZM-TDF directory, in the “DHZM-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 “DHZM-TDF_Rules.pdf” file.

3.2 - Data Rendering Constraint Rules

3.2.1 - Purpose

Rendering rules define constraints on the rendering and display of DHZM-TDF.XML documents. The intent is to inform the development of systems capable of rendering or displaying DHZM-

TDF.XML data for use by individuals not familiar with the details of the DHZM-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.

3.2.2 - Rendering Constraint Rules

The following table contains the information for the DHZM-TDF.XML data rendering constraint rules.

Table 3 - 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 DHZM-TDF.XML 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 DHZM-TDF.XML specification whose purpose is to hold multiple forms of user content in-line.] There are four extension points within DHZM-TDF.XML:

1. **`tdf:StringStatement`**
2. **`tdf:Base64BinaryStatement`**
3. **`tdf:StructuredStatement`**
4. **`tdf:Base64BinaryPayload`**

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. **`sfhashv:ContentEncodedHashVerification`** and **`sfhashv:ContentDecodedHashVerification`** contains hash verification information with regards to the referenced statement or payload and is not referring to the hash verification of any intermediate URI redirects that may exist.

[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`** is referred to as *string content*.]

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

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

4.2 - Why a verbose validation strategy is required

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

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

4.3 - How to determine the ISM version within structured content

The version of *XML Data Encoding Specification for Information Security Marking Metadata* (ISM.XML^[13]) 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.XML^[13] version is defined to be the same as the ISM.XML^[13] markings used within the parent DHZM-TDF.XML structure (TDO).

4.4 - Required Order of Handling Assertions

The use of handling assertions is optional in DHZM-TDF.XML. If handling assertions are used, the required order is detailed in the “Required Order of Handling Assertions” section of the “Conformance Validation” chapter in BASE-TDF.XML^[2].



Note

[Definition: The ISM.XML^[13] 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.XML^[13] markings for the entire instance (i.e., the “roll-up”).

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 Trusted Data Object (TDO) structure. For more information, please see Step 1 of the “TDO Validation Steps” section of the “Conformance Validation” chapter in IC-TDF.XML^[7].

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. For more information, please see Step 2 of the “TDO Validation Steps” section of the “Conformance Validation” chapter in IC-TDF.XML^[7].

4.5.3 - Step 3 – TDO structure constraints

This step is intended to verify that ISM.XML^[13] markings within the *TDO structure* are consistent. If EDH is used, please see Step 3 of the “TDO Validation Steps” section of the “Conformance Validation” chapter in IC-TDF.XML^[7].

4.5.4 - Step 4 – ISM consistency constraints

This step is intended to verify that ISM.XML^[13] markings contained within *structured content* match the corresponding ISM.XML^[13] markings within the *TDO structure* and does not currently apply for DHZM-TDF.XML.

4.6 - TDC Validation Steps

This section outlines the required steps to fully validate a TrustedDataCollection (TDC). For detailed step information, please see the “TDC Validation Steps” section of the “Conformance Validation” chapter in IC-TDF.XML^[7].

Appendix A Feature Summary

The following tables summarize major features by version for DHZM-TDF.XML. The “Required date” is the date when systems SHOULD support a feature based on the specified driver. Executive Orders, Information Security Oversight Office (ISOO) notices, ICDs and other policy documents have a variety of effective dates. The “Required date” may be later than the date of applicable policy based on the effective date defined in the policy (e.g., The IC Marking System Register and Manual^[4] has an implementation date of one year after issuance).

Table 4 - 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. DHZM-TDF Feature Summary

Table 5 - DHZM-TDF Feature comparison

Required date	Feature	V2021-NOV
December 3, 2021	Defines the DHZM-TDF Profile of IC-TDF	F

Appendix B Change History

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

Table 6 - DES Version Identifier History

Version	Date	Purpose
2021-NOV	December 3, 2021	Initial Release. For details, see Section B.1 - V2021-NOV Initial Release Summary

B.1 - V2021-NOV Initial Release Summary

Significant drivers for Version V2021-NOV include:

- Creation of DHZM-TDF.XML specification.

The following table summarizes the initial release in V2021-NOV.

Table 7 - Data Encoding Specification V2021-NOV Initial Release Summary

#	Change	Artifacts changed	Compatibility Notes
1	Creation of DHZM-TDF.XML specification. (CR-2020-050, CR-2021-008, CR-2021-003)	Documentation Schema Schematron XSL	Initial Release.

Appendix C Glossary

This appendix lists terms, definitions and sources of the definitions for terms used in this document.

Uncaveated

Uncaveated means the document bears no FD&R markings and no AEA markings, SAP markings, and/or dissemination control marking(s) (i.e., all IC and non-IC dissemination controls). SCI controls are intentionally not listed. If only an SCI marking is present, the information is considered uncaveated.

Source: IC Markings Register & Manual^[3]

Appendix D List of Abbreviations

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

AEA	Atomic Energy Act
ANLYS	Analysis Assertion
ARH	Access Rights and Handling
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DHZM	Digital Hazardous Material
DNI	Director of National Intelligence
EDH	Enterprise Data Header
FD&R	Foreign Disclosure & Release
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC ESB	Intelligence Community Enterprise Standards Baseline
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
MIME	Media Type
SAP	Special Access Program
SCI	Sensitive Compartmented Information
TDF	Trusted Data Format
TDO	Trusted Data Object
URL	Uniform Resource Locator
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language

XSLT

XSL Transformations

Appendix E Bibliography

[1] ANLYS.XML

Office of the Director of National Intelligence. *XML DES Encoding Specification for Analysis Assertion (ANLYS.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/LNjJFsj> (case sensitive – Lima November juliet Juliet Foxtrot sierra juliet)

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

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

[2] BASE-TDF.XML

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

Available online Intelink-TS at: <https://go.ic.gov/GC4VEXo> (case sensitive – Golf Charlie 4 Victor Echo Xray oscar)

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

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

[3] IC Markings AUG 2019

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 30 Aug 2019.

Available online Intelink-TS at: <https://go.ic.gov/gbMr5fv> (case sensitive – golf bravo Mike romeo 5 foxtrot victor)

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

[4] IC Markings

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*.

Available online Intelink-TS at: <https://go.ic.gov/tGXkwGO> (case sensitive – tango Golf Xray kilo whiskey Golf Oscar)

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

[5] IC-EDH.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Enterprise Data Header (IC-EDH.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/5Pg1r8s> (case sensitive – 5 Papa golf 1 romeo 8 sierra)

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

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

[6] IC-SF.XML

Office of the Director of National Intelligence. *Intelligence Community Specification Framework (IC-SF.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/pNFyuVg> (case sensitive – papa November Foxtrot yankee uniform Victor golf)

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

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

[7] IC-TDF.XML

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

Available online Intelink-TS at: <https://go.ic.gov/hdwc8fn> (case sensitive – hotel delta whiskey charlie 8 foxtrot november)

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

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

[8] ICD 500

Office of the Director of National Intelligence. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.

Available online Intelink-TS at: <https://go.ic.gov/U7v6ZRL> (case sensitive – Uniform 7 victor 6 Zulu Romeo Lima)

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

[9] ICD 501

Office of the Director of National Intelligence. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.

Available online Intelink-TS at: <https://go.ic.gov/fTBM8OS> (case sensitive – foxtrot Tango Bravo Mike 8 Oscar Sierra)

Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[10] ICD 710

Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.

Available online Intelink-TS at: <https://go.ic.gov/oSj9K7O> (case sensitive – oscar Sierra juliet 9 Kilo 7 Oscar)

Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[11] ICPM 200-01

Office of the Director of National Intelligence. *Intelligence Community Standards and Procedures for Revised or Recalled Intelligence Products*. Intelligence Community Policy Memorandum 2020-200-01. 27 February 2020.

Available online at: https://www.dni.gov/files/documents/ICPM_2020_200-01_U-FOUO_SIGNED-FINAL_Redacted.pdf

[12] ICS 500-20

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.

Available online Intelink-TS at: <https://go.ic.gov/kh8NMVJ> (case sensitive – kilo hotel 8 November Mike Victor Juliet)

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-20>

[13] ISM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/qoNICy7> (case sensitive – quebec oscar November India Charlie yankee 7)

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

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

[14] DHZM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for DigitalHazMat Assertion (DHZM.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/OuEJhNd> (case sensitive – Oscar uniform Echo Juliet hotel November delta)

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

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

[15] REVRECALL.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Revision Recall (RevRecall.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/cC4WFa0> (case sensitive – charlie Charlie 4 Whiskey Foxtrot alpha 0)

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

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

[16] Schematron

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

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

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

[17] 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 F Points of Contact

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

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

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

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

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

Appendix G IC CIO Approval Memo

An IC CIO Approval Memo should accompany this enterprise technical data specification bearing the signature of the IC CIO or an IC CIO-designated official(s). If an IC CIO 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 IC CIO staffing and coordination process leading to signature of the IC CIO Approval Memo. The signature date of the IC CIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the IC CIO 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 Intelligence Community Enterprise Standards Baseline (IC ESB) as defined in ICS 500-20^[12].