



Intelligence Community Technical Specification

XML Data Encoding Specification for Community Shared Resources Technical Specification Profiles

Version 2017-MAY

May 22, 2017

Distribution Notice:

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

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.3 - Background	1
1.4 - Enterprise Need	2
1.5 - Audience and Applicability	3
1.6 - Conventions	3
1.6.1 - Language	3
1.6.2 - Typography	3
1.6.3 - Terminology	4
1.6.4 - XML Namespaces	4
1.7 - Dependencies	4
1.8 - Conformance	4
Chapter 2 - Development Guidance	5
2.1 - Profiles	5
2.1.1 - Example MIME Types	6
2.2 - Mandatory Profile Set	6
Chapter 3 - Definitions, Interfaces, and Constraints	8
Chapter 4 - Conformance Validation	9
4.1 - CSR Systems Receiving data	9
4.2 - CSR Systems Producing data	9
4.3 - IC ITE CSR Systems	9
Chapter 5 - CSRProfile.CVE	10
5.1 - Overview	10
5.2 - Specification Summary	10
5.3 - Specification Combinations	10
5.4 - CSRProfile.CVE.v2017-MAY	11
Chapter 6 - CSRProfile.Audit	12
6.1 - Overview	12
6.2 - Specification Summary	12
6.3 - Relevant CVE Specifications	13
6.4 - Specification Combinations	14
6.5 - CSRProfile.Audit.v2015-FEB	14
6.6 - CSRProfile.Audit.v2016-SEP	14
Chapter 7 - CSRProfile.Discovery	15
7.1 - Overview	15
7.2 - Specification Summary	16
7.3 - Relevant CVE Specifications	16
7.4 - Specification Combinations	17
7.5 - CSRProfile.Discovery.v2014-MAR	17
7.6 - CSRProfile.Discovery.v2015-AUG	18
7.7 - CSRProfile.Discovery.v2015-NOV	18
7.8 - CSRProfile.Discovery.v2016-SEP	18
Chapter 8 - CSRProfile.DOMEX	19
8.1 - Overview	19
8.2 - Specification Summary	19

8.3 - Relevant CVE Specifications	20
8.4 - Specification Combinations	21
8.5 - CSRProfile.DOMEX.v2015-AUG	21
8.6 - CSRProfile.DOMEX.v2015-NOV	21
8.7 - CSRProfile.DOMEX.v2016-SEP	21
Chapter 9 - CSRProfile.DTI	22
9.1 - Overview	22
9.2 - Specification Summary	23
9.3 - Relevant CVE Specifications	24
9.4 - Specification Combinations	24
9.5 - CSRProfile.DTI.v2014-MAR	25
9.6 - CSRProfile.DTI.v2015-AUG	25
9.7 - CSRProfile.DTI.v2015-NOV	25
9.8 - CSRProfile.DTI.v2016-SEP	25
Chapter 10 - CSRProfile.Entities	26
10.1 - Overview	26
10.2 - Specification summary	26
10.3 - Relevant CVE Specifications	26
10.4 - Specification Combinations	27
10.5 - CSRProfile.Entities.v2016-SEP	27
Chapter 11 - CSRProfile.MsgTransport	28
11.1 - Overview	28
11.2 - Specification Summary	28
11.3 - Relevant CVE Specifications	29
11.4 - Specification Combinations	30
11.5 - CSRProfile.MsgTransport.v2015-FEB	30
11.6 - CSRProfile.MsgTransport.v2016-SEP	31
Chapter 12 - CSRProfile.TDE	32
12.1 - Overview	32
12.2 - Specification Summary	33
12.3 - Relevant CVE Specifications	33
12.4 - Specification Combinations	34
12.5 - CSRProfile.TDE.v2014-MAR	34
12.6 - CSRProfile.TDE.v2015-AUG	35
12.7 - CSRProfile.TDE.v2016-SEP	35
Appendix A - Feature Summary	36
A.1 - CSR Specification Feature Comparison	36
Appendix B - Change History	37
B.1 - 2017-MAY Change Summary	37
B.2 - V2017-MAR Change Summary	37
B.3 - V2016-SEP Change Summary	38
B.4 - V2015-NOV Change Summary	38
B.5 - V2015-AUG Change Summary	39
Appendix C - List of Abbreviations	40
Appendix D - Bibliography	42
Appendix E - Points of Contact	49
Appendix F - IC CIO Approval Memo	50

List of Figures

Figure 1 - CSRProfile.CVE Related Specifications	10
Figure 2 - CSRProfile.Audit Related Specifications	13
Figure 3 - CSRProfile.Discovery Related Specifications	16
Figure 4 - CSRProfile.DOMEX Related Specifications	20
Figure 5 - CSRProfile.DTI Related Specifications	23
Figure 6 - CSRProfile.Entities Related Specifications	26
Figure 7 - CSRProfile.MsgTransport Related Specifications	29
Figure 8 - CSRProfile.TDE Related Specifications	33

List of Tables

Table 1 - XML Namepaces	4
Table 2 - CSRProfile.CVE Profile Sets	10
Table 3 - Feature Summary Legend	12
Table 4 - Feature Summary Legend	12
Table 5 - CSRProfile.Audit Feature Comparison	12
Table 6 - Relevant CVE Specifications	13
Table 7 - CSRProfile.Audit Profile Sets	14
Table 8 - Feature Summary Legend	15
Table 9 - Feature Summary Legend	15
Table 10 - CSRProfile.Discovery Feature Comparison	15
Table 11 - Relevant CVE Specifications	17
Table 12 - Specification Combinations	17
Table 13 - Feature Summary Legend	19
Table 14 - Feature Summary Legend	19
Table 15 - CSRProfile.DOMEX Feature Comparison	19
Table 16 - Relevant CVE Specifications	20
Table 17 - CSRProfile.DOMEX Profile Sets	21
Table 18 - Feature Summary Legend	22
Table 19 - Feature Summary Legend	22
Table 20 - CSRProfile.DTI Feature Comparison	23
Table 21 - Relevant CVE Specifications	24
Table 22 - CSRProfile.DTI Profile Sets	24
Table 23 - Relevant CVE Specifications	27
Table 24 - CSRProfile.Entities Profile Sets	27
Table 25 - Feature Summary Legend	28
Table 26 - Feature Summary Legend	28
Table 27 - CSRProfile.MsgTransport Feature Comparison	28
Table 28 - Relevant CVE Specifications	30
Table 29 - CSRProfile.MsgTransport Profile Sets	30
Table 30 - Feature Summary Legend	32
Table 31 - Feature Summary Legend	32
Table 32 - CSRProfile.TDE Feature Comparison	32
Table 33 - Relevant CVE Specifications	34
Table 34 - CSRProfile.TDE Profile Sets	34
Table 35 - Feature Summary Legend	36
Table 36 - Feature Summary Legend	36
Table 37 - CSR Specification Feature Comparison	36
Table 38 - DES Version Identifier History	37
Table 39 - Data Encoding Specification 2017-MAY Change Summary	37
Table 40 - Data Encoding Specification V2017-MAR Change Summary	38
Table 41 - Data Encoding Specification V2016-SEP Change Summary	38
Table 42 - Data Encoding Specification V2015-NOV Change Summary	39
Table 43 - Data Encoding Specification V2015-AUG Change Summary	39

Chapter 1 - Introduction

1.1 - Purpose

The Intelligence Community (IC) technical specifications are decoupled, which allows different versions of dependent specifications to be used together. Decoupling provides useful functionality to the enterprise, but the possible number of combinations of versions is overwhelming to systems and can potentially impair interoperability. To mitigate the burden of decoupling and foster interoperability, this specification, Community Shared Resources Technical Specification Profiles (CSR.XML), defines subsets of versions of dependent specifications that **MUST** be supported by Community Shared Resources (CSRs). These subsets are defined based on functional areas such as audit, disseminated textual information, and trustable data exchange.

1.2 - Scope

This specification is applicable to the IC and information produced by, stored, or shared within the IC. This specification may have relevance outside the scope of intelligence; however, prior to applying outside of this defined scope, it should be closely scrutinized and differences separately documented and assessed for applicability.

More specifically, this specification is targeted at CSRs in the enterprise services that produce or consume data. It is essential that CSRs meet the minimum requirements put forth in this specification to facilitate information sharing without undue and overwhelming burden on data providers and data consumers.

The specifications profiled in this document are limited to those that are in the Enterprise Standards Baseline (ESB) that are owned by the IC or the Department of Defense (DoD) and are either IC Chief Information Officer (IC CIO) authored, or direct dependencies of an IC CIO authored specification.

1.3 - Background

The Intelligence Community Chief Information Officer (IC CIO) is leading the IC's enterprise transformation to an "interoperable federated architecture." Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer* ^[16] grants the IC CIO the authority and responsibility to:

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

In the area of enterprise standardization, the IC CIO is called upon to establish common Information Technology (IT) standards, protocols, and interfaces, to establish uniform information security standards, and to ensure information technology infrastructure, enterprise architecture, systems, standards, protocols, and interfaces support the overall information sharing strategies and policies of the IC as established in relevant law, policy, and directives.

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse. As detailed in Intelligence Community Standard (ICS) 500-21, *Tagging of Intelligence and Intelligence-Related Information* ^[21] the extensive and consistent use of Extensible Markup Language (XML) within data encoding specifications allows for improved data exchanges and processing of information, thereby facilitating achievement of the IC's data discovery, data sharing, and interoperability goals.

An encoding specification defines a concrete implementation – a file format for example – for concepts in the *IC Abstract Data Definition* ^[1]. Many IC encoding specifications are based on XML, but other technologies are possible. For example, IC-ID^[13] defines a plain-text format for IC Identifiers as well as an associated XML structure.

1.4 - Enterprise Need

All systems at the enterprise level need to be able send and receive with a common vocabulary to permit understanding. Even one system not sending or receiving in the common vocabularies places extraneous burden on the other systems to implement superfluous vocabularies. Since the decoupling of the IC Technical Specifications from one another, permitting them to revision independently, the potential combinations of versions of the specifications that can be mixed-and-matched together have grown exponentially. The number of combinations will only continue to grow as newer versions and new specifications are produced. This puts a large burden on data producers and consumers in the enterprise to be able to produce and/or interpret all possible combinations. The ever-growing number of combinations leads to a need to have a minimal number of sets of combinations that CSRs, or enterprise-level resources, must be able to produce/consume to relieve them of the infeasible burden of being able to produce/consume all possible combinations.

A few limited common sets of vocabulary for communication on the enterprise reduces the level of efforts of both producers and consumers in system maintenance while still providing the producers the ability to select one of the vocabulary sets that best meets their needs and reduces the amount of system revisions they have to implement to keep up with the common language of the enterprise.

Enterprise consumers will have to understand the common vocabulary sets of the enterprise or they may be unable to consume something a producer sends when they start using a different vocabulary set. Failure to accept all common vocabulary sets will result in a failure of ubiquitous communication on the enterprise.

Enterprise needs and requirements for this specification can be found in the following Office of the Director of National Intelligence (ODNI) policies and implementation guidance:

- IC Information Technology Enterprise (IC ITE):
 - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan^[9]
- 500 Series:
 - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer^[16]

- Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC^[17]
- 200 Series:
 - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide^[19]

1.5 - Audience and Applicability

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

The governance of this specification and the data it describes, including any requirement to use this specification or prohibition thereof, is explicitly outside the scope of this specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*,^[20] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element. *Department of Defense Instruction (DODI) 8310.01, Information Technology Standards in the DoD*,^[6] requires DoD elements to use the DoD IT Standards Registry (DISR).

Use of this specification must be consistent with applicable Federal statutes, Executive Orders, Presidential Directives, Attorney General approved guidelines, IC Policy, IC element policies, established concepts of operation, agreements, contractual obligations, etc. However, the determination of any such requirements or restrictions is the sole responsibility of each implementing entity. Implementers may wish to consult the Office of General Counsel for their cognizant agency to determine existing requirements and restrictions for the use of this DES and to determine if new agreements or policy changes are required related to the use of this DES.

1.6 - Conventions

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

1.6.1 - Language

When appearing in all capital letters in this technical specification, the keywords "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" are to be interpreted as described in IETF RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels."^[23] When these words appear in regular case, they are meant in their natural-language sense.

1.6.2 - Typography

Certain typography is used throughout the body of this document to convey certain meanings, in particular:

- *Italics* – A title of a referenced work or a specialized or emphasized term
- Underscore – An abstract data element
- **Bold** – An XML element or attribute

1.6.3 - Terminology

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

- *Normative*: considered to be prescriptive and necessary to conform to the standard.
- *Informative*: serving to instruct, enlighten or inform.

1.6.4 - XML Namespaces

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

Table 1 - XML Namespaces

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

1.7 - Dependencies

This document has no specific direct dependencies as it merely gives guidance on sets of specification versions to be used together.

1.8 - Conformance

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

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

Informative: serving to instruct, enlighten or inform.

The information and guidance laid forth in [Section 2.2 - Mandatory Profile Set](#) is considered normative for this specification.

Chapter 2 - Development Guidance

2.1 - Profiles

This specification defines the version sets of IC CIO specifications — called profiles — that CSRs must support. Dependent specifications are grouped into profiles by functional areas, and a CSR is only required to implement profiles based on functional areas applicable to that CSR. CSRs are not required to implement version sets not mandated by this specification. For example, a CSR that ingests Document and Media Exploitation (DOMEX) information **MUST** support all DOMEX profiles defined in this specification, and a DOMEX producer must support at least one DOMEX profile defined in this specification. Grouping specifications into profile sets enables stakeholders to clearly and conveniently communicate specification version dependencies.

Consuming CSRs have an important role in the enterprise. If CSRs fail to use current specifications, they cause compliance issues that risk data leaks and impede information sharing. CSRs must be able to consume information and provide that information to downstream systems. Profile sets were created to ease the burden of keeping CSRs up-to-date with current specifications by limiting the combinations of specification versions that must be supported. Profile sets reduce the cost of protecting resources and meeting mission needs. The profile sets are discussed in detail in [Section 2.2 - Mandatory Profile Set](#).

Profiles are chosen based on enterprise use cases; the profiles defined in this specification should be able to meet the needs of all data shared in the enterprise. The set of profiles defined in this document will evolve over time to meet these needs, adding new profiles as needed and retiring profiles that are no longer useful or that violate policy. Since profile sets are use case driven, it is possible that not all versions of the specifications in the enterprise baseline may be included in a profile set. Subsequent versions are still valid for use above and beyond the profile sets defined in this document.

Profiles may be described using MIME types. Implementing the use of a core MIME Type in the format 'application/dni-tdf+xml' with additional parameters specifying the appropriate CSRs and/or the appropriate individual specifications. This enables consuming systems to properly interpret or request the data according to the named specification and version. The Content-Type parameters **MUST** conform to RFC-2231 ^[24] this introduces conventions such as replacing periods with dashes to avoid having to escape the periods.

This specification defines the MIME Content-Type format using the formal language known as Augmented Backus-Naur format (ABNF). See http://en.wikipedia.org/wiki/Augmented_Backus-Naur_Form. The following ABNF rules explicitly define the content of an Content-Type with optional parameters. ABNF is used to provide a formal description independent of any particular technology.

Content-Type := type "/" subtype *[";" parameter]

Mime Content-Type Format

[1] Content-Type : := [Type-SubType](#) *[";" [CSRProfile](#)] *[";" [CSRCVEProfile](#)] *[";" [SpecExeptions](#)]

- [2] Type- : := application/dni-tdf+xml
 SubType
- [3] CSRProfile : := csr=[CSRProfileName](#)-"[CSRProfileVersion](#)
- [4] CSRProfileName : := The name of the CSR Profile with periods "."
 replaced by dash "-" (e.g., CSRProfile-Audit)
- [5] CSRProfileVersion : := The version of the CSR Profile (e.g., v2015-AUG)
- [6] CSRCVEProfile : := cve="CSRProfile.CVE-"[CSRCVEProfileVersion](#)
 e
- [7] CSRCVEProfileVersion : := The version of the CVE Profile (e.g., v2015-AUG)
- [8] SpecExceptions : := spec="[SpecName](#)-"[SpecVersion](#)"
 ns
- [9] SpecName : := The name of the Specification short name with
 periods "." replaced by dash "-" (e.g., ISM-XML)
- [1] SpecVersion : := The version of the specification (e.g., v2015-AUG)
 0]

2.1.1 - Example MIME Types

Below are several examples of MIME type Content-Type headers, note some of the versions are fictional.

- Content-Type : application/dni-tdf+xml; csr=CSRProfile-DTI-v2015-AUG; csr=CSRProfile-Discovery-v2015-AUG ; cve=CSRProfile.CVE-v2015-AUG;
- Content-Type : application/dni-tdf+xml; csr=CSRProfile-DTI-v2015-AUG; csr=CSRProfile-Discovery-v2015-AUG ; cve=CSRProfile.CVE-v2015-AUG; spec=ISM-XML-v2015-SEP
- Content-Type : application/dni-pubs+xml; csr=CSRProfile-DTI-v2015-AUG; csr=CSRProfile-Discovery-v2015-AUG ; cve=CSRProfile.CVE-v2015-AUG;
- Content-Type : application/dni-tdf+xml; csr=CSRProfile-DTI-v2015-AUG; csr=CSRProfile-Discovery-v2015-AUG ; cve=CSRProfile.CVE-v2015-AUG; spec=ISM-CAT-XML-v2015-NOV

2.2 - Mandatory Profile Set

There is a minimum set of profiles that all consuming CSRs MUST support. However, a formal waiver may be submitted to the IC CIO, using the process defined in ICS 500-20,^[20] to exempt a consuming CSR from supporting a particular profile if there is a demonstrable need for an exemption. Mandatory profiles are defined and explained in the following chapters. Producing CSRs MUST support at least one of the mandatory profiles.

Support of combinations of specification versions beyond the profiles defined in this specification is permissible, however, there is no guarantee that other enterprise systems will produce or consume those combinations.

Each profile described in this specification is chosen to fit certain needs and each profile has different levels of support for different use cases. Production systems are encouraged to choose the profile(s) that most fit their needs and development cycles.

**Note**

It should be noted that the Controlled Vocabulary Enumeration (CVE) Profile discussed in [Chapter 5 - CSRProfile.CVE](#) is a singular profile that includes all CVEs. A system implementing one of the functional profiles sets is only responsible for implementing those CVEs that are dependent within that profile set; the system is not responsible for implementing the remaining CVEs.

Each profile should be composed of combinations of specification versions that are tested to work together.

Chapter 3 - Definitions, Interfaces, and Constraints

The CSR profiles are defined by functional use cases that require groupings of structural specifications, which define allowed elements and attributes, with the vocabularies used to populate these structures. As vocabularies tend to change more rapidly than structural specifications, this decoupling allows CSRs to quickly support new vocabularies with minimal impact to the more stable functional specifications. The special set CSRProfile.CVE combines all CVE specifications into a single functional profile for reuse in other functional profiles.

The functional areas are:

1. [Chapter 5 - CSRProfile.CVE](#) A profile of Controlled Vocabulary Enumerations.
2. [Chapter 6 - CSRProfile.Audit](#) A profile for Audit records conforming to ICS 500-27, *Collection and Sharing of Audit Data for Intelligence Community Information Resources by IC Elements*.^[22]
3. [Chapter 7 - CSRProfile.Discovery](#) A profile for Discovery Metadata conforming to ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information*.^[21]
4. [Chapter 8 - CSRProfile.DOMEX](#) A profile for tagging of Document and Media Exploitation (DOMEX) information conforming to DoD Directive 3300.03.^[5]
5. [Chapter 9 - CSRProfile.DTI](#) A profile for Distributed Textual Information (DTI) conforming to ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information*.^[21]
6. [Chapter 10 - CSRProfile.Entities](#) A profile for exchanging Unified Identity Attribute Set (UIAS) and Full Service Directory (FSD) entity attribute information.
7. [Chapter 11 - CSRProfile.MsgTransport](#) A profile for exchanging message records using Information Transport System (ITS) between Community Shared Resource (CSR) systems, such as Audit records.
8. [Chapter 12 - CSRProfile.TDE](#) A profile for Trustable Data Exchange (TDE) using IC Trusted Data Format (IC-TDF) wrapped data conforming to ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information*.^[21]

Chapter 4 - Conformance Validation

4.1 - CSR Systems Receiving data

A CSR system receiving one of the functional profiles:

1. MUST implement all of the currently valid profiles in that functional grouping.
2. SHOULD validate according to the validation strategy for the profile.
3. MUST validate safeguarding information according to the validation strategy for the profile.
4. MUST adhere to all appropriate Access Control Encoding Specification (ACES) that apply to the data.



Note

If the ACES is silent on a specific mark, the CSR MUST follow the IC Markings System Register and Manual^[10] or consult with the originating data steward.

5. SHOULD index appropriate information to enable the functional use case of the profile.

4.2 - CSR Systems Producing data

A CSR system producing one of the functional profiles:

1. MUST implement at least one of the currently valid profiles in that functional grouping.
2. SHOULD validate according to the validation strategy for the profile.
3. MUST validate safeguarding information according to the validation strategy for the profile.
4. MUST adhere to all appropriate ACES that apply to the data.



Note

If the ACES is silent on a specific mark, the CSR MUST follow the IC Markings System Register and Manual^[10] or consult with the originating data steward.

4.3 - IC ITE CSR Systems

A CSR system in IC ITE SHOULD NOT use the Individual portion of the Group & Individual Profile. Due to concerns with long-term maintenance and other enterprise level impacts, IC ITE strongly discourages the use of the Individual portion of the Group & Individual Profile. Access control to an individual can be achieved through the creation of a group containing one or more individuals, which may be placed on one or more documents. A CSR in IC ITE MAY reject information that requires the use of the Individual portion of the Group & Individual Profile.

Chapter 5 - CSRProfile.CVE

5.1 - Overview

The CSRProfile.CVE profile is a collection of CVE Encoding Specifications. It is used in conjunction with other profiles to produce a functioning specification set for implementation, however, not every CVE included in this profile may be necessary for completion of one of the other profiles. In that case, it is permissible to only implement the dependent CVE Encoding Specifications. There is no feature comparison for this functional area because there is only one profile. For detailed information about specific features that a profile set supports, please refer to the Feature Matrix appendix of each specification identified in the profile set.

5.2 - Specification Summary

[Figure 1](#) is an informative, graphical representation of the IC CIO specifications related to this CSR profile. The graphic depicts direct and transitive dependencies. However, the representation 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.

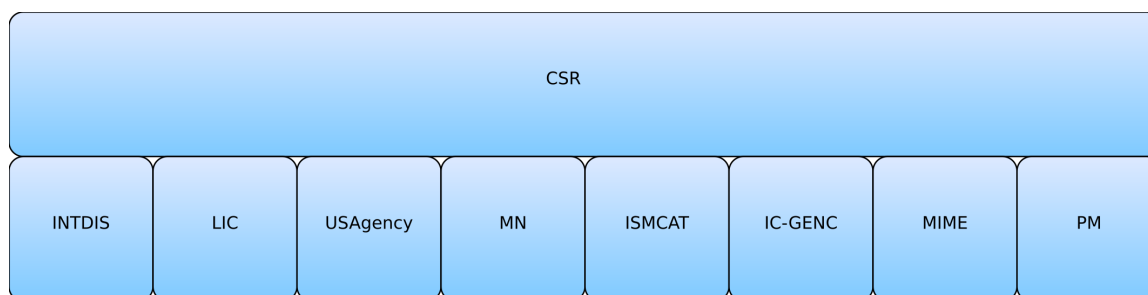


Figure 1 : CSRProfile.CVE Related Specifications

5.3 - Specification Combinations

Table 2 - CSRProfile.CVE Profile Sets

Specification	Profile Sets
	v2017-MAY
IC-GENC ^[12]	v2016-SEP
IntDis ^[25]	v2016-SEP
ISMCAT ^[28]	v2016-SEP
LIC ^[30]	v2015-AUG
MIME ^[31]	v2016-SEP
MN ^[32]	v2017-MAY

Specification	Profile Sets
	v2017-MAY
PM ^[35]	v2017-MAY
USAgency ^[41]	v2017-MAR

5.4 - CSRProfile.CVE.v2017-MAY

CSRProfile.CVE.v2017-MAY is using the latest versions of all relevant specifications at the time of publishing.

Chapter 6 - CSRProfile.Audit

6.1 - Overview

CSRProfile.Audit profiles are for systems that conform with ICS 500-27^[22] and exchange Enterprise Audit data. Each profile is used in conjunction with the CSRProfile.CVE profile to produce a functioning specification set for implementation. [Table 5](#) is a high-level comparison of key features. For detailed information about specific features that a profile set supports, please refer to the Feature Matrix appendix of each specification identified in the profile set.

Table 3 - 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	

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	

Table 5 - CSRProfile.Audit Feature Comparison

Feature	v2015-FEB	v2016-SEP
Updated Network Values	N	F
Compliant with NTK.XML refactoring	N	F
Integrated with UIAS Schema	N	F
Support for unified "MIME Type" CVE	N	F
Support for multiple Responsible Entities and DataSet element	N	F

6.2 - Specification Summary

[Figure 2](#) is an informative, graphical representation of the IC CIO specifications related to this CSR profile. The graphic depicts direct and transitive dependencies. However, the representation 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.

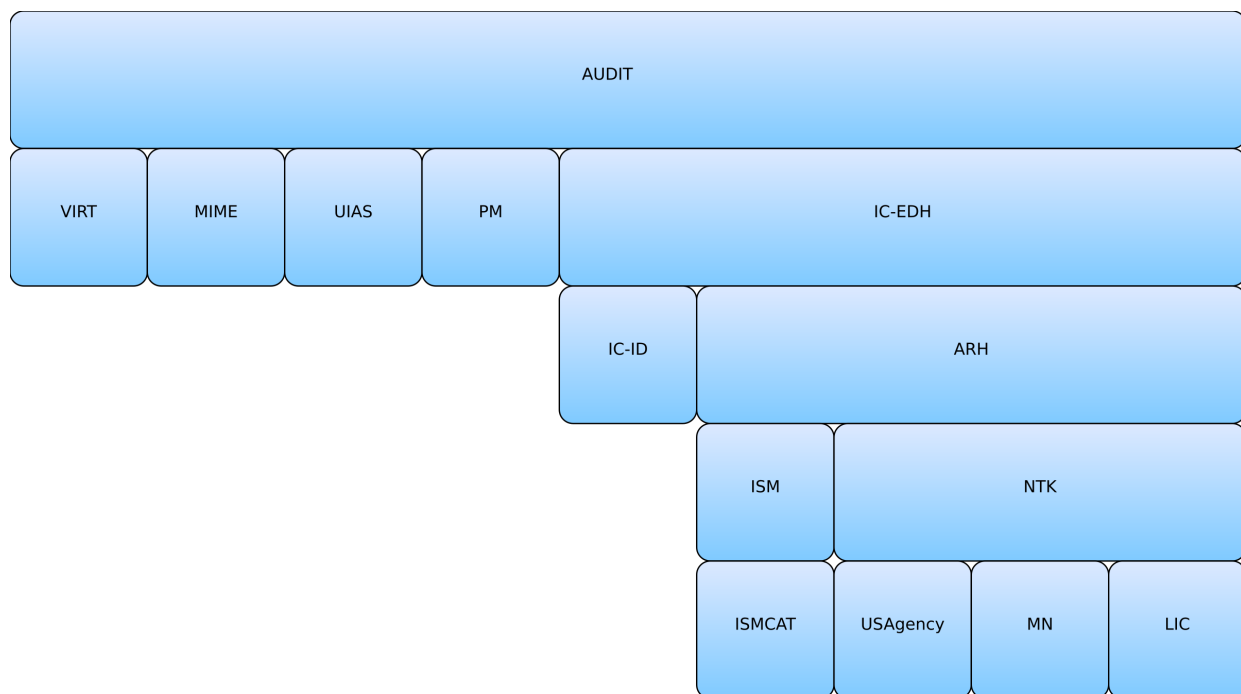


Figure 2 : CSRProfile.Audit Related Specifications

6.3 - Relevant CVE Specifications

The CVE specifications that are relevant to this functional area are listed below. “X” indicates the specification is relevant. The appropriate version of a CVE may be found in the [Chapter 5 - CSRProfile.CVE](#) section.

Table 6 - Relevant CVE Specifications

Specification	Profile Sets	
	v2015-FEB	v2016-SEP
IC-GENC ^[12]		
IntDis ^[25]		
ISMCAT ^[28]	X	X
LIC ^[30]		X
MIME ^[31]		X
MN ^[32]		X
PM ^[35]		X
USAgency ^[41]	X	X

6.4 - Specification Combinations

Table 7 - CSRProfile.Audit Profile Sets

Specification	Profile Sets	
	v2015-FEB	v2016-SEP
AUDIT ^[3]	v2014-DEC	v2016-SEP
IC-EDH ^[11]	v4	v2016-SEP
ARH ^[2]	v3	v3
OC-NTK ^[34]	v1	n/a
ICO-NTK ^[18]	v1	n/a
PROPIN-NTK ^[36]	v1	n/a
NTK ^[33]	v10	v2015-AUG
ISM ^[27]	v2014-DEC	v2016-SEP
VIRT ^[42]	v1	v2015-AUG
IC-ID ^[13]	v1	v1

6.5 - CSRProfile.Audit.v2015-FEB

CSRProfile.Audit.v2015-FEB enhances AUDIT with the 2014-DEC version and updates ISM.

- Does not correctly deal with several ISM issues.
- Does not support 2015-AUG NTK refactor which includes new profiles for Misson-Need, EXDIS, NODIS, Permissive, Restrictive, and updated representation for Groups & Individuals.

6.6 - CSRProfile.Audit.v2016-SEP

CSRProfile.Audit.v2016-SEP enhances AUDIT with significant changes to the AUDIT spec itself including inclusion of UIAS, and updates related to changes in ISM and IC-EDH.

Chapter 7 - CSRProfile.Discovery

7.1 - Overview

CSRProfile.Discovery profiles are for systems that conform with ICS 500-21^[21] and send or receive discovery metadata. Each profile is used in conjunction with the CSRProfile.CVE profile to produce a functioning specification set for implementation. [Table 10](#) is a high-level comparison of key features. For detailed information about specific features that a profile set supports, please refer to the Feature Matrix appendix of each specification identified in the profile set.

Table 8 - 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	

Table 9 - 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	

Table 10 - CSRProfile.Discovery Feature Comparison

CSRProfile.Discovery Feature Comparison				
Feature	v2014-MAR	v2015-AUG	v2015-NOV	v2016-SEP
Support for PM	N	N	F	F
Support for unified "MIME Type" CVE	N	N	N	F
Support for multiple Responsible Entities and DataSet element	N	N	N	F
Support for ISM attributes "noAggregation" and "hasApproximateMarkings."	N	N	N	F

CSRProfile.Discovery Feature Comparison				
Feature	v2014-MAR	v2015-AUG	v2015-NOV	v2016-SEP
Support for improved releasability decisions by incorporation of Tetragraph Taxonomy into ISM Schematron rules.	N	N	N	F

7.2 - Specification Summary

[Figure 3](#) is an informative, graphical representation of the IC CIO specifications related to this CSR profile. The graphic depicts direct and transitive dependencies. However, the representation 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.

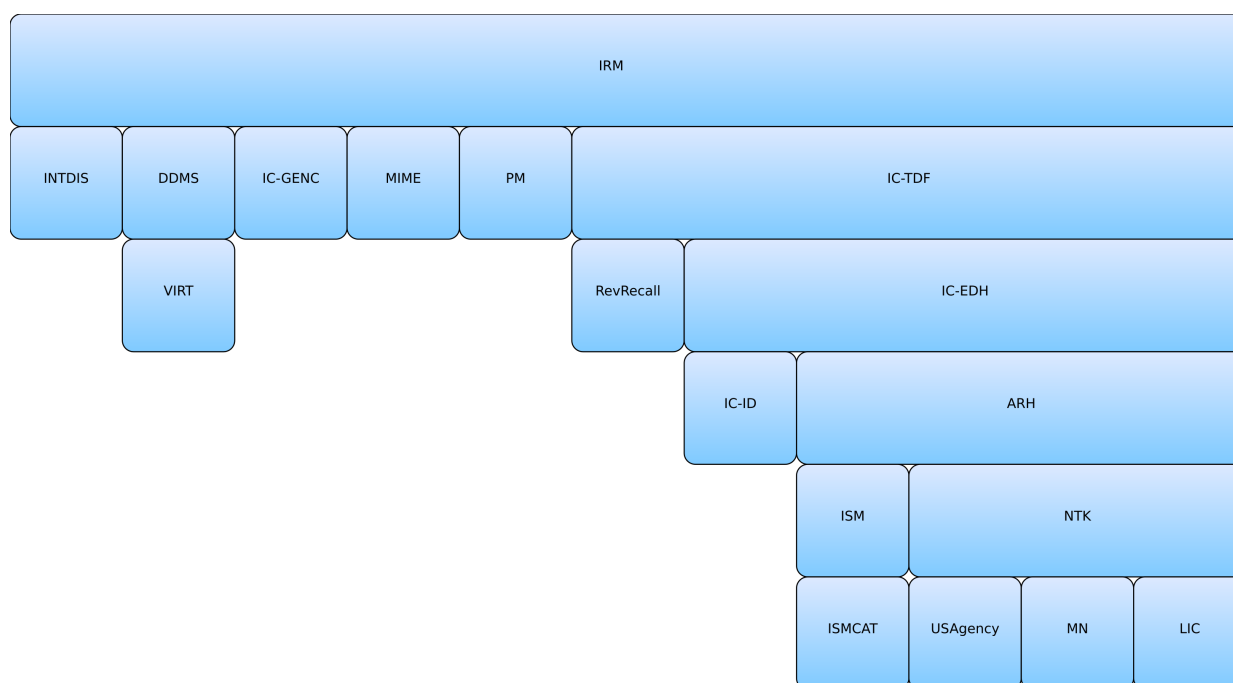


Figure 3 : CSRProfile.Discovery Related Specifications

7.3 - Relevant CVE Specifications

The CVE specifications that are relevant to this functional area are listed below. “X” indicates the specification is relevant. The appropriate version of a CVE may be found in the [Chapter 5 - CSRProfile.CVE](#) section.

Table 11 - Relevant CVE Specifications

Specification	Profile Sets			
	v2014-MAR	v2015-AUG	v2015-NOV	v2016-SEP
IC-GENC ^[12]	X	X	X	X
IntDis ^[25]				X
ISMCAT ^[28]	X	X	X	X
LIC ^[30]		X	X	X
MIME ^[31]				X
MN ^[32]		X	X	X
PM ^[35]			X	X
USAgency ^[41]	X	X	X	X

7.4 - Specification Combinations

Table 12 - Specification Combinations

Specification	Profile Sets			
	v2014-MAR	v2015-AUG	v2015-NOV	v2016-SEP
IRM ^[26]	v12	v2014-DEC	v2015-NOV	v2016-SEP
DDMS ^[4] ^a	v5	v5	v5	v5
IC-TDF ^[14]	v3	v2014-DEC	v2014-DEC	v2014-DEC
IC-EDH ^[11]	v4	v2015-AUG	v2015-AUG	v2016-SEP
ARH ^[2]	v3	v3	v3	v3
RevRecall ^[38]	v1	v2014-DEC	v2014-DEC	v2014-DEC
ICO-NTK ^[18]	v1	n/a	n/a	n/a
PROPIN-NTK ^[36]	v1	n/a	n/a	n/a
OC-NTK ^[34]	v1	n/a	n/a	n/a
NTK ^[33]	v10	v2015-AUG	v2015-AUG	v2015-AUG
ISM ^[27]	v13	v2015-AUG	v2015-AUG	v2016-SEP
VIRT ^[42]	v1	v2015-AUG	v2015-AUG	v2015-AUG
IC-ID ^[13]	v1	v1	v1	v1

^a DDMS is a direct dependency of IRM and is not authored by the IC CIO. It is included in this table for informational purposes only.

7.5 - CSRProfile.Discovery.v2014-MAR

CSRProfile.Discovery.v2014-MAR does not support:

- The correct use of attributes on ddms:subDivisionCode rule (using codespace and code instead of qualifier and value).

- Requiring a DDMS assertion if an IRM Trusted Data Object structured statement exists.
- Does not support 2015-AUG refactor of NTK which includes new profiles for Misson-Need, EXDIS, NODIS, Permissive, Restrictive, and updated representation for Groups & Individuals enabling better access control mechanisms.

7.6 - CSRProfile.Discovery.v2015-AUG

CSRProfile.Discovery.v2015-AUG uses the latest versions of all relevant specifications as of the 2015-AUG publishing.

7.7 - CSRProfile.Discovery.v2015-NOV

CSRProfile.Discovery.v2015-NOV is updated to use the new IRM.

- Does not support the updated EDH harmonizing with NSA EDH. Producers of documents that need to use the Originator Role for ResponsibleEntity should use CSRProfile.Discovery.v2016-SEP instead of CSRProfile.Discovery.v2015-NOV.
- Producers of documents that are part of a dataset should consider using CSRProfile.Discovery.v2016-SEP instead of CSRProfile.Discovery.v2015-NOV.
- Does not support harmonized MIME type CVE in IRM.. Producers of documents that need MIME types found in CSRProfile.Discovery.v2016-SEP, but not in CSRProfile.Discovery.v2015-NOV, should use CSRProfile.Discovery.v2016-SEP.

7.8 - CSRProfile.Discovery.v2016-SEP

CSRProfile.Discovery.v2016-SEP is updated to use the new MIME CVE and updated IC-EDH, ISM, and NTK.

Chapter 8 - CSRProfile.DOMEX

8.1 - Overview

CSRProfile.DOMEX profiles are for systems that exchange Document and Media Exploitation (DOMEX) data. Each profile is used in conjunction with the CSRProfile.CVE profile to produce a functioning specification set for implementation. [Table 15](#) is a high-level comparison of key features. For detailed information about specific features that a profile set supports, please refer to the Feature Matrix appendix of each specification identified in the profile set.

Table 13 - 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	

Table 14 - 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	

Table 15 - CSRProfile.DOMEX Feature Comparison

Feature	v2015-AUG	v2015-NOV	v2016-SEP
Dependency on PM	N	F	F
Support for unified "MIME Type" CVE	N	N	F
Support for multiple Responsible Entities and DataSet element	N	N	F

8.2 - Specification Summary

[Figure 4](#) is an informative, graphical representation of the IC CIO specifications related to this CSRProfile. The graphic depicts direct and transitive dependencies. However, the representation 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.

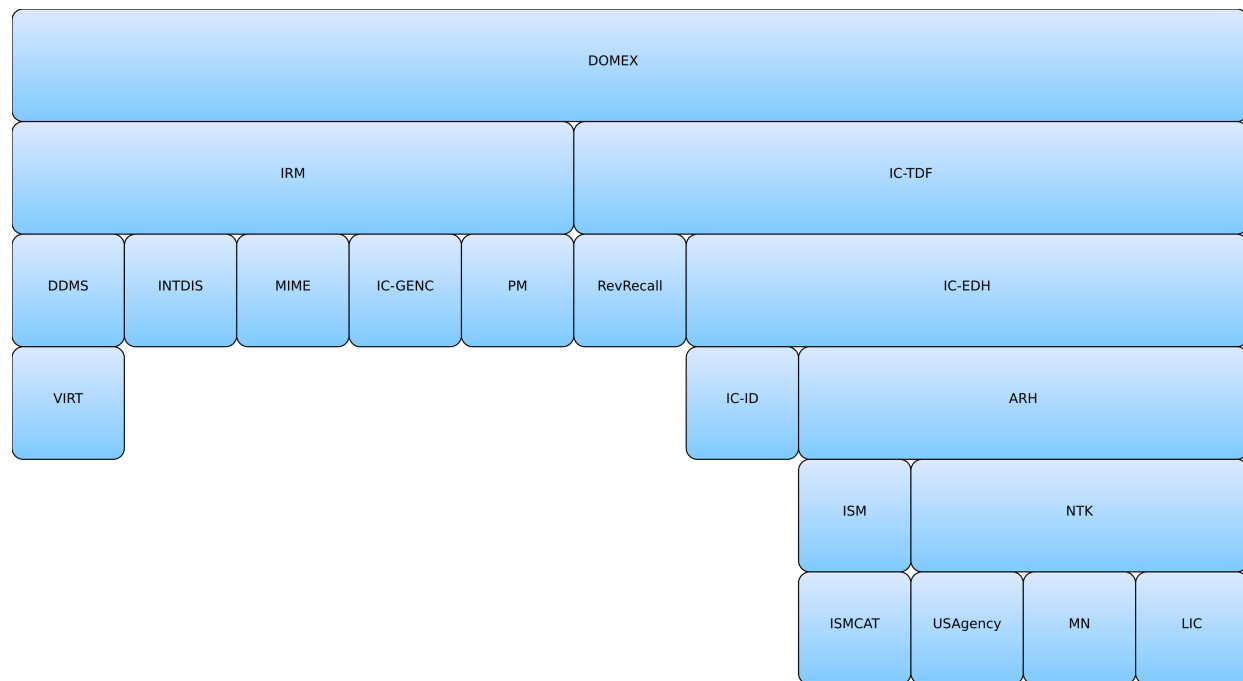


Figure 4 : CSRProfile.DOMEX Related Specifications

8.3 - Relevant CVE Specifications

The CVE specifications that are relevant to this functional area are listed below. “X” indicates the specification is relevant. The appropriate version of a CVE may be found in the [Chapter 5 - CSRProfile.CVE](#) section.

Table 16 - Relevant CVE Specifications

Specification	Profile Sets		
	v2015-AUG	v2015-NOV	v2016-SEP
IC-GENC ^[12]	X	X	X
IntDis ^[25]			X
ISMCAT ^[28]	X	X	X
LIC ^[30]	X	X	X
MIME ^[31]			
MN ^[32]	X	X	X
PM ^[35]		X	X
USAgency ^[41]	X	X	X

8.4 - Specification Combinations

Table 17 - CSRProfile.DOMEX Profile Sets

Specification	v2015-AUG	v2015-NOV	v2016-SEP
DOMEX ^[7]	v2015-AUG	v2015-AUG	v2015-AUG
IRM ^[26]	v2014-DEC	v2015-NOV	v2016-SEP
DDMS ^[4] ^a	v5	v5	v5
IC-TDF ^[14]	v2014-DEC	v2014-DEC	v2014-DEC
IC-EDH ^[11]	v2015-AUG	v2015-AUG	v2016-SEP
ARH ^[2]	v3	v3	v3
RevRecall ^[38]	v2014-DEC	v2014-DEC	v2014-DEC
NTK ^[33]	v2015-AUG	v2015-AUG	v2015-AUG
ISM ^[27]	v2015-AUG	v2015-AUG	v2016-SEP
VIRT ^[42]	v2015-AUG	v2015-AUG	v2015-AUG
IC-ID ^[13]	v1	v1	v1

^a DDMS is a direct dependency of IRM and is not authored by the IC CIO. It is included in this table for informational purposes only.

8.5 - CSRProfile.DOMEX.v2015-AUG

CSRProfile.DOMEX.v2015-AUG used the latest versions of all relevant specifications from 2015-AUG.

8.6 - CSRProfile.DOMEX.v2015-NOV

CSRProfile.DOMEX.v2015-NOV is updated to use the new IRM.

- Does not support the updated EDH harmonizing with NSA EDH.
- Does not support harmonized MIME type CVE in IRM.

8.7 - CSRProfile.DOMEX.v2016-SEP

CSRProfile.DOMEX.v2016-SEP is updated to use the new IRM, MIME CVE and ISM.

Chapter 9 - CSRProfile.DTI

9.1 - Overview

CSRProfile.DTI profiles are for systems that conform with ICS 500-21^[21] and exchange “Disseminated Textual Information” (DTI) as defined by ICS 500-21.^[21] Each profile is used in conjunction with the CSRProfile.CVE profile to produce a functioning specification set for implementation. [Table 20](#) is a high-level comparison of key features. For detailed information about specific features that a profile set supports, please refer to the Feature Matrix appendix of each specification identified in the profile set.

ICS 500-21^[21] definitions for reference:

- Disseminated Textual Information

Textual information (see definition below) that is broadly provided to the enterprise for discovery and retrieval by appropriate consumers, either through the ordinary course of business or in response to a request following discovery.

- Textual Information

Information consisting of mostly text supplemented by interspersed non-textual information, such as assessments, studies, estimates, compilations, reports, and other document-oriented information.

Table 18 - 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	

Table 19 - Feature Summary Legend

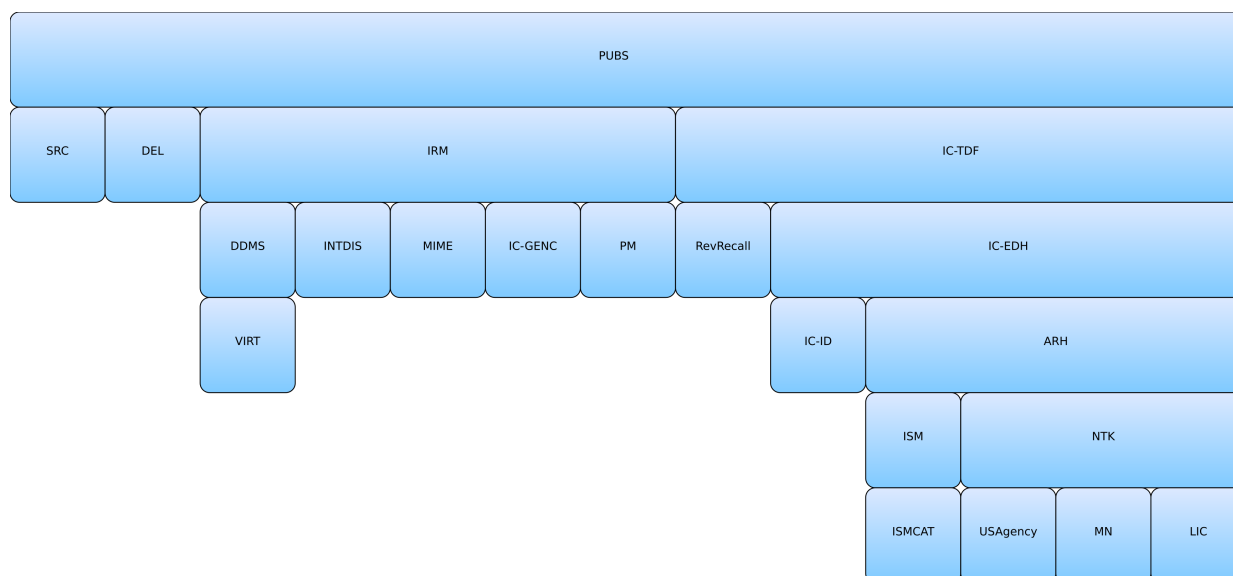
Key	Description
F	Full (able to comply and verified by spec to some degree)
P	Partial (Able to comply but not verifiable)
N	Non-compliance (Can't comply)
N/A	Not Applicable. Feature is no longer required.
Cell Colors represent the same information as the Key value	

Table 20 - CSRProfile.DTI Feature Comparison

Feature	v2014-MAR	v2015-AUG	v2015-NOV	v2016-SEP
Dependency on PM	N	N	F	F
Support for unified "MIME Type" CVE	N	N	N	F
Support for multiple Responsible Entities and DataSet element	N	N	N	F
Support for ISM attributes "noAggregation" and "hasApproximateMarkings."	N	N	N	F
Support for improved releasability decisions by incorporation of Tetragraph Taxonomy into ISM Schematron rules.	N	N	N	F

9.2 - Specification Summary

[Figure 5](#) is an informative, graphical representation of the IC CIO specifications related to this CSR profile. The graphic depicts direct and transitive dependencies. However, the representation 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.

**Figure 5 : CSRProfile.DTI Related Specifications**

9.3 - Relevant CVE Specifications

The CVE specifications that are relevant to this functional area are listed below. “X” indicates the specification is relevant. The appropriate version of a CVE may be found in the [Chapter 5 - CSRProfile.CVE](#) section.

Table 21 - Relevant CVE Specifications

Specification	Profile Sets			
	v2014-MAR	v2015-AUG	v2015-NOV	v2016-SEP
IC-GENC ^[12]	X	X	X	X
IntDis ^[25]		X	X	X
ISMCAT ^[28]	X	X	X	X
LIC ^[30]		X	X	X
MIME ^[31]				X
MN ^[32]		X	X	X
PM ^[35]			X	X
USAgency ^[41]	X	X	X	X

9.4 - Specification Combinations

Table 22 - CSRProfile.DTI Profile Sets

Specification	v2014-MAR	v2015-AUG	v2015-NOV	v2016-SEP
PUBS ^[37]	v12	v2015-AUG	v2015-AUG	v2016-SEP
IRM ^[26]	v12	v2014-DEC	v2015-NOV	v2016-SEP
DDMS ^[4] a	v5	v5	v5	v5
IC-TDF ^[14]	v3	v2014-DEC	v2014-DEC	v2014-DEC
IC-EDH ^[11]	v4	v2015-AUG	v2015-DEC	v2016-SEP
ARH ^[2]	v3	v3	v3	v3
RevRecall ^[38]	v1	v2014-DEC	v2014-DEC	v2014-DEC
OC-NTK ^[34]	v1	n/a	n/a	n/a
ICO-NTK ^[18]	v1	n/a	n/a	n/a
PROPIN-NTK ^[36]	v1	n/a	n/a	n/a
NTK ^[33]	v10	v2015-AUG	v2015-AUG	v2015-AUG
ISM ^[27]	v13	v2015-AUG	v2015-AUG	v2016-SEP
VIRT ^[42]	v1	v2015-AUG	v2015-AUG	v2015-AUG
IC-ID ^[13]	v1	v1	v1	v1

Specification	v2014-MAR	v2015-AUG	v2015-NOV	v2016-SEP
SRC ^[39]	n/a	v2015-AUG	v2015-AUG	v2015-AUG

^a DDMS is a direct dependency of IRM and is not authored by the IC CIO. It is included in this table for informational purposes only.

9.5 - CSRProfile.DTI.v2014-MAR

CSRProfile.DTI.v2014-MAR concerns:

- Has duplicate and potentially contradictory revision/recall information in PUBS that was removed in PUBS.v2014-DEC.
- Does not correctly deal with several ISM issues.
- Does not support the new location of Revision Recall in a TDF; this may hamper its use where revision recall is a priority.
- Does not support full set of requirements for Source Citations as defined in the 23 January 2015 version of ICD 206^[15]. Does support the mandatory fields but not all the optional fields including Appended Reference Citations (ARCs).
- Does not support 2015-AUG refactor of NTK which includes new profiles for Misson-Need, EXDIS, NODIS, Permissive, Restrictive, and updated representation for Groups & Individuals enabling better access control mechanisms.

9.6 - CSRProfile.DTI.v2015-AUG

CSRProfile.DTI.v2015-AUG is using the latest versions of all relevant specifications from 2015-AUG.

9.7 - CSRProfile.DTI.v2015-NOV

CSRProfile.DTI.v2015-NOV is updated to use the new IRM.

- Does not support the updated EDH harmonizing with NSA EDH. Producers of documents that need to use the Originator Role for ResponsibleEntity should use CSRProfile.DTI.v2016-SEP instead of CSRProfile.DTI.v2015-NOV.
- Producers of documents that are part of a dataset should consider using CSRProfile.DTI.v2016-SEP instead of CSRProfile.DTI.v2015-NOV.
- Does not support harmonized MIME type CVE in IRM and PUBS. Producers of documents that need MIME types found in CSRProfile.DTI.v2016-SEP, but not in CSRProfile.DTI.v2015-NOV, should use CSRProfile.DTI.v2016-SEP.

9.8 - CSRProfile.DTI.v2016-SEP

CSRProfile.DTI.v2016-SEP is updated to use the new IRM, MIME CVE and ISM.

Chapter 10 - CSRProfile.Entities

10.1 - Overview

CSRProfile.Entities profiles are for systems that exchange UIAS entity attribute information. Each profile is used in conjunction with the CSRProfile.CVE profile to produce a functioning specification set for implementation. There is no feature comparison for this functional area because there is only one profile. For detailed information about specific features that a profile set supports, please refer to the Feature Matrix appendix of each specification identified in the profile set.

10.2 - Specification summary

[Figure 6](#) is an informative, graphical representation of the IC CIO specifications related to this CSR profile. The graphic depicts direct and transitive dependencies. However, the representation 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.

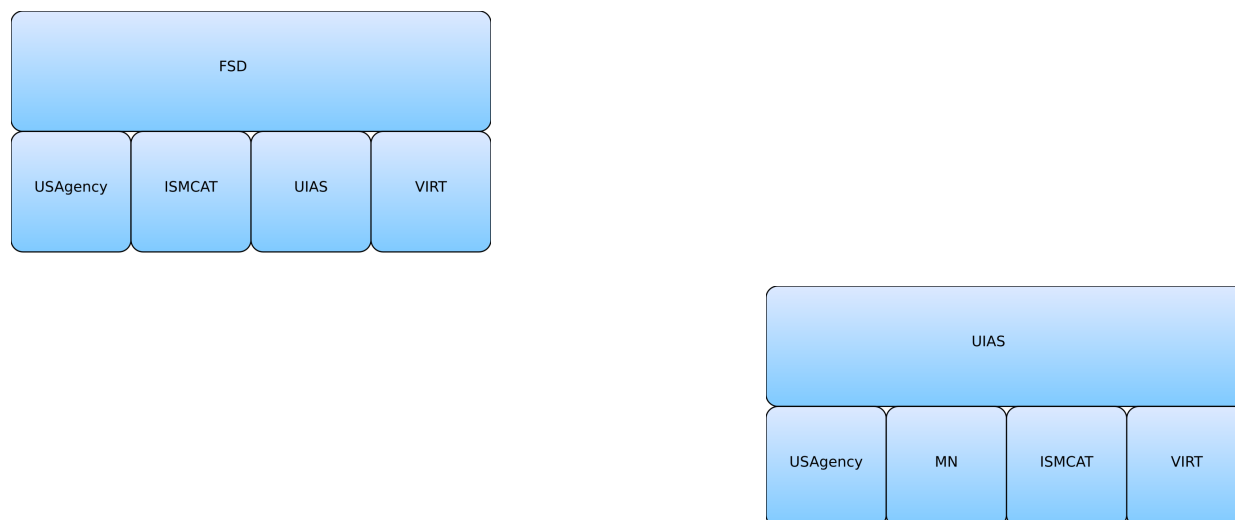


Figure 6 : CSRProfile.Entities Related Specifications

10.3 - Relevant CVE Specifications

The CVE specifications that are relevant to this functional area are listed below. “X” indicates the specification is relevant. The appropriate version of a CVE may be found in the [Chapter 5 - CSRProfile.CVE](#) section.

Table 23 - Relevant CVE Specifications

Specification	Profile Sets
	v2016-SEP
IC-GENC ^[12]	
IntDis ^[25]	
ISMCAT ^[28]	
LIC ^[30]	
MN ^[32]	X
PM ^[35]	
USAgency ^[41]	X

10.4 - Specification Combinations

Table 24 - CSRProfile.Entities Profile Sets

Specification	v2016-SEP
FSD ^[8]	v2015-AUG
UIAS.XML ^[40]	v2016-SEP
VIRT ^[42]	v2015-AUG

10.5 - CSRProfile.Entities.v2016-SEP

CSRProfile.Entities.v2016-SEP is using the latest versions of all relevant specifications at the time of publishing.

Chapter 11 - CSRProfile.MsgTransport

11.1 - Overview

CSRProfile.MsgTransport profiles are for systems that transmit message records via the ITS, such as Audit Records. Each profile is used in conjunction with the CSRProfile.CVE profile to produce a functioning specification set for implementation. For detailed information about specific features that a profile set supports, please refer to the Feature Matrix appendix of each specification identified in the profile set.

Table 25 - 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	

Table 26 - 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	

Table 27 - CSRProfile.MsgTransport Feature Comparison

Feature	v2015-FEB	v2016-SEP
Compliant with NTK.XML refactoring	N	F
Support for multiple Responsible Entities and DataSet element	N	F

11.2 - Specification Summary

[Figure 7](#) is an informative, graphical representation of the IC CIO specifications related to this CSR profile. The graphic depicts direct and transitive dependencies. However, the representation 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.

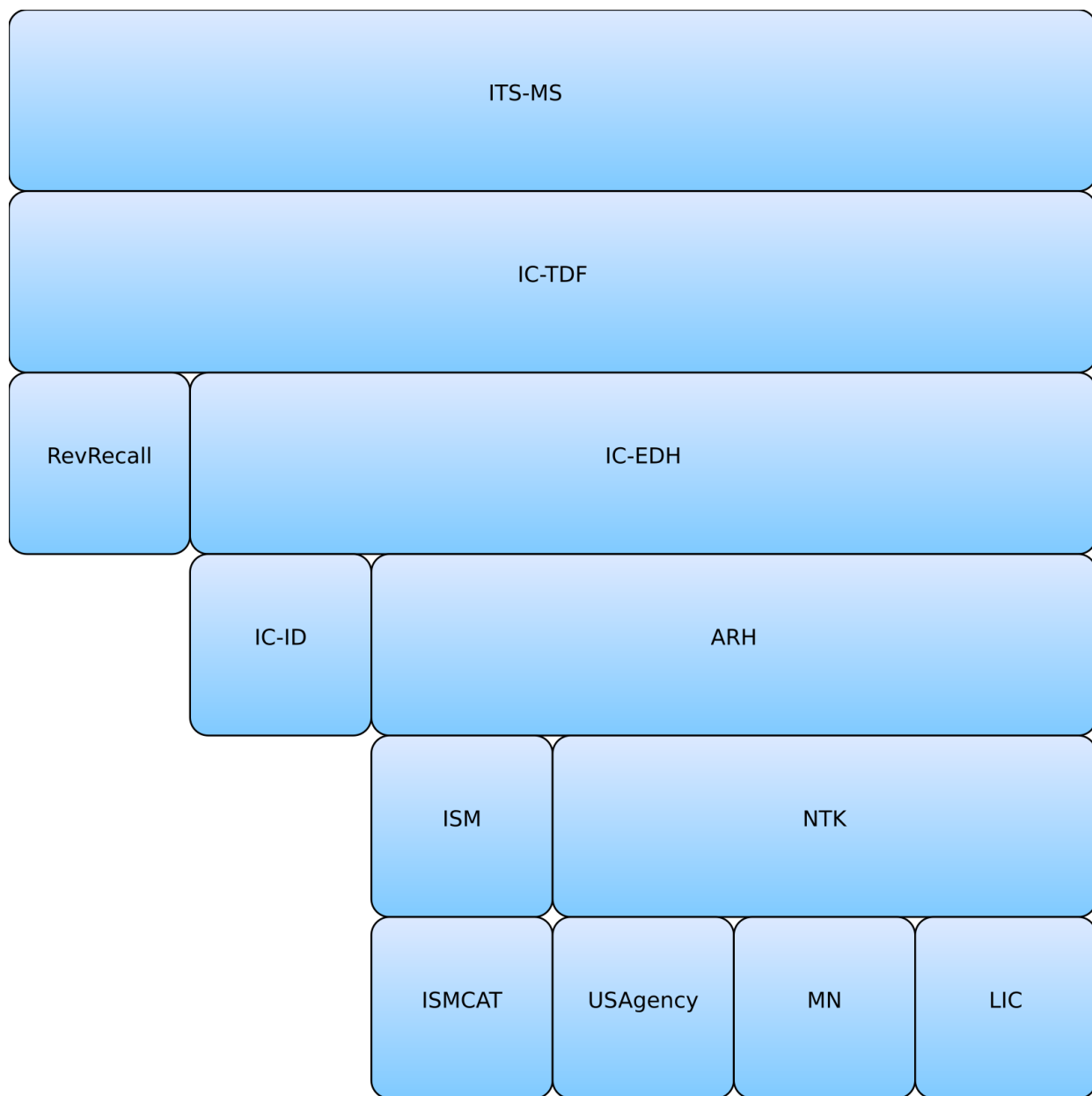


Figure 7 : CSRProfile.MsgTransport Related Specifications

11.3 - Relevant CVE Specifications

The CVE specifications that are relevant to this functional area are listed below. “X” indicates the specification is relevant. The appropriate version of a CVE may be found in the [Chapter 5 - CSRProfile.CVE](#) section.

Table 28 - Relevant CVE Specifications

Specification	Profile Sets	
	v2015-FEB	v2016-SEP
IC-GENC ^[12]		
IntDis ^[25]		
ISMCAT ^[28]	X	X
LIC ^[30]		X
MN ^[32]		X
PM ^[35]		
USAgency ^[41]	X	X

11.4 - Specification Combinations

Table 29 - CSRProfile.MsgTransport Profile Sets

Specification	Profile Sets	
	v2015-FEB	v2016-SEP
ITS-MS ^[29]	v2015-FEB	v2015-FEB
IC-TDF ^[14]	v2014-DEC	v2014-DEC
IC-EDH ^[11]	v4	v2016-SEP
ARH ^[2]	v3	v3
RevRecall ^[38]	v2014-DEC	v2014-DEC
OC-NTK ^[34]	v1	n/a
ICO-NTK ^[18]	v1	n/a
PROPIN-NTK ^[36]	v1	n/a
NTK ^[33]	v10	v2015-AUG
ISM ^[27]	v2014-DEC	v2016-SEP
VIRT ^[42]	v1	v2015-AUG
IC-ID ^[13]	v1	v1

11.5 - CSRProfile.MsgTransport.v2015-FEB

CSRProfile.MsgTransport.v2015-FEB is using the 2014-DEC and 2015-FEB versions of the relevant specifications:

- Does not correctly deal with several ISM issues.
- Does not support 2015-AUG NTK refactor which includes new profiles for Mission-Need, EXDIS, NODIS, Permissive, Restrictive, and updated representation for Groups & Individuals enabling better access control mechanisms.

11.6 - CSRProfile.MsgTransport.v2016-SEP

CSRProfile.MsgTransport.v2016-SEP is using the latest versions of all relevant specifications at the time of publishing.

Chapter 12 - CSRProfile.TDE

12.1 - Overview

CSRProfile.TDE profiles are for systems that need to wrap data with security and handling information for Trustable Data Exchange (TDE) across the IC enterprise. Each profile is used in conjunction with the CSRProfile.CVE profile to produce a functioning specification set for implementation. [Table 32](#) is a high level comparison of key features. For detailed information about specific features that a profile set supports, please refer to the Feature Matrix appendix of each specification identified in the profile set.

Table 30 - 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	

Table 31 - 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	

Table 32 - CSRProfile.TDE Feature Comparison

Feature	v2014-MAR	v2015-AUG	v2016-SEP
Support for multiple Responsible Entities and DataSet element	N	N	F
Support for ISM attributes "noAggregation" and "hasApproximateMarkings."	N	N	F
Support for improved releasability decisions by incorporation of Tetragraph Taxonomy into ISM Schematron rules.	N	N	F

12.2 - Specification Summary

[Figure 8](#) is an informative, graphical representation of the IC CIO specifications related to this CSR profile. The graphic depicts direct and transitive dependencies. However, the representation 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.

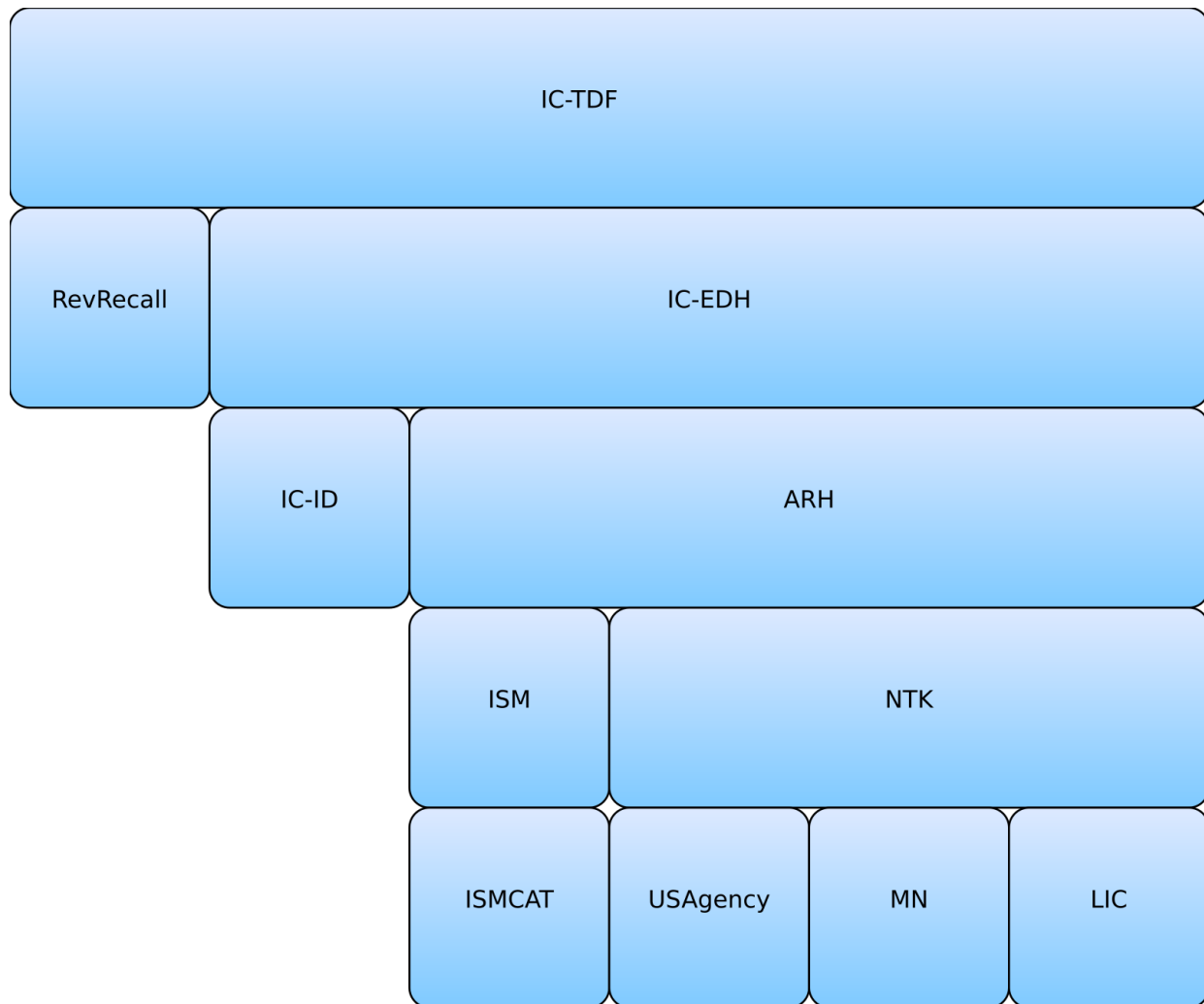


Figure 8 : CSRProfile.TDE Related Specifications

12.3 - Relevant CVE Specifications

The CVE specifications that are relevant to this functional area are listed below. “X” indicates the specification is relevant. The appropriate version of a CVE may be found in the [Chapter 5 - CSRProfile.CVE](#) section.

Table 33 - Relevant CVE Specifications

Specification	Profile Sets		
	v2014-MAR	v2015-AUG	v2016-SEP
IC-GENC ^[12]			
IntDis ^[25]			
ISMCAT ^[28]	X	X	X
LIC ^[30]		X	X
MN ^[32]		X	X
PM ^[35]			
USAgency ^[41]	X	X	X

12.4 - Specification Combinations

Table 34 - CSRProfile.TDE Profile Sets

Specification	v2014-MAR	v2015-AUG	v2016-SEP
IC-TDF ^[14]	v3	v2014-DEC	v2014-DEC
IC-EDH ^[11]	v4	v2015-AUG	v2016-SEP
ARH ^[2]	v3	v3	v3
RevRecall ^[38]	v1	v2014-DEC	v2014-DEC
OC-NTK ^[34]	v1	n/a	n/a
ICO-NTK ^[18]	v1	n/a	n/a
PROPIN-NTK ^[36]	v1	n/a	n/a
NTK ^[33]	v10	v2015-AUG	v2015-AUG
ISM ^[27]	v13	v2015-AUG	v2016-SEP
IC-ID ^[13]	v1	v1	v1

12.5 - CSRProfile.TDE.v2014-MAR

CSRProfile.TDE.v2014-MAR concerns:

- Does not correctly deal with several ISM issues.
- Does not support the new location of Revision Recall in a TDF this may hamper its use where revision recall is a priority.
- Does not support 2015-AUG NTK refactor which includes new profiles for Mission-Need, EXDIS, NODIS, Permissive, Restrictive, and updated representation for Groups & Individuals enabling better access control mechanisms.

12.6 - CSRProfile.TDE.v2015-AUG

CSRProfile.TDE.v2015-AUG is using the latest versions of all relevant specifications from 2015-AUG.

- Does not support the updated EDH harmonizing with NSA EDH.
- Does not support harmonized MIME type CVE in IRM.

12.7 - CSRProfile.TDE.v2016-SEP

CSRProfile.TDE.v2016-SEP is using the latest versions of all relevant specifications at the time of publishing.

Appendix A Feature Summary

The following table summarizes major features by version for CSR and all dependent specs. The “Required date” is the date when systems should support a feature based on the specified driver. Executive Orders, ISOO notices, ICD and other policy documents have a variety of effective dates.

A.1. CSR Specification Feature Comparison

Table 35 - 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	

Table 36 - 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	

Table 37 - CSR Specification Feature Comparison

Feature	v1	v2015-AUG	v2015-NOV	v2016-SEP	v2017-MAR	v2017-MAY
Profiles are complete sets named after dogs	F	N/A	N/A	N/A	N/A	N/A
Profiles are broken up into functional grouping	N	F	F	F	F	F
A CVE profile separated from "structural" profiles to allow mixing	N	F	F	F	F	F
Updated DISCOVERY, DOMEX, and DTI profiles to use IRM and PM	N	N	F	F	F	F

Appendix B Change History

[Table 38](#) summarizes the version identifier history for this DES.

Table 38 - DES Version Identifier History

Version	Date	Purpose
1	14 March 2014	Initial Release
2015-AUG	13 August 2015	Routine revision to technical specification. For details of changes, see Section B.5 - V2015-AUG Change Summary
2015-NOV	20 November 2015	Routine revision to technical specification. For details of changes, see Section B.4 - V2015-NOV Change Summary
2016-SEP	9 September 2016	Routine revision to technical specification. For details of changes, see Section B.3 - V2016-SEP Change Summary
2017-MAR	13 March 2017	Routine revision to technical specification. For details of changes, see Section B.2 - V2017-MAR Change Summary
2017-MAY	22 May 2017	Routine revision to technical specification. For details of changes, see Section B.1 - 2017-MAY Change Summary

B.1 - 2017-MAY Change Summary

Significant drivers for Version 2017-MAY include:

- DDII updates to values in PM, MN, MNT as of 2017-05-18

The following table summarizes the changes made to 2017-MAR in developing 2017-MAY.

Table 39 - Data Encoding Specification 2017-MAY Change Summary

Change	Artifacts Changed	Compatibility Notes
Updated to new PM, MN, and MNT CVEs. (CR-2017-019)	DES	Systems may need to be updated to handle new/updated values.

B.2 - V2017-MAR Change Summary

Significant drivers for Version v2017-MAR include:

- New version of USAgency CVE published.

The following table summarizes the changes made to v2017-SEP in developing v2017-MAR.

Table 40 - Data Encoding Specification V2017-MAR Change Summary

Change	Artifacts changed	Compatibility Notes
Update CVE profile for USAgency from 2016-SEP to 2017-MAR (CR-2017-012)	DES	Data generation and Ingestion systems that rely on these profiles need to be updated.

B.3 - V2016-SEP Change Summary

Significant drivers for Version v2016-SEP include:

- Removed v2014-MAR profiles for AUDIT and DOMEX as they contained retired specifications.
- Added v2016-SEP profiles for new sets.

The following table summarizes the changes made to v2015-NOV in developing v2016-SEP.

Table 41 - Data Encoding Specification V2016-SEP Change Summary

Change	Artifacts changed	Compatibility Notes
Removed v2014-MAR profiles for AUDIT and DOMEX	DES	Data generation and Ingestion systems that rely on these profiles need to be updated.
Added v2016-SEP profiles for new sets	DES	Data generation and Ingestion systems need to be updated to handle the updated profiles.
Updated CVE profile	DES	Data generation and Ingestion systems that rely on these profiles need to be updated.
Update applicability section to reflect a requirement to comply with Law/Policy (CR-2016-063)	Documentation	Implementers must verify that they are complying with applicable laws and policies.

B.4 - V2015-NOV Change Summary

Significant drivers for Version v2015-NOV include:

- Enhancements to CSR updating IRM, DOMEX, and DTI profiles to use PM in 2015-NOV release.

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

Table 42 - Data Encoding Specification V2015-NOV Change Summary

Change	Artifacts changed	Compatibility Notes
Updated DISCOVERY, DOMEX, and DTI profiles to use PM in 2015-NOV release.	DES	Data generation and Ingestion systems need to be updated to handle the updated profiles.

B.5 - V2015-AUG Change Summary

Significant drivers for Version v2015-AUG include:

- Enhancement to CSR adding MIME Type to designate the specific CSR version
- Refactoring of CSR to have functional groupings

The following table summarizes the changes made to V1 in developing v2015-AUG.

Table 43 - Data Encoding Specification V2015-AUG Change Summary

Change	Artifacts changed	Compatibility Notes
Added MIME Type to indicate any/all applicable CSR versions.	DES	Data generation and Ingestion systems need to be updated to utilize MIME Type for CSR version(s).
Removed the previous naming convention and created functional groupings.	DES	Data generation and Ingestion systems need to be updated to handle the profiles.

Appendix C List of Abbreviations

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

ABNF	Augmented Backus-Naur Form
ACES	Access Control Encoding Specification
CSR	Community Shared Resource
CVE	Controlled Vocabulary Enumeration
DDMS	Department of Defense Discovery Metadata Specification
DES	Data Encoding Specification
DNI	Director of National Intelligence
DOD	Department of Defense
DOMEX	Document and Media Exploitation
DTI	Disseminated Textual Information
EDH	Enterprise Data Header
ESB	Enterprise Standards Baseline
FSD	Full Service Directory
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IETF	Internet Engineering Task Force
IRM	Information Resource Metadata
ISM	Information Security Markings
ISOO	Information Security Oversight Office

IT	Information Technology
ITS	Information Transport Service
MIME	Multipurpose Internet Mail Extensions
NSA	National Security Agency
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PM	Production Metrics
PUBS	Intelligence Publications
RFC	Request for Comments
TDE	Trustable Data Exchange
TDF	Trusted Data Format
UIAS	Unified Identity Attribute Set
XML	Extensible Markup Language

Appendix D Bibliography

Bibliography

[1] ADD

ADD

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

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

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

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

[2] ARH.XML

ARH.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Access Rights and Handling (ARH.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/Fub6Gnw>

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

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

[3] AUDIT.XML

AUDIT.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Enterprise Audit Exchange (AUDIT.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/mCNQV5X>

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

[4] DDMS V5

DDMS V5

Department of Defense. *DoD Discovery Metadata Specification*. 5.

Available online at: <http://go.ic.gov/IDsfli>

[5] DoD Directive 3300.03

DoD Directive 3300.03

Secretary of Defense. *DoD Document and Media Exploitation (DOMEX)*. 3300.03. 11 January 2011.

Available online at: <http://www.dtic.mil/whs/directives/corres/pdf/330003p.pdf>

[6] DoD Instruction 8310.01

DoD Instruction 8310.01

DoD CIO. *Information Technology Standards in the DoD*. 8310.01. 2 February 2015.

Available online at: <http://www.dtic.mil/whs/directives/corres/pdf/831001p.pdf>

[7] DOMEX

DOMEX

Office of the Director of National Intelligence. *XML Data Encoding Specification for Document and Media Exploitation (DOMEX)*.

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

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

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

[8] FSD

FSD

Office of the Director of National Intelligence. *Data Encoding Specification for IC Full Service Directory Schema (FSD)*.

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

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

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

[9] IC ITE INC1 IMPL

IC ITE INC1 IMPL

Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.

Available online Intelink-TS at: <http://go.ic.gov/4X6TOc1>

[10] IC Markings

IC Markings

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

Available online Intelink-TS at: <http://go.ic.gov/5DjqgWz>

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

[11] IC-EDH.XML

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: <http://go.ic.gov/TQjVx3d>

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

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

[12] IC-GENC.CES

IC-GENC.CES

Office of the Director of National Intelligence. *XML CVE Encoding Specification for Geopolitical Entities, Names, and Codes (IC-GENC.CES)*.

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

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

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

[13] IC-ID.XML

IC-ID.XML

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

Available online Intelink-TS at: <http://go.ic.gov/mQ4lUDk>

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

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

[14] IC-TDF.XML

IC-TDF.XML

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

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

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

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

[15] ICD 206

ICD 206

Office of the Director of National Intelligence. *Sourcing Requirements for Disseminated Analytic Products*. Intelligence Community Directive 206. 22 January 2015.

Available online at: <http://www.dni.gov/files/documents/ICD/ICD%20206.pdf>

[16] ICD 500

ICD 500

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

Available online Intelink-TS at: <http://go.ic.gov/5Ot5sbK>

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

[17] ICD 501

ICD 501

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

Available online Intelink-TS at: <http://go.ic.gov/GG61roi>

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

[18] ICO-NTK

ICO-NTK

Office of the Director of National Intelligence. *XML Data Encoding Specification for Intelligence Community Only Need-To-Know Profile (ICO-NTK.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/6N0E0Ru>

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

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

[19] ICPM 2007-200-2

ICPM 2007-200-2

Office of the Director of National Intelligence. *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide*. Intelligence Community Policy Memorandum 2007-200-2 . 11 December 2007.

Available online at: <http://www.dni.gov/files/documents/IC%20Policy%20Memos/ICPM%202007-200-2%20Responsibility%20to%20Provide.pdf>

[20] ICS 500-20

ICS 500-20

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

Available online Intelink-TS at: <http://go.ic.gov/sLKNq3N>

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

[21] ICS 500-21

ICS 500-21

Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.

Available online Intelink-TS at: <http://go.ic.gov/cWYv9nw>

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-21>

[22] ICS 500-27

ICS 500-27

Director of National Intelligence Chief Information Officer. *Intelligence Community Standard for Collection and Sharing of Audit Data*. Intelligence Community Standard 500-27. 2 June 2011.

Available online Intelink-TS at: <http://go.ic.gov/3czwVuQ>

[23] IETF-RFC 2119

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>

[24] IETF-RFC 2231

IETF-RFC 2231

Internet Engineering Task Force. *MIME Value and Encoded Word Extensions: Character Sets, Languages, and Continuations*. November 1997.

Available online at: <http://www.ietf.org/rfc/rfc2231.txt>

[25] INTDIS.CES

INTDIS.CES

Office of the Director of National Intelligence. *XML CVE Encoding Specification for Intelligence Discipline (INTDIS.CES)*.

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

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

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

[26] IRM.XML

IRM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Resource Metadata (IRM.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/9g8Osir>

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

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

[27] ISM.XML

ISM.XML

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

Available online Intelink-TS at: <http://go.ic.gov/3oipfOY>

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

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

[28] ISMCAT.CES

ISMCAT.CES

Office of the Director of National Intelligence. *XML CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES)*.

Available online Intelink-TS at: <http://go.ic.gov/xhPfil3>

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

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

[29] ITS-MS.XML

ITS-MS.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Transport Service Messaging Service (ITS-MS.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/A0lkEWH>

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

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

[30] LIC.CES

LIC.CES

Office of the Director of National Intelligence. *XML CVE Encoding Specification for License (LIC.CES)*.

Available online Intelink-TS at: <http://go.ic.gov/mssZ6bc>

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

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

[31] MIME.CES

MIME.CES

Office of the Director of National Intelligence. *XML CVE Encoding Specification for Media Type (MIME.CES)*.

[32] MN.CES

MN.CES

Office of the Director of National Intelligence. *XML CVE Encoding Specification for Mission-Need (MN.CES)*.

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

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

[33] NTK.XML

NTK.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML)*.

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

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

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

[34] OC-NTK.XML

OC-NTK.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Originator Control Need-To-Know Profile (OC-NTK.XML)*.

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

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

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

[35] PM.CES

PM.CES

Office of the Director of National Intelligence. *XML CVE Encoding Specification for Production Metrics (PM.CES)*.

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

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

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

[36] PROPIN-NTK.XML

PROPIN-NTK.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Proprietary Need-To-Know (PROPIN-NTK.XML)*.

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

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

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

[37] PUBS.XML

PUBS.XML

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

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

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

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

[38] REVRECALL.XML

REVRECALL.XML

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

Available online Intelink-TS at: <http://go.ic.gov/8HB0HUh>

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

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

[39] SRC.XML

SRC.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Source Citations (SRC.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/Za6YKsA>

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

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

[40] UIAS.XML

UIAS.XML

Office of the Director of National Intelligence. *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/H8RwEw8>

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

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

[41] USAgency.CES

USAgency.CES

Office of the Director of National Intelligence. *XML CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*.

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

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

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

[42] VIRT.XML

VIRT.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Virtual Coverage (VIRT.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/HGb1I2P>

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

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

Appendix E Points of Contact

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

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

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

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

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

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.^[20]