TAXII Content Binding Reference Version 3.0

Working Draft 01

30 June 2015

Technical Committee:

[OASIS Cyber Threat Intelligence (CTI) TC](https://www.oasis-open.org/committees/cti/)

Chairs:

Mark Davidson ([mdavidson@mitre.org](mailto:mdavidson@mitre.org)), [Mitre Corporation](http://www.mitre.org/)

Bret Jordan ([bret.jordan@bluecoat.com](mailto:bret.jordan@bluecoat.com)), [Blue Coat Systems, Inc.](http://www.bluecoat.com/)

Editor:

Bret Jordan ([bret.jordan@bluecoat.com](mailto:bret.jordan@bluecoat.com)), [Blue Coat Systems, Inc.](http://www.bluecoat.com/)

Mark Davidson ([mdavidson@mitre.org](mailto:mdavidson@mitre.org)), [Mitre Corporation](http://www.mitre.org/)

Related work:

This specification replaces or supersedes:

* *The TAXII Content Binding Reference Version 3*. <http://taxii.mitre.org/specifications/version1.1/TAXII_ContentBinding_Reference_v3.pdf>.

This specification is related to:

TAXII Version 1.1.1, a Work Product which consists of:

* *TAXII Version 1.1.1 Part 1: Overview*. [URI – “Latest version”]
* *TAXII Version 1.1.1 Part 2: Services*. [URI]
* *TAXII Version 1.1.1 Part 3: HTTP Protocol Binding*. [URI]
* *TAXII Version 1.1.1 Part 4: XML Message Binding*. [URI]
* *TAXII Version 1.1.1 Part 5: Default Query*. [URI]

Abstract:

The Trusted Automated eXchange of Indicator Information (TAXII) specifies mechanisms for exchanging structured cyber threat information between parties over the network. This document contains non-normative mappings of content formats to Content Binding IDs.

Status:

This [Working Draft](https://www.oasis-open.org/policies-guidelines/tc-process#dWorkingDraft) (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or [approved](https://www.oasis-open.org/policies-guidelines/tc-process#committeeDraft) as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document [Approval Process](https://www.oasis-open.org/policies-guidelines/tc-process#standApprovProcess) begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

URI patterns:

Initial publication URI:  
http://docs.oasis-open.org/cti/taxii-content-binding/v3.0/csd01/taxii-content-binding-v3.0-csd01.doc

Permanent “Latest version” URI:  
http://docs.oasis-open.org/cti/taxii-content-binding/v3.0/taxii-content-binding-v3.0.doc

(Managed by OASIS TC Administration; please don’t modify.)

Copyright © OASIS Open 2015.  All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](https://www.oasis-open.org/policies-guidelines/ipr) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Portions copyright © United States Government 2012-2015.  All Rights Reserved.  
  
STIX™, TAXII™, AND CybOX™ (STANDARD OR STANDARDS) AND THEIR COMPONENT PARTS ARE PROVIDED “AS IS” WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY THAT THESE STANDARDS OR ANY OF THEIR COMPONENT PARTS WILL CONFORM TO SPECIFICATIONS, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR FREEDOM FROM INFRINGEMENT, ANY WARRANTY THAT THE STANDARDS OR THEIR COMPONENT PARTS WILL BE ERROR FREE, OR ANY WARRANTY THAT THE DOCUMENTATION, IF PROVIDED, WILL CONFORM TO THE STANDARDS OR THEIR COMPONENT PARTS. IN NO EVENT SHALL THE UNITED STATES GOVERNMENT OR ITS CONTRACTORS OR SUBCONTRACTORS BE LIABLE FOR ANY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF, RESULTING FROM, OR IN ANY WAY CONNECTED WITH THESE STANDARDS OR THEIR COMPONENT PARTS OR ANY PROVIDED DOCUMENTATION, WHETHER OR NOT BASED UPON WARRANTY, CONTRACT, TORT, OR OTHERWISE, WHETHER OR NOT INJURY WAS SUSTAINED BY PERSONS OR PROPERTY OR OTHERWISE, AND WHETHER OR NOT LOSS WAS SUSTAINED FROM, OR AROSE OUT OF THE RESULTS OF, OR USE OF, THE STANDARDS, THEIR COMPONENT PARTS, AND ANY PROVIDED DOCUMENTATION. THE UNITED STATES GOVERNMENT DISCLAIMS ALL WARRANTIES AND LIABILITIES REGARDING THE STANDARDS OR THEIR COMPONENT PARTS ATTRIBUTABLE TO ANY THIRD PARTY, IF PRESENT IN THE STANDARDS OR THEIR COMPONENT PARTS AND DISTRIBUTES IT OR THEM “AS IS.”

Table of Contents

[1 Introduction 4](#_Toc424193809)

[1.1 Versioning of this Reference 4](#_Toc424193810)

[1.2 Terminology 4](#_Toc424193811)

[1.3 Normative References 4](#_Toc424193812)

[1.4 Non-Normative References 4](#_Toc424193813)

[2 Canonical Content Binding IDs 6](#_Toc424193814)

[2.1 Table of Binding IDs 6](#_Toc424193815)

[2.2 Structured Threat Information eXpression (STIX) 6](#_Toc424193816)

[2.3 Common Alerting Protocol (CAP) 7](#_Toc424193817)

[2.4 XML Encryption 7](#_Toc424193818)

[2.5 S/MIME 8](#_Toc424193819)

[2.5.1 Sample S/MIME Content Block 8](#_Toc424193820)

[3 Third Party Defined Content Bindings 9](#_Toc424193821)

[4 # Conformance 10](#_Toc424193822)

[5 Revision Record 11](#_Toc424193823)

[Appendix A. Acknowledgments 12](#_Toc424193824)

[Appendix B. Example Title 13](#_Toc424193825)

[B.1 Subsidiary section 13](#_Toc424193826)

[B.1.1 Sub-subsidiary section 13](#_Toc424193827)

[B.1.1.1 Sub-sub-subsidiary section 13](#_Toc424193828)

[Appendix C. Revision History 14](#_Toc424193829)

# Introduction

This document provides canonical Content Binding IDs for common forms of content (i.e., structured information for characterizing and responding to cyber threats) that appear within TAXII Messages. Content Binding IDs appear in several TAXII message fields. They can be used to indicate the types of content that are used in a TAXII Data Feed, the types of content a TAXII Service is capable of processing, or to filter the content a TAXII Consumer receives as part of an established subscription.

This document adds no normative requirements to TAXII. Instead, it contains recommended ID values associated with specific types of TAXII content. Implementers may ignore this document and remain conformant to TAXII, but it is strongly encouraged that, when indicating payloads described in this document, the Content Binding IDs given in this document be used as this increases interoperability.

Readers of this document are assumed to be familiar with the terms and requirements that appear in the TAXII Services Specification.

## Versioning of this Reference

The TAXII Content Binding Reference is revised independently of the other TAXII specifications and is not bound to any particular version of TAXII. Instead, it represents a growing list of IDs to be used when indicating a particular content format. Content Binding IDs are never removed from this document, although some may be deprecated in favor of new terms. Thus, all revisions of this document are always backwards compatible. For this reason, this document only uses a single, increasing "revision number" to distinguish between versions.

This document may be revised (i.e., new Content Binding IDs may be added) at any time. In particular, this may occur between releases of the core TAXII specifications.

# Canonical Content Binding IDs

This section establishes canonical values for Content Binding IDs. Note that this section includes no requirements or recommendations with regard to how the listed content formats are used. Use of a particular Content Binding ID is only used to indicate that some content conforms to the indicated format's requirements.

## Table of Binding IDs

This section provides a quick look-up table of Content Binding IDs. Each content binding is discussed in more detail in subsequent sections:

Table 1 - Content Binding IDs

|  |  |  |
| --- | --- | --- |
| **Content Format** | | **Content Binding ID** |
| STIX | |  |
| STIX XML 1.0 | urn:stix.mitre.org:xml:1.0 |
| STIX XML 1.0.1 | urn:stix.mitre.org:xml:1.0.1 |
| STIX XML 1.1 | urn:stix.mitre.org:xml:1.1 |
| STIX XML 1.1.1 | urn:stix.mitre.org:xml:1.1.1 |
| CAP | |  |
| CAP 1.1 | urn:oasis:names:tc:emergency:cap:1.1 |
| CAP 1.2 | urn:oasis:names:tc:emergency:cap:1.2 |
| XML Encryption, December 2002 | | http://www.w3.org/2001/04/xmlenc# |
| S/MIME | | application/pkcs7-mime |

## Structured Threat Information eXpression (STIX)

"STIX is a collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information." [2] STIX was developed by the MITRE Corporation under contract from the U.S. Department of Homeland Security. The STIX schemas and documentation are available at http://stix.mitre.org/. STIX is a trademark of The MITRE Corporation. The STIX schemas and documentation are copyright by The MITRE Corporation. See the STIX web site for terms of use.

STIX content is currently expressed using XML, but other format bindings may be developed (e.g., JSON). In addition, in the STIX XML schema, the target namespace only indicates the major version of STIX that it defines but does not reflect minor revisions. For these reasons, the STIX XML schema target namespace is not used as the TAXII Content Binding ID and instead a special URI is constructed using the following rules:

"urn:oasis:cti:stix:" + *format* + ":" + *version*

In this production *format* reflects the format of the content (e.g., XML, JSON, etc.) while *version* is the major, minor, and (if present) update number associated with a particular release of STIX. As such, the TAXII Content Binding IDs for STIX XML are:

|  |  |
| --- | --- |
| **STIX Version** | **Content Binding ID** |
| STIX XML 1.0 http://stix.mitre.org/language/version1.0/ | urn:stix.mitre.org:xml:1.0 |
| STIX XML 1.0.1  http://stix.mitre.org/language/version1.0.1/ | urn:stix.mitre.org:xml:1.0.1 |
| STIX XML 1.1  http://stix.mitre.org/language/version1.1/ | urn:stix.mitre.org:xml:1.1 |
| STIX XML 1.1.1  http://stix.mitre.org/language/version1.1.1/ | urn:stix.mitre.org:xml:1.1.1 |

## Common Alerting Protocol (CAP)

"The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks." [3] [4] CAP was developed by the Organization for the Advancement of Structured Information Standards (OASIS). The CAP 1.1 specification is available at https://www.oasis-open.org/committees/download.php/14759/emergency-CAPv1.1.pdf. The CAP 1.2 specification is available at http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf. The CAP specification is copyright by OASIS. See the specification for terms of use.

CAP content is expressed using XML. The TAXII Content Binding for CAP is the target namespace of the CAP XML schema. The TAXII Content Binding IDs for CAP are:

|  |  |
| --- | --- |
| **CAP Version** | **Content Binding ID** |
| CAP 1.1  https://www.oasis-open.org/standards#capv1.1 | urn:oasis:names:tc:emergency:cap:1.1 |
| CAP 1.2  https://www.oasis-open.org/standards#capv1.2 | urn:oasis:names:tc:emergency:cap:1.2 |

## XML Encryption

XML Encryption "specifies a process for encrypting data and representing the result in XML." [5] XML Encryption was developed by the World Wide Web Consortium (W3C). The XML Encryption specification is available at http://www.w3.org/TR/xmlenc-core/. The XML Encryption specification is copyright by the W3C. See the XML Encryption specification for terms of use.

XML Encryption is expressed in XML. The TAXII Content Binding ID for XML Encryption is the target namespace of the XML Encryption XML schema. For the latest release of XML Encryption (as of April 2013), the TAXII Content Binding is:

http://www.w3.org/2001/04/xmlenc#

Note that it is generally assumed that XML Encryption will be used to encrypt some other content. See the TAXII Services Specification section on Content Nesting and Encryption (Section 5.3) for more information.

## S/MIME

"S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a consistent way to send and receive secure MIME data." [6] The most recent S/MIME specification is available at http://tools.ietf.org/html/rfc5751. The S/MIME specification is copyright by the IETF Trust. See the S/MIME specification for terms of use.

TAXII users can use S/MIME to express encrypted content directly within a TAXII Content Block. The TAXII Content Binding ID for S/MIME is the MIME type of S/MIME. For S/MIME, the TAXII Content Binding is:

application/pkcs7-mime

For enhanced interoperability within TAXII applications, applications using this Content Binding ID are recommended to follow these additional guidelines when using S/MIME:

1. The Content-Type MIME Header should specify a type of ‘application/x-pks7-mime’
2. If the S/MIME object will be placed in an XML document (i.e., if it is used with the TAXII XML Message Binding), the Content-Transfer-Encoding MIME header should specify a value of ‘base64’.
3. When processing a Content Block that uses the S/MIME Content Binding, care should be taken to preserve whitespace in the Content field. Whitespace, specifically newlines, delineate header fields in MIME and modifying whitespace may result in rendering the Content field unparseable.

Note that it is generally assumed that S/MIME will be used to encrypt some other content. See the TAXII Services Specification section on Content Nesting and Encryption (Section 5.3) for more information.

### Sample S/MIME Content Block

This section contains a sample S/MIME Content Block that uses the S/MIME Content Binding and adheres to the Additional Guidelines.

<taxii\_11:Content\_Block>  
    <taxii\_11:Content\_Binding binding\_id="application/pkcs7-mime"/>  
    <taxii\_11:Content>MIME-Version: 1.0   
        Content-Disposition: attachment; filename="smime.p7m"  
        Content-Type: application/x-pkcs7-mime; smime-type=enveloped-data; name="smime.p7m"  
        Content-Transfer-Encoding: base64  
        MIICbgYJKoZIhvcNAQcDoIICXzCCAlsCAQAxggEzMIIBLwIBADCBlzCBiTELMAkG  
        A1UEBhMCVVMxCzAJBgNVBAgMAk1BMRAwDgYDVQQHDAdCZWRmb3JkMQ4wDAYDVQQK  
        DAVNSVRSRTEQMA4GA1UECwwHSW5mb1NlYzEVMBMGA1UEAwwMTWFya0Rhdmlkc29u  
        MSIwIAYJKoZIhvcNAQkBFhNtZGF2aWRzb25AbWl0cmUub3JnAgkAhGhsCeaFoHkw  
        DQYJKoZIhvcNAQEBBQAEgYBLpRCKUjGKrrCrW2ZTJY/FfVANbFQaO2CtsuNb3HtB  
        JHAU8oav9Ijk5SxBTfaRdUx8/xoOIONMFZhl0j14XZ/C7Hb7oosnK2iZ36oLG0Gp  
        O06KJV6H1Rc2t1Lvbz3aCwY0EkTVeeTCqYzNZ8cLlYxOeh0EnXnni49J02RPzuI3  
        GjCCAR0GCSqGSIb3DQEHATAdBglghkgBZQMEASoEEFo5tj7JprSvS1PV27n3FoqA  
        gfB+lafh7zSsmHeCq7W5J0GaahPWsTRJBeNmetFiUip5wtuq8Dhvy5X9OVAxv3sK  
        VWWemAnvpJ9ZIJXbbFhXfX3lqNr6I9GI3KabF/QXxyLlR8HgZfQPI1ieEIBIiVM1  
        iswlTgkhRRovJBhnSxmqrpmvvYVGAPCY1b9NYwnix0jb3iPt1nFKMV6yp4T0RvkV  
        z6mmC0NKyV7roR1Q/EwErmSJ9m/o+PaHqqxTTGBztwLtZ/EeptX/hgvtR2IZccEp  
        0gQ3TDX50VNbT7eqhATUegR3mVqL/HDp79TarwDwXPxHBM7Jy+BIAKXlmBFUpPB8   
 nx4=  
    </taxii\_11:Content>  
</taxii\_11:Content\_Block>

# Third Party Defined Content Bindings

Third parties may define their own Content Binding IDs for any form of content. The TAXII Services Specification prohibits Content Binding IDs defined by third parties from duplicating Content Binding IDs that appear in this document.

Third parties that define their own Content Binding IDs are encouraged to submit these IDs to the TAXII community to encourage greater interoperability between TAXII users. If there is significant interest in the identified binding, it may be incorporated in this document.

# Conformance

This document is informational in nature and contains no conformance clauses.

# Revision Record

* Version 1 - First version. Includes bindings for STIX 1.0, CAP 1.1, and XML Encryption from December 2002
* Version 2 - Added a binding for CAP 1.2
* Version 3 – Added Content Binding IDs for S/MIME, STIX 1.0.1, STIX 1.1, and STIX 1.1.1.
* Version 4 – Re-release of Version 3 as an OASIS Work Product

1. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

[Participant Name, Affiliation | Individual Member]

[Participant Name, Affiliation | Individual Member]

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| 1 | July 2015 | Mark Davidson | Initial draft based on TAXII Content Binding Reference Version 3 |