

THE MITRE CORPORATION

The TAXII Content Binding Reference

Version 2

Mark Davidson, Charles Schmidt

05/23/2013

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.

Trademark Information

TAXII and STIX are trademarks of The MITRE Corporation. Other marks or brands are the property of their respective owners.

This technical data was produced for the U. S. Government under Contract No. HSHQDC-11-J-00221, and is subject to the Rights in Technical Data-Noncommercial Items clause at DFARS 252.227-7013 (NOV 1995)

©2012 - 2013 The MITRE Corporation. All Rights Reserved.

Feedback

Feedback on this or any of the other TAXII specifications is welcome and can be sent to taxii-discussion-list@lists.mitre.org after signing up on the community registration page (<http://taxii.mitre.org/community/registration.html>).

Comments, questions, suggestions, and concerns are all appreciated.

Table of Contents

Trademark Information.....	1
Feedback	1
1 Introduction	3
1.1 Versioning of this Reference	3
2 Canonical Content Binding IDs.....	3
2.1 Table of Binding IDs	4
2.2 Structured Threat Information eXpression (STIX).....	4
2.3 Common Alerting Protocol (CAP).....	4
2.4 XML Encryption	5
3 Third Party Defined Content Bindings	5
4 Bibliography	6
5 Revision Record.....	6

1 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 version 1.0 [1].

1.1 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.

2 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.

2.1 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 XML 1.0		urn:stix.mitre.org:xml:1.0
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#

2.2 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:stix.mitre.org:" + 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. Currently, the only format supported by STIX is XML and the STIX schema is in version 1.0. As such, the TAXII Content Binding ID for the STIX XML format 1.0 is:

`urn:stix.mitre.org:xml:1.0`

2.3 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] CAP was developed by the Organization for the Advancement of Structured Information Standards (OASIS). The CAP specification is available at <https://www.oasis-open.org/committees/download.php/14759/emergency-CAPv1.1.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.

For CAP version 1.1, the TAXII Content Binding ID is:

```
urn:oasis:names:tc:emergency:cap:1.1
```

For CAP version 1.2, the TAXII Content Binding ID is:

```
urn:oasis:names:tc:emergency:cap:1.2
```

2.4 XML Encryption

XML Encryption "specifies a process for encrypting data and representing the result in XML." [4] 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.

3 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.

4 Bibliography

- [1] The MITRE Corp., "The TAXII Services Specification 1.0," The MITRE Corp., 2013.
- [2] The MITRE Corp., "STIX - Structured Threat Information Expression," 18 April 2013. [Online]. Available: <https://stix.mitre.org/>.
- [3] Organization for the Advancement of Structured Information Standards (OASIS), "Common Alerting Protocol, v. 1.1," OASIS, 2005.
- [4] T. Imamura, B. Dillaway and E. Simon, "XML Encryption Syntax and Processing," W3C, 2002.

5 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