THE MITRE CORPORATION

The TAXII Payload Binding Reference

Version 1.0 DRAFT

Mark Davidson, Charles Schmidt

04/30/2013

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 Payload Binding IDs.

Trademark Information

Feedback

Community input is necessary for the success of TAXII. Feedback on this or any of the other TAXII specifications is welcome and can be sent to taxii@mitre.org. 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 Payload Binding IDs 3

2.1 Structured Threat Information eXpression (STIX) 4

2.2 Common Alerting Protocol (CAP) 4

2.3 XML Encryption 5

3 Third Party Defined Payload Bindings 5

4 Development 5

5 Bibliography 6

1 Introduction

Trusted Automated eXchange of Indicator Information (TAXII ™) is a set of services and message exchanges that enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII defines protocols and data formats for securely exchanging cyber threat information for the detection, prevention, and mitigation of cyber threats at machine speed. TAXII is not an information sharing initiative or application and it does not attempt to define trust agreements, governance, or non-technical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats, and enables organizations to easily share the information they choose with the partners they choose. For more information on TAXII, see "Trusted Automated eXchange of Indicator Information (TAXII ™)" [1].

This document provides canonical Payload Binding IDs for common forms of content (i.e., structured information for characterizing and responding to cyber threats) that appear as payloads within TAXII Messages. Payload 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 payloads. Implementers may ignore this document and remain conformant to TAXII, but it is strongly encouraged that, when indicating payloads described in this document, the Payload Binding IDs given in this document be used as this increases interoperability.

Readers of this document are assumed to be familiar with the terms, definitions, and requirements that appear in the TAXII Services Specification version 1.0.

1.1 Versioning of this Reference

The TAXII Payload 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 that should be used when indicating a particular payload format. No defined Payload Binding IDs are ever 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 Payload Binding IDs may be added) at any time. In particular, this may occur between releases of the core TAXII specifications.

2 Canonical Payload Binding IDs

This section sets out canonical values for Payload 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 Payload Binding ID is only used to indicate that some payload conforms to the indicated format in accordance to the format's schema and/or specification.

2.1 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, 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 Payload Binding ID and instead a special string is constructed using the following rules:

`"STIX_"` + *format* + `"_"` + *version*

In this production, the *format* reflects the format of the content (e.g., XML, JSON, etc.) while the *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 Payload Binding ID for the STIX XML format 1.0 is:

```
STIX_XML_1.0
```

Note that, although STIX documents may contain content expressed using other schemas (e.g., MAEC, CybOX, etc.) it is not expected to be treated as a "wrapping" format. As such, a STIX payload that contained MAEC content would generally not be indicated as nested content, but simply as STIX content. See the section on payload nesting and encryption in the TAXII Services Specification for more information.

2.2 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 Payload Binding for CAP content is the target namespace of the XML schema associated with CAP. For CAP version 1.1 (the latest version of CAP as of April 2013), the TAXII Payload Binding ID is:

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

2.3 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 Payload Binding ID for XML Encryption is the target namespace of the XML schema associated with XML Encryption. For the latest release of XML Encryption (dated December 10, 2002), the TAXII Payload 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 payload content. See the section on payload nesting and encryption in the TAXII Services Specification for more information.

3 Third Party Defined Payload Bindings

Third parties may define their own Payload Binding IDs for any form of content. As noted in the TAXII Services Specification, Payload Binding IDs defined by third parties should not duplicated Payload Binding IDs that appear in this document. Moreover, third party Payload Binding IDs must not include the star (*) character, as this is reserved to indicate nesting.

Third parties that define their own Payload Binding IDs are encouraged to submit these IDs to the TAXII community to encourage greater interoperability between TAXII users.

4 Development

TAXII and its component specifications are expected to continue to evolve based on user needs. Feedback, suggestions, and comments with regard to this or any of the other TAXII specifications are welcome. The TAXII web site (http://taxii.mitre.org/) contains the latest news and resources with regard to TAXII, including the latest version of all TAXII specifications. There is also a mailing list for the discussion of the specifications and where users can pose questions. Interested parties can sign up for this mailing list via the TAXII web site (http://taxii.mitre.org/community/registration.html). Finally, there is also a repository on GitHub.com (https://github.com/TAXIIProject/). This site will host code development efforts as well as modified versions of the TAXII specifications with changes that may be included in future releases of TAXII.

Users of TAXII are encouraged to make use of these resources, both to empower their own use of TAXII and to provide feedback that will help TAXII evolve to meet the needs of its users.

5 Bibliography

[1] U.S. Department of Homeland Security, "Trusted Automated eXchange of Indicator Information (TAXII ™)," U.S. Department of Homeland Security, Washington D.C., 2012.

[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.