THE MITRE CORPORATION

# The TAXII XML Message Binding Specification

## Version 1.0 DRAFT

**Mark Davidson, Charles Schmidt**

**04/22/2013**



The Trusted Automated eXchange of Indicator Information (TAXII™) specifies mechanisms for exchanging structured cyber threat information between parties over the network. This document describes how to express TAXII messages using an XML binding.

## 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

# 1 Introduction

Trusted Automated eXchange of Indicator Information (TAXII ™) is a set of technical specifications and supporting documentation to 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 describes how to express TAXII Messages using XML [2] syntax. The use of these messages to support TAXII Services is described separately in the TAXII Services Specification. It is recommended that the reader familiarize themself with the TAXII Services Specification prior to reading this document.

## 1.1 TAXII Specifications

TAXII is defined by multiple, interrelated specifications. This section describes the specifications that define TAXII.

**Services Specification** - The TAXII Services Specification provides requirements that govern TAXII Services and Message Exchanges. It does not provide details on data formatting or how TAXII Messages are transported over a network - such details and requirements can be found in the Message Binding Specifications and Protocol Binding Specifications, respectively.

**Message Binding Specification** - Message Binding Specifications define the requirements for representing TAXII Messages in a particular format (e.g., XML). They provide detailed guidance about how TAXII Messages, as defined in the Services Specification, are formatted. There may be multiple Message Binding Specifications created for TAXII with each Message Binding Specification defining a binding of TAXII Messages using a different format.

**Protocol Binding Specification** - Protocol Binding Specifications define the requirements for transporting TAXII Messages over some network protocol (e.g., HTTP). They provide requirements about how the TAXII Services are supported by these network protocols. There may be multiple Protocol Binding Specifications created for TAXII with each Protocol Binding Specification defining requirements for transporting TAXII Messages using a different network protocol.

Figure 1 shows how these specifications relate to each other. This specification is a TAXII Message Binding Specification. Its relationship to other TAXII specifications is highlighted in the diagram.

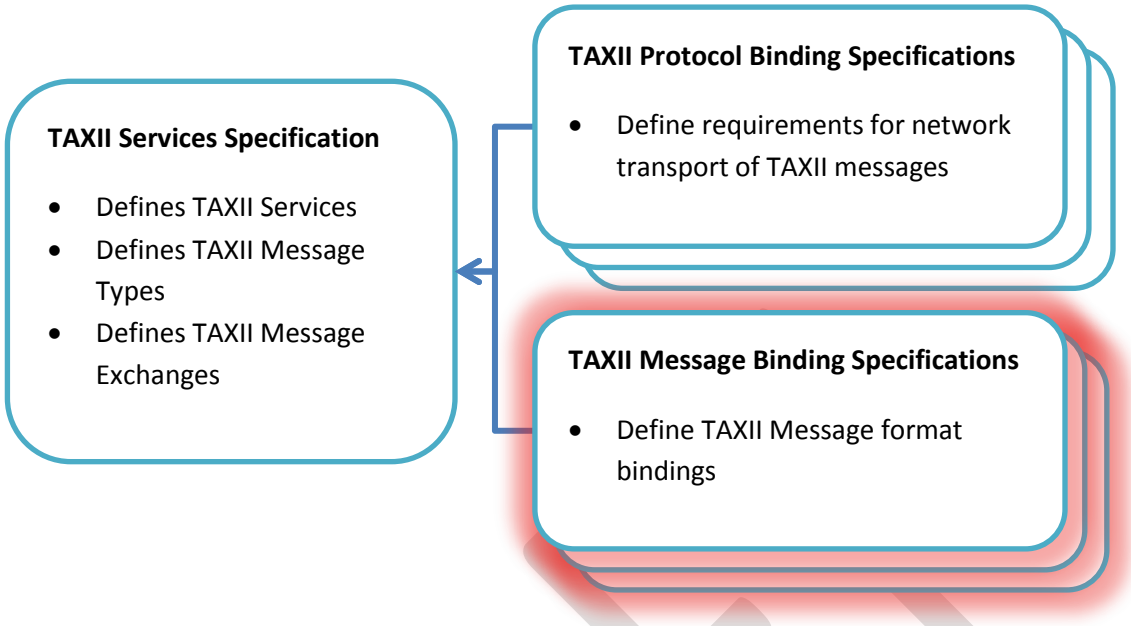


Figure 1 - TAXII Specification Hierarchy

Separation of the Services Specification, Message Binding Specifications, and Protocol Binding Specifications exists to support flexibility as TAXII evolves. Threat information sharing communities often have specific constraints on the types of protocols they are able to support. Rather than binding TAXII to a specific protocol that excludes portions of the community, TAXII's core concepts (i.e., its Services and Exchanges) are defined separately from the protocol-level support for those concepts. When there is a need for a new protocol or message binding, it can be created, either as part of a new official release of TAXII or as a third-party extension for TAXII, without affecting TAXII's core components.

Two groups that use the same network protocol and message bindings will be capable of automated exchanges of structured threat information. The sharing policies of the participants can limit these exchanges as needed, but the use of compatible TAXII Services ensures that whatever sharing is permitted by policy can be effected by the TAXII mechanisms. Groups that use different protocol or message bindings for TAXII will not be able to communicate directly with each other, but because they are still using TAXII Messages and Services at the core of their communications it is possible to create gateways that will allow interaction to occur.

### 1.1.1 The TAXII XML Message Binding Specification

This specification provides normative text on the expression of TAXII Message using XML syntax. It does not provide details about how TAXII Messages are transported, leaving that to a Protocol Binding Specification. Descriptions of the TAXII Services and TAXII Message Exchanges that these Messages support, as well as a detailed discussion of the meaning of message fields, are discussed in detail in the TAXII Services specification.

#### 1.1.1.1 TAXII Message Binding Version ID for XML

This document makes references to TAXII "Version IDs", specifically TAXII Services Version IDs, TAXII Protocol Binding Version IDs, and TAXII Message Binding Version IDs. The network protocols that carry TAXII Messages as well as the TAXII Messages themselves sometimes need to indicate the version of TAXII and versions of the various bindings that are being used. The TAXII Version IDs are strings that are used to denote specific versions of specific TAXII specifications within TAXII exchanges. Each TAXII specification identifies its own TAXII Version ID. Different versions of each specification provide a different Version ID. Version IDs may be referenced in TAXII specifications as a way to identify specific versions of TAXII and its bindings.

The TAXII Message Binding Version ID for the version of the XML Binding described in this specification is:

TAXII_XML_BINDING_1.0

#### 1.1.1.2 The TAXII XML Schema

This document is accompanied by an XML schema as a means to clarify the requirements surrounding TAXII XML Message structures. The schema is provided as an aid to developers and implementers but is not normative. In all cases, this document should be considered to specify the normative requirements for TAXII's XML message binding and if there is ever disagreement between the specification and the schema the specification should be considered correct. In particular, due to the limitations of XML schemas, the schema permits some structures that are prohibited by the specification.

#### 1.1.1.3 Specification Versioning

This document describes version 1.0 of the TAXII XML Message Binding specification. Changes to this specification that impact content or tools are indicated by incrementing the major or minor version numbers of this document, depending on the magnitude of the change. Such changes result in a new TAXII Message Binding Version ID. Fixing of typos, clarification of concepts, and other changes that do not affect content or tool behavior do not change the major or minor version numbers, but instead are reflected by an updated release date for the document. For such changes the TAXII Message Binding Version ID is not updated.

An XML schema is provided for each major and minor release of this specification. The full version of this specification associated with a given schema is reflected in the version attribute in the top-level `<schema>` element of the schema file. The major version of the specification also appears as part of the XML target namespace of the defined schema. For version 1.0 and all subsequent minor releases within this major release, the target namespace of the TAXII XML Message Binding schema is `"http://taxii.mitre.org/messages/taxii_xml_binding-1"`. Changes to the schema that do not affect content or processing (e.g., correcting or clarifying documentation in the schema) are denoted by a change to the `<date>` element in the `<annotation>` at the beginning of the schema. No changes to the schema that affected content or processing are made without an accompanying change to the specification. Note that for every major and minor release of the specification there is an XML schema that denotes that same major and minor release. However, the release dates of the

specification and the schema, reflected by the document release date and `<date>` element, respectively, may not match.

### 1.1.2 Content and Payloads

TAXII is designed to support the sharing of structured information for characterizing and responding to cyber threats. Any such information is referred to as "content". When this information is contained in a TAXII Message, it is called a "payload". TAXII is capable of transporting a range of payloads.

This specification does not provide details about the underlying content formats transmitted as payloads within TAXII. All payloads are a "black-box" as far as TAXII is concerned - none of the behaviors described in this specification require inspection of any information stored within message payloads.

### 1.1.3 Document Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this specification are to be interpreted as described in IETF RFC 2119. [3]

When making references to XML elements and attributes as well as other XML literals (such as enumerated values), this document uses `Courier New Font`. XML element names are denoted by non-namespaced text surrounded by angle brackets (e.g., `<TAXII_Discovery_Request>`) while attribute names are preceded by an "at" symbol (e.g., `@message_id`).

## 1.2 Terms and Definitions

This document uses the Terms and Definitions defined in the TAXII Services Specification. In addition, this document defines terms that are assigned a specific meaning within this specification.

### 1.2.1 XML Binding Terms

The TAXII Services Specification identifies a number of fields for each TAXII Message Type. This specification specifies those fields as XML structures. The Services Specification discusses fields in terms of general concepts they are meant to convey, while this specification represents fields as precise character patterns to represent information. When the distinction between these two uses of "field" is important, this document uses the following terms:

**Data Model Field** - A field defined in the TAXII Message data model that appears in the TAXII Services Specification. For example, all messages have a "Message ID" Data Model Field that contains a message identifier.

**XML Field** - A field expressed using the XML syntax defined in this specification. XML Fields correspond to either an XML element or an XML attribute. For example, all messages have a "`@message_id`" XML Field that contains a value identifying the message using the XML string type.

Note that there is not always a one-to-one mapping between a Data Model Field and an XML Field. Such situations are noted where they occur.

# 2 TAXII XML Message Binding Overview

This section considers some of the underlying concepts behind the TAXII XML Message Binding. It considers the overall structure of a TAXII Message in this binding and also considers the meanings of certain Data Model Field values and the details of their expression using XML Field values.

## 2.1 TAXII XML Message Binding Structure

The TAXII XML Message Binding defines requirements regarding the overall structuring of TAXII Messages using XML. These requirements are described in the following subsections.

### 2.1.1 Messages are Root Elements

A separate XML element is defined to represent each type of TAXII Message. Each element that represents a TAXII Message can appear as a root element in an XML "document". (The term "document" here denotes a block of XML that would conform to the requirements in this document.) In XML schema parlance, this means all TAXII Message elements are global elements. Moreover, this specification does not define any elements that contain TAXII Message elements. As such, within this TAXII Message Binding, TAXII Message elements do not appear as descendants of other elements.

One side effect of this is that this specification does not define any way to include multiple TAXII Messages within a single XML "document". This reflects that, in TAXII Message Exchanges, there is no situation where multiple TAXII Messages may be sent in a single transmission.

### 2.1.2 No Header and Body Field Distinction

All TAXII Messages consist of a header and a body. TAXII Header fields represent information that is required by all TAXII Message Body Types, while TAXII Body fields contain information that is specific to a particular TAXII Message Body Type. This specification does not distinguish between TAXII Header fields and TAXII Body fields. In other words, there is not a dedicated region containing all TAXII Header content and a separate region containing all TAXII body content. Instead, both types of fields exist as peers in the XML of a TAXII Message. This document does not treat the header and body fields separately or otherwise differentiate between them.

### 2.1.3 Strict Ordering of Elements

In this specification, all XML fields that use XML elements use a strict ordering of fields. (In XML schema parlance, elements are defined in a sequence.) This allows parsers to quickly locate specific fields and to know how many times a given field appears without needing to parse the entire document.

XML attributes may appear in any order within their parent XML element.

### 2.1.4 Message Schema Validation

Neither senders nor recipients are required to perform schema validations on messages that they send or receive, respectively. This noted, senders of messages that use this message binding are required to conform to the requirements of this specification. If a message recipient detects an incorrectly formatted message, either through schema validation or other means, the recipient SHOULD respond with a Status Message with a status type of "Bad Message".

## 2.2 Special Field Values

Several TAXII Message fields appear in multiple TAXII Messages and have a specialized structure and/or important meaning. This section looks at these fields, identifies the requirements that govern their values, and explains how they are represented in XML.

### 2.2.1 Message ID

Every TAXII Message has a Message ID field. Message ID values are used to link requests with responses. Specifically, if TAXII Message B is sent in response to TAXII Message A, Message B will contain an "In Response To" field whose value is equal to the value of the Message ID field in Message A.

The TAXII XML Message Binding requires XML Fields that contain Message IDs be XML strings. Recipients of a TAXII Message should be sure they are able to handle XML string values as a Message ID.

### 2.2.2 Feed Name

Every TAXII Data Feed has a unique identifier relative to the other TAXII Data Feeds from the same Producer. Producers may use any syntax they wish for their Feed Names - names can be human-readable titles, hexadecimal numbers, or anything else.

The TAXII XML Message Binding requires XML Fields that contain Feed Names be XML strings. If the Producer's chosen Feed Name is not directly expressible as an XML string (e.g., it is a binary blob or it contains reserved XML characters), it needs to be converted to an XML string before it is used in this binding.

### 2.2.3 Subscription ID

For convenience when manipulating existing subscriptions, TAXII defines Subscription IDs. When a Consumer successfully establishes a subscription on a Producer, the Producer assigns that subscription a Subscription ID. From then on, both the Consumer and Producer may refer to this subscription in messages using this Subscription ID value.

The TAXII XML Message Binding requires XML Fields that contain Subscription IDs to be XML strings. If the Producer's chosen Subscription ID is not expressible as an XML string (e.g., it is a binary blob or contains reserved XML characters), it needs to be converted to an XML string before it is used in this binding.

### 2.2.4 Timestamp Labels

In TAXII, each piece of content within a TAXII Data Feed is assigned a unique Timestamp Label value. Timestamp Labels are used to allow Consumers to indicate which parts of a TAXII Data Feed they are requesting in a Poll Request Message.

The TAXII XML Message Binding requires XML Fields that contain Timestamp Labels to be XML dateTime values. In addition, these values MUST include a time zone component (i.e., either "Z" or a numerical offset), in accordance with the date-time production in RFC 3339 [4]. Timestamp Labels field values MUST NOT contain fractional seconds with more than six decimal places of precision.

### 2.2.5 Third party Values

Some fields allow a third party to create their own field values instead of using values defined in the TAXII Specifications. For example, TAXII allows senders to define their own status types and supply them in a TAXII Status Message. In all cases, the XML Fields where third party defined values can appear have a type of XML string. As such, third party defined values must be expressible using an XML string.

#### *2.2.5.1 Extended Headers*

TAXII allows the specification of extended headers in all TAXII Messages. All extended headers are defined by third parties outside the TAXII specifications. Extended headers in TAXII are represented as name-value pairs.

In the TAXII XML Message Binding, extended header names are contained in an XML attribute with a type of XML string. As such, if the Producer's chosen extended-header name is not expressible as an XML string (e.g., it is a binary blob or contains reserved XML characters), it needs to be converted to an XML string before it is used in this binding.

Values in an extended header can be any content, including other XML elements. In this binding, the value undergoes lax processing - if the provider of the third party value includes XML elements that conform to some other XML schema then XML validation can check for schema conformance. However, if such a schema is not available (either because it does not exist or because it cannot be located by the entity reading the message) this should not cause schema validation of the message to fail.

#### *2.2.5.2 Status Types*

TAXII permits third parties to define their own status type value for use in TAXII Status Messages. These may be used to indicate an error condition specific to a particular TAXII implementation or user group. Third party-defined status type values MUST NOT indicate a successful condition since unrecognized status types are interpreted as "Failure". Third party-defined status type values MUST NOT duplicate status type values given in this specification. In order to avoid collisions between third party-defined status type values and future releases of this specifications, third party-defined status type values SHOULD begin with "X_" as no status type values in any revision of this specification will start with those characters.

Some status types defined in the TAXII Services Specification include a Status Detail value that conveys machine-readable information relevant to the status type. For status types defined in the TAXII Services Specification for which Status Detail values are provided, third parties MUST NOT add to or alter the contents of the Status Detail field. Third parties MAY add Status Detail content to status types defined in the TAXII Services Specification which do not suggest Status Detail values. Third parties MAY also add Status Detail content for status types that they define. Third parties SHOULD NOT add to or alter the contents of the Status Detail field for status types defined by a different third party without corrdinating with that party to ensure there will not be misinterpretation.

Status Detail fields can contain any content, including other XML elements. In this binding, the Status Detail undergoes lax processing - if the provider of the third party value includes XML elements that conform to some other XML schema then XML validation can check for schema conformance. However,

if such a schema is not available (either because it does not exist or because it cannot be located by the entity reading the message) this should not cause schema validation of the message to fail.

#### *2.2.5.3 Version and Binding IDs*

TAXII permits third parties to identify their own protocol, message, and payload bindings for TAXII communication. These can be specified instead of, or sometimes in addition to, using TAXII Version IDs or Payload Binding IDs, respectively, as described in the TAXII specifications. In the XML Message Binding, fields that contain Version and Payload Binding IDs are XML strings. Third party-defined Version and Binding IDs MUST NOT duplicate any Version ID from any TAXII specification or any Payload Binding ID from the TAXII Payload Binding Reference.

Third party Payload Binding IDs MUST not include the star (*) character as this is interpreted as an indication of nesting by TAXII. If the binding format is defined by an XML schema and the target namespace of the schema is suitably unique and precisely identifies the version of this binding format, it is recommended that the schema's target namespace be used as the Payload Binding ID for that binding format.

Note that, in terms of processing, the TAXII XML Message Binding Specification does not distinguish between Version IDs and Payload Binding IDs that are defined by TAXII specifications and those defined by third parties. Use of the terms Protocol Version ID, Message Version ID, and Payload Binding ID are used throughout this document without regard to the source of that ID.

# 3 TAXII XML Messages

This section defines the XML structures used to express TAXII Messages. Each TAXII Message type is described below using tables that contain each Message Type's fields. XML elements may have child attributes or elements. Parent-child relationships are reflected in the tables below by indenting the attributes and child elements relative to their parent. XML elements in TAXII Messages MUST appear in the order in which they appear in these tables. XML attributes may appear in TAXII Messages in any order within their parent element.

For each XML Field, the following information is provided:

- XML Name - The element name or attribute name of an XML Field. If the XML Field is an element it appears between angle brackets (<>) and if it is an attribute it appears preceded by an "at" sign (@).
- Data Model Name - The name of the Data Model Field as provided in the TAXII Message data model in the TAXII Services Specification. Note that if multiple XML Fields are needed to convey the meaning in a single Data Model Field, all of these XML Fields would be assigned the same Data Model Name value.
- # - The number of times the XML Field may appear within a parent element, expressed either as a single digit or a range. If a field is optional, it is always expressed as a range with a lower bound of '0'. If a field may appear an unlimited number of times, it is always expressed as a

range with an upper bound of 'n'. Note that a field may be "required" in the Message Data Model, but be optional in the XML structure. This can happen either by assigning a default value to the XML Field or otherwise ascribing meaning to an XML Field's absence. Note also that a required field that is a child of an optional field would only be present if its parent field was present.

- Value - Constraints on the permissible values of this XML Field. This would include the XML data type and other requirements.

The following sections define XML structures for all defined TAXII Message.

## 3.1 TAXII Status Message

Table 1 - TAXII Status Message Fields

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Status_Message> | Message Body Type | 1 | The element name indicates the message body type. Its body MUST consist only of the indicated XML Fields. |
| @message_id | Message ID | 1 | An XML string |
| @in_response_to | In Response To | 1 | An XML string equal to the value of the @message_id field to which this message is a response |
| @status_type | Status Type | 1 | A string value; either one of the values provided in Table 2 or a third party defined value. |
| <Extended_Headers> | Extended-Header | 0-1 | Contains one or more <Extended_Header> elements. |
| <Extended_Header> | Extended-Header | 1-n | The body of this element supports mixed content and may contain any XML, as described in Section 2.2.5.1. |
| @name | Extended-Header | 1 | An XML string with the name of this extended header. |
| <Status_Detail> | Status Detail | 0-1 | The body of this element supports mixed content and may contain any XML, as described in Section 2.2.5.2. This field SHOULD be present if and only if the given @status_type value defines a value for it. For @status_type values that appear in Table 2, this field (if present) MUST contain only the information identified in that table. |
| <Message> | Message | 0-1 | An XML string. |
| <ds:Signature> | Signature | 0-1 | This element is defined in the XML Signature Syntax and Processing specification [5]. The scope of this signature is the entire TAXII Message. |

The @status_type field identifies the type of status expressed in this message. Standard status types are defined in Table 2. In addition, the TAXII Status Message sender may define their own status types. If the recipient does not recognize a third party defined status type, the status type should be treated as a "Failure" status type.

Certain @status_type values define a value for the <Status_Detail> field. If the <Status_Detail> field is present with one those @status_type values the <Status_Detail> field MUST only contain specifically formatted information appropriate to that status. Table 2 identifies the @status_type field values which SHOULD have a corresponding <Status_Detail> field and what that <Status_Detail> MUST contain if present. Status types that are empty in the "<Status_Detail> Value" column MAY include third party defined information in a <Status_Detail> field. For third party defined status types, that that third party may determine whether or not an <Status_Detail> field should be present and what value it should take.

Table 2 - Defined Status Types

| @status_type Value | Error Status Type | <Status_Detail> Value |
|---|---|---|
| BAD_MESSAGE | Bad Message | |
| DENIED | Denied | |
| FAILURE | Failure | |
| NOT_FOUND | Not Found | |
| POLLING_UNSUPPORTED | Polling Not Supported | |
| RETRY | Retry | A timestamp indicating a time when the request might be repeated and fulfilled. The timestamp MUST conform to the RFC 3339 production for a date-time value [4]. |
| SUCCESS | Success | |
| UNAUTHORIZED | Unauthorized | |
| UNSUPPORTED_MESSAGE | Unsupported Message Binding | A space-separated list of Message Binding IDs indicating supported message bindings. If a Message Binding ID contains whitespace this whitespace MUST be URI-encoded [6] before it is added to this field. |
| UNSUPPORTED_PAYLOAD | Unsupported Payload Binding | A space-separated list of Payload Binding IDs indicating supported payloads. If a Payload Binding ID contains whitespace this whitespace MUST be URI-encoded before it is added to this field. |

| @status_type Value | Error Status Type | <Status_Detail> Value |
|---|---|---|
| UNSUPPORTED_PROTOCOL | Unsupported Protocol | A space-separated list of Protocol Binding IDs indicating supported protocol bindings. If a Protocol Binding ID contains whitespace this whitespace MUST be URI-encoded before it is added to this field. |

## 3.2 TAXII Discovery Request

Table 3 - TAXII Discovery Request Fields

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Discovery_Request> | Message Body Type | 1 | The element name indicates the message body type. Its body MUST consist only of the indicated XML Fields. |
| @message_id | Message ID | 1 | An XML string |
| <Extended_Headers> | Extended-Header | 0-1 | Contains one or more <Extended_Header> elements. |
| <Extended_Header> | Extended-Header | 1-n | The body of this element supports mixed content and may contain any XML, as described in Section 2.2.5.1. |
| @name | Extended-Header | 1 | An XML string with the name of this extended header. |
| <ds:Signature> | Signature | 0-1 | This element is defined in the XML Signature Syntax and Processing specification [5]. The scope of this signature is the entire TAXII Message. |

## 3.3 TAXII Discovery Response

Table 4 - TAXII Discovery Response Fields

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Discovery_Response> | Message Body Type | 1 | The element name indicates the message body type. Its body MUST consist only of the indicated XML Fields. |
| @message_id | Message ID | 1 | An XML string. |
| @in_response_to | In Response To | 1 | An XML string equal to the value of the @message_id field to which this message is a response |
| <Extended_Headers> | Extended-Header | 0-1 | Contains one or more <Extended_Header> elements. |
| <Extended_Header> | Extended-Header | 1-n | The body of this element supports mixed content and may contain any XML, as described in Section 2.2.5.1. |

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| @name | Extended-Header | 1 | An XML string with the name of this extended header. |
| <Service_Instance> | Service Instance | 0-n | Contains only the indicated XML Fields. This element may appear any number of times with each instance corresponding to a single reported TAXII Service instance. |
| @service_type | Service Type | 1 | This field MUST contain one of the values given in Table 5. |
| @service_version | Services Version | 1 | An XML string containing a Services Version ID. |
| @available | Available | 0-1 | An xml boolean. If present, indicates if the requester is known to have access to this service. If absent, treat access as unknown. |
| <Protocol_Binding> | Protocol Binding | 1 | An XML string containing a Protocol Binding Version ID. |
| <Address> | Service Address | 1 | An XML string representing a network address. |
| <Message_Binding> | Message Binding | 1-n | An XML string containing a Message Binding Version ID. This field may appear one or more times with each instance indicating a different supported binding. |
| <Payload_Binding> | Inbox Service Accepted Payload | 0-n | An XML string containing a Payload Binding ID. If the @service_type value of is something other than INBOX, this field SHOULD NOT be included by the sender and MUST be ignored by the message recipient. If present, each instance of this field indicates a different supported binding. If @service_type="INBOX" but there are no instances of this field, this indicates that the identified Inbox Service accepts all payload bindings. |
| <Message> | Message | 0-1 | An XML string. |
| <ds:Signature> | Signature | 0-1 | This element is defined in the XML Signature Syntax and Processing specification [5]. The scope of this signature is the entire TAXII Message. |

The @service_type field identifies the type of service reported in the given <Service_Instance>. Its value MUST be one of the values provided in Table 5.

Table 5 - Service Types

| Service | @service_type Value |
|---|---|
| Discovery Service | DISCOVERY |
| Feed Management Service | FEED_MANAGEMENT |
| Inbox Service | INBOX |
| Poll Service | POLL |

## 3.4 TAXII Feed Information Request

Table 6 - TAXII Feed Information Request Fields

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Feed_Information_Request> | Message Body Type | 1 | The element name indicates the message body type. Its body MUST consist only of the indicated XML Fields. |
| @message_id | Message ID | 1 | An XML string |
| <Extended_Headers> | Extended-Header | 0-1 | Contains one or more <Extended_Header> elements. |
| <Extended_Header> | Extended-Header | 1-n | The body of this element supports mixed content and may contain any XML, as described in Section 2.2.5.1. |
| @name | Extended-Header | 1 | An XML string with the name of this extended header. |
| <ds:Signature> | Signature | 0-1 | This element is defined in the XML Signature Syntax and Processing specification [5]. The scope of this signature is the entire TAXII Message. |

## 3.5 TAXII Feed Information Response

Table 7 - TAXII Feed Information Response Fields

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Feed_Information_Response> | Message Body Type | 1 | The element name indicates the message body type. Its body MUST consist only of the indicated XML Fields. |
| @message_id | Message ID | 1 | An XML string |
| @in_response_to | In Response To | 1 | An XML string equal to the value of the @message_id field to which this message is a response |

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Extended_Headers> | Extended-Header | 1 | Contains one or more <Extended_Header> elements. |
| <Extended_Header> | Extended-Header | 1-n | The body of this element supports mixed content and may contain any XML, as described in Section 2.2.5.1. |
| @name | Extended-Header | 1 | An XML string with the name of this extended header. |
| <Feed> | Feed Information | 0-n | Contains only the indicated child fields. Appears once for each TAXII Data Feed reported in this message. |
| @feed_name | Feed Name | 1 | An XML string containing the Feed Name for this TAXII Data Feed. |
| @available | Available | 0-1 | An xml boolean. If present, indicates if the requester is known to have access to this service. If absent, treat access as unknown. |
| <Description> | Feed Description | 1 | An XML string. |
| <Payload_Binding> | Supported Payload | 1-n | An XML string containing a Payload Binding ID. Each instance indicates a binding used by content in this TAXII Data Feed. |
| <Push_Method> | Push Method | 0-n | The body of this element MUST consist only of the indicated XML Fields. Each instance of this field indicates one set of bindings that may be used to push content to a Consumer's Inbox Service. At least one instance of a <Push_Method> or <Polling_Service> element MUST be present. Both types of elements MAY be present. |
| <Protocol_Binding> | Push Protocol | 1 | An XML string containing a Protocol Binding Version ID. |
| <Message_Binding> | Push Message Binding | 1-n | An XML string containing a Message Binding Version ID. This field may appear one or more times with each instance indicating a different supported binding. |

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Polling_Service> | Polling Service Instance | 0-n | The body of this element MUST consist only of the indicated XML Fields. Each instance of this field indicates one Poll Service instance that may be used to poll for content from this Data Feed. At least one instance of a <Push_Method> or <Polling_Service> element MUST be present. Both types of elements MAY be present. |
| <Protocol_Binding> | Poll Protocol | 1 | An XML string containing a Protocol Binding Version ID. |
| <Address> | Poll Address | 1 | An XML string representing a network address. |
| <Message_Binding> | Poll Message Binding | 1-n | An XML string containing a Message Binding Version ID. This field may appear one or more times with each instance indicating a different supported binding. |
| <Subscription_Service> | Subscription Method | 0-n | The body of this element MUST consist only of the indicated XML Fields. Each instance of this field indicates one Feed Management Service that may be used to establish a subscription to this Data Feed. If no instances of this field are present, subscriptions cannot be established using TAXII messages. |
| <Protocol_Binding> | Subscription Protocol | 1 | An XML string containing a Protocol Binding Version ID. |
| <Address> | Subscription Address | 1 | An XML string representing a network address. |
| <Message_Binding> | Subscription Message Binding | 1-n | An XML string containing a Message Binding Version ID. This field may appear one or more times with each instance indicating a different supported binding. |
| <ds:Signature> | Signature | 0-1 | This element is defined in the XML Signature Syntax and Processing specification [5]. The scope of this signature is the entire TAXII Message. |

## 3.6 TAXII Manage Feed Subscription Request

Table 8 - TAXII Feed Information Request Fields

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Subscription_Management_Request> | Message Body Type | 1 | The element name indicates the message body type. Its body MUST consist only of the indicated XML Fields. |
| @message_id | Message ID | 1 | An XML string |
| @action | Action | 1 | This field MUST contain one of the values given in Table 9. |
| @feed_name | Feed Name | 1 | A string containing the Feed Name for the TAXII Data Feed. |
| @subscription_id | Subscription ID | 0-1 | An XML string containing a Subscription ID value. This field MUST be present if @action="UNSUBSCRIBE". For other values of @action senders SHOULD NOT include this field and recipients MUST ignore this field. |
| <Extended_Headers> | Extended-Header | 0-1 | Contains one or more <Extended_Header> elements. |
| <Extended_Header> | Extended-Header | 1-n | The body of this element supports mixed content and may contain any XML, as described in Section 2.2.5.1. |
| @name | Extended-Header | 1 | An XML string with the name of this extended header. |
| <Push_Parameters> | Delivery Parameters | 0-1 | The body of this element, if present, MUST consist only of the indicated XML Fields. For values of @action other than SUBSCRIBE senders SHOULD NOT include this field and recipients MUST ignore this field. If @action="SUBSCRIBE" and this field is absent then the sender is indicating that it does not want content pushed to an Inbox service. (I.e., the sender will poll for content.) |
| <Protocol_Binding> | Inbox Protocol | 1 | An XML string containing a Protocol Binding Version ID. |
| <Address> | Inbox Address | 1 | An XML string representing a network address. |
| <Message_Binding> | Delivery Message Binding | 1 | An XML string containing a Message Binding Version ID. |

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Payload_Binding> | Payload Binding | 0-n | An XML string containing a Payload Binding ID. Each instance indicates an acceptable binding for pushed content. If there are no instances of this field, this indicates that the identified Inbox Service accepts all payload bindings. |
| <ds:Signature> | Signature | 0-1 | This element is defined in the XML Signature Syntax and Processing specification [5]. The scope of this signature is the entire TAXII Message. |

The @action field contains a value indicating what subscription management action is to be taken. Possible values for this field appear in Table 9.

Table 9 - Feed Management Actions

| @action Value | Management Action |
|---|---|
| SUBSCRIBE | SUBSCRIBE - Request a subscription to the named TAXII Data Feed |
| UNSUBSCRIBE | UNSUBSCRIBE - Request cancellation of an existing subscription to the named TAXII Data Feed |
| STATUS | STATUS - Request information on all subscriptions the requester has established for the named TAXII Data Feed. |

## 3.7 TAXII Manage Feed Subscription Response

Table 10 - TAXII Feed Information Response Fields

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Subscription_Management_Response> | Message Body Type | 1 | The element name indicates the message body type. Its body MUST consist only of the indicated XML Fields. |
| @message_id | Message ID | 1 | An XML string |
| @in_response_to | In Response To | 1 | An XML string equal to the value of the @message_id field to which this message is a response |
| @feed_name | Feed Name | 1 | A string containing the Feed Name for the TAXII Data Feed. |
| <Extended_Headers> | Extended-Header | 1 | Contains one or more <Extended_Header> elements. |
| <Extended_Header> | Extended-Header | 1-n | The body of this element supports mixed content and may contain any XML, as described in Section 2.2.5.1. |

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| @name | Extended-Header | 1 | An XML string with the name of this extended header. |
| <Message> | Message | 0-1 | An XML string. |
| <Subscription> | Subscription Instance | 0-n | This field contains only the indicated child fields. It may appear any number of times (including 0) if this message is in response to a Manage Feed Subscription Request message with @action="STATUS". Each instance reports a different subscription to the named Data Feed. This field MUST appear exactly once for all other @action values. |
| @subscription_id | Subscription ID | 1 | An XML string containing a Subscription ID value. |
| <Push_Parameters> | Delivery Parameters | 0-1 | This field contains only the indicated child fields. This field MUST be present if and only if this message is in response to a request with @action="STATUS" and the request that established this subscription included a <Push_Parameters>. (I.e., they requested feed content be pushed to an Inbox Service.) This XML Field SHOULD NOT be included by the sender and MUST be ignored by the recipient when responding to requests with an @action value other than STATUS. Note that, the TAXII Services Specification does not prohibit Delivery Parameters from being present when responding to actions other than STATUS, but this specification overrides that to avoid ambiguity: this field MUST be absent when the @action value that precipitated this message is anything other than STATUS. |
| <Protocol_Binding> | Inbox Protocol | 1 | An XML string containing a Protocol Binding Version ID. Contains an exact copy of the <Protocol_Binding> field from the Manage Feed Subscription Request Message that established this subscription. |
| <Address> | Inbox Address | 1 | An XML string representing a network address. Contains an exact copy of the <Address> field from the Manage Feed Subscription Request Message that established this subscription. |

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Message_Binding> | Delivery Message Binding | 1 | An XML string containing a Message Binding Version ID. Contains an exact copy of the <Message_Binding> field from the Manage Feed Subscription Request Message that established this subscription. |
| <Payload_Binding> | Payload Binding | 0-n | An XML string containing a Payload Binding ID. Contains an exact copy of the <Payload_Binding> field from the Manage Feed Subscription Request Message that established this subscription. One instance of this field MUST appear for each instance in the request that established the subscription. Note that if this field is absent in the request establishing this subscription it will be absent here as well. |
| <Poll_Instance> | Poll Instance | 0-n | This field contains only the indicated child fields. If this message is in response to a Manage Feed Subscription Request message with @action value other than UNSUBSCRIBE, then this field MUST be present if the requester indicated that they wanted to poll for content. (I.e., there was no <Push_Parameters> field in the request that established this subscription.) It SHOULD NOT be present for requests with an @action value of UNSUBSCRIBE. It MAY be present in all other circumstances. |
| <Protocol_Binding> | Poll Protocol | 1 | An XML string containing a Protocol Binding Version ID. |
| <Address> | Poll Address | 1 | An XML string representing a network address. |
| <Message_Binding> | Poll Message Binding | 1-n | An XML string containing a Message Binding Version ID. |
| <ds:Signature> | Signature | 0-1 | This element is defined in the XML Signature Syntax and Processing specification [5]. The scope of this signature is the entire TAXII Message. |

## 3.8 TAXII Poll Request

Table 11 - TAXII Poll Request Fields

| XML Name | Data Model Name | # | Value |
|---|---|---|---|

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Poll_Request> | Message Body Type | 1 | The element name indicates the message body type. Its body MUST consist only of the indicated XML Fields. |
| @message_id | Message ID | 1 | An XML string |
| @feed_name | Feed Name | 1 | A string containing the Feed Name for the TAXII Data Feed. |
| @subscription_id | Subscription ID | 0-1 | An XML string containing a Subscription ID value. |
| <Extended_Headers> | Extended-Header | 0-1 | Contains one or more <Extended_Header> elements. |
| <Extended_Header> | Extended-Header | 1-n | The body of this element supports mixed content and may contain any XML, as described in Section 2.2.5.1. |
| @name | Extended-Header | 1 | An XML string with the name of this extended header. |
| <Exclusive_Begin_Timestamp> | Exclusive Begin Timestamp Label | 0-1 | An XML dateTime value containing a Timestamp Label. If this field is absent, it indicates this request has no lower bound. |
| <Inclusive_End_Timestamp> | Inclusive End Timestamp Label | 0-1 | An XML dateTime value containing a Timestamp Label. If this field is absent, it indicates this request has no upper bound. |
| <Payload_Binding> | Supported Payload | 0-n | An XML string containing a Payload Binding ID. Each instance indicates an acceptable binding for content in the Poll Response message. If there are no instances of this field, this indicates that all payload bindings are acceptable. |
| <ds:Signature> | Signature | 0-1 | This element is defined in th XML Signature Syntax and Processing specification [5]. The scope of this signature is the entire TAXII Message. |

Note that if both <Exclusive_Begin_Timestamp> and <Inclusive_End_Timestamp> are present in this message, the value in <Inclusive_End_Timestamp> MUST be greater than the value in <Exclusive_Begin_Timestamp>.

## 3.9 TAXII Poll Response

Table 12 - TAXII Poll Request Fields

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Poll_Response> | Message Body Type | 1 | The element name indicates the message body type. Its body MUST consist only of the indicated XML Fields. |
| @message_id | Message ID | 1 | An XML string |
| @in_response_to | In Response To | 1 | An XML string equal to the value of the @message_id field to which this message is a response |
| @feed_name | Feed Name | 1 | A string containing the Feed Name for the TAXII Data Feed. |
| @subscription_id | Subscription ID | 0-1 | An XML string containing a Subscription ID value. |
| <Extended_Headers> | Extended-Header | 1 | Contains one or more <Extended_Header> elements. |
| <Extended_Header> | Extended-Header | 1-n | The body of this element supports mixed content and may contain any XML, as described in Section 2.2.5.1. |
| @name | Extended-Header | 1 | An XML string with the name of this extended header. |
| <Message> | Message | 0-1 | An XML string. |
| <Inclusive_Begin_Timestamp> | Inclusive Begin Timestamp Label | 0-1 | An XML dateTime value containing a Timestamp Label. If this field is absent, it indicates the response covers the earliest content within the Data Feed. |
| <Inclusive_End_Timestamp> | Inclusive End Timestamp Label | 1 | An XML dateTime value containing a Timestamp Label. |
| <Payload_Block> | Payload Block | 0-n | This field contains only the indicated child fields. |
| <Payload_Binding> | Payload Binding | 1 | An XML string containing a Payload Binding ID. |
| <Payload> | Payload | 1 | The body of this element supports mixed content and may contain any XML. |
| <Timestamp_Label> | Timestamp Label | 0-1 | An XML dateTime value containing a Timestamp Label. |
| <Padding> | Padding | 0-1 | An XML string. |

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <ds:Signature> | Signature | 0-n | This element is defined in the XML Signature Syntax and Processing specification [5]. This signature is scoped to the <Payload_Block> element in which it resides. |
| <ds:Signature> | Signature | 0-1 | This element is defined in the XML Signature Syntax and Processing specification [5]. The scope of this signature is the entire TAXII Message. |

## 3.10 TAXII Inbox Message

Table 13 - TAXII Inbox Message Fields

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Inbox_Message> | Message Body Type | 1 | The element name indicates the message body type. Its body MUST consist only of the indicated XML Fields. |
| @message_id | Message ID | 1 | An XML string |
| <Extended_Headers> | Extended-Header | 0-1 | Contains one or more <Extended_Header> elements. |
| <Extended_Header> | Extended-Header | 1-n | The body of this element supports mixed content and may contain any XML, as described in Section 2.2.5.1. |
| @name | Extended-Header | 1 | An XML string with the name of this extended header. |
| <Message> | Message | 0-1 | An XML string. |
| <Source_Subscription> | Subscription Information | 0-1 | This field contains only the indicated child fields. |
| @feed_name | Feed Name | 0-1 | A string containing the Feed Name for the TAXII Data Feed. |
| @subscription_id | Subscription ID | 0-1 | An XML string containing a Subscription ID value. |
| <Inclusive_Begin_Timestamp> | Inclusive Begin Timestamp Label | 0-1 | An XML dateTime value containing a Timestamp Label. If this field is absent, it indicates the response covers the earliest content within the Data Feed. |

| XML Name | Data Model Name | # | Value |
|---|---|---|---|
| <Inclusive_End_Timestamp> | Inclusive End Timestamp Label | 1 | An XML dateTime value containing a Timestamp Label. |
| <Payload_Block> | Payload Block | 0-n | This field contains only the indicated child fields. |
| <Payload_Binding> | Payload Binding | 1 | An XML string containing a Payload Binding ID. |
| <Payload> | Payload | 1 | The body of this element supports mixed content and may contain any XML. |
| <Timestamp_Label> | Timestamp Label | 0-1 | An XML dateTime value containing a Timestamp Label. |
| <Padding> | Padding | 0-1 | An XML string. |
| <ds:Signature> | Signature | 0-n | This element is defined in the XML Signature Syntax and Processing specification [5]. This signature is scoped to the <Payload_Block> element in which it resides. |
| <ds:Signature> | Signature | 0-1 | This element is defined in the XML Signature Syntax and Processing specification [5]. The scope of this signature is the entire TAXII Message. |

# 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] T. Bray, J. Paoli, C. M. Sperberg-McQueen, E. Maler and F. Yergeau, "Extensible Markup Language (XML) 1.0 (Fifth Edition)," W3C, 2008.

[3] S. Bradner, "RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels," The Internet Engineering Task Force, 1997.

[4] G. Klyne and C. Newman, "RFC 3339 - Date and Time on the Internet: Timestamps," The Internet Engineering Task Force, 2002.

[5] M. Bartel, J. Boyer, B. Fox, B. LaMacchia and E. Simon, "XML Signature Syntax and Processing," W3C, 2008.

[6] T. Berners-Lee, R. Fielding and L. Masinter, "RFC 3986 - Uniform Resource Identifier (URI): Generic Syntax," The Internet Engineering Task Force, 2005.