THE MITRE CORPORATION

The TAXII Services Specification

Version 1.0 DRAFT

Mark Davidson, Charles Schmidt

04/15/2013

The Trusted Automated eXchange of Indicator Information (TAXII™) specifies mechanisms for exchanging structured cyber threat information between parties over the network. This document describes TAXII's Capabilities, Services, Messages, and Message Exchanges.

Trademark Information

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)

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 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].

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, the TAXII Services Specification, is highlighted.

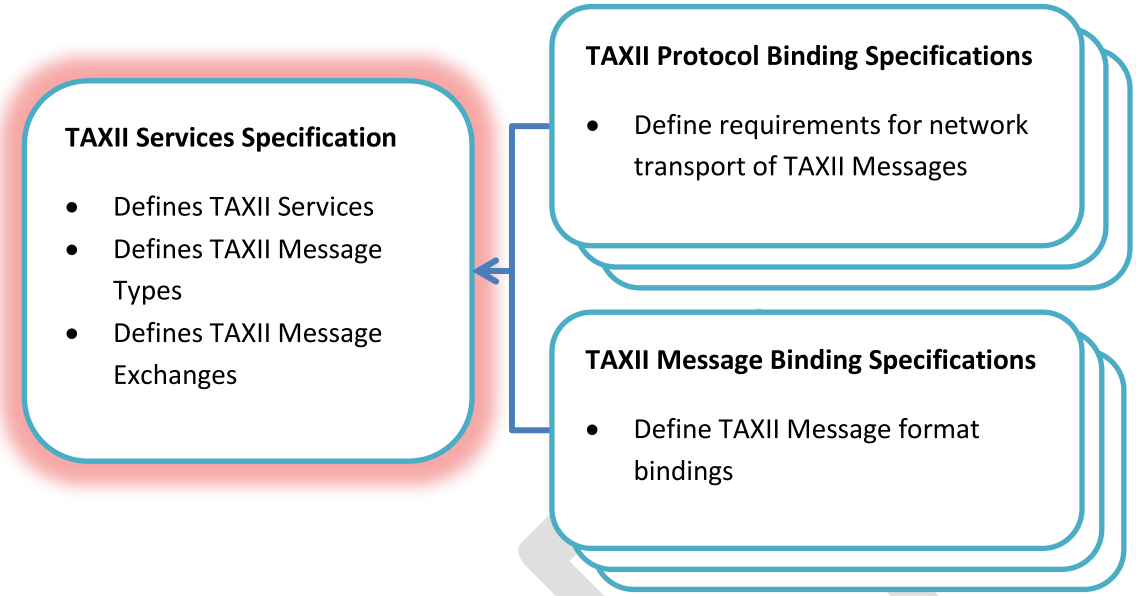
TAXII Services Specification
Defines TAXII Services
Defines TAXII Message Types
Defines TAXII Message Exchanges
TAXII Protocol Binding Specifications
Define requirements for network transport of TAXII Messages
TAXII Message Binding Specifications
Define TAXII Message format bindings

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 Services Specification

This specification provides normative text on TAXII Services, Messages, and Message Exchanges. It does not provide details about how TAXII Messages are transported, leaving that to Protocol Binding Specifications. Likewise, this document identifies the information conveyed in each TAXII Message, but does not provide details about how TAXII Messages are expressed, leaving that to Message Binding Specifications.

1.1.1.1 TAXII Services Version ID

This document makes references to TAXII "Version IDs", specifically the TAXII Services Version ID, the TAXII Protocol Binding Version ID, and the TAXII Message Binding Version ID. 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 Services Version ID for the version of TAXII described in this specification is:

TAXII_1.0

1.1.1.2 Specification Versioning

This document describes version 1.0 of the TAXII Services Specification. Changes to this specification that impact content or tools are indicated by incrementing the major or minor version number, depending on the magnitude of the change. Such changes result in a new TAXII Services 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 Services Version ID is not updated.

1.1.2 Payloads

TAXII is designed to support the sharing of structured information for characterizing and responding to cyber threats. When this information is contained in a TAXII Message, it is called a payload. One way of structuring cyber threat information is provided by the 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] Those interested in learning more about STIX are directed to the STIX web site at https://stix.mitre.org/. TAXII is capable of transporting a range of payloads, including STIX.

This specification does not provide details about the underlying payload structures. All payloads, including STIX, 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.

1.1.2.1 Payload Binding Identifier

A Payload Binding Identifier is a string that identifies the format and version of a payload type in a TAXII Message. The TAXII Payload Binding Reference (described in section 1.1.2.2) defines a canonical list of Payload Binding Identifiers for a core set of supported message payload types. In addition, Payload Binding Identifiers may be defined by third parties to designate payload types beyond this core set.

1.1.2.2 The TAXII Payload Binding Reference

The TAXII Payload Binding Reference is an independent document associated with the TAXII Specification. It contains no normative text (and as such is not counted as one of the core TAXII specifications) but instead provides a canonical list of Payload Binding Identifiers and a description and/or reference to the payload format that identifier indicates. 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 identifiers that should be used when indicating a particular payload format. When indicating a payload format that appears in the TAXII Payload Binding Reference, it is strongly encouraged that the Payload Binding Identifier associated with that format in the TAXII Payload Binding Reference be used. Doing so increases compatibility between users of TAXII.

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]

1.2 Terms and Definition

This section defines terms that are assigned a specific meaning within all TAXII specifications:

1.2.1 TAXII Concepts

These terms are used throughout the TAXII specifications to define concepts central to definition of TAXII.

Cyber Threat Information - Any information of interest to those who analyze or respond to cyber threats. This includes, but is not limited to, indication about malware, threat actors, campaigns, cyber incidents, significant observables corresponding to a threat, and other information needed to provide context or appropriate handling of cyber threat details.

TAXII Data Feed - A collection of structured cyber threat information that can be exchanged using TAXII. Each TAXII Data Feed has a name that uniquely identifies it among feeds from a given source of Cyber Threat Information. For more on TAXII Data Feed Names, see Section 4.1.2.

TAXII Content - A piece of TAXII Content is a piece of structured cyber threat information which can be viewed as "atomic" within a particular TAXII Data Feed. Specifically, within TAXII data requests can identify and request one piece of content versus another but they cannot specify a request at a sub-content level. In other words, one can request a single piece of content, but cannot request just a part of a piece of content. Certain pieces of content might be filtered or altered for certain recipients, but as far as each recipient is concerned they are getting a single, atomic piece of information.

Timestamp Label - A label in the form of a timestamp that is assigned to each piece of content within a TAXII Data Feed. Each piece of content within a TAXII Data Feed has a unique Timestamp Label. For more on Timestamp Labels, see Section 4.1.3.

TAXII Message - A discrete block of information that is passed from one entity to another over the network.

TAXII Payload - A piece of TAXII Content within a TAXII Message.

TAXII Message Exchange - A defined sequence of TAXII Messages undertaken by two parties, usually in the form of a request-response pair.

TAXII Service - Functionality that is accessed or invoked through the use of one or more TAXII Message Exchanges. TAXII Services support one or more message exchanges to provide functionality.

TAXII Capability - A high-level activity supported by TAXII through the use of one or more TAXII Services.

1.2.2 TAXII Roles

TAXII Roles are used to denote participants in TAXII according to their high-level objectives in the use of TAXII Services.

Producer - The role of an entity (e.g., a person, organization, agency, etc.) that is the source of structured cyber threat information for others.

Consumer - The role of an entity that is the recipient of structured cyber threat information.

Note that these roles are not mutually exclusive - one entity might be both a Consumer and a Producer of structured cyber threat information.

1.2.3 TAXII Functional Units

TAXII functional units represent discrete sets of activities required to support TAXII. Note that this does not mean that separate software is needed for each functional unit - a single software application could encompass multiple functional units or multiple applications could cooperate to serve as a single TAXII functional unit. A functional unit simply represents some component with a well-defined role in TAXII.

TAXII Transfer Agent (TTA) - A network-connected functional-unit that sends and/or receives TAXII Messages. A TTA interacts with other TTAs over the network and handles the details of the protocol requirements from one or more TAXII Protocol Binding Specifications. A TTA provides TAXII Messages to a TAXII Message Handler (defined below) allowing the TAXII Message Handler to be agnostic to the utilized network protocol. By the same token, the TTA can be agnostic as to the content of TAXII Messages, leaving the handling of this information to the TAXII Message Handler.

TAXII Message Handler (TMH) - A functional-unit that produces and consumes TAXII Messages. The TMH is responsible for parsing and constructing messages formatted according to one or more TAXII Message Binding Specifications. A TMH interacts with the TTA, which handles the details required to transmit those messages over the network. The TAXII Back-end interacts with the TMH to turn the information from the Back-end into TAXII Messages and to perform activities based on the TAXII Messages that the TMH receives.

TAXII Back-end - A term covering all functional units in a TAXII architecture other than the TTA and the TMH. This could cover data storage, subscription management, access control decisions, filtering of content prior to dissemination, and other activities. The TAXII specifications provide no requirements on how capabilities are implemented in a TAXII Back-end beyond noting that TAXII Back-ends must be able to interact with a TMH. Individual implementers and organizations can decide which TAXII Back-end capabilities are necessary given the TAXII Services they wish to support and how they wish to provide this support.

TAXII Architecture - The term TAXII Architecture covers all functional-units of a single Producer or Consumer's infrastructure that provide and/or utilize TAXII Services. A TAXII Architecture includes a TTA, a TMH, and a TAXII Back-end. As noted above, implementation details of a TAXII Back-End are outside of the scope of the TAXII specifications.

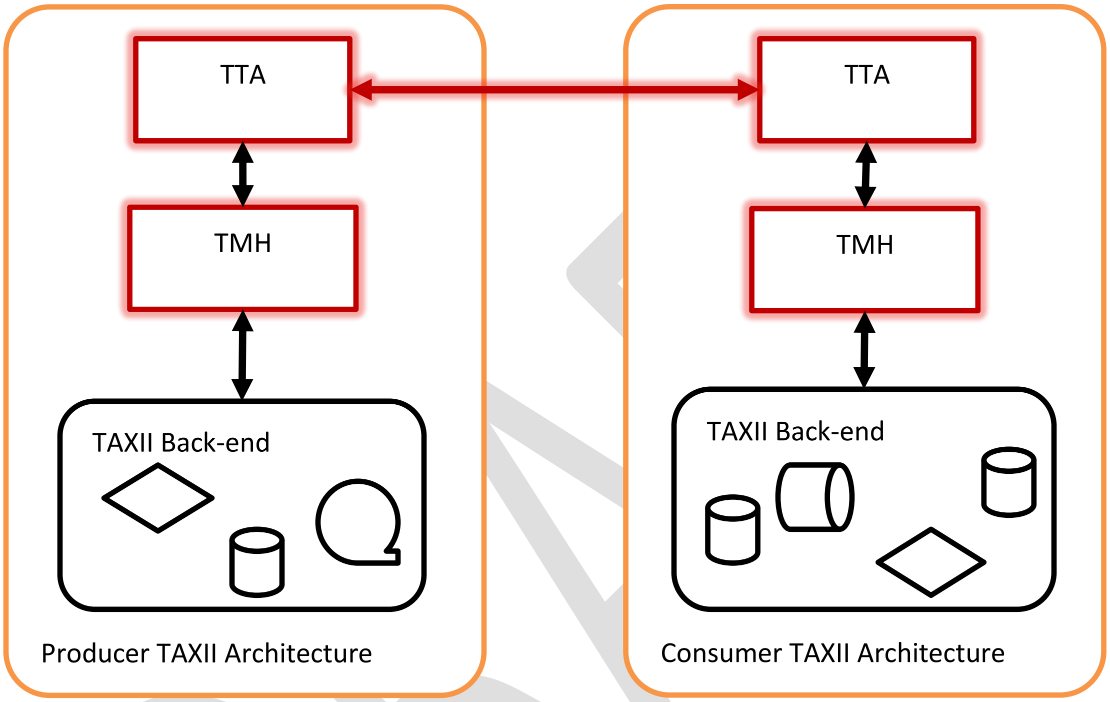

Figure 2 - The Interaction of TAXII Functional Units

Figure 2 shows a notional interaction between a TAXII Producer and a TAXII Consumer. The two TTAs communicate with each other over the network using protocols defined in a Protocol Binding Specification. The recipient's TTA then extracts the TAXII Message from the network and passes it to the TMH. The TMH parses the TAXII Message and interacts with the TAXII Back-end to determine the appropriate response. The TMH then takes this response, packages it as a TAXII Message, and passes it on to the TTA for transmission. The TAXII specifications provide normative requirements for the components that appear in red. Specifically, they provide requirements with regard to how TAXII Messages are exchanged between TAXII Architectures and also provide requirements which dictate the behavior of TTAs and TMHs. Note that the TAXII specifications do not require or anticipate uniformity in the implementation of TAXII Back-ends.

1.2.4 TAXII Network Components

The following terms are used to define the components of a TAXII Implementation using a typical client-server model. Note that these do not map directly to the TAXII Roles previously defined: For example, an entity might both host a TAXII Daemon and use a TAXII Client in their role as a TAXII Consumer. The defined network components represent a network-centric view of TAXII participants while the defined roles represent an activity-centric view.

TAXII Implementation - A specific implementation of a TAXII Architecture.

TAXII Daemon - The part of a TAXII Implementation that provides one or more TAXII Services. To support this functionality, it is assumed that a TAXII Daemon is persistently listening for new TAXII requests over a network.

TAXII Client - The part of a TAXII Implementation that initiates an exchange with a remote TAXII Daemon. A TAXII Client does not need a persistent connection on the network to operate but can open a connection when it wishes to interact with a TAXII Daemon and disconnect from the network when this interaction has concluded.

2 TAXII Capabilities

TAXII exists to provide specific capabilities for sharing structured cyber threat information. TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilities that the current version of TAXII supports: push messaging, pull messaging, and discovery.

2.1 Push Messaging

Structured cyber threat information can be pushed from a Producer to a Consumer. This may reflect a pre-existing relationship between the Producer and Consumer, where the Consumer has requested to receive periodic content pushes from the Producer. On the other end of the spectrum, push messaging can be used in a case where a Consumer is willing to accept contributions from any party and any Producer can volunteer content at any time without any pre-existing relationship. An example of the former is a Consumer who subscribed to a Producer's TAXII Data Feed, while an example of the latter is a Consumer that is acting as a repository of published information and allows anyone to volunteer data.

2.2 Pull Messaging

A Consumer can request to pull structured cyber threat information from a Producer. This not only allows the Consumer to control when they receive cyber threat data, but allows the consumer to receive data without having to listen for incoming connections. As with push messaging, the Producer and Consumer may have an existing agreement for the Consumer to have access to the Producer's content. Alternately, a Producer may make their information available publicly and any Consumer can contact them requesting the data.

This version of TAXII does not support arbitrary querying of the cyber threat data. Instead, this version of TAXII limits Consumers to making requests against the Producer's TAXII Data Feeds. The Producer has full discretion as to how their content is organized into TAXII Data Feeds. Within a TAXII Data Feed, individual pieces of data are assigned a Timestamp Label. Consumers can use Timestamp Labels to request a particular subset of the overall TAXII Data Feed. The pull messaging Capability in this version of TAXII is tied to this understanding of a Producer's content.

2.3 Discovery

TAXII implementers have a great deal of flexibility in which TAXII Services and Capabilities they support. Moreover, as noted earlier, TAXII is bound to neither a particular network protocol nor to a particular message binding. In order to facilitate automated communication, TAXII supports the ability to discover the specific TAXII Services a TAXII user (or group of TAXII users) supports, as well as the network addresses and specific bindings the associated TAXII Daemons support. This does not remove the need for human involvement in the establishment of sharing agreements - sharing agreement negotiation is outside the scope of TAXII. Discovery does, however, allow for the automated exchanging of information about what TAXII Capabilities a Producer might support and what technical mechanisms they employ in doing so.

3 TAXII Services

TAXII Services represent a set of mechanisms necessary to support some TAXII Capability or Capabilities. A TAXII Implementation may support some, all, or even none of the defined TAXII Services. (On the latter note, one can still make use of some TAXII Capabilities without ever hosting a TAXII Daemon that supports any of the described TAXII Services.)

TAXII defines the following Services:

- Discovery Service – Provide information about offered TAXII Services.
- Feed Management Service – Support management of TAXII Data Feed subscriptions.
- Inbox Service – Support Producer-initiated pushes of cyber threat information.
- Poll Service - Support Consumer-initiated pulls of cyber threat information.

The following sections look at each of these services in more detail.

3.1 Discovery Service

The Discovery Service is the mechanism for communicating information related to the availability and use of TAXII Services. The Discovery Service provides a requester with a list of TAXII Services and how these Services may be invoked (i.e., the address of the TAXII Daemon that implements that service and the bindings that Daemon supports). A single Discovery Service might report on TAXII Services hosted by TAXII Daemons on multiple endpoints or even across multiple organizations - the owner of a Discovery Service can define its scope as they wish, as long as they comply with legal, ethical, and other considerations. A Discovery Service is not required to disclose all TAXII Services of which it is aware; a Discovery Service may use a variety of factors to determine which Services to disclose to the requester, including but not limited to the requester's identity. In order to facilitate automation, each TAXII Protocol Binding Specification defines a recommended default address for the Discovery Service.

A Discovery Service implementation MUST support the Discovery Message Exchange.

3.2 Feed Management Service

The Feed Management Service is the mechanism by which a Consumer may request information about TAXII Data Feeds, request subscriptions to TAXII Data Feeds, or terminate existing subscriptions to TAXII Data Feeds. The Feed Management Service does not deliver TAXII Data Feed content (i.e., the threat information the Producer publishes in association with the named TAXII Data Feed). Instead, TAXII Data Feed content is either sent to a Consumer's TAXII Daemon implementing an Inbox Service in Producer-initiated exchanges or in direct response to Consumer requests to the Producer's Poll Service.

A Feed Management Service implementation MUST support at least one of the Subscription Management Exchange and the Feed Information Exchange.

A Feed Management Service implementation MAY support both the Subscription Management Exchange and the Feed Information Exchange.

3.3 Inbox Service

The Inbox Service is the mechanism by which a Consumer accepts messages from a Producer in Producer-initiated exchanges (i.e., push messaging). A Consumer may implement this Service in order to receive TAXII Data Feed content via Producer-initiated exchanges. Such content might be the result of the Consumer's establishment of subscriptions on a Producer or may be unsolicited data.

An Inbox Service implementation MUST support the Inbox Exchange.

3.4 Poll Service

The Poll Service is the mechanism by which a Producer allows Consumer-initiated pulls from a TAXII Data Feed (i.e., pull messaging). A Consumer contacts the Poll Service to explicitly request TAXII Data Feed content. Consumers can contact the Poll Service to request TAXII Data Feed content at the Consumer's convenience. Note that Producers may choose to offer TAXII Data Feed content through a combination of Producer-initiated pushes to the Consumer's Inbox Service and Consumer-initiated pulls from the Producer's Poll Service.

A Poll Service implementation MUST support the Feed Poll Exchange.

4 TAXII Messages

This section defines TAXII Messages, their contents and their purposes. Some messages, such as the TAXII Status Message, are used in multiple message exchanges while others are only used in a single message exchange. The messages defined here are the only allowed messages that may be sent as part of a TAXII message exchange. While the values of some fields may be customized by implementers, implementers may not create new message types.

This section is limited to a description of the data models representing TAXII Messages. This section does not prescribe any particular binding for this data model - such details are provided by TAXII Message Binding Specifications. This section describes what information a TAXII Message must convey, while the TAXII Message Binding Specifications define how to express that information. As a result, there are not always one-to-one mappings between fields in the data model and fields in the data bindings. For example, some bindings may require multiple field structures (e.g., elements and attributes in an XML [4] binding) to account for the intended meaning of a single field as described in this document. Alternatively, a field's value might be conveyed without any transmitted structure. For example, an XML binding might specify default values for some field structures allowing that field to be dropped from the actual message structure during communications. It is important to keep in mind that this section describes the conceptual fields in the data model; the message bindings follow those concepts, but may include structural differences to account for limitations or capabilities of the particular binding. Implementers need to consult the appropriate TAXII Message Binding Specification for binding requirements and details.

All TAXII Messages consist of two parts: a header and a body. The header contains information relevant to all message body types, while the body contains information relevant to a particular message type. The following sections describe the use of the header and body types and list their fields. Each field is listed with the following information:

- Name - A handle by which the TAXII specifications refer to this field. This may not be exactly identical to the structural field names (e.g., XML element or attribute names) that appear in the TAXII Message Binding Specifications.
- Required? - Whether the message must convey the indicated information. Note that in a particular message binding default values may allow a required field to be absent in the actual exchanged content. The fact that the default value is implicitly conveyed fulfills the requirement for the field's presence.
- Multiple? - Whether field indicates a single value or whether it can indicate multiple values.
- Description - A description of the information the field conveys between the message sender and recipient.

Details such as the data type of the field and the definition of controlled vocabularies used by a field are outside the scope of this document and are instead covered in each TAXII Message Binding Specification. Some fields are noted as having "sub-fields" - this is simply an organizational convenience for this document and not a requirement imposed on their representation in any given binding. The "Required?" and "Multiple?" values for a given sub-field reflect its use only within its parent field. A sub-field might not allow multiple values, but the sub-field is still be able to appear and hold a single value in each of multiple instances of its parent field.

4.1 Message Concepts

This section contains requirements and information for concepts applicable to all TAXII Messages.

4.1.1 Message IDs

Every TAXII Message has a Message ID field. Message IDs 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 the Message ID of Message A. This allows the recipient of Message B to know to which of their requests this is a response.

Message IDs SHOULD be unique to a particular message between a given sender and a given recipient. More specifically, a message sender should not reuse a particular Message ID if it is still expecting a response to an earlier request that used that same Message ID as this could lead to confusion as to which message a given response was responding to.

4.1.2 Data Feed Names

Every TAXII Data Feed has a unique identifier relative to the other TAXII Data Feeds from the same Producer. (Technically, Feed Names only need to be unique on a given Feed Management Service and on a given Poll Service, but in practice, Producers will likely wish to ensure that no two of their TAXII Data Feeds have the same Feed Names regardless of how those feeds map to Feed Management and Poll Services.) There is no problem if two different Producers use the same Feed Name unless those Producers share a Feed Management or Poll Service.

Consumers use Feed Names as handles to a Producer's TAXII Data Feeds in their request messages. Note that because Feed Names are unique relative to a Producer rather than globally unique, it is possible that a single Consumer may interact with multiple Producers and, during the course of these interactions, encounter two distinct TAXII Data Feeds with identical Feed Names. For this reason, Consumers should track both the Feed Name and the associated Producer identity together since the combination of these values should be globally unique.

Producers may use any syntax they wish for their Feed Names - names can be human-readable titles, hexadecimal numbers, or anything else. This said, Feed Names should stick to strings consisting of alphanumeric values to avoid possible conflicts with message binding formats. (For example, the greater-than character (<), while legal in a Feed Name, is problematic for message bindings that use XML since it is a reserved character in that format.)

4.1.3 Timestamp Labels

In TAXII, each piece of content within a TAXII Data Feed is assigned a unique Timestamp Label value. As defined earlier, a piece of TAXII Content is considered "atomic" within a TAXII Data Feed. While a Timestamp Label is in the form of a timestamp, it is important to note that, for any given piece of content, the Timestamp Label assigned to that content does not necessarily correspond to any chronological event nor do they necessarily align with any timestamps that appear within that content. The Timestamp Label is just a label, rather than a reference to some meaningful chronological time.

Timestamp Labels must conform to a specific set of rules:.

1. Timestamp Labels MUST comply with the date-time construct as defined in IETF RFC 3339 [7].
2. Each piece of content in a TAXII Data Feed MUST have a unique Timestamp Label (i.e., Timestamp Labels are unique within a TAXII Data Feed).
3. When a new piece of content is added to a TAXII Data Feed, that content MUST be assigned a Timestamp Label later than the Timestamp Label of any other piece of content within that feed. Note that this property must be maintained even if the Producer assigns Timestamp Labels that use different time zones - new Timestamp Labels must be chronologically later than all other previous Timestamp Labels within that TAXII Data Feed. (In other words, one must be able to

use Timestamp Labels to create an unambiguous total ordering of content within a TAXII Data Feed.)

4. Timestamp Labels are precise up to 6 decimal places with regard to fractional seconds. A Timestamp Label with more than 6 decimal places of fractional seconds MUST be truncated to have only 6 decimal places of precision before processing. In other words, these Timestamp Labels are all considered distinct:
   - 2013-04-30T01:59:59.999999Z
   - 2013-04-30T02:00:00Z
   - 2013-04-30T02:00:00.000001Z

   However, the following Timestamp Labels are treated as identical because, after truncating to 6 decimal places of precision, they are all the same value:
   - 2013-04-30T02:00:00.000001Z
   - 2013-04-30T02:00:00.0000012Z
   - 2013-04-30T02:00:00.0000019Z

4.2 TAXII Header

This section defines the conceptual model for the header fields of a TAXII Message.

Table 1 - TAXII Header Fields

Name	Required?	Multiple?	Description
Message ID	Yes	No	A value identifying this message.
Message Body Type	Yes	No	The type of the TAXII Message. Only identifiers for defined TAXII Messages are allowed in this field. (I.e., third parties may not define their own TAXII Message Body Types.)
In Response To	Yes, if this message is a response.	No	Contains the Message ID of the message to which this is a response, if applicable.
Extended-Header	No	Yes	Third parties may define their own additional header fields. Extended-Header fields that are not recognized by a recipient SHOULD be ignored. Extended-Headers fields MUST be expressible as name-value pairs, although there is no restriction on what is permissible as either a name or a value.
Signature	No	No	This field contains a signature for this TAXII Message. The scope of this signature is the entire TAXII Message (i.e., Signatures contained in this field may sign all or any parts of the TAXII Message).

4.3 TAXII Message Bodies

TAXII Message bodies are used to support specific TAXII Message Exchanges. The Message Body Types defined in this specification are:

- TAXII Status Message

- TAXII Discovery Request
- TAXII Discovery Response
- TAXII Feed Information Request
- TAXII Feed Information Response
- TAXII Manage Feed Subscription Request
- TAXII Manage Feed Subscription Response
- TAXII Poll Request
- TAXII Poll Response
- TAXII Inbox Message

Each permissible TAXII Message Body Type is described in detail in the following sub-sections:

4.3.1 TAXII Status Message

A TAXII Status Message is used to indicate a condition of success or error. Status Messages are always sent from a TAXII Daemon to a TAXII Client in response to a TAXII Message. A TAXII Status Message is used to indicate success or failure to perform some requested action. Failure may occur because the request itself was invalid or because the recipient was unwilling or unable to honor the request.

Table 2 - TAXII Status Types

Status Type	Description
Bad Message	The message sent could not be interpreted by the TAXII Daemon. This may be because it was malformed.
Denied	This is used in cases where the TAXII Client's action is being denied for reasons other than a failure to provide appropriate authentication credentials. For example, a Feed Management Service might limit the number of subscriptions a given Consumer is allowed to create. In this case, if a Consumer attempts to create a too many subscriptions, a TAXII Daemon might send a Status Message of type "Denied".
Failure	A general indication of failure. This may be sent because of some problem other than those outlined above, but may also be sent in place of any other TAXII Status Messages if a TAXII Daemon does not wish to disclose details for the failure of a request.
Not Found	The request named some target (e.g., a TAXII Data Feed name) but that target does not exist on the TAXII Daemon.
Retry	The request cannot be completed immediately. The Error Detail field SHOULD contain a timestamp indicating when a retry of the request might be successful. The requested action will not occur until and unless the request is repeated.
Success	The message sent was interpreted by the TAXII Daemon and the requested action was completed successfully. Note that some request messages have a corresponding response message used to indicate successful completion of a request. In these cases, that response message MUST be used instead of sending a Status Message of type "Success".

Status Type	Description
Unauthorized	The requested activity requires authentication, but either the TAXII Client did not provide authentication or their authenticated identity did not have appropriate access rights. (Note that any authentication credentials are provided at the protocol level rather than as part of a TAXII Message.)
Unsupported Message Binding	The requester identified a set of message bindings to be used in the fulfillment of its request, but none of those message bindings are supported for the requested action. The Status Detail field SHOULD contain a list of acceptable message bindings.
Unsupported Message Type	Indicates that the requester sent a message type that is unsupported by the TAXII Daemon that received it. The Status Detail field SHOULD contain a list of acceptable message types.
Unsupported Payload Binding	The requester identified a set of payload bindings to be used in the fulfillment of its request, but none of those payload bindings are supported for the requested action. The Status Detail field SHOULD contain a list of acceptable Payload Binding Identifiers.
Unsupported Protocol Binding	The requester identified a set of protocol bindings to be used in the fulfillment of its request, but none of those protocol bindings are supported for the requested action. The Status Detail field SHOULD contain a list of acceptable protocol bindings.
Polling Not Supported	The requester attempted to create a subscription where the requester polls for content, but the associated TAXII Data Feed is not available via polling. (I.e., the TAXII Data Feed is not hosted by a Poll Service.)

Table 3 - TAXII Status Message Fields

Name	Required?	Multiple?	Description
Status Type	Yes	No	One of the Status Types defined in Table 2 or a third party-defined status type.
Status Detail	Per Status Type	No	A field for additional information about this status in a machine-readable format. (The details of this format appear in the appropriate TAXII Message Binding Specification.) The individual status types indicate what should be present in this field (if anything). For status types defined in Table 2, this field SHOULD only be present when the status type indicates and MUST only contain the indicated information. For third party defined status types, a Status Detail message MAY be defined.
Message	No	No	Additional information for the status. There is no expectation that this field must be interpretable by a machine and is instead targeted to human readers.

TAXII Daemons reporting an error condition SHOULD provide as much detail as possible in the Message field. Third parties MAY define additional error types. If the recipient of this status does not recognize the status type, it SHOULD be treated as a Status Type of "Failure". The individual TAXII Message Binding

Specifications indicate how vendors may indicate the use of a proprietary status type using that message binding.

4.3.2 TAXII Discovery Request

This message is sent to a Discovery Service to request information about provided TAXII Services. Such information includes what TAXII Services are offered, how the TAXII Daemons that support those Services may be accessed, and what protocols and message bindings are supported. The body of this message is empty.

4.3.3 TAXII Discovery Response

This message is sent from a Discovery Service in response to a TAXII Discovery Request if the request is successful. If there is an error condition, a TAXII Status Message indicating the nature of the error is sent instead.

Table 4 - TAXII Discovery Response Message Fields

Name	Required?	Multiple?	Description
Service Instance	No	Yes	This field may appear any number of times (including 0), each time identifying a different instance of a TAXII Service. This field has several sub-fields.
Service Type	Yes	No	This field identifies the Service Type of this Service Instance (e.g., Poll, Inbox, Feed Management, or Discovery).
TAXII Services Version	Yes	No	This field identifies the TAXII Services Specification to which this Service conforms. This must be a TAXII Services Version ID as defined in a TAXII Services Specification.
Protocol Binding	Yes	No	This field identifies the protocol binding supported by this Service. This should be a TAXII Protocol Binding Version ID as defined in a TAXII Protocol Binding Specification. This may be an identifier for a protocol binding defined by a third party.
Message Binding	Yes	Yes	This field identifies the message bindings supported by this Service instance. Each message binding should be a TAXII Message Binding Version ID as defined in a TAXII Message Binding Specification. This may include identifiers for message bindings defined by a third party.
Inbox Service Accepted Payload	Only if the Service Type is an Inbox Service	Yes	This field SHOULD NOT be present for any Service Type other than Inbox; recipients MUST ignore this field if the Service Type is not Inbox, as it has no meaning. This field identifies payload bindings that this Inbox Service is willing to accept. Each Inbox Service Accepted Payload should be a Payload Binding Identifier as defined in the TAXII Payload Binding Reference. This field may include Payload Binding Identifiers defined by a third party. A special value is provided by all TAXII Message Binding Specifications to indicate that the Inbox Service accepts content using any payload binding.

Name	Required?	Multiple?	Description
Service Address	Yes	No	This field identifies the network address of the TAXII Daemon that hosts this Service. The Service Address MUST use a format appropriate to the Protocol Binding field value.
Available	No	No	This field indicates whether the identity of the requester (authenticated or otherwise) is allowed to access this TAXII Service. True indicates that the identity of the requester is allowed to access the given Service. False indicates that the identity is denied access or that the identity's access rights are currently unknown.
Message	No	No	This field contains a message regarding this Service instance. This message is not required to be machine readable and is usually a message for a human operator.

Each Service Instance record identifies one instance of a TAXII Service as hosted by a particular TAXII Daemon. Each instance identifies a single TAXII Protocol Binding Specification and a network address for that binding. An instance may identify multiple TAXII Message Binding Specifications and (if the TAXII Service is an Inbox Service) a set of payload bindings. Note that, within a single Service Instance record, it is expected that every combination of message bindings and payload bindings is acceptable. In other words, if the record for an Inbox Service lists two acceptable message bindings (1 and 2) and three acceptable payload bindings (A, B, and C), all six message binding-payload binding combinations are considered valid (1A, 1B, 1C, 2A, 2B, and 2C). If a given Inbox Service only accepts certain combinations of message bindings and payload bindings it may need to be represented by multiple Service Instance records to avoid incorrectly indicating support for an unsupported combination. For example, if a particular Inbox Service supported two message bindings (1 and 2) and three payload bindings (A, B, and C), but only supported the a subset of all possible combinations (e.g., it only supported 1A, 1B, 2B, and 2C), this service would need to be represented by multiple Service Instance records (i.e., one record that noted support for message binding 1 and payload bindings A and B, and a second record that noted support for message binding 2 and payload bindings B and C). Note that situation only arises when describing an instance of an Inbox Service, and only when that instance supports multiple message and payload bindings but fails to support certain combinations of the two.

Note that the Discovery Service is not required to list all existing TAXII Services of which it is aware. For example, some TAXII Services might only be publicized to specific, authenticated parties. As such, different requesters may get different responses to a Discovery Request sent to the same Discovery Service.

4.3.4 TAXII Feed Information Request

This message is sent to a Feed Management Service to request information about the available feeds. The body of this message is empty.

4.3.5 TAXII Feed Information Response

This message is sent in response to a TAXII Feed Information Request if the request is successful. If there is an error condition, a TAXII Status Message indicating the nature of the error is sent instead. Note that the Producer is under no obligation to list all feeds and may exclude any or all feeds from this response for any reason. For example, the Producer may wish to exclude feeds created for a specific customer from a list of all feeds. As such, different requesters may be given different lists of feeds to their requests to the same Feed Management Service.

Table 5 - TAXII Feed Information Response Fields

Name	Required?	Multiple?	Description
Feed Information	No	Yes	This field may appear any number of times (including 0), each time identifying a different TAXII Data Feed. It has several sub-fields.
Feed Name	Yes	No	This field contains the name by which this TAXII Data Feed is identified. Each TAXII Data Feed managed by a single Feed Management Service MUST have a unique Feed Name.
Feed Description	Yes	No	This field contains a prose description of this TAXII Data Feed. This field may explain how to gain access to this TAXII Data Feed if access is restricted. (E.g., pay a fee, only available to members of some organization, etc.)
Supported Payload	Yes	Yes	This field contains the Payload Binding Identifiers indicating which types of payloads are currently expressed in this TAXII Data Feed. Each Supported Payload should be a Payload Binding Identifier as defined in the TAXII Payload Binding Reference. This field may include Payload Binding Identifiers defined by a third party.
Available	No	No	This field indicates whether the identity of the requester (authenticated or otherwise) is allowed to access this TAXII Service. True indicates that the identity of the requester is allowed to access the given TAXII Data Feed. False indicates that the identity is denied access or that the identity's access rights are currently unknown.
Push Method	At least one of Push Method and Poll Service Instance MUST be present. Both MAY be present.	Yes	This field identifies the protocols that may be used to receive pushed content via a subscription. If content from this TAXII Data Feed may be pushed via multiple protocols, this field may appear multiple times. This field has multiple sub-fields.

Name	Required?	Multiple?	Description
Push Protocol	Yes	No	This field identifies a protocol binding that can be used to push content to an Inbox Service instance. This should be a TAXII Protocol Binding Version ID as defined in a TAXII Protocol Binding Specification. This may be an identifier for a protocol binding defined by a third party.
Push Message Binding	Yes	Yes	This field identifies the message bindings that can be used to push content to an Inbox Service instance using the protocol identified in the Push Protocol field. Each message binding should be a TAXII Message Binding Version ID as defined in a TAXII Message Binding Specification. This may include identifiers for message bindings defined by a third party.
Polling Service Instance	At least one of Push Method and Poll Service Instance MUST be present. Both MAY be present.	Yes	This field identifies the bindings and address a Consumer can use to interact with a Poll Service instance that supports this TAXII Data Feed. If multiple Poll Services support this TAXII Data Feed, this field may appear multiple times. A subscription may or may not be required before content from this data feed can be polled. This field has multiple sub-fields.
Poll Protocol	Yes	No	This field identifies the protocol binding supported by this Poll Service instance. This should be a TAXII Protocol Binding Version ID as defined in a TAXII Protocol Binding Specification. This may be an identifier for a protocol binding defined by a third party.
Poll Address	Yes	No	This field identifies the address of the TAXII Daemon hosting this Poll Service instance. This field MUST use a format appropriate to the Poll Protocol field value.
Poll Message Binding	Yes	Yes	This field identifies the message bindings supported by this Poll Service instance. Each message binding should be a TAXII Message Binding Version ID as defined in a TAXII Message Binding Specification. This may include identifiers for message bindings defined by a third party.
Subscription Method	No	No	This field identifies the protocol and address of the TAXII Daemon hosting the Feed Management Service that can process subscriptions for this TAXII Data Feed. This field may be absent if there is not a TAXII Service that processes subscription requests for this feed. In that case subscriptions, if supported, must be established by mechanisms other than TAXII. In the case of alternative subscription methods, the Feed Description field should explain the procedures for subscribing.

Name	Required?	Multiple?	Description
Subscription Protocol	Yes	No	This field identifies the protocol binding supported by this Feed Management Service instance. This should be a TAXII Protocol Binding Version ID as defined in a TAXII Protocol Binding Specification. This may be an identifier for a protocol binding defined by a third party.
Subscription Address	Yes	No	This field identifies the address of the TAXII Daemon hosting this Feed Management Service instance. This field MUST use a format appropriate to the Subscription Protocol field value.
Subscription Message Binding	Yes	Yes	This field identifies the message bindings supported by this Feed Management Service Instance. Each message binding should be a TAXII Message Binding Version ID as defined in a TAXII Message Binding Specification. This may include identifiers for message bindings defined by a third party.

4.3.6 TAXII Manage Feed Subscription Request

This message is used to manage (i.e., subscribe, unsubscribe, or request the status of) a subscription. The Feed Management Service responds with a TAXII Manage Feed Subscription Response if the request is successful and will be honored or with a TAXII Status Message if the request is being rejected or there was an error.

Table 6 - TAXII Manage Feed Subscription Request Fields

Name	Required?	Multiple?	Description
Feed Name	Yes	No	This field identifies the name of the TAXII Data Feed to which the action applies. Each TAXII Data Feed managed by a single Feed Management Service MUST have a unique Feed Name.
Action	Yes	No	This field identifies the requested action to take. The action MUST be one of the following: ○ SUBSCRIBE - Request a subscription to the named TAXII Data Feed. ○ UNSUBSCRIBE - Request cancellation of an existing subscription to the named TAXII Data Feed. ○ STATUS - Request information on all subscriptions the requester has established for the named TAXII Data Feed. No subscription state is changed in response to this action.
Subscription ID	Per Action	No	This field contains the ID of a previously created subscription. For the UNSUBSCRIBE action this field MUST be present. This field MUST be ignored if present in a SUBSCRIBE or STATUS action message.

Name	Required?	Multiple?	Description
Delivery Parameters	Yes	No	This field identifies the delivery parameters for this request. This field contains multiple sub-fields. If the subscription action is SUBSCRIBE, subfields indicates how the requester is requesting to have messages pushed to their Inbox Service. A special value is provided by all TAXII Message Binding Specifications to indicate that the requester is not requesting pushed content and will poll for subscription content instead use a Poll Service hosted by the data provider. In this case, if the TAXII Data Feed cannot be polled, a Status Message with a status of 'Polling Not Supported' should be returned. For actions of UNSUBSCRIBE and STATUS, this field MUST be ignored by recipients and SHOULD NOT be included by senders.
Inbox Protocol	Yes, if requesting push messaging	No	This field identifies the protocol that should be used when pushing TAXII Data Feed content to a Consumer's TAXII Inbox Service implementation. If the Data Feed does not support the named Inbox Protocol, a Status Message with a status of 'Unsupported Protocol Binding' should be returned. The Inbox Protocol should be a TAXII Protocol Binding Version ID as defined in a TAXII Protocol Binding Specification or by a third party.
Inbox Address	Yes, if requesting push messaging	No	This field identifies the address of the TAXII Daemon hosting the Inbox Service to which the Consumer requests content for this TAXII Data Feed to be delivered. The address MUST be of the appropriate type for the network protocol identified in the Inbox Protocol field.
Delivery Message Binding	Yes, if requesting push messaging	No	This field identifies the message binding that should be used to send pushed content for this subscription. If the TAXII Data Feed does not support the Delivery Message Binding, a Status Message with a status of 'Unsupported Message Binding' SHOULD be returned. Each Delivery Message Binding should be a TAXII Message Binding Version ID as defined in a TAXII Message Binding Specification. This may include an identifier for a message binding defined by third parties.

Name	Required?	Multiple?	Description
Payload Binding	Yes, if requesting push messaging	Yes	This field contains Payload Binding Identifiers indicating which types of payloads the Consumer requests to receive for this TAXII Data Feed. This field should contain a Payload Binding Identifiers as defined in the TAXII Payload Binding Reference. This field may include Payload Binding Identifiers defined by a third party. If none of the listed Payload Binding values are supported by the Data Feed, a Status Message with a status of 'Unsupported Payload Binding' SHOULD be returned. A special value is provided by all TAXII Message Binding Specifications to indicate that the requester is indicating that all TAXII Data Feed content should be sent regardless of the format it uses.

Responses to subscription management requests should be processed using the following criteria in order:

1. Any attempt to manage subscriptions that require authentication where the request comes from a source that lacks appropriate authentication SHOULD result in an appropriate TAXII Status Message (normally "Unauthorized") without changing existing subscriptions. This takes precedence over all other conditions.
2. Attempts to manage feeds where the requested Feed Name does not correspond to an existing Feed Name SHOULD result in an appropriate TAXII Status Message (normally "Not Found") without changing existing subscriptions.
3. Attempts to unsubscribe (UNSUBSCRIBE action) where the Subscription ID does not correspond to an existing subscription on the named TAXII Data Feed by the identified Consumer SHOULD be treated as a successful attempt to unsubscribe and result in a TAXII Manage Feed Subscription Response without changing existing subscriptions. In other words, the requester should be informed that there is now no subscription with that Subscription ID (even though there never was one in the first place).
4. Attempts to create a new subscription (SUBSCRIBE action) where the requested Inbox Protocol, Delivery Message Binding, or Payload Binding of the subscription to be created is not supported SHOULD result in an appropriate TAXII Status Message (normally "Unsupported Protocol Binding", "Unsupported Message Binding", or "Unsupported Payload Binding" respectively) without changing existing subscriptions.
5. Attempts to create a new subscription (SUBSCRIBE action) where the subscription to be created is identical to an existing subscription (i.e., same Feed Name and Delivery Parameters) SHOULD result in a TAXII Manage Feed Subscription Response that returns that existing subscription's Subscription ID without changing existing subscriptions. That is, the Feed Management Service SHOULD not create exact duplicates of existing subscriptions, but the client SHOULD be informed that the requested subscription is established.

4.3.7 TAXII Manage Feed Subscription Response

This message is returned in response to a TAXII Manage Feed Request Message if the requested action was successfully completed.

Table 7 - TAXII Manage Feed Subscription Response Fields

Name	Required?	Multiple?	Description
Feed Name	Yes	No	This field identifies the name of the TAXII Data Feed to which the action applies. Each TAXII Data Feed managed by a single Feed Management Service MUST have a unique Feed Name.
Message	No	No	This field contains a message associated with the subscription response. This message is not required to be machine readable and is usually a message for a human operator.
Subscription Instance	Yes	Yes	This field contains information about existing subscriptions by the requester to the given TAXII Data Feed. It appears any number of times (including 0) if this message is in response to a STATUS action, or exactly once if responding to any other action.
Subscription ID	Yes	No	This field contains an identifier that is used to reference the given subscription in subsequent exchanges.
Delivery Parameters	Yes if message is responding to a STATUS action	No	This field contains a copy of the Delivery Parameters of the Manage Feed Subscription Request Message that established this subscription. This field MUST be present if this message is responding to a STATUS action. This field MAY be present when responding to other actions.
Inbox Protocol	Yes, if requested push messaging	No	This field contains a copy of the Inbox Protocol field in the Manage Feed Subscription Request Message that established this subscription.
Inbox Address	Yes, if requested push messaging	No	This field contains a copy of the Inbox Address field in the Manage Feed Subscription Request Message that established this subscription.
Delivery Message Binding	Yes, if requested push messaging	No	This field contains a copy of the Delivery Message Binding field in the Manage Feed Subscription Request Message that established this subscription.
Payload Binding	Yes, if requested push messaging	Yes	This field contains a copy of the Payload Binding field(s) in the Manage Feed Subscription Request Message that established this subscription.

Name	Required?	Multiple?	Description
Poll Instance	Yes, if action was SUBSCRIBE and the request was for polling. Optional otherwise	Yes	Each Poll Instance represents an instance of a Poll Service that may be contacted to retrieve content associated with the new Subscription. If the Manage Feed Subscription Request Message indicated that the requester wished to poll for content there must be at least one Poll Instance in the response to a SUBSCRIBE action. This field indicates where Poll Request Messages can be sent for the given subscription. If the requester is requesting pushed content the Subscription Response Message MAY contain one or more Poll Instances if the subscriber is also allowed to poll for content in addition to receiving pushed content. This field MAY be present for requests actions other than SUBSCRIBE.
Poll Protocol	Yes	No	The protocol binding supported by this instance of a Polling Service. This field should be a TAXII Protocol Binding Version ID as defined in a TAXII Protocol Binding Specification. This may include protocol bindings defined by third parties.
Poll Address	Yes	No	This field identifies the address of the TAXII Daemon hosting this Poll Service. This field MUST use a format appropriate to the Poll Protocol field value.
Poll Message Binding	Yes	Yes	This field identifies one or more message bindings that may be used when interacting with this Poll Service instance. Each message binding should be a TAXII Message Binding Version ID as defined in a TAXII Message Binding Specification. This may include identifiers for message bindings defined by a third party.

4.3.8 TAXII Poll Request

This message is sent from a Consumer to a TAXII Poll Service to request that data from the TAXII Data Feed be returned to the Consumer. Poll Requests are always made against a specific TAXII Data Feed. Whether or not the Consumer must already be subscribed to that TAXII Data Feed in order to receive content is left to the Producer and may vary across Data Feeds. If the TAXII Data Feed content should only be disseminated to authorized parties, it may make sense to require a subscription. Alternately, Poll Service implementers may allow requests without requiring the Consumer to have established a subscription. This might make sense if the Poll Service supports public feeds as the Producer may not wish to track subscriptions from a large body of users.

Table 8 - TAXII Poll Request Fields

Name	Required?	Multiple?	Description
Feed Name	Yes	No	This field identifies the name of the TAXII Data Feed that is being polled. Each TAXII Data Feed managed by a single Poll Service MUST have a unique Feed Name.

Name	Required?	Multiple?	Description
Exclusive Begin Timestamp Label	Yes	No	This field contains a Timestamp Label indicating the beginning of the range of TAXII Data Feed content the requester wishes to receive. This field is exclusive (e.g., the requester is asking for content where the content's Timestamp Label > this field value). A special value is provided by all TAXII Message Binding Specifications to indicate that the requested range has no lower bound.
Inclusive End Timestamp Label	Yes	No	This field contains a Timestamp Label indicating the end of the range of TAXII Data Feed content the requester wishes to receive. This range is inclusive (e.g., the requester is asking for content where the content's Timestamp Label <= this field value). A special value is provided by all TAXII Message Binding Specifications to indicate that the requested range has no upper bound.
Subscription ID	No	No	This field identifies the existing subscription the Consumer wishes to poll. If the Poll Service does not require subscriptions, this field MAY be ignored by the Poll Service. If the Poll Service requires established subscriptions for polling and this field is not present, the Poll Service SHOULD respond with a TAXII Status Message with a status of "Denied".
Payload Binding	Yes	Yes	This field indicates the type of content that is requested in the response to this poll. Each Payload Binding should be a Payload Binding Identifier as defined in the TAXII Payload Binding Reference. This field may include Payload Binding Identifiers defined by a third party. A special value is provided by all TAXII Message Binding Specifications to indicate that the client accepts any type of content.

4.3.9 TAXII Poll Response

This message is sent from a Poll Service in response to a TAXII Poll Request. This message indicates the time bounds within which TAXII Data Feed content was considered in the fulfillment of this request. Note that, as with any content provided by a Producer, the Producer may edit or eliminate content for any reason prior to providing it to a Consumer. As such, two Consumers polling the same Poll Service using identical parameters may receive different TAXII Data Feed content. For this reason, the Poll Response Begin Timestamp and End Timestamp fields reflect the range of timestamps the Producer *considers*, but not all content in the considered range is necessarily included in the Poll Response message. Nominally, the timestamp bounds in the Poll Response will be identical to the bounds provided in the Poll Request, with a "No Upper Bound" value replaced by the latest timestamp the Producer considered for inclusion. Under some circumstances, the Producer might provide a different bound - for example, if the Producer only considered some sub-segment of the Consumer's requested timestamp bounds when producing their response.

Table 9 - TAXII Poll Response Fields

Name	Required?	Multiple?	Description
Feed Name	Yes	No	This field indicates the name of the TAXII Data Feed that was polled. Each TAXII Data Feed managed by a single Poll Service MUST have a unique Feed Name.
Inclusive Begin Timestamp Label	Yes	No	This field contains a Timestamp Label indicating the beginning of the time range this Poll Response covers. A special value is provided by all TAXII Message Binding Specifications to indicate that the Poll Response covers the earliest time for this data feed. This field is inclusive.
Inclusive End Timestamp Label	Yes	No	This field contains a Timestamp Label indicating the end of the time range this Poll Response covers. This field is inclusive.
Subscription ID	No	No	This field contains the Subscription ID for which this content is being provided. This field is only present if this content is being provided as part of an established subscription to a TAXII Data Feed.
Message	No	No	This field contains additional information for the message recipient. There is no expectation that this field must be interpretable by a machine and is instead targeted to human readers.
Payload Block	No	Yes	This field contains a payload and additional information related to the payload. This field may appear 0 or more times. See section 4.3 for the definition of a Payload Block.

4.3.10 TAXII Inbox Message

A TAXII Inbox Message is used to push content from one entity to the TAXII Inbox Service of another entity.

Table 10 - TAXII Inbox Message Fields

Name	Required?	Multiple?	Description
Message	No	No	This field contains prose information for the message recipient. This message is not required to be machine readable and is usually a message for a human operator.
Subscription Information	No	No	This field is only present if this message is being sent to provide content in accordance with an existing TAXII Data Feed subscription. It has three sub fields:
Subscription ID	Yes	No	This field contains the Subscription ID for which this content is being provided.
Inclusive Begin Timestamp Label	Yes	No	This field contains a Timestamp Label indicating the beginning of the time range this Inbox Message covers. A special value is provided by all TAXII Message Binding Specifications to indicate that the Inbox Message covers the earliest time for the subscribed TAXII Data Feed. This field is inclusive.

Name	Required?	Multiple?	Description
Inclusive End Timestamp Label	Yes	No	This field contains a Timestamp Label indicating the end of the time range this Inbox Message covers. This field is inclusive.
Payload Block	No	Yes	This field contains a payload and additional information related to the payload. This field may appear 0 or more times. See section 4.3 for the definition of a Payload Block.

4.4 TAXII Payload Block

A TAXII Payload Block contains a payload of structured cyber threat information. A TAXII Payload Block may contain data that is encrypted, signed, and/or padded.

Table 11 - TAXII Payload Block

Name	Required?	Multiple?	Description
Payload Binding	Yes	No	This field contains a Payload Binding Identifier (defined in Section 1.1.2.1) indicating the type of content contained in the Payload field of this Payload Block. The Payload Binding should be a Payload Binding Identifier as defined in the TAXII Payload Binding Reference. This field may be a Payload Binding Identifier defined by a third party.
Payload	Yes	No	This field contains a payload in the type specified by the Payload Binding.
Signature	No	Yes	This field contains a signature associated with this Payload Block. The scope of this field is limited to the Payload Block that contains this field.
Timestamp Label	No	No	This field contains the Timestamp Label associated with this Payload Block. It is at the sender's discretion as to whether this is included.
Padding	No	No	This field contains an arbitrary amount of padding for this Payload Block. This is typically used to obfuscate the size of the Payload Block when the Payload is encrypted. This field should be ignored when processing a Payload Block.

4.4.1 Payload Nesting and Encryption

As noted above, the Payload Binding field in a Payload Block indicates the type of content contained in the Payload Block's Payload field. Much of the time the Payload can be used directly. For example, if the payload is STIX content, that STIX content can be directly ingested by a STIX-compatible tool once it has been extracted from the Payload Block. In other cases, however, content of one type must be extracted from content of another type before it can be used. For example, if STIX content is encrypted, compressed, or otherwise encoded in the Payload field, the content of the Payload field needs to be manipulated to extract the STIX content before the STIX content can be used. TAXII supports multiple methods for embedding one form of content inside another.

For the discussion below, suppose a hypothetical "Encryption Structure" exists and is assigned a Payload Binding Identifier of EncStr. The Encryption Structure contains a field in which one may place a binary blob representing the encrypted form of some content. The following sections describe three valid ways in which one might use this Encryption Structure to transmit an encrypted payload. Note that these examples look at encryption, but compression and other encoding structures are supported using identical methods.

4.4.1.1 Blind Nesting

The Payload Binding field identifies the "outer-most" payload only. In the case of the hypothetical Encryption Structure, this looks something like:

```
Payload Binding = EncStr
```

The recipient of a Payload Block with this Payload Binding knows that they have received an Encryption Structure (and thus can hand the Payload contents off to a subroutine that can process payloads of this type, presumably decrypting their contents). However, the Payload Binding gives no hint as to the nature of the content contained within the Encryption Structure. The recipient will need to determine the nature of the contained content through other means.

4.4.1.2 Explicit Nesting

The Payload Binding field can identify the type of content at each level of nesting. It does this by listing out each Payload Binding Identifier, in order from outer-most to inner-most, separated by a star (*) character. If an Encryption Structure contains STIX content, this looks something like the following:

```
Payload Binding = EncStr*STIX
```

This makes the type of content the recipient is ultimately receiving clear, although they must extract it from one or more other payload types first. This type of Payload Binding value is much easier for recipients because it removes any guesswork about the nature of the content within an enclosing structure. On the downside, it also means that an outside observer will know the nature of the content inside the encryption structure, even if they are not able to read that content.

4.4.1.3 Opaque Nesting

Instead of containing another payload type directly, an outer payload type can contain another TAXII Payload Block. This looks like the following:

```
Payload Binding = EncStr*PayloadBlock
```

The following figure demonstrates encryption using Opaque Nesting.

```
A = Payload Block {
        Payload Binding = STIX
        Payload = STIX payload
        Signature = Digital signature scoped to A
        Padding = ASDFGHJKL...
}

A' = A, encrypted and represented in the fictional "Encryption Struct" format

B = Payload Block {
        Payload Binding = EncStr*PayloadBlock
        Payload = A'
        Signature = Digital signature scoped to B
}
```

Figure 3 - Opaque Nesting of STIX Content

In the above example, **A** represents a Payload Block with a STIX payload. The optional Signature field contains a digital signature scoped to this Payload Block. The Padding field contains arbitrary data to extend the size of the Payload Block.

B represents another Payload Block. In this Payload Block the payload is expressed using the Encryption Struct. For this example, this encrypted material is an encrypted version of the Payload Block **A**. The Payload Binding field of **B** indicates that the Payload field is expressed in the Encryption Struct format and that this structure is wrapping another Payload Block. In **B**, the digital signature is scoped to the B Payload Block. Note that because **A** is now encrypted, its Padding field obscures the size of the Payload field of **A**.

Opaque nesting combines the best aspects of blind and explicit nesting: the type of the inner payload is provided explicitly to the recipient once they have extracted and decrypted the Payload field from **B** since this information is given explicitly in the Payload Binding field of Payload Block **A**. At the same time, however, an outside observer can learn nothing about the type of the content being conveyed. In addition, one can see how the Padding field can be used in the inner Payload Block to obscure the actual size of the conveyed payload.

For the reasons noted above, opaque nesting is the recommended way of handling payload encryption in TAXII.

5 TAXII Message Exchanges

This section describes the TAXII Message Exchanges needed to support the TAXII Services defined earlier. These exchanges only consider TAXII Messages and are agnostic to the network protocols over which those messages travel. In particular, those network protocols may require additional network exchanges prior to transmitting TAXII Messages (e.g., a SSL/TLS handshake) or break a single TAXII Message into multiple portions that are transmitted independently. The diagrams below represent the conceptual sequence in which TAXII Messages are transmitted and acted upon.

The columns in the exchanges correspond to a TAXII Daemon supporting a specific TAXII Service, as described in the Services section, or a TAXII Client. Note that a single TAXII Daemon may implement multiple TAXII Services. For this discussion we will use a shorthand notation of denoting a TAXII Daemon that supports the ABC Service as an "ABC Daemon". (I.e., a TAXII Daemon that supports the Inbox Service is referred to as an "Inbox Daemon".)

5.1.1 Inbox Exchange

In this exchange, an Inbox Message is transmitted from a TAXII Client to a listening Inbox Daemon. The Inbox Message may be solicited (e.g., a message sent to the recipient as part of a registered subscription) or unsolicited (e.g., an alert sent by some unaffiliated researcher to some public repository). The Inbox Daemon may be capable of filtering messages based on the authenticated identity of the sender.

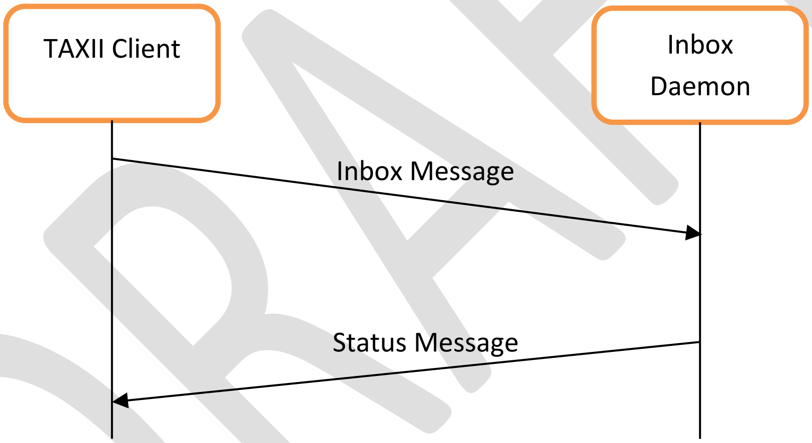

Figure 4 - Inbox Exchange

In this exchange, the TAXII Client sends an Inbox Message to the Inbox Daemon. The Inbox Daemon may pass the Inbox Message, along with any authenticated identity information, on to its TAXII Back-end. The TAXII Client receives a Status Message in response from the Inbox Daemon indicating the success or failure of the message exchange. Note that a Status Message of type "Success" indicates only that the Inbox Daemon successfully received and parsed the message. The message might still be discarded by the recipient's TAXII Back-end but the sender receives no indication if this occurs. A Status Message with an error type is used to indicate a problem with the received message.

5.1.2 Discovery Exchange

In this exchange, a TAXII Client requests information about the TAXII Services offered by a particular party. The contacted Discovery Daemon responds with a list of TAXII Services. Note that the Discovery Daemon is not required to reveal all of the TAXII Services of which it is aware to all TAXII Clients.

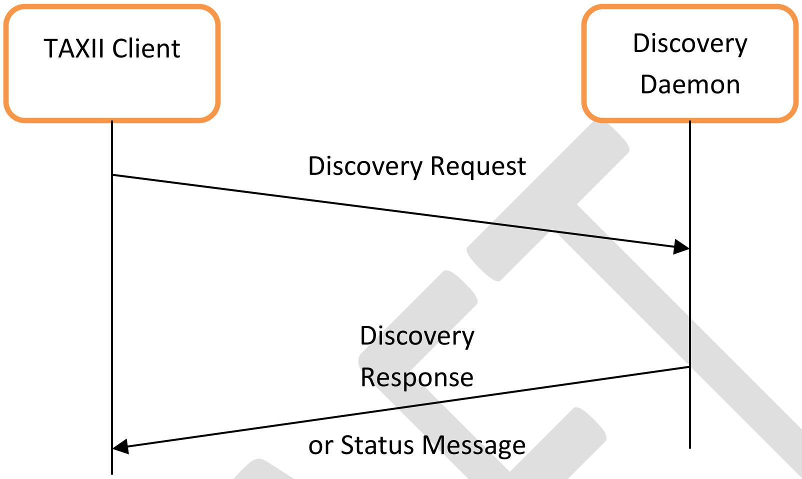

Figure 5 - Discovery Exchange

In this exchange, the TAXII Client sends a Discovery Request to the Discovery Daemon. When the Discovery Daemon receives the Discovery Request Message it may return a TAXII Status Message, indicating an error condition, or pass the relevant information to its TAXII Back-end. Relevant information may include the authenticated identity, if provided. The TAXII Back-end uses this information, along with its own access control policy, to create a list of TAXII Services to be returned or determine that the request will not be fulfilled. (E.g., the request might be denied due to a lack of authorization on the part of the requester.) If the request is honored, the list of TAXII Services is packaged into a Discovery Response which is sent back to the TAXII Client. The TAXII Client receives this message and passes the information to its own TAXII Back-end for processing. The TAXII Status Message MUST only be returned to indicate an error occurred or that the request was denied.

5.1.3 Feed Information Exchange

In this exchange, a TAXII Client requests information about the TAXII Data Feeds available on a Feed Management Daemon. The Feed Management Daemon then responds with a list of available TAXII Data Feeds. The Feed Daemon's response is dictated by its TAXII Back-end and may consider appropriate access control decisions in composing this response. Note that the Feed Management Daemon is not required to reveal all of the TAXII Data Feeds of which it is aware to all TAXII Clients.

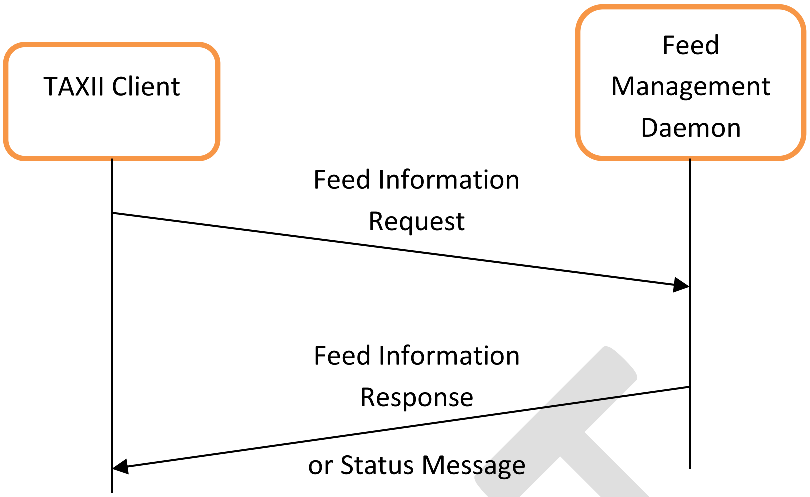

Figure 6 - Feed Information Exchange

In this exchange, the TAXII Client sends a Feed Information Request to the Feed Management Daemon. When the Feed Management Daemon receives the Feed Information Request Message it may return a TAXII Status Message, indicating an error condition, or pass the relevant information to its TAXII Back-end. Relevant information may include the authenticated identity, if any. The TAXII Back-end uses this information, along with its own access control policy, to create a list of feeds to be returned or to determine that the request will not be fulfilled. If the request is honored, the list is packaged into a Feed Information Response that is sent back to the TAXII Client. The TAXII Client receives this message and passes the TAXII Data Feed content to its own TAXII Back-end for processing. The TAXII Status Message MUST only be returned to indicate an error condition or that the request was denied.

5.1.4 Subscription Management Exchange

In this exchange, a client attempts to create, delete, or request the status of subscriptions to a named TAXII Data Feed by sending a Subscription Management Request to a Feed Management Daemon. The Feed Management Daemon passes the request to its TAXII Back-end, which determines a response. The response is then returned to the TAXII Client.

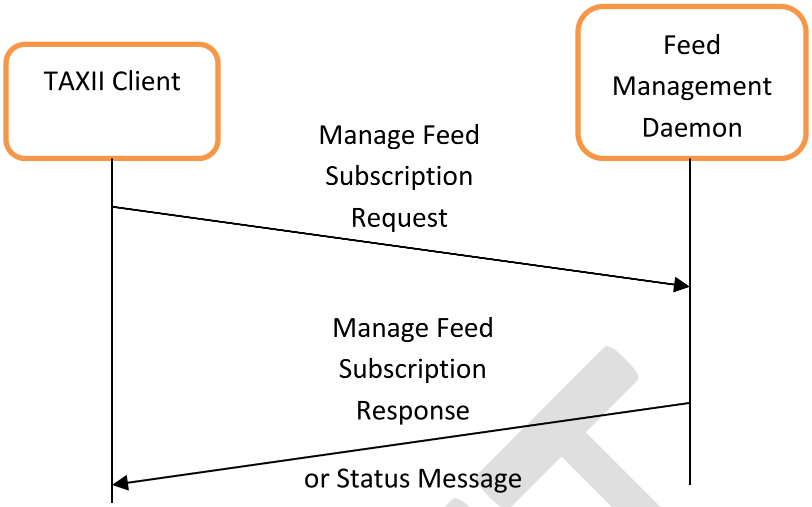
TAXII Client
Feed Management Daemon
Manage Feed Subscription Request
Manage Feed Subscription Response
or Status Message

Figure 7 - Subscription Management Exchange

In this exchange, the TAXII Client sends a Manage Feed Subscription Request to the Feed Daemon. The Feed Daemon may immediately return a TAXII Status Message, indicating an error condition, or it may pass the relevant information to its TAXII Back-end. Relevant information may include the authenticated identity, if any, the parameters for the subscription to be managed, and the action to be taken. The TAXII Back-end uses this information, along with its own access control policy, to determine whether the action is allowed. Depending on this response, the Feed Daemon may return a TAXII Status Message to indicate an error condition or send a Manage Feed Subscription Response. The TAXII Status Message MUST only be returned to indicate an error condition or that the request was denied.

5.1.5 Feed Poll Exchange

This exchange is used by a Consumer to request content from a Producer's TAXII Data Feed. The TAXII Data Feed content is returned to the Consumer in the same exchange. This allows the Consumer to retrieve the TAXII Data Feed content on its own timetable and without needing to field an Inbox Daemon or accept inbound connections. Note that the Poll Daemon is not required to provide all requested content and may exclude or alter any content in accordance with its policies.

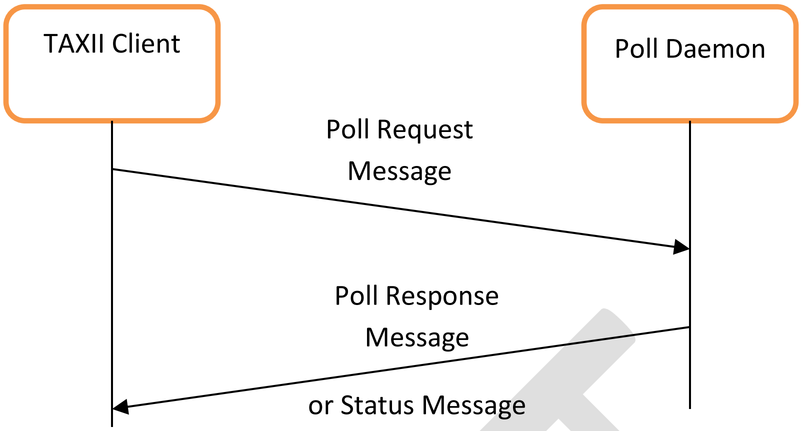

Figure 8 - Feed Poll Exchange

The Consumer's TAXII Client initiates the exchange by sending a Poll Request message to the Producer's Poll Daemon. The Poll Daemon may return an immediate TAXII Status Message, indicating an error condition, or pass the relevant information to its TAXII Back-end. Relevant information may include the Feed Name, Delivery Parameters, Timestamp Labels indicating the interval of information the Consumer is requesting, and the Consumer's authenticated identity, if provided. The TAXII Back-end evaluates this information to determine a response. If the TAXII Back-end decides to honor the request, a Poll Response Message is created encapsulating the provided content. If the TAXII Back-end rejects the request, a TAXII Status message is sent to the client indicating that the request was denied.

In all cases, the TAXII Client receives the appropriate message and passes this information on to its TAXII Back-end for processing. The TAXII Status Message MUST only be returned to indicate an error condition.

6 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.

7 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," 1 October 2012. [Online]. Available: https://stix.mitre.org/. [Accessed 19 October 2012].

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

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

[5] Defense Advanced Research Projects Agency, "RFC 793 - Transmission Control Protocl," The Internet Engineering Task Force, 1981.

[6] J. Postel, "RFC 768 - User Datagram Protocol," The Internet Engineering Task Force, 1980.

[7] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners-Lee, "RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1," The Internet Engineering Task Force, 1999.

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