THE MITRE CORPORATION

The TAXII XML Message Binding Specification

Version 1.0 (draft)

Mark Davidson, Charles Schmidt

11/16/2012

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

TAXII and STIX are trademarks of The MITRE Corporation.

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 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 in real time. TAXII is not a specific information sharing initiative or technology, 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 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 Protocol Binding Specifications and Message Binding Specifications.

Protocol Binding Specification - Protocol Binding Specifications define the requirements for transporting TAXII messages over the network. There may be multiple Protocol Binding Specifications created for TAXII. Each Protocol Binding Specification defines requirements for transporting TAXII messages using some network protocol (e.g., HTTP). They provide requirements about how the TAXII Services are supported by these network protocols.

Message Binding Specification - Message Binding Specifications define the requirements for representing TAXII messages in a particular format. There may be multiple Message Binding Specifications created for TAXII. Each Messaging Binding Specification defines a binding for TAXII messages (e.g., XML). They provide detailed guidance about how the information in the TAXII messages, as defined in the Services Specification, is actually expressed.

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

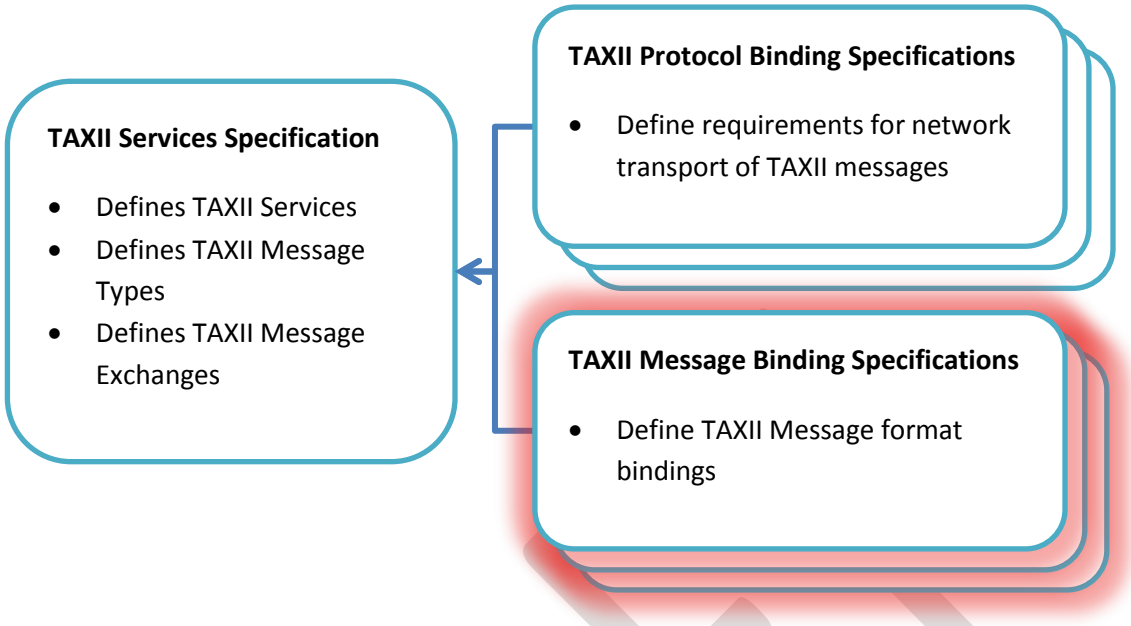

Figure 1 - TAXII Specification Hierarchy

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 evidence of significant community interest in new protocol and message bindings, TAXII can define support for those bindings without changing its 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 permissible 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 means that 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 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 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 will 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.

1.1.1.3 Specification Versioning

This document describes version 1.0 of the TAXII XML Message Binding specification. Changes to this specification that would impact content or tools will be indicated by incrementing the major or minor version numbers of this document, depending on the magnitude of the change. Such changes would also be associated with a new TAXII Message Binding Version ID string. Fixing of typos, clarification of concepts, and other changes that should not affect content or tool behavior will not change the major or minor version numbers, but will instead be reflected by an updated release date for the document. For such changes the TAXII Message Binding Version ID would not be 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/xml/1"`.) Changes to the schema that do not affect content or processing (e.g., correcting or clarifying documentation in the schema) would be 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 would be made without an accompanying change to the specification. Note that for every major and minor release of the specification there will be 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 STIX

TAXII is designed to support the sharing of structured cyber threat information. The structuring of this 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." [3]

This specification does not provide details about the underlying structures defined in the STIX specification, apart from noting that all cyber threat information transported by TAXII is expressed in "STIX documents". Those interested in learning more about STIX are directed to the STIX web site at https://stix.mitre.org/.

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. [4]

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 elements are denoted by non-namespaced text surrounded by angle brackets (e.g., `<TAXII_DiscoveryRequest>`) while attributes are preceded by an "at" symbol (e.g., `@message-id`).

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 document to define concepts central to definition of TAXII.

TAXII Data Feed - A collection of structured cyber threat information expressible in one or more STIX documents that can be exchanged using TAXII. All TAXII Data Feeds MUST be assigned a name that uniquely identifies them on a given Producer. Individual pieces of cyber threat information within a TAXII Data Feed are labeled with a timestamp and may have other labels at the producer's discretion.

TAXII Message - A discrete block of information that is passed from one entity to another. A TAXII Message represents either a request (e.g., “Can I subscribe to this TAXII Data Feed?”) or a response (e.g., “Yes.”).

TAXII Message Exchange - A defined sequence of request and response TAXII Messages undertaken by two parties to accomplish a specific activity.

TAXII Service - Functionality hosted by some entity that is accessed or invoked through the use of one or more TAXII Message Exchanges.

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

1.2.2 TAXII Functional Units

TAXII functional units represent discrete sets of activities required to support TAXII. Note that this does not mean that separate software would be needed for each functional unit - a single software application could encompass multiple functional units. 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. A TMH passes TAXII Messages to the TTA, which then handles the details required to transmit those messages over the network. The TAXII Back-end interacts with the TMH to turn its content 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. 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-ends 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, the TAXII Back-End is outside of the scope of the TAXII specifications - the TAXII specifications only cover the definition of services and how these services are supported over the network.

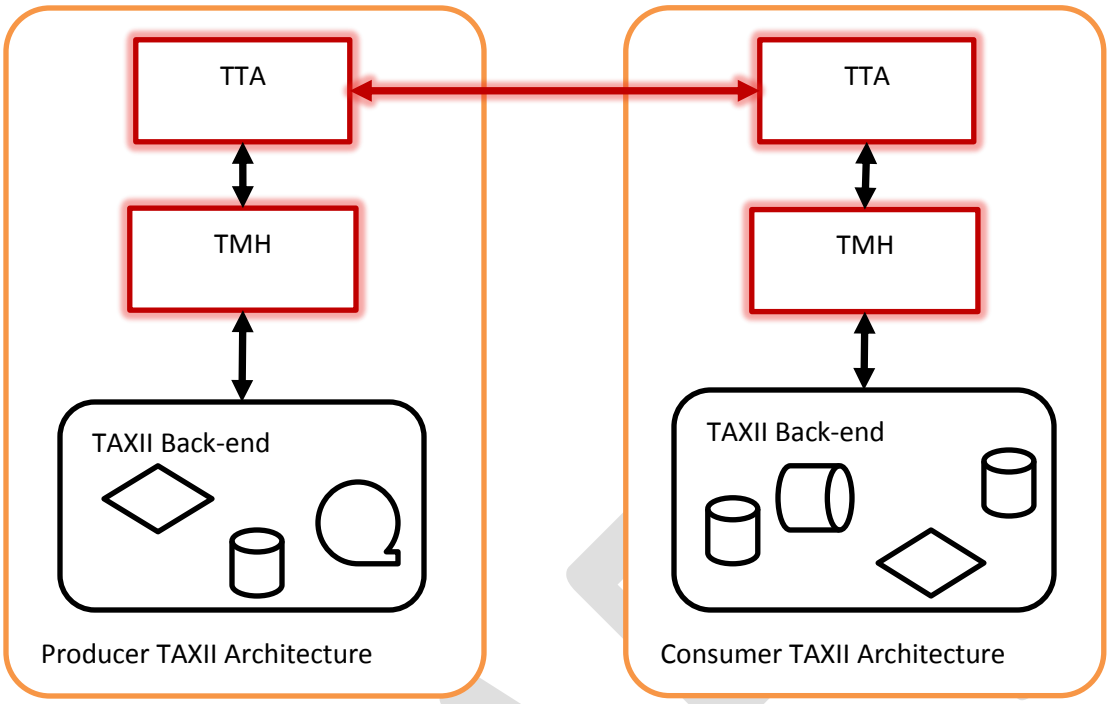

Figure 2: The Interaction of TAXII Functional Units

Figure 2 shows the TAXII functional units 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 packets 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 Implementations 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 the TAXII Back-end.

1.2.3 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.

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

1.2.4 TAXII Network Components

These terms are used to define the components of a TAXII Implementation using a typical client-server model. Note that these should be considered orthogonal to the TAXII Roles previously defined: An entity

might both host a TAXII Server 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 Server - A TAXII Implementation that provides one or more TAXII services. To support this functionality, it is assumed that a TAXII Server is persistently listening for new TAXII network traffic.

TAXII Client - A TAXII Implementation that initiates an exchange with a TAXII Server. 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 server and disconnect from the network when this interaction has concluded.

TAXII Endpoint - A general term used to denote a TAXII Implementation that is a TAXII Server and/or a TAXII Client.

1.2.5 XML Binding Terms

The TAXII Services Specification identifies a number of "fields" for each TAXII Message Type. Likewise, this specification specifies fields as XML structures. The former discusses field in terms of the general concepts they are meant to convey, while the latter represent 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 data 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 unique message identifier.

XML Field - A data field expressed using the XML syntax defined in this specification. XML Fields correspond to either a single XML element or a single XML attribute. For example, all messages have a "`@message-id`" XML Field that contains a unique XML string representing a GUID.

Note that there is not always a one-to-one mapping between a Data Model Field and an XML Field.

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 of these "TAXII Message Elements" 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 parlance, this means all TAXII message elements are "global elements". Moreover, this specification does not define any elements that contain other TAXII Message Elements. As such, within this TAXII Message Binding, TAXII Message Elements do not appear wrapped within other elements.

One side effect of this is that this specification does not define any way to include multiple TAXII Messages within a single "document". This reflects that, in TAXII Message Exchanges, there is no situation where multiple TAXII Messages may be conjoined 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. There is not a strong division between TAXII Header fields and TAXII Body fields within the defined TAXII XML Message Binding structures. 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 can exist as peers in the XML of a TAXII message. For this reason, in defining the XML structure of TAXII messages this document does not treat the header and body fields separately or otherwise discriminate between them.

2.1.3 Strict Ordering of Elements

Elements in XML can be organized in several ways. 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. This does, however, mean that the creation of TAXII Messages using this message binding must comply with this ordering.

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

2.2 Special Field Values

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

2.2.1 Feed Name

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 Producers use the same Feed Name unless those Producers share a Feed Management or Poll Service.

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 to be XML strings, so anything expressible as an XML string will be acceptable in an XML Field that holds a Feed Name. If the Producer's chosen Feed Name is not expressible as an XML string (e.g., it is a binary blob), it will need to be converted to an XML string before it is used in this binding.

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 store both the Feed Name and the associated Producer identity together since the combination of these values should be globally unique.

2.2.2 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. This allows the recipient of Message B to know to which of their requests this is a response.

The TAXII XML Message Binding uses a Globally Unique Identifier (GUID) [5] such as the IETF's UUID [6] for Message ID fields. Specifically, the value of a Message ID field (and, by extension, an In Response To field) consists of 32 case-insensitive hexadecimal values. It may be interspersed with other characters (spaces and dashes being most typical) that MUST be ignored when performing comparisons. No sender should ever send out two messages with the same Message ID values. TAXII implementers may use any means of generating GUIDs for their Message IDs providing those methods have a statistically low chance of generating the same GUID twice over the life of the implementation.

2.2.3 Subscription ID

TAXII Consumers may establish subscriptions to TAXII Data Feeds provided by TAXII Producers. Nominally, the intent of a subscription is twofold: to denote the Consumer's suitability to receive that TAXII Data Feed's content and to request that the Producer periodically push updates from this TAXII Data Feed to the Consumer using specific distribution mechanisms. Consumers that prefer to pull their TAXII Data Feed updates instead of having them pushed can indicate this at the time a subscription is established.

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 value. From then on, both the Consumer and Producer may refer to this subscription in messages using this Subscription ID value.

Producers use any syntax for their Subscription IDs. The only requirement is that two subscriptions to the same TAXII Data Feed by the same Consumer cannot be given the same Subscription ID. Multiple subscriptions may be assigned the same Subscription ID value by a given Producer as long as those

subscriptions differ in the identity of the TAXII Data Feed Consumer, the Feed Name of the TAXII Data Feed, or both.

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

2.2.4 Timestamps

Timestamps are used by multiple fields in TAXII Messages, both to indicate chronological time and as a means of labeling TAXII Data Feed content. All XML Fields that contain timestamps use the XML dateTime data type. Timestamps MAY include fractional seconds. If fractional seconds are not explicitly expressed, treat this as expressing a fractional second of .0. All timestamps SHOULD indicate a time zone in a format that complies with the XML dateTime data type. If a timestamp is not included, it should be assumed that the timestamp is expressed in the TAXII Producer's local time zone.

2.2.5 Sender-defined Values

Some fields allow the TAXII Message sender to create their own field values instead of using values defined in the TAXII specifications. For example, TAXII allows senders to define their own Error Types and supply them in a TAXII Error Message. In all cases, the XML Fields where sender-defined values can appear have a type of XML string. As such, sender-defined values must be expressible using an XML string. In addition, sender-defined values MUST NOT duplicate permissible values for the corresponding field defined in the TAXII specifications as this would have the effect of redefining the meaning of those values.

There are some special cases of sender-defined values that should be noted: TAXII permits senders to identify their own protocol and message bindings for TAXII communication. These can be specified instead of, or sometimes in addition to, using the appropriate TAXII Version ID strings, as described in the TAXII specifications. To simplify discussion of field values in these cases, the following terms are defined:

TAXII Protocol Binding Designator - This is used to indicate either a TAXII Protocol Binding Version ID string as defined in a TAXII Protocol Binding Specification or a sender-defined value that corresponds to a sender-defined TAXII protocol binding. Sender-defined values MUST NOT contains spaces but may otherwise contain any character valid in an XML string.

TAXII Feed Protocol Binding Designator - This consists of all valid TAXII Protocol Binding Designators and also the literal value `POLL`, which is used to designate access to TAXII Data Feed content using a Polling Service.

TAXII Message Binding Designator - This is used to indicate either a TAXII Message Binding Version ID string as defined in a TAXII Message Binding Specification or a sender-defined value that corresponds to a sender-defined TAXII message binding. Sender-defined values MUST NOT contains spaces but may otherwise contain any character valid in an XML string.

2.2.6 STIX Version IDs

Some TAXII Message fields are used to designate the binding and version of STIX used to convey structured cyber threat information. These fields require a Version ID string similar to the Version ID strings defined in the TAXII specifications. STIX Version ID values are not defined in the STIX specification but are instead defined here.

Specifically, an XML binding of STIX content should be expressed using a STIX Version ID string of:

STIX_XML_*version*

where "*version*" is the value of the `@version` attribute of in the root `<schema>` element of the appropriate STIX schema file. This version of the TAXII XML Message Binding only supports expressing STIX using an XML binding.

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 Types' 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.
- Count - 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 if a field may be "required" in the Message Data Model, but be optional in this XML binding if it has a default value. 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 Error Message

Table 1 - TAXII Error Message Fields

XML Name	Data Model Name	Count	Value
<TAXII_ErrorMessage>	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	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive).
@in-response-to	In Response To	0-1	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive). This field value MUST be equal to the @message-id value of a previous message to which this message is responding.
<extended-headers>	Other-Headers	0-1	Child elements of the <extended-header> element represent additional header fields defined by the message sender. They may have any structure as long as its root is an XML element. (I.e., <extended-headers> may not have free text as its immediate content nor may it be given attributes.)
any	Other-Headers	0-n	
@error-type	Error Type	1	A string value, either one of the values provided in Table 2 or a sender-defined value.
<error-detail>	Error Detail	0-1	A string value. This field SHOULD be present if and only if the given @error-type value defines a value for it. Under these circumstances, if present, it MUST contain only the appropriate information as identified in Table 2.
<message>	Message	0-1	A string value, intended to convey a human-readable message.

The @error-type field identifies the type of error expressed in this message. Standard error types are defined in Table 2. In addition, the TAXII Error Message sender may define their own error types. If the recipient does not recognize a sender-defined error type, the error type should be treated like a Failure error type.

The <error-detail> field SHOULD only be present for certain values of the @error-type field, and for those values, if present, MUST only contain specifically formatted information appropriate to

that error. Table 2 identifies the `@error-type` field values which SHOULD have a corresponding `<error-detail>` field and what that `<error-detail>` MUST contain if present. Error Types that are empty in the "`<error-detail>` Value" column SHOULD NOT include an `<error-detail>` field. For sender-defined error types, that sender may also determine whether or not an `<error-detail>` field should be present and what value it should take.

Table 2 - Defined Error Types

Error Type	`@error-type` Value	`<error-detail>` Value
Bad Message	`BAD-MESSAGE`	
Unsupported Service	`UNSUPPORTED-SERVICE`	
Unauthorized	`UNAUTHORIZED`	
Denied	`DENIED`	
Unsupported Protocol	`UNSUPPORTED-PROTOCOL`	A space-separated list of TAXII Protocol Binding Designators indicating supported protocol bindings.
Unsupported Message Binding	`UNSUPPORTED-MESSAGE`	A space-separated list of TAXII Message Binding Designators indicating supported message bindings.
Unsupported Content Binding	`UNSUPPORTED-CONTENT`	A space-separated list of STIX Version ID strings indicating supported STIX versions and bindings.
Not Found	`NOT-FOUND`	
Unrecognized Field Value	`UNRECOGNIZED-VALUE`	The XML Field name of the field with the bad value (without a preceding @ or surrounding <>) followed by an equals (=) followed by a double-quote (") followed by the unrecognized value(s) and then a final double-quotations marks ("). For example, if the problem was a `<send-to>` field with a bad value (`<send-to>hhh</send-to>`) the error detail on the returned error would be: `send-to="hhh"`
Failure	`FAILURE`	
Pending	`PENDING`	A timestamp indicating a time when the request might be repeated and fulfilled.

3.2 TAXII Discovery Request

Table 3 - TAXII Discovery Request Fields

XML Name	Data Model Name	Count	Value
<TAXII_DiscoveryRequest>	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	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive).
@in-response-to	In Response To	0-1	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive). This field value MUST be equal to the @message-id value of a message that was previously received and to which this message is responding.
<extended-headers>	Other-Headers	0-1	Child elements of the <extended-header> element represent additional header fields defined by the message sender. They may have any structure as long as its root is an XML element. (I.e., <extended-headers> may not have free text as its immediate content nor may it be given attributes.)
any	Other-Headers	0-n	

3.3 TAXII Discovery Response

Table 4 - TAXII Discovery Response Fields

XML Name	Data Model Name	Count	Value
<TAXII_DiscoveryResponse>	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	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive).

XML Name	Data Model Name	Count	Value
`@in-response-to`	In Response To	0-1	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive). This field value MUST be equal to the `@message-id` value of a message that was previously received and to which this message is responding.
`<extended-headers>`	Other-Headers	0-1	Child elements of the `<extended-header>` element represent additional header fields defined by the message sender. They may have any structure as long as its root is an XML element. (I.e., `<extended-headers>` may not have free text as its immediate content nor may it be given attributes.)
any	Other-Headers	0-n	
`<service-instance>`	Service Instance	0-n	Contains only the indicated child fields. This element may appear any number of times with each instance corresponding to a single reported TAXII Service.
`@service-type`	Service Type	1	Indicates the reported TAXII Service type using one of the values given in Table 5.
`@service-version`	Services Version	1	A TAXII Services Version ID string indicating the version of the TAXII Services Specification with which the identified TAXII Service complies.
`@available`	Available	0-1	Boolean. `true` = The requester is known to have access to the reported TAXII Service. `false` = The requester is denied access or the requester's access is unknown.
`<protocol-binding>`	Service Protocol Binding	1	A TAXII Protocol Binding Designator indicating the TAXII Protocol Binding which may be used to contact the indicated TAXII Service.
`<message-binding>`	Service Message Binding	1-n	One or more instances of this element may appear, each containing a TAXII Message Binding Designator indicating a TAXII Message Bindings which may be used to contact the indicated TAXII Service.

XML Name	Data Model Name	Count	Value
<content-binding>	Inbox Service Accepted Content	0-n	This field MUST be present if @service-type="INBOX". If present, each instance of this field contains a STIX Version Identifier string indicating a version and binding of STIX the Inbox Service is capable of accepting. This field SHOULD NOT be present for any other values of @service-type.
<service-address>	Service Address	1	A string, representing a network address that can be used to contact the TAXII Service using the TAXII Protocol Binding specified in the <protocol-binding> field.
<message>	Message	0-1	A string value, intended to convey a human-readable message.

The @service-type field identifies the type of service reported in the given <service-instance>. It must be one of the values provided in

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	Count	Value
<TAXII_FeedInformationRequest>	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	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive).

XML Name	Data Model Name	Count	Value
@in-response-to	In Response To	0-1	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive). This field value MUST be equal to the @message-id value of a message that was previously received and to which this message is responding.
<extended-headers>	Other-Headers	0-1	Child elements of the <extended-header> element represent additional header fields defined by the message sender. They may have any structure as long as its root is an XML element. (I.e., <extended-headers> may not have free text as its immediate content nor may it be given attributes.)
any	Other-Headers	0-n	

3.5 TAXII Feed Information Response

Table 7 - TAXII Feed Information Response Fields

XML Name	Data Model Name	Count	Value
<TAXII_FeedInformationResponse>	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	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive).
@in-response-to	In Response To	0-1	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive). This field value MUST be equal to the @message-id value of a message that was previously received and to which this message is responding.
<extended-headers>	Other-Headers	0-1	Child elements of the <extended-header> element represent additional header fields defined by the message sender. They may have any structure as long as its root is an XML element. (I.e., <extended-headers> may not have free text as its immediate content nor may it be given attributes.)
any	Other-Headers	0-n	

XML Name	Data Model Name	Count	Value
<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	A string containing this Discovery Service's unique Feed Name for this TAXII Data Feed.
@available	Available	0-1	Boolean. true = The requester is known to have access to the reported TAXII Data Feed. false = The requester is denied access or the requester's access is unknown.
<description>	Feed Description	1	A string conveying human-readable information about this TAXII Data Feed.
<delivery-method>	Delivery Method	1-n	One or more instances of this element may appear. Each instance contains a TAXII Feed Protocol Binding Designator indicating a TAXII Protocol Binding which may be used to deliver content for this TAXII Data Feed. Note a value of POLL may be included to indicate the presence of a Poll Service that may be used to collect content for this TAXII Data Feed.
<message-binding>	Supported Message Bindings	1-n	One or more instances of this element may appear. Each instance contains a TAXII Message Binding Designator indicating a TAXII Message Bindings which may be used to receive content from this TAXII Data Feed.
<content-binding>	Supported Content	1-n	One or more instances of this element may appear. Each instance contains a STIX Version Identifier string indicating a version of STIX that may be used to express the content of this this TAXII Data Feed.

3.6 TAXII Manage Feed Subscription Request

Table 8 - TAXII Feed Information Request Fields

XML Name	Data Model Name	Count	Value
<TAXII_SubscriptionManagementRequest>	Message Body Type	1	The element name indicates the message body type. Its body MUST consist only of the indicated XML Fields.

XML Name	Data Model Name	Count	Value
`@message-id`	Message ID	1	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive).
`@in-response-to`	In Response To	0-1	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive). This field value MUST be equal to the `@message-id` value of a message that was previously received and to which this message is responding.
`<extended-headers>`	Other-Headers	0-1	Child elements of the `<extended-header>` element represent additional header fields defined by the message sender. They may have any structure as long as its root is an XML element. (I.e., `<extended-headers>` may not have free text as its immediate content nor may it be given attributes.)
any	Other-Headers	0-n	
`<feed-name>`	Feed Name	1	A string containing the Feed Name for the TAXII Data Feed.
`<action>`	Action	1	One of the values indicated in Table 9 indicating the requested management action.
`<subscription-id>`	Subscription ID	0-1	This field MUST be present if `<action>="UNSUBSCRIBE"`, `"PAUSE"`, `"RESUME"`, or `"MODIFY"`. It SHOULD NOT be present for other values of `<action>`. It contains a Subscription ID string that the receiving Producer assigned to a previously established subscription.
`<subscription>`	Subscription Parameters	0-1	This field MUST be present if `<action>="SUBSCRIBE"` or `"MODIFY"`. It SHOULD NOT be present otherwise. It contains only the indicated child fields.
`<delivery-method>`	Delivery Method	1	A TAXII Feed Protocol Binding Designator indicating how TAXII Data Feed content MUST be delivered for this subscription. Note that a value of `POLL` may be used to indicate the Consumer will contact a Poll Service to receive content.

XML Name	Data Model Name	Count	Value
<message-binding>	Response Message Binding	1	A TAXII Message Binding Designator indicating how TAXII Data Feed content MUST be delivered for this subscription.
<content-binding>	Content Binding	1	A STIX Version ID string indicating how TAXII Data Feed content MUST be expressed for this subscription.
<send-to>	Send-To	1	A string, representing the network address that can be used to contact an Inbox Service using the TAXII Protocol Binding specified in the <delivery-method> field. If <delivery-method>="POLL" then the value of this field is ignored and SHOULD be empty.

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	Create a new subscription to a TAXII Data Feed
UNSUBSCRIBE	Delete an existing subscription to a TAXII Data Feed
PAUSE	Suspend sending of updates for the identified subscription
RESUME	Resume sending of updates for the identified subscription
MODIFY	Change the subscription parameters of an existing subscription
STATUS	Request information on all subscriptions from this requester to this TAXII Data Feed.

3.7 TAXII Manage Feed Subscription Response

Table 10 - TAXII Feed Information Response Fields

XML Name	Data Model Name	Count	Value
<TAXII_SubscriptionManagementResponse>	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	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive).

XML Name	Data Model Name	Count	Value
@in-response-to	In Response To	0-1	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive). This field value MUST be equal to the @message-id value of a message that was previously received and to which this message is responding.
<extended-headers>	Other-Headers	0-1	Child elements of the <extended-header> element represent additional header fields defined by the message sender. They may have any structure as long as its root is an XML element. (I.e., <extended-headers> may not have free text as its immediate content nor may it be given attributes.)
any	Other-Headers	0-n	
<feed-name>	Feed Name	1	A string containing the identifier for the TAXII Data Feed.
<message>	Message	0-1	A string value, intended to convey a human-readable message.
<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". It will appear exactly once for all other request actions.
@subscription-id	Subscription ID	1	A Subscription ID string that the Producer assigned to the identified subscription.
<delivery-method>	Delivery Method	1	A TAXII Feed Protocol Binding Designator indicating how TAXII Data Feed content will be delivered for this subscription.
<message-binding>	Response Message Binding	1	A TAXII Message Binding Designator indicating how TAXII Data Feed content will be delivered for this subscription.
<content-binding>	Content Binding	1	A STIX Version ID string indicating how TAXII Data Feed content will be expressed for this subscription.

XML Name	Data Model Name	Count	Value
<send-to>	Send-To	1	A string, representing the network address of the Inbox Service to which TAXII Data Feed content will be sent. If <delivery-method>="POLL" then the value of this field is ignored and SHOULD be empty.

3.8 TAXII Poll Request

Table 11 - TAXII Poll Request Fields

XML Name	Data Model Name	Count	Value
<TAXII_PollRequest>	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	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive).
@in-response-to	In Response To	0-1	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive). This field value MUST be equal to the @message-id value of a message that was previously received and to which this message is responding.
<extended-headers>	Other-Headers	0-1	Child elements of the <extended-header> element represent additional header fields defined by the message sender. They may have any structure as long as its root is an XML element. (I.e., <extended-headers> may not have free text as its immediate content nor may it be given attributes.)
any	Other-Headers	0-n	
<feed-name>	Feed Name	1	A string containing the identifier for the TAXII Data Feed.
<begin-timestamp>	Begin Timestamp	0-1	A DateTime value indicating the lower-bound of the range of the TAXII Data Feed's timestamps from which results should be collected. If absent, indicates the search has no lower bound.

XML Name	Data Model Name	Count	Value
<end-timestamp>	End Timestamp	0-1	A DateTime value indicating the upper-bound of the range of the TAXII Data Feed's timestamps from which results should be collected. If absent, indicates there is no upper bound. If both a <begin-timestamp> and <end-timestamp> value are present, former must express a point in time no later than the latter.
<subscription-id>	Subscription ID	1	A Subscription ID string that the Producer assigned to an existing subscription. This field MUST be present if and only if <content-binding> is not present.
<content-binding>	Content Binding		A STIX Version ID string indicating how TAXII Data Feed content will be expressed in the TAXII Poll Response Message. This field MUST be present if and only if <subscription-id> is not present.

3.9 TAXII Poll Response

Table 12 - TAXII Poll Request Fields

XML Name	Data Model Name	Count	Value
<TAXII_PollResponse>	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	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive).
@in-response-to	In Response To	0-1	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive). This field value MUST be equal to the @message-id value of a message that was previously received and to which this message is responding.
<extended-headers>	Other-Headers	0-1	Child elements of the <extended-

XML Name	Data Model Name	Count	Value
any	Other-Headers	0-n	header> element represent additional header fields defined by the message sender. They may have any structure as long as its root is an XML element. (I.e., <extended-headers> may not have free text as its immediate content nor may it be given attributes.)
<begin-timestamp>	Begin Timestamp	0-1	A DateTime value indicating the lower-bound of the range of the TAXII Data Feed's timestamps from which results were collected. If absent, indicates the range included the lowest timestamp value in the TAXII Data Feed.
<end-timestamp>	End Timestamp	1	A DateTime value indicating the upper-bound of the range of the TAXII Data Feed's timestamps from which results were collected.
<subscription-id>	Subscription ID	0-1	A Subscription ID string that the Producer assigned to the subscription corresponding to the poll request, as provided in the <subscription-id> field of the TAXII Poll Request. This field is not present if the poll response is not servicing an existing subscription.
<message>	Message	0-1	A string value, intended to convey a human-readable message.
<content-binding>	Content Binding	1	A STIX Version ID string indicating how TAXII Data Feed content is expressed in the <stix:STIX> field.
<stix:STIX>	STIX Content	0-n	STIX content expressed using the STIX binding and version identified in the <content-binding> field.

3.10 TAXII STIX Message

Table 13 - TAXII STIX Message Fields

XML Name	Data Model Name	Count	Value
<TAXII_STIXMessage>	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	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive).

XML Name	Data Model Name	Count	Value
`@in-response-to`	In Response To	0-1	A globally unique identifier consisting of 32 hexadecimal digits (case insensitive). This field value MUST be equal to the `@message-id` value of a message that was previously received and to which this message is responding.
`<extended-headers>`	Other-Headers	0-1	Child elements of the `<extended-header>` element represent additional header fields defined by the message sender. They may have any structure as long as its root is an XML element. (I.e., `<extended-headers>` may not have free text as its immediate content nor may it be given attributes.)
any	Other-Headers	0-n	
`<subscription-id>`	Subscription ID	0-1	A Subscription ID string that the Producer assigned to the subscription served by this message. This field is only present if this message services an existing subscription.
`<message>`	Message	0-1	A string value, intended to convey a human-readable message.
`<content-binding>`	Content Binding	1	A STIX Version ID string indicating how TAXII Data Feed content is expressed in the `<stix:STIX>` field.
`<stix:STIX>`	STIX Content	1-n	STIX content expressed using the STIX binding and version identified in the `<content-binding>` field.

4 Message Handling

The functional unit of the TAXII Architecture responsible for processing TAXII messages is the TAXII Message Handler (TMH). While the actual processing of most individual message fields would be handled by functionality associated with the TAXII Back-end, the TMH functional unit is responsible for the following actions:

- Assignment of Message ID field values - The TMH MUST use a GUID generator to assign a locally unique Message ID to each outbound message it sends.
- Aligning Message ID field values to In Response To field values - There are two parts to this responsibility. First, if the TMH is responding to an incoming request, when it formats a response it MUST ensure that this response includes an In Response To field with a value equal

to the request's Message ID field. Secondly, when sending a request, the TMH SHOULD record the outgoing Message ID field value so that it can recognize the response to that request.

- Recognition of certain error conditions related to TAXII Messages. These include:
  - Messages that cannot be parsed due to formatting errors or the use of unknown message bindings
  - Improper message order (such as receiving a response without having sent a request)

The objective of this is to allow TAXII Back-end implementations to be agnostic as to Message ID tracking and also to avoid exposing the TAXII Back-end to nonsensical messages.

It should be emphasized that the mapping of software applications to functional units is neither defined nor constrained by the TAXII specifications. As such, the TMH functionality could exist in the same piece of software that supports TTA and TAXII Back-end functionality, or the TMH functionality could be split across multiple pieces of software. The critical point is that the functionality must be implemented - how that implementation manifests in software is beyond the scope of TAXII.

5 The TAXII XML Message Binding Schema

This specification is accompanied by an XML schema that encapsulates most of the requirements provided in this specification. It should be emphasized that this schema is informative rather than normative. When the specification and schema conflict, the specification should be taken as correct.

The TAXII XML Message Binding Schema defines global XML types and XML elements associated with all TAXII Message Body Types. In addition, it defines a global abstract element of TAXII_Message, which is the parent of a substitution group populated by all TAXII Message Elements. Implementers who wish to do so can utilize this element to represent "any TAXII Message" in schemas and tools.

6 Conclusion

This specification defines a standard XML format for TAXII Messages allowing automated processing of exchanges in support of the defined TAXII Services. The sharing of cyber threat information is an important component in the defenses of modern enterprises. Rapid sharing of information about attacks significantly increases an adversary's costs to operate by making reuse of techniques and tools less likely to succeed. TAXII can serve as a technical foundation for such a sharing environment, allowing many steps that are currently manual to be handled in an automated fashion. It is hoped that TAXII will provide the means not only to simplify and accelerate the activities of the existing cyber threat information sharing communities, but to expand this community so that new parties will be able to contribute to the total understanding of the threats facing our cyber resources and benefit from the knowledge provided by others.

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

[3] The MITRE Corp., "STIX - Structured Threat Information Expression," 1 October 2012. [Online]. Available: https://stix.mitre.org/. [Accessed 19 October 2012].

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

[5] Wikipedia, "Globally unique identifier," Wikipedia, 27 October 2012. [Online]. Available: http://en.wikipedia.org/wiki/Globally_unique_identifier. [Accessed 5 November 2012].

[6] P. Leach, M. Mealling and R. Salz, "RCF 4122 - A Universally Unique IDentifier (UUID) URN Namespace," The Internet Engineering Task Force, 2005.