THE MITRE CORPORATION

The TAXII Services 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 TAXII's Capabilities, Services, Messages, and Message Exchanges as well as how TAXII can support popular threat information sharing models.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00001

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)

©2012 The MITRE Corporation. All Rights Reserved.

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.

DRAFT

Copyright © 2012, The MITRE Corporation. All rights reserved.

Table of Contents

Trademark Information 1
Feedback 1
1 Introduction 4
1.1 TAXII Specifications 4
1.1.1 The TAXII Services Specification 5
1.1.2 STIX 6
1.1.3 Document Conventions 6
1.2 Terms and Definition 6
1.2.1 TAXII Concepts 7
1.2.2 TAXII Functional Units 7
1.2.3 TAXII Roles 9
1.2.4 TAXII Network Components 9
2 TAXII Capabilities 9
2.1 Push Messaging 9
2.2 Pull Messaging 10
2.3 Discovery 10
3 TAXII Services 10
3.1 Discovery Service 11
3.2 Feed Management Service 11
3.3 Inbox Service 11
3.4 Poll Service 11
4 TAXII Messages 12
4.1 TAXII Header 13
4.2 TAXII Message Bodies 13
4.2.1 TAXII Error Message 14
4.2.2 TAXII Discovery Request 15
4.2.3 TAXII Discovery Response 15
4.2.4 TAXII Feed Information Request 16
4.2.5 TAXII Feed Information Response 16
4.2.6 TAXII Manage Feed Subscription Request 17

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00003

DRAFT

4.2.7 TAXII Manage Feed Subscription Response 20
4.2.8 TAXII Poll Request 20
4.2.9 TAXII Poll Response 21
4.2.10 TAXII STIX Message 22
5 TAXII Message Exchanges 22
5.1.1 Data Push Exchange 23
5.1.2 Discovery Exchange 23
5.1.3 Feed Information Exchange 24
5.1.4 Subscription Management Exchange 25
5.1.5 Feed Poll Exchange 26
6 TAXII's Use of Network Protocols 27
6.1 Reliability 28
6.2 Protection and Authentication 28
6.3 TAXII Protocol Bindings 28
7 Using TAXII 29
7.1 Source/Subscriber 29
7.2 Peer-to-Peer 32
7.3 Hub and Spoke 34
8 Conclusion 36
9 Bibliography 36
10 Appendix A - Roadmap 37

DRAFT

Copyright © 2012, The MITRE Corporation. All rights reserved.

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].

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, the TAXII Services Specification, is highlighted.

Copyright © 2012, The MITRE Corporation. All rights reserved.

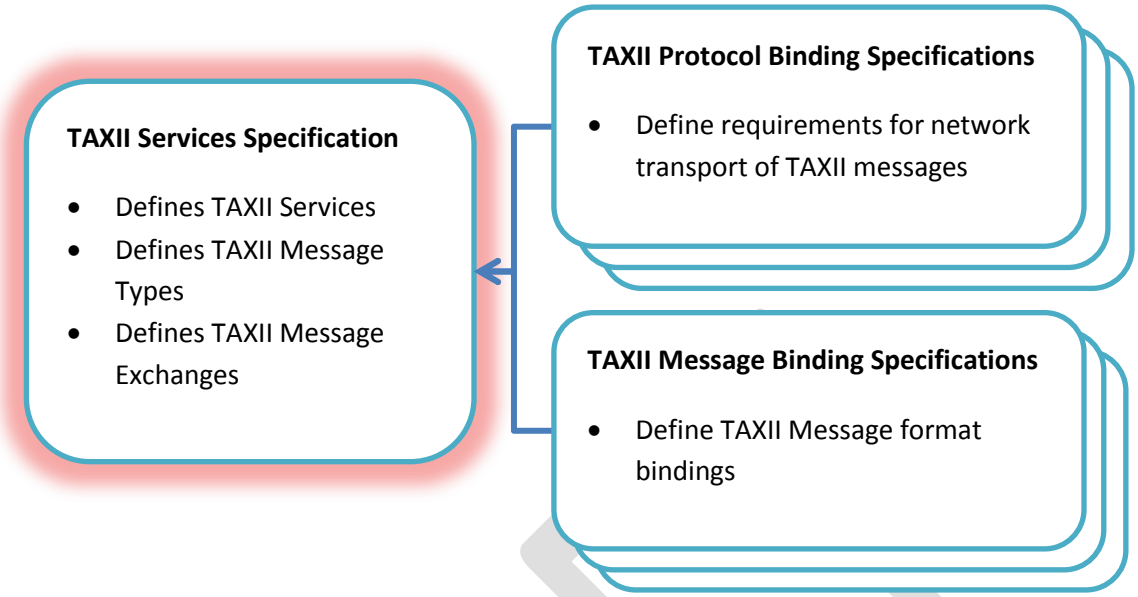


Figure 1 - TAXII Specification Hierarchy

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 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 a Protocol Binding Specification. 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 a Message Binding Specification.

Copyright © 2012, The MITRE Corporation. All rights reserved.

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 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 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 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 Services 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 Services Version ID would not be updated.

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." [2]

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". STIX content is a "black-box" as far as TAXII is concerned - none of the behaviors described in this specification require inspection of any information stored within STIX. 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. [3]

1.2 Terms and Definition

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

Copyright © 2012, The MITRE Corporation. All rights reserved.

1.2.1 TAXII Concepts

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

Cyber Threat Information - For the purposes of TAXII, Cyber Threat Information is any information representable as STIX. This includes, but is not limited to, Observables, Indicators, Incidents, TTPs (Tactics, Techniques, and Procedures), Exploit Targets, Campaigns, Threat Actors, and Courses of Action. For more information on each of the listed concepts, please refer to STIX [2].

TAXII Data Feed - A collection of structured cyber threat information expressible in one or more STIX documents that can be exchanged using TAXII. Each TAXII Data Feed MUST be assigned a name that uniquely identifies it among feeds from 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. Note that TAXII is agnostic as to whether TAXII Data Feed timestamps map to any timestamps in the STIX structures that TAXII Messages encapsulate.

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 TAXII Messages undertaken by two parties.

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 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. 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 its content into TAXII messages, and to perform activities based on the TAXII messages that the TMH receives.

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00008

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-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, the TAXII Back-End is outside of the scope of the TAXII specifications.

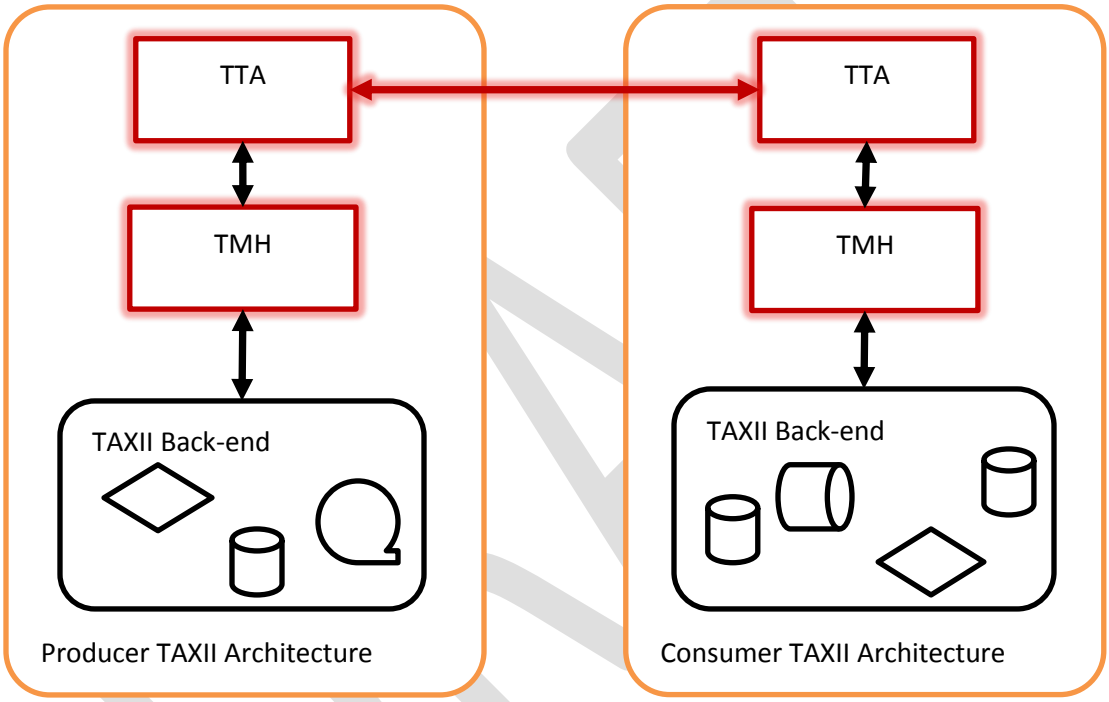


Figure 2: The Interaction of TAXII Functional Units

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.

Copyright © 2012, The MITRE Corporation. All rights reserved.

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 may not map directly to the TAXII Roles previously defined: For example, 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.

2 TAXII Capabilities

TAXII exists to provide specific capabilities to those interested in sharing structured cyber threat information. TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilities that this 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 bi-lateral relationship between the Producer and Consumer, where the Consumer has requested to receive periodic content updates from the Producer. It could also 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. An example of the former is a Consumer who subscribed to a Producer's mailing list, while an example of the latter is a Consumer that was acting as a repository of published information and wished to allow anyone to submit data.

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00010

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 this data without the need to accept 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 supports a specific version of pull messaging. Specifically, it does not support arbitrary querying based on the underlying cyber threat data. Instead, this version of TAXII limits Consumers to making requests against the Producer's organization of the data rather than against the data itself. All Producer-provided data that can be pulled must be organized into (potentially overlapping) groups called "TAXII Data Feeds". Individual pieces of information within a given TAXII Data Feed are labeled using timestamps. The Producer has full discretion as to how their content maps into TAXII Data Feeds and as to the exact meaning of the timestamp. The pull messaging capability in 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 capabilities to discover the specific TAXII Services a TAXII Server (or group of TAXII Servers) offers, as well as the specific bindings these services support. This does not remove the need for human involvement in the establishment of sharing agreements - agreement negotiation is outside the scope of TAXII. It 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 implement some, all, or even none of the defined TAXII Services. (One can still make use of some TAXII capabilities without ever hosting any of the described TAXII Services.)

TAXII defines the following services:

- Discovery Service – Used to receive and respond to messages that request information about offered services.
- Feed Management Service – Used to receive and respond to messages intended for the management of TAXII Data Feed subscriptions.
- Inbox Service – Used to receive cyber threat information via Producer-initiated exchanges at intervals dictated by the Producer.
- Poll Service - Used to receive and respond to Consumer-initiated messages requesting cyber threat information from a TAXII Data Feed.

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00011

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. For a given request to the Discovery Service, the service returns a list of TAXII services and how these services may be invoked. Note that a single Discovery Service might report on TAXII Services hosted on multiple endpoints or even across multiple organizations - the owners of the discovery service can define its scope as they wish. A Discovery Service may use a variety of factors to determine which services to disclose to the requester, including but not limited to the identity of the TAXII Client.

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 modify existing subscriptions to TAXII Data Feeds. The Feed Management Service facilitates the exchange of messages that manage 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 sent to a Consumer's Inbox Service in Producer-initiated exchanges or in direct response to Consumer requests to the Poll Service.

A Feed Management Service implementation MUST support the Subscription Management Exchange.

A Feed Management Service implementation MAY support 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. 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 the Producer, content based on other pre-arrangements, or unsolicited data.

An Inbox Service implementation MUST support the Data Push Exchange.

3.4 Poll Service

The Poll Service is provided by a Producer to allow Consumer-initiated pulls from a TAXII Data Feed. 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 Data Poll Exchange.

Copyright © 2012, The MITRE Corporation. All rights reserved.

4 TAXII Messages

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

This section is limited to a description of the data models representing TAXII messages. It does not prescribe any particular binding for this data model - such details are provided by the TAXII Message Binding Specifications. In other words, 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 will not always be a one-to-one mapping 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 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 structures to be elided during communications. It is important to keep in mind that this section describes the conceptual fields in the data model; the actual bindings will follow those concepts, but may include structural differences to account for limitations or capabilities of the particular binding. Implementers will 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. 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 bindings, default values may define that allow a required field to be absent in the actual exchanged content, but the fact that the default value is (implicitly) conveyed would fulfill the requirement for the field.
- Multiple? - Whether field is expected to identify a single value or whether it can indicate multiple values.
- Description - A description of the information the field is intended to convey 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 the TAXII Message Binding Specification for each type of message binding. 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

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00013

its parent field. A sub-field might not allow multiple values, but the sub-field would still be able to appear and hold a (single) value in multiple instances of its parent field. Note that discussions of TAXII Messages make frequent mention of authenticated identities, encryption, and integrity checks, but TAXII Messages themselves do not contain any fields for these purposes. Instead, TAXII Messages rely on protocol bindings, as defined in the TAXII Protocol Binding Specifications, to provide these protections.

4.1 TAXII Header

This section defines the data model of the header fields of a TAXII Message. Each Message Binding Specification will define the requirements for representing TAXII Headers in that format.

Table 1 - TAXII Header Fields

Name	Required?	Multiple?	Description
Message ID	Yes	No	A globally unique value identifying this message. Message IDs should never be reused.
Message Body Type	Yes	No	The identifier of the type of the TAXII Message. Only identifiers for defined TAXII messages are allowed in this field. (I.e., Implementers may not define their own TAXII Message Body Types.)
In Response To	No	No	Contains the Message ID of the message to which this is a response, if applicable.
Other-Headers	No	Yes	Anyone may define their own additional header fields. Other-Header fields that are not recognized by a recipient MUST be ignored. Other-headers MUST be expressible as name-value pairs, although there is no restriction on what is permissible as either a name or a value.

4.2 TAXII Message Bodies

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

- TAXII Error 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 STIX Message

Copyright © 2012, The MITRE Corporation. All rights reserved.

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

4.2.1 TAXII Error Message

A TAXII Error Message is used to indicate an error condition. They are always sent from a TAXII Server to a TAXII Client in response to a TAXII Message. A TAXII Error Message is used to indicate a failure to perform some requested action. This may be because the request itself was invalid or that the recipient was unwilling or unable to honor the request.

Table 2 - TAXII Error Types

Error Type	Description
Bad Message	The message sent could not be interpreted by the TAXII Server. This may be because it was malformed, or may be because it represents a version of TAXII the TAXII Server does not support or recognize.
Unsupported Service	The TAXII Server does not support the service that would process the request. For example, requesting a TAXII Data Feed subscription from a TAXII Server that does not support TAXII Data Feed subscriptions.
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.
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 Server might send a DENIED message.
Unsupported Protocol	The TAXII Client's requested protocol binding for TAXII Data Feed content deliver is not supported by the TAXII Server. The Error Detail field SHOULD contain a list of acceptable protocol bindings.
Unsupported Message Binding	The TAXII Client's requested message binding for TAXII Data Feed content delivery is not supported by the TAXII Server. The Error Detail field SHOULD contain a list of acceptable message bindings.
Unsupported Content Binding	The TAXII Client's requested protocol binding for TAXII Data Feed content delivery is not supported by the TAXII Server. The Error Detail field SHOULD contain a list of acceptable content bindings.
Not Found	The request named some target (e.g., a TAXII Data Feed name) but that name does not exist on the TAXII Server.
Unrecognized Field Value	Indicates that processing could not complete because a field value could not be parsed. Generally, this occurs when a vendor supplies a field value to indicate some proprietary binding or functionality and the TAXII Server does not recognize that value's meaning. The Error Detail field SHOULD identify the problematic field and value.
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 Error Messages if a TAXII Server does not wish to disclose details for the failure of a request.

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00015

Error Type	Description
Pending	The request cannot be completed immediately but is being processed. The Error Detail fields SHOULD contain a timestamp indicating when the sender should retry their request. The requested action will not occur until the request is repeated.

Table 3 - TAXII Error Message Fields

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

As noted above, TAXII Servers SHOULD provide as much detail about the cause of the error as possible in their TAXII Error Messages. Implementers MAY define additional error types. If the recipient of this error does not recognize the error type, it SHOULD be treated as a FAILURE error. The individual TAXII Message Binding Specifications indicate how vendors may indicate the use of a proprietary error type using that specification's binding.

4.2.2 TAXII Discovery Request

This message is sent to a Discovery Service to request information about provided TAXII services, how those services may be accessed, and what protocols and message bindings are supported. The body of this message is empty.

4.2.3 TAXII Discovery Response

This message is sent from a Discovery Service in response to a TAXII Discovery Request.

Table 4 - TAXII Discovery Response Message Fields

Name	Required?	Multiple?	Description
Service Instance	Yes	Yes	This field may appear any number of times (including 0), each time identifying a different Service Type, Service Protocol Binding, and/or Service Message Binding. This field has several sub-fields.

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00016

Name	Required?	Multiple?	Description
Service Type	Yes	No	This field identifies a TAXII Service type.
Services Version	Yes	No	Identify the version of the TAXII Services Specification this Service uses. This must be a TAXII Services Version ID string as defined in a TAXII Services Specification.
Service Protocol Binding	Yes	No	Identify a protocol binding supported by this Service. Each TAXII Protocol Binding Specification defines a TAXII Protocol Binding Version ID that would be used in this field to indicate the specification's protocol. This may be an identifier for a vendor-defined protocol.
Service Message Binding	Yes	Yes	Identify message bindings supported by this Service. Each TAXII Message Binding Specification defines a TAXII Message Binding Version ID that would be used in this field to indicate the specification's message binding. This may include identifiers for vendor-defined protocols.
Inbox Service Accepted Content	If Service is an Inbox Service	Yes	This field MUST be present if this record is describing an Inbox Service and is ignored for all other Service Type values. It identifies the versions and bindings of content that this Inbox Service can receive. This should be expressed using the appropriate STIX Release Version ID(s).
Service Address	Yes	No	Identify an address by which this Service can be reached. It should use a format appropriate to the identified Service Protocol Binding.
Available	No	No	True if the identity (authenticated or otherwise) of the requester is allowed to access the given Service. False if the identity is denied access or if the identity's access rights are currently unknown.
Message	No	No	A message regarding the indicated Service Instance. This message is not expected to be machine readable but is instead some message to a human operator.

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

4.2.4 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.

4.2.5 TAXII Feed Information Response

This message (or a TAXII Error message) is sent in response to a TAXII Feed Information Request. Note that the Producer is under no obligation to list all feeds and may elide any and all feeds from this response for any reason. For example, the Producer likely would wish to exclude feeds created for a

Copyright © 2012, The MITRE Corporation. All rights reserved.

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 record may appear any number of times (including 0), each time identifying a different Feed Name. It has several sub-fields.
Feed Name	Yes	No	A string by which the TAXII Data Feed may be identified. Each TAXII Data Feed managed by a single Feed Management Service MUST have a unique Feed Name.
Feed Description	Yes	No	A prose description of the purpose of the TAXII Data Feed. This section may also 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.)
Delivery Method	Yes	Yes	The service may indicate the protocols that may be used to receive updates via this subscription. Each TAXII Protocol Binding Specification defines a TAXII Protocol Binding Version ID that would be used in this field to indicate the specification's protocol. This may include identifiers for vendor-defined protocols. The Producer may supply a POLL value to indicate that feed content may be requested using a Poll Service.
Supported Message Bindings	Yes	Yes	The service may indicate the message bindings that may be used to receive updates via this subscription. Each TAXII Message Binding Specification defines a TAXII Message Binding Version ID that would be used in this field to indicate the specification's message binding. This may include identifiers for vendor-defined bindings.
Supported Content	Yes	Yes	The service may indicate the content bindings and versions in which TAXII Data Feed content is expressed. This should be expressed using the appropriate STIX Release Version ID(s).
Available	No	No	True if the identity (authenticated or otherwise) of the requester is allowed to access the given service. False if the identity is denied access or if the identity's access rights are currently unknown.

4.2.6 TAXII Manage Feed Subscription Request

This message is used to manage (e.g., create or remove) a subscription. The Feed Management Service will respond either with a Manage Feed Successful Response or a TAXII Error Message.

Copyright © 2012, The MITRE Corporation. All rights reserved.

Table 6 - TAXII Manage Feed Subscription Request Fields

Name	Required?	Multiple?	Description
Feed Name	Yes	No	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	The action to take. Must be one of the following: o SUBSCRIBE - Request to receive TAXII Data Feed updates in the future. o UNSUBSCRIBE - Request to cease receiving updates for the named TAXII Data Feed. o PAUSE - Suspend receipt of updates without unsubscribing. o RESUME - Resume sending of a paused subscription. o MODIFY - Change an existing subscription. o STATUS - Request information on all subscriptions the Consumer has established for the named TAXII Data Feed. No subscription state is changed in response to this action.
Subscription ID	Per Action	No	If for any management action other than SUBSCRIBE or STATUS, this field MUST be present. This field is ignored if present in a SUBSCRIBE or STATUS action message. This field contains the ID of a previously created subscription.
Subscription Parameters	Per Action	No	This field MUST be present for SUBSCRIBE and MODIFY actions and is ignored for all other actions. This field contains multiple sub-fields. For a SUBSCRIBE action, it specifies how the Consumer wishes TAXII Data Feed content to be delivered. For a MODIFY action, the existing subscription identified by the Subscription ID field is modified to use the delivery methods defined in these fields.
Delivery Method	Yes	No	The method by which the Consumer wishes updates for this TAXII Data Feed to be delivered. Each TAXII Protocol Binding Specification defines a TAXII Protocol Binding Version ID that would be used in this field to indicate the specification's protocol. This may include identifiers for vendor-defined protocols. Alternately, the Consumer may supply a POLL value to indicate that it will query the Poll Service to retrieve TAXII Data Feed messages.
Send-To	Yes	No	The address to send TAXII Data Feed content. This must be appropriate for the indicated Delivery Method. The appropriate value of this field corresponding to a POLL Delivery Method is defined in the appropriate TAXII Message Binding Specification.

Copyright © 2012, The MITRE Corporation. All rights reserved.

Name	Required?	Multiple?	Description
Response Message Binding	Yes	No	The message binding by which the Consumer wishes to receive updates for this TAXII Data Feed. Each TAXII Message Binding Specification defines a TAXII Message Binding Version ID that would be used in this field to indicate the specification's message binding. This may include identifiers for vendor-defined bindings.
Content Binding	Yes	No	The version and binding of the content the Consumer wishes to receive for this TAXII Data Feed. This should be expressed using the appropriate STIX Release Version ID(s).

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 Error Message (nominally 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 Error Message (nominally NOT FOUND) without changing existing subscriptions.
3. Attempts to unsubscribe (UNSUBSCRIBE action) where the Subscription ID does not correspond to any existing subscription on the named TAXII Data Feed by the identified Consumer SHOULD result in a Manage Feed Successful Response without changing existing subscriptions.
4. Any action other than SUBSCRIBE, UNSUBSCRIBE, or STATUS where the Subscription ID does not correspond to any existing subscription on the named TAXII Data Feed by the identified Consumer SHOULD result in an appropriate TAXII Error Message (nominally NOT FOUND) without changing existing subscriptions.
5. Attempts to create a new subscription (SUBSCRIBE action) or to modify an existing subscription (MODIFY action) where the requested protection, protocol binding, message binding, or content binding of the subscription to be created is not supported SHOULD result in an appropriate TAXII Error Message (nominally UNSUPPORTED PROTOCOL, PROTECTION UNSUPPORTED, UNSUPPORTED MESSAGE BINDING, or UNSUPPORTED CONTENT BINDING respectively) without changing existing subscriptions.
6. 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, Protocol Binding, Send-To, Response Message Binding, and Content Binding values) SHOULD result in a Manage Feed Successful 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.

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00020

4.2.7 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. For requested actions other than STATUS, a single Subscription Instance is returned. A request for a STATUS action can return any number of Subscription Instances, from 0 (indicating the Consumer has no existing subscriptions for the named TAXII Data Feed) to many (indicating multiple existing subscriptions for the named TAXII Data Feed).

Table 7 - TAXII Manage Feed Subscription Response Fields

Name	Required?	Multiple?	Description
Feed Name	Yes	No	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	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.
Subscription Instance	Per Action being responded to	Yes	This field will appear 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. It identifies the parameters of the managed subscription and also provides a Subscription ID that may be used in subsequent attempts to manage this subscription
Delivery Method	Yes	No	The protocol by which the Consumer receives TAXII Data Feed content for this subscription.
Send-To	Yes	No	The address to which TAXII Data Feed content is sent for this subscription.
Response Message Binding	Yes	No	The message binding by which the Consumer receives TAXII Data Feed content for this subscription.
Content Binding	Yes	No	The version and binding of the content that is sent to the Consumer for this subscription.
Subscription ID	Yes	No	An identifier that can be used to indicate the given subscription in subsequent exchanges.

4.2.8 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, but whether or not the Consumer must already be subscribed to that TAXII Data Feed is left to the Producer. If the TAXII Data Feed content should only be disseminated to authorized parties, it may make sense to require a pre-existing subscription. This allows the Poll Service to respond quickly since the authorized identity of the Consumer has already been approved for the TAXII Data Feed content. If this is the case, a request by some Consumer who had not previously been approved for a given subscription should result in a DENIED TAXII Error Message. Alternately, Poll Service implementers may allow requests without first requiring the Consumer to have established a subscription. This might make sense

Copyright © 2012, The MITRE Corporation. All rights reserved.

if the Poll Service supports public feeds as the Producer may not wish to track subscriptions from a large body of anonymous users.

Table 8 - TAXII Poll Request Fields

Name	Required?	Multiple?	Description
Feed Name	Yes	No	The name of the TAXII Data Feed that is being polled. Each TAXII Data Feed managed by a singly Poll Service MUST have a unique Feed Name.
Begin Timestamp	No	No	A timestamp indicating the beginning of the range of TAXII Data Feed content the requester wishes to receive. The lack of a timestamp should be interpreted as meaning "The range of considered Data Feed content has no lower bound".
End Timestamp	No	No	A timestamp indicating the end of the range of TAXII Data Feed content the requester wishes to receive. The lack of a timestamp should be interpreted as meaning "The range of considered TAXII Data Feed content has no upper bound".
Subscription ID	No	No	Identifies the existing subscription the Consumer wishes to poll. If the Poll Service does not support subscriptions, they may ignore this field. If the Poll Service requires established subscriptions for polling and this field is not present, the Poll Service SHOULD respond with a DENIED TAXII Error Message
Content Binding	Yes, if no Subscription ID	No	This field should only be present if the Consumer did not include a Subscription ID field. This field indicates the version and binding of the content in the Poll Service's response.

4.2.9 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 subscriptions 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 will necessarily be 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, albeit with an empty End Timestamp 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.

Copyright © 2012, The MITRE Corporation. All rights reserved.

Table 9 - TAXII Poll Response Fields

Name	Required?	Multiple?	Description
Begin Timestamp	No	No	A timestamp indicating the beginning of the range from which TAXII Data Feed content was collected. If this field is absent, this indicates that the range from which TAXII Data Feed is considered has no lower bound.
End Timestamp	Yes	No	A timestamp indicating the end of the range of TAXII Data Feed content from which the returned content was collected. If the End Timestamp field in the Poll Request is empty, the range from which content is collected should have no upper bound.
Subscription ID	No	No	If this content is being provided as part of an established subscription to a TAXII Data Feed, this field contains the Subscription ID for that subscription.
Message	No	No	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.
Content Binding	Yes	No	The version and binding of the contained content. This should be expressed using the appropriate STIX Release Version ID(s).
STIX Content	No	Yes	STIX document(s).

4.2.10 TAXII STIX Message

All threat information is exchanged using STIX messages. This includes results of queries and posts sent due to TAXII Data Feed subscriptions, as well as unsolicited submissions.

Table 10 - TAXII STIX Message Fields

Name	Required?	Multiple?	Description
Message	No	No	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.
Subscription ID	No	No	If this content is being provided as part of an established subscription to a TAXII Data Feed, this field contains the Subscription ID for that subscription.
Content Binding	Yes	No	The version and binding of the contained content. This should be expressed using the appropriate STIX Release Version ID(s).
STIX Content	Yes	Yes	STIX document(s).

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

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00023

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

5.1.1 Data Push Exchange

In this exchange, a STIX message is transmitted from a TAXII Client to a listening Inbox Server. The STIX 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 Server MAY be capable of filtering messages based on the authenticated identity of the sender. Messages sent in this exchange should not have an In Response To field in their Header.

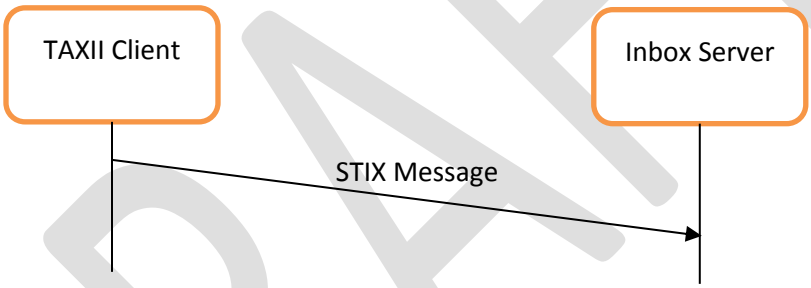


Figure 3 - Data Push Exchange

In this exchange, the TAXII Client sends a STIX Message to the Inbox Server. The Inbox Server may drop the message or pass the STIX Message, along with any authenticated identity information, on to its TAXII Back-end. The TAXII Client receives no response from the Inbox Server and will not know if the Message has been accepted or dropped by the Inbox Server, although the message reliability provided by the underlying network protocols will be able to confirm that the message was successfully delivered to the TTA portion of the Inbox Server. The Inbox Server will not send a TAXII Error Message if there is a problem with the STIX Message.

5.1.2 Discovery Exchange

In this exchange, a TAXII Client requests information about the TAXII Services offered by a Producer. The Producer's Discovery Server responds with a list of services. Note that just because a requester is informed of the existence of a service does not mean that the requester will have immediate access to the service (e.g. because a service might require some out-of-band transaction such as payment or acceptance of terms of use prior to use).

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00024

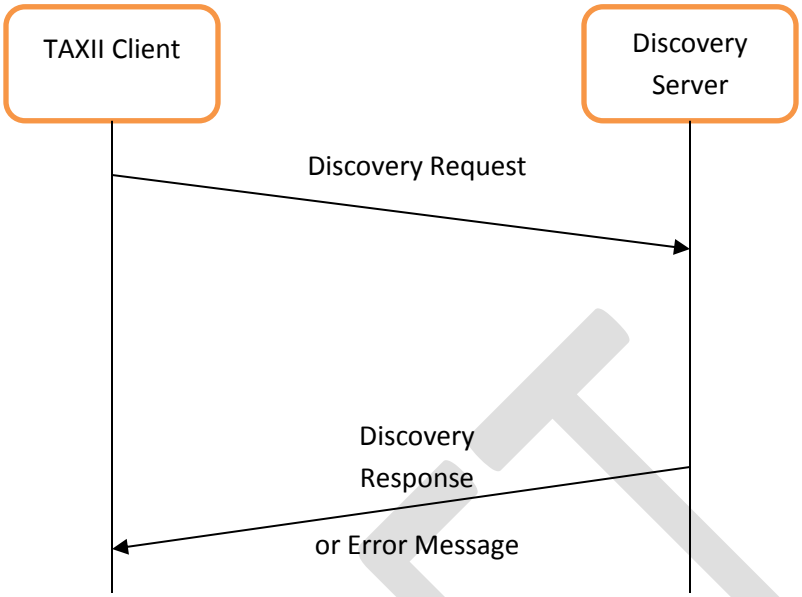


Figure 4 - Discovery Exchange

In this exchange, the TAXII Client sends a Discovery Request to the Discovery Server. When the Discovery Server receives the Discovery Request Message it may return a TAXII Error Message or pass the relevant information to its TAXII Back-end. Relevant information would include the authenticated identity, if provided. The TAXII Back-end would use this information, along with its own access control policy, to create a list of services to be returned. This would be packaged into a Discovery Response which would be sent back to the TAXII Client. The TAXII Client receives this message and passes the service information to its own TAXII Back-end for processing.

5.1.3 Feed Information Exchange

In this exchange, a TAXII Client requests information about the feeds available on a Feed Server. The Feed Server then responds with a list of available feeds. The Feed Server's response is dictated by its TAXII Back-end and may consider appropriate access control decisions in composing this response.

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00025

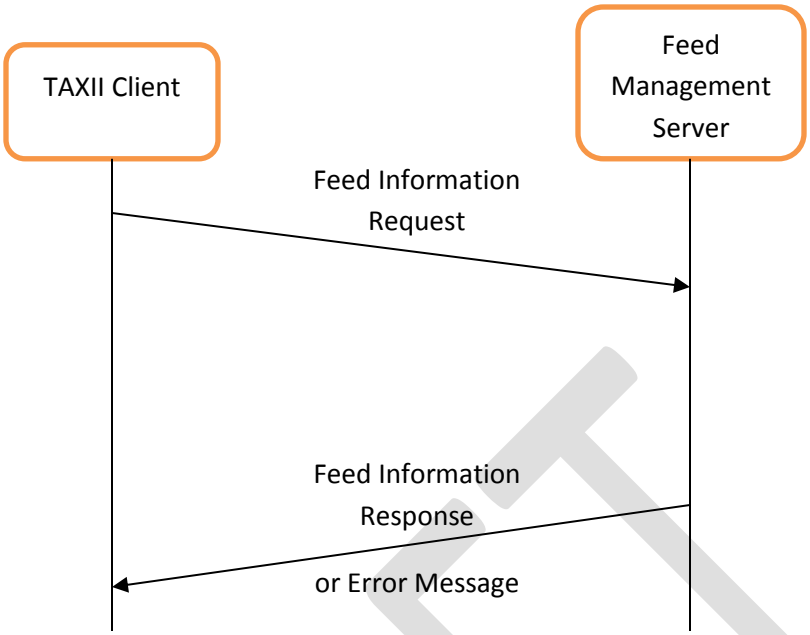


Figure 5 - Feed Information Exchange

In this exchange, the TAXII Client sends a Feed Information Request to the Feed Server. When the Feed Server receives the Feed Information Request Message it may return a TAXII Error Message or pass the relevant information to its TAXII Back-end. Relevant information would include the authenticated identity, if any. The TAXII Back-end would use this information, along with its own access control policy, to create a list of feeds to be returned. This list would be packaged into a Feed Information Response which would be 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.

5.1.4 Subscription Management Exchange

In this exchange, a client attempts to establish, delete, pause, resume, or modify a subscription to a named TAXII Data Feed by sending a subscription management request to a Feed Server. The Feed Server passes the request to its TAXII Back-end, which determines a response. This response is then returned to the TAXII Client.

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00026

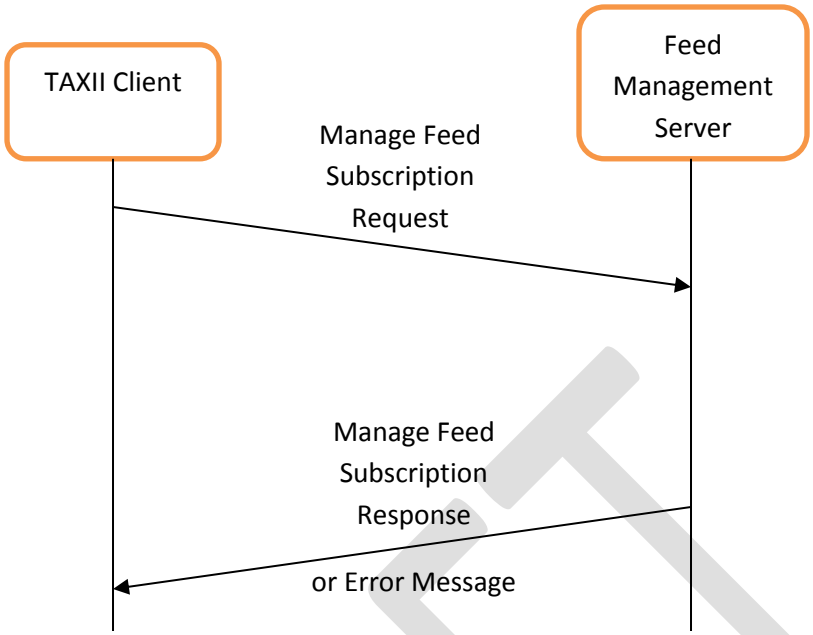


Figure 6 - Subscription Management Exchange

In this exchange, the TAXII Client sends a Manage Feed Subscription Request to the Feed Server. The Feed Server may immediately return a TAXII Error Message or it may pass the relevant information to its TAXII Back-end. Relevant information would include the authenticated identity, if any, the parameters that identify the subscription to be managed/created, and the action to be taken. The TAXII Back-end would use this information, along with its own access control policy and the functionality it supports, to determine whether the action is allowed. Depending on this response, the Feed Server may return a TAXII Error Message or send a Manage Feed Successful Response.

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 Server or accept inbound connections.

Copyright © 2012, The MITRE Corporation. All rights reserved.

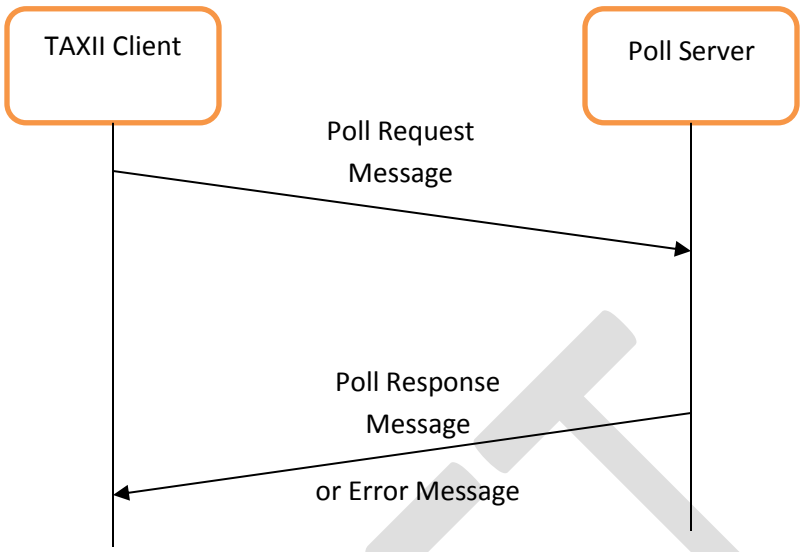


Figure 7 - Feed Poll Exchange

The Consumer's TAXII Client initiates the exchange by sending a Poll Request message to the Producer's Poll Server. The Poll Server may return an immediate TAXII Error Message or pass the relevant information to its TAXII Back-end. Relevant information includes the Feed Name, Subscription Parameters, timestamps 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. There are two possible types of response:

1. The requested information may be denied. In this case, the Poll Server will create a TAXII Error Message and return it to the TAXII Client.
2. Some set of TAXII Data Feed content may be provided. In this case, the Poll Server will construct and send a Poll Response Message. This message indicates both the time interval covering the TAXII Data Feed content that is being transmitting and the STIX Messages Bodies that convey this TAXII Data Feed content.

In all cases, the TAXII Client receives the appropriate message and passes this information on to its TAXII Back-end for processing.

6 TAXII's Use of Network Protocols

As noted earlier, TAXII Messages are conveyed over the network through the use of other network protocols. In addition to facilitating the conveyance of these messages, TAXII relies on some important capabilities to be provided by the network protocols used for these transmissions. This section lists these requirements, although it does not dictate how a TAXII implementation actually meets them.

Copyright © 2012, The MITRE Corporation. All rights reserved.

6.1 Reliability

TAXII requires a reliable transmission mechanism for its messages. This means that, if a message is sent from endpoint A to endpoint B, endpoint A will know whether or not the message was delivered. Moreover, A will know that B was able to accurately reconstruct the messages, even if they were broken up during transmission. Specific Protocol Bindings are free to satisfy the requirement for reliable delivery as they see fit. For example, some Protocol Bindings might rely on a reliable transport protocol such as TCP [5], others might implement message delivery confirmation on top of protocols such as UDP [6]. TMHs MUST be able to assume that their messages have been successfully delivered unless explicitly informed otherwise.

6.2 Protection and Authentication

In some uses of TAXII the sensitivity of the data being conveyed may require additional protections, such as cryptographic assurances of integrity and confidentiality. In TAXII this functionality is provided by the protocol binding. A TAXII Server may support protected and/or unprotected protocol bindings. Likewise, the mechanisms for authentication of TAXII Endpoints are also a function of the selected protocol binding. In order to ensure exchanges with a TAXII Server are protected, a TAXII Client should contact that TAXII Server using a protocol binding that includes the appropriate protections. (A TAXII Server's supported protocol bindings would be indicated in the Service Protocol Binding field of a Discovery Request Message.) See the TAXII Protocol Binding Specifications for details on how individual protocol bindings support authentication and message protection.

6.3 TAXII Protocol Bindings

As noted a multiple points in this document, TAXII messages are transported using network protocols such as HTTP [7]. Only the TAXII Transfer Agent (TTA) deals with these network protocols. TAXII Message Handlers (TMHs) and TAXII Back-ends are agnostic as to the protocol used to transport TAXII Messages over the network. In effect, these protocols are being used as convenient distribution mechanisms to route an incoming message to an appropriate TMH.

There are a few requirements that the TTA must meet to support TAXII. Details of how a given protocol binding is expected to support them are provided in the appropriate TAXII Protocol Binding Specification:

- The TTA MUST ensure that TAXII messages are handed off to the TMH. This means that the TTA must recognize that the network protocol exchange is conveying a TAXII message and route it to the appropriate TMH, especially if the TTA is also fielding messages for non-TAXII services. (For example, an HTTP server might serve regular requests for web content and also field TAXII messages to pass on to a TMH.)
- The TTA MUST ensure that the TAXII message itself, travelling in the body of the relevant network protocol, is delivered intact and unmodified to the TMH. If the content was encoded in order to support transport over the relevant application protocol, this encoding must be reversed before the content is handed off to the TMH. For example, if the TAXII message was

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00029

URI-encoded [8]prior to transmission, this encoding must be reversed prior to hand-off to the recipient's TMH.

- The TTA MUST ensure that any authentication credentials are passed to the TMH along with the TAXII message itself. These credentials would have been established during any transport-layer security exchange and, as such, the TTA would need to collect and transfer these to the TMH. The format of these credentials is beyond the scope of this specification but need to be compatible with the access control mechanisms used in the TAXII Back-end.

7 Using TAXII

Previous work [1] has identified three models used by cyber threat information sharing communities to exchange threat information. These models are:

- Source/subscriber - The information provider pushes out regular information to all subscribers
- Peer-to-peer - Participants share and receive threat data directly
- Hub and spoke - One entity controls receipt and dissemination of cyber threat data that might be collected from multiple sources

This section considers each of these models and outlines how the TAXII Services defined in this specification can be used to support each of these information sharing models. Note that these sections are intended only to serve as examples and organizations are free to leverage TAXII Services in whatever manner meets their needs.

7.1 Source/Subscriber

In this model there is one entity that is the Source of cyber threat information and some number of Subscribers who each enter into agreements with this Source to receive periodic content updates. The Subscribers are likely to be unknown to each other, so this represents a set of bi-lateral agreements that each Subscriber makes with the single Source. In this model, the Source is a TAXII Producer, while the Subscribers are TAXII Consumers.

TAXII supports this sharing model through the use of its Discovery, Feed Management, Inbox, and Poll Services. An organization that wishes to subscribe to the Source's TAXII Data Feeds would need to first learn what TAXII Services the Source offered and how to contact them. While this could be handled by out-of-band mechanisms (such as posting this information on the Source's web page) this could also be accomplished by contacting the Source's Discovery Service. From there, the would-be Subscriber could contact the identified Feed Management Service(s) to learn what feeds the Source offered and, potentially, what restrictions were placed on their access. If the Source is a commercial entity, access might require a paid subscription. If the Source is the repository of some closed community, those who wish to receive content may need to apply for membership to this community. Alternative, some or all feeds might be distributed freely and subscription may automatically be permitted for all who request. The details of how a Subscriber might go about meeting subscription requirements (if any) are outside the scope of TAXII and would need to be handled through some other mechanism. This mechanism

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00030

could be as simple as providing a credit card number to the company's web site, or may require more elaborate background checks or other validations of the would-be Subscriber's authorization to receive the information. Producers are free to use whatever processes they wish, and to subdivide their would-be Subscribers however they see fit, possibly granting some Subscribers greater access to data than others.

If TAXII Data Feed content is restricted to only certain authorized parties and the Source has determined that the Subscriber is allowed to receive content, the Source and Subscriber need to agree on how the Subscriber will authenticate. Depending on the protocol bindings that the Source supports, this can be done by having the Subscriber establish a password, having the Subscriber share a PKI certificate, or through some other means provided both parties had the technical means to convey this information using mutually supported protocols. If a TAXII Data Feed's content is open and does not require authentication, this step is unnecessary when establishing subscriptions to that TAXII Data Feed.

Once the Source is capable of authenticating the Subscriber (if necessary), the Subscriber can contact the Source's Feed Management Service and request subscriptions to the Source's feeds. The Source can compare these requests to their own understanding of what the Subscriber is allowed to receive and grant or deny these requests as appropriate. The Source then can send content to the Subscriber's Inbox Service at the appropriate interval. Alternately, the Subscriber could contact the Source's Poll Service to pull desired content.

DRAFT

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00031

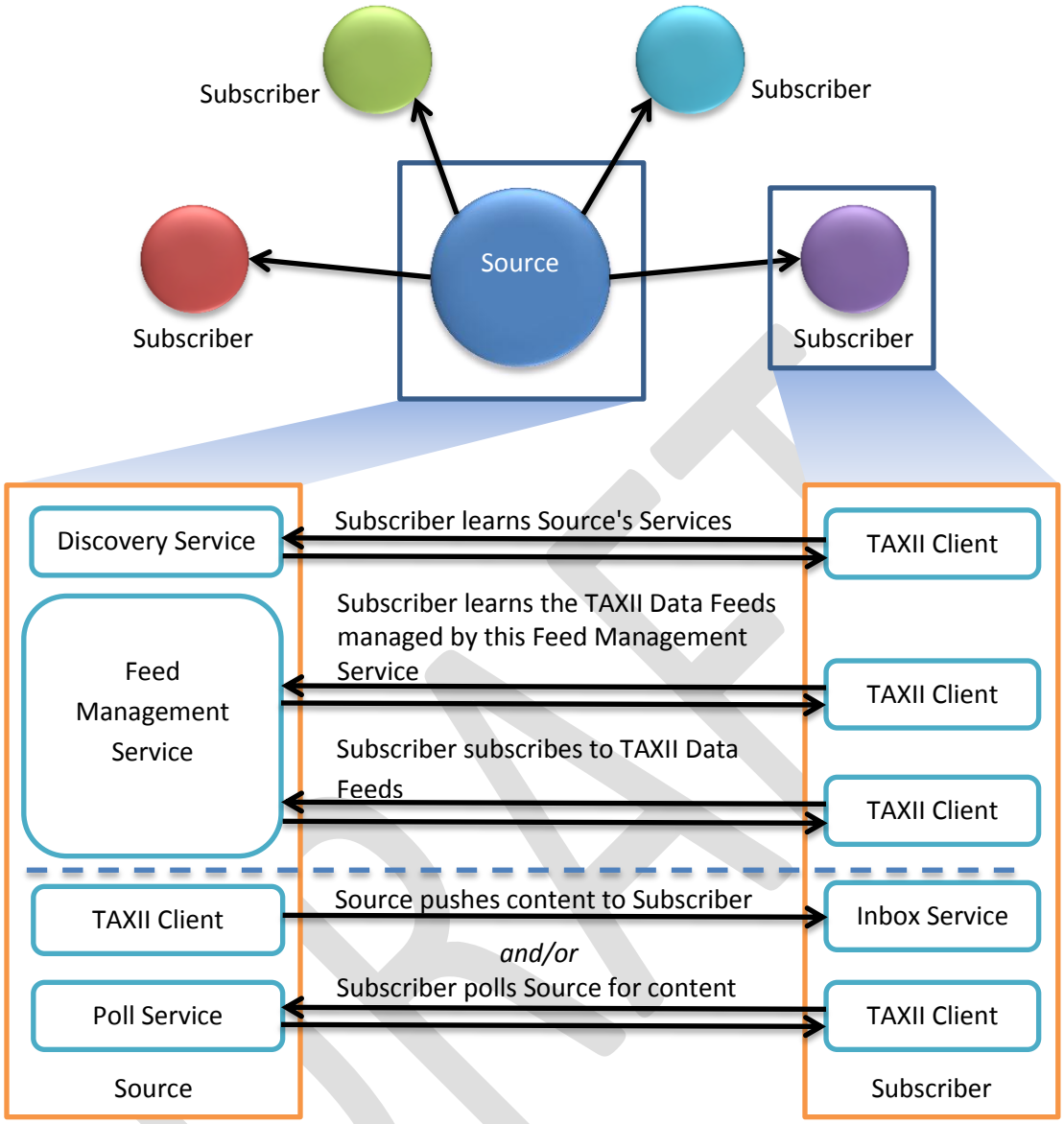


Figure 8 - Source/Subscriber Sharing Model

Figure 8 shows how a Source/Subscriber sharing model could be supported by TAXII Services. The diagram focuses on the TAXII Message Exchanges and does not show any out-of-band communication, such as coordination to gain access to protected services or establish authentication credentials. Note that the diagram includes arrows showing the Subscriber receiving cyber threat data via both push and pull mechanisms, but only one of those exchanges is necessary to communicate threat information. Note also that, once the Subscriber's subscription has been established (through the exchanges above the dashed line), cyber threat data can be exchanged repeatedly without needing to repeat the subscription process (as shown in the exchanges below the dashed line).

Copyright © 2012, The MITRE Corporation. All rights reserved.

7.2 Peer-to-Peer

In a Peer-to-Peer model, pairs of organizations enter into a mutual agreement to share their cyber threat information with each other. In this model, each Peer may operate as both Producer and Consumer. The Peers in this exchange may each set up feeds using a procedure similar to that outlined in the Source/Subscriber model. Alternately, they may simply agree to push or pull content with each other without setting up any formal subscription. Skipping any formal subscription would allow a Peer to host an Inbox Service without any need for a Feed Management Service.

Note that Peer-to-Peer sharing models actually have two variants: community-based sharing arrangements and ad-hoc sharing arrangements. In a community-based Peer-to-Peer environment a sharing community might constitute many of these pairwise arrangements where all members of such a community agree to a single sharing policy with an understanding that all community members will share with each other. However, unlike the other two models which have a central point from which information is disseminated, all sharing occurs on a point-to-point basis between Peers. If any two Peers wish to receive cyber threat data from each other directly, they will need to establish an appropriate agreement with each other so the Peers know to send each other information.

Alternately, Peer-to-Peer sharing could be used for individual sharing agreements on an ad-hoc basis. This might occur if two companies make individual agreements to share with each other. In this case, the agreements on what to share would be specific to those particular parties. A single entity might engage in both variants of Peer-to-Peer sharing, belonging to one or more communities where members share with each other according to some communal agreement while also negotiation individual sharing arrangements with other entities. Of course, information received through one sharing agreement might not be re-sharable to Peers who are not part of this particular agreement. As such, a participant would likely need to track who provided any given piece of cyber threat information, but the details of how this would be tracked and how a Peer would use this information to constrain further sharing are functions of the Peer's TAXII Back-end and thus outside the scope of the TAXII specifications.

Copyright © 2012, The MITRE Corporation. All rights reserved.

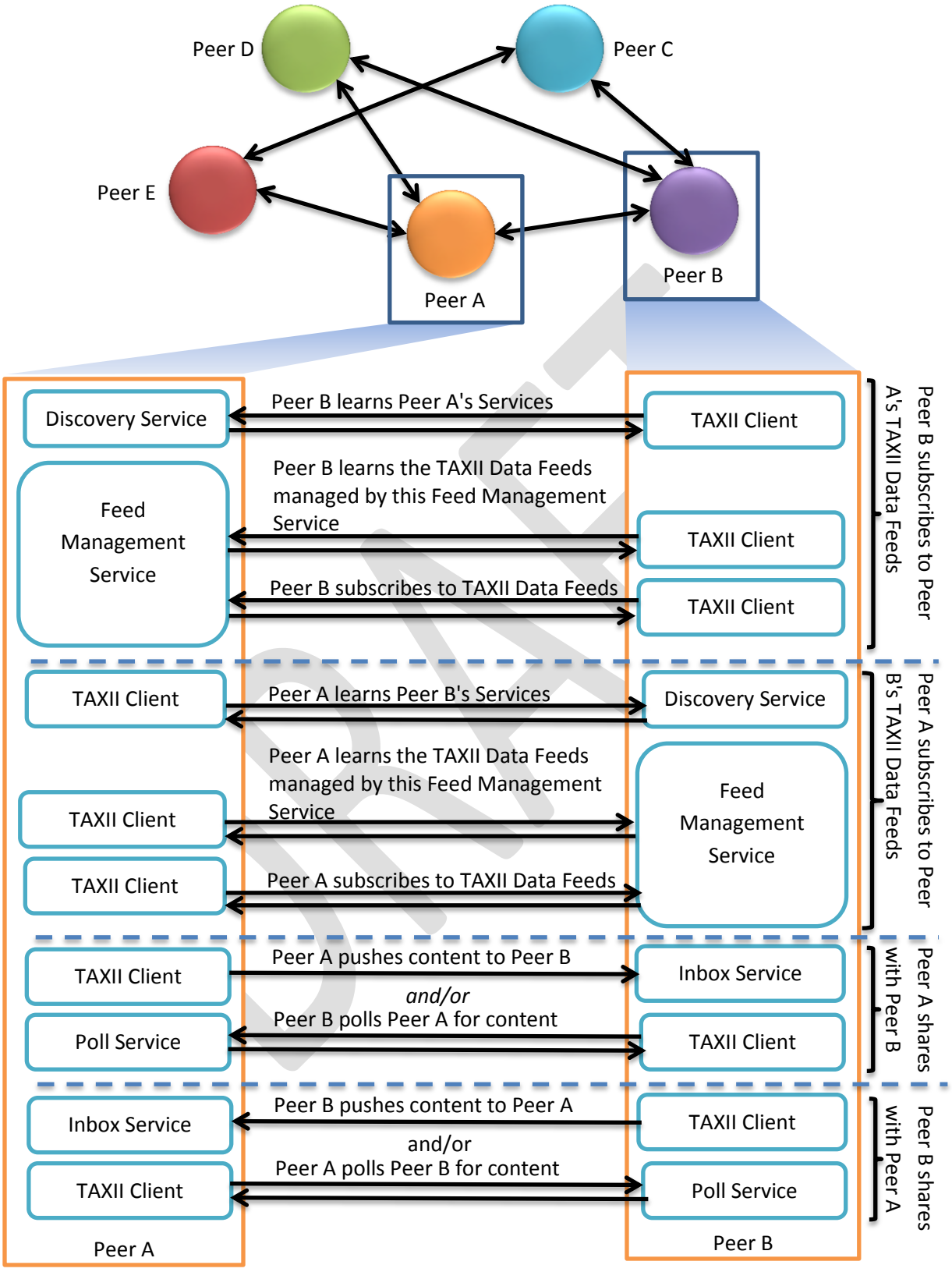


Figure 9 - Peer-to-Peer Sharing Model

Copyright © 2012, The MITRE Corporation. All rights reserved.

Figure 9 shows how a Peer-to-Peer sharing model could be supported by TAXII Services. In this model, all agreements are between two parties although many such pair-wise agreements may exist within any community. As noted earlier, all that is happening here is both Peers are contacting each other to request subscriptions to cyber threat data. In this diagram it is assumed that both Peers have a Feed Management Service that is used to manage all subscription requests. As noted above, one or both of a set of Peers could arrange for subscriptions to be created using out-of-band methods. Doing so would eliminate the need for one or both of the first two groups of exchanges where both parties subscribe to the other's feeds.

7.3 Hub and Spoke

In a Hub and Spoke model, one entity acts as a clearing-house for cyber threat information. This represents the familiar "open mailing-list" model, where parties can send posts to a mail-list server which then copies those posts to all subscribers of the mailing list. In this model, the Hub is both a Consumer of provided information and a Producer who pushes information to the Spokes. A Spoke could be a Producer, providing information to the Hub, a Consumer, receiving updates from the Hub, or both. The Hub can use an Inbox Service to receive cyber threat information from anyone willing to volunteer information and/or it might poll certain sources of content in order to aggregate them in a single location. From there, the Hub can serve as a Source in the Source/Subscriber model while the Spokes would all be Subscribers in this model. The Hub can adopt any policy with regard to information it receives, ranging from automatically passing everything on, to only passing on messages from recognized senders, to performing detailed edits and analysis before sharing information back out.

DRAFT

Copyright © 2012, The MITRE Corporation. All rights reserved.

Netskope Ex. 1014
Netskope v. Fortinet IPR2026-00515
Page 00035

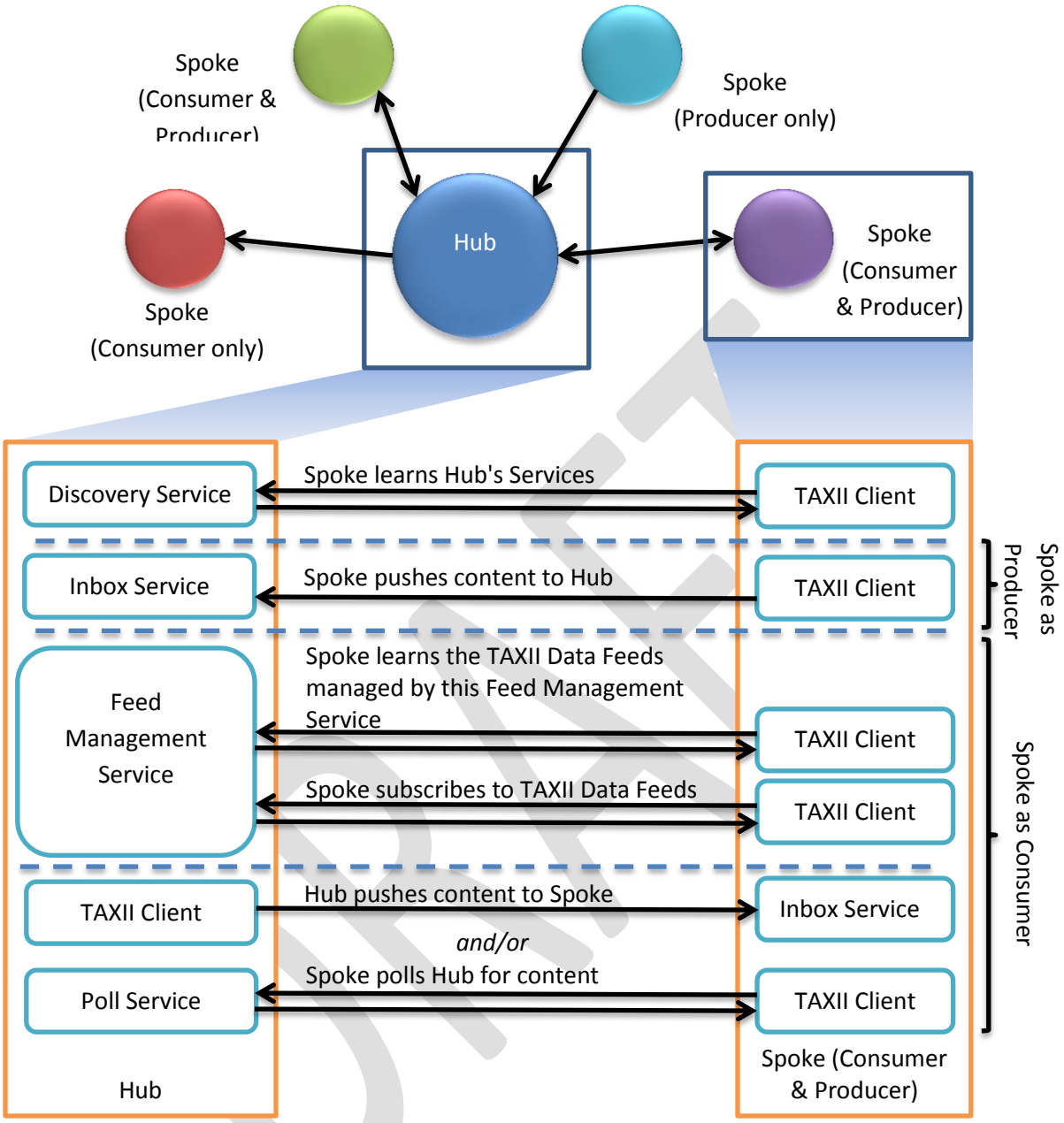


Figure 10 - Hub and Spoke Sharing Model

Figure 10 shows how a Hub and Spoke sharing model could be supported by TAXII Services. Note that in this model some Spokes may be Consumers, some may be Producers, and some may be both. The diagram above shows the exchanges that could be used for a Spoke that acts as both a Producer and Consumer; if the Spoke was only to act in one of these roles, only the relevant exchange(s) would be necessary. Note that regardless of the role the Spoke was playing (Consumer and/or Producer) it would need to learn how to contact the relevant TAXII Services on the Hub. The diagram above shows the Spoke doing this using the Hub's Discovery Service, although this could also be accomplished using out-of-band mechanisms.

Copyright © 2012, The MITRE Corporation. All rights reserved.

8 Conclusion

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.

9 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.

Copyright © 2012, The MITRE Corporation. All rights reserved.

10 Appendix A - Roadmap

The set of services in TAXII 1.0 are designed to provide a baseline of functionality required for the most common cyber security information sharing use-cases. Additional capabilities have been identified as potentially useful and are under consideration for inclusion in future TAXII Specifications. Those items are listed here with a brief description.

- Query Message Exchange & related services- A mechanism for asking a sharing peer a question and getting a response.
- Payload encryption - Requirements for encrypting TAXII messages independently of the transport layer. Currently, TAXII relies on the transport layer for this protection.
- Additional Message Binding Specifications - Some groups may want to use data formats other than XML. Additional Message Binding Specification will be included based on community feedback.
- Additional Protocol Binding Specifications – The TAXII 1.0 release will include a single Protocol Binding Specification for HTTP/TLS. It is expected that some organizations or use-cases may require protocols other than HTTP. Additional Protocol Binding Specifications will be included based on community feedback.
- A specification for the interaction between TAXII Transfer Agents and TAXII Message Handlers.

DRAFT

Copyright © 2012, The MITRE Corporation. All rights reserved.