THE MITRE CORPORATION

The TAXII HTTP Protocol Binding Specification

Version 1.0 (draft)

Mark Davidson, Charles Schmidt

11/16/2012

DRAFT

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 use HTTP to convey TAXII messages.

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.

Open Issues

Sections 8 and 9 of this document require significant development.

DRAFT 1

Table of Contents

DRAFT 1

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

DRAFT 1

1 Introduction

The TAXII HTTP Binding defines the requirements for using HTTP/1.1 [1] or HTTP Over TLS [2]to send and receive TAXII Messages. This document normatively references HTTP/1.1, defining extensions and restrictions of HTTP/1.1 where necessary to support TAXII Services and TAXII Message Exchanges as defined in the TAXII Services Specification [3]. This specification defines requirements for HTTP Requests and Responses.

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

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

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 HTTP Binding Specification, is highlighted.

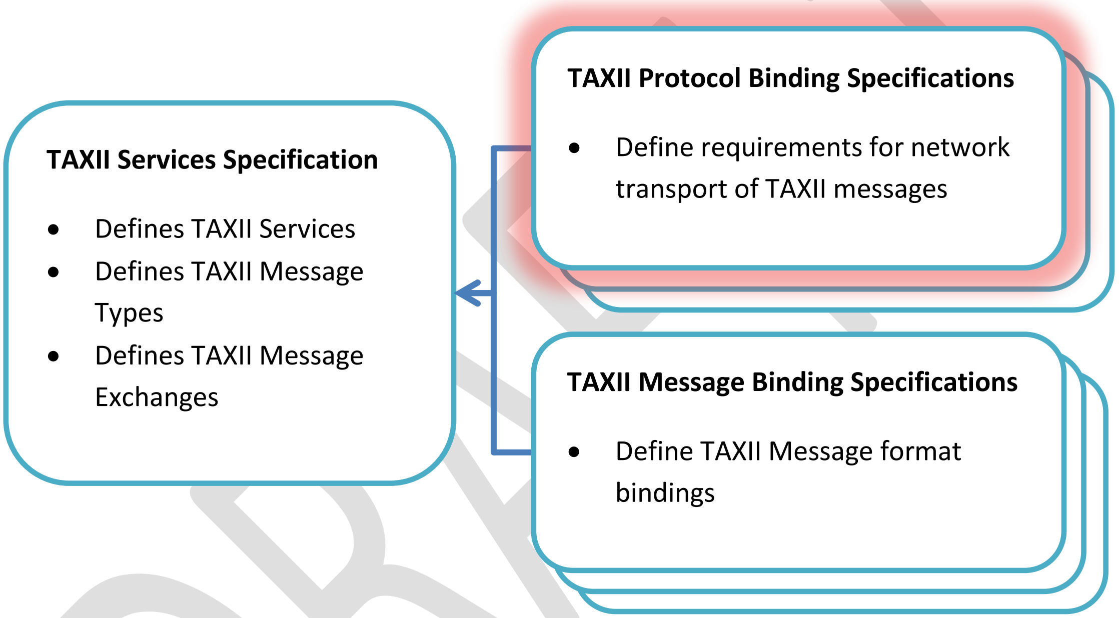
TAXII Services Specification
• Defines TAXII Services
• Defines TAXII Message Types
• Defines TAXII Message Exchanges
TAXII Protocol Binding Specifications
• Define requirements for network transport of TAXII messages
TAXII Message Binding Specifications
• Define TAXII Message format bindings

Figure 1 - TAXII Specification Hierarchy

Separation of the Services Specification, Message Binding Specifications, and Protocol Binding Specifications exists to support flexibility as TAXII evolves. Threat 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

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

DRAFT

permissible by policy can be effected by the TAXII mechanisms. Groups that use different protocol and/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 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 RFC 2119. [4]

1.2 Terms and Definitions

This document references the Terms and Definitions from the TAXII Services Specification, version 1.0. Those Terms and Definitions are repeated here.

1.2.1 TAXII Concepts

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

DRAFT

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

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

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.

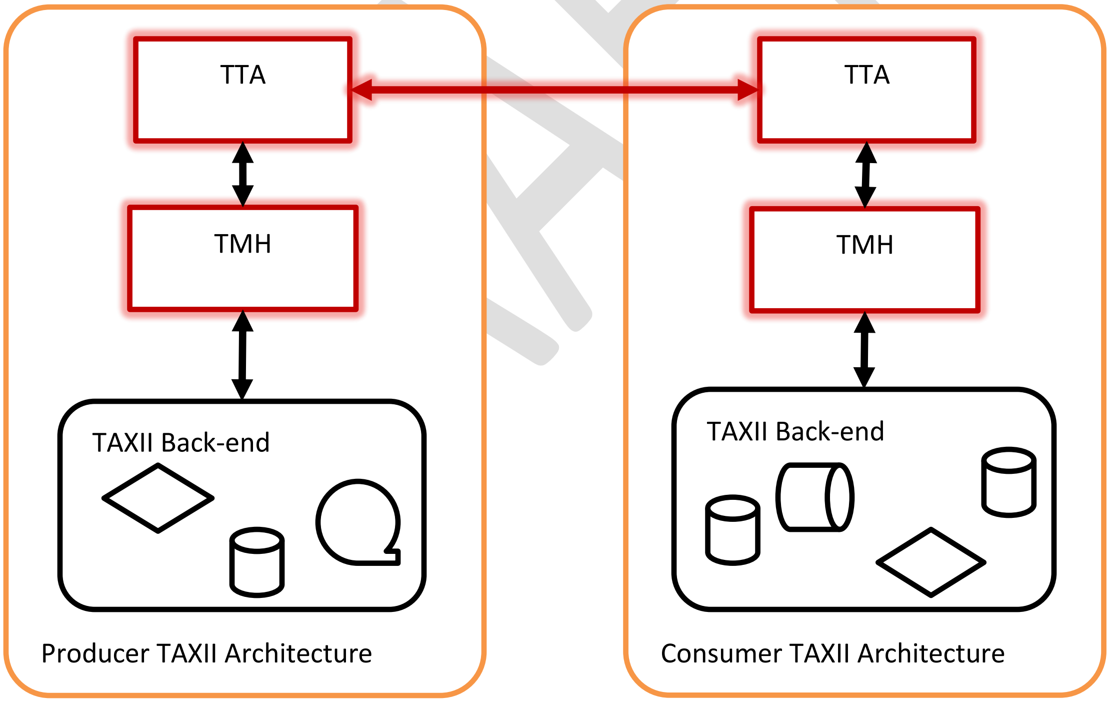

Figure 2: The Interaction of TAXII Functional Units

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

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

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 HTTP Binding Terms

This section defines terms that are specific to this specification.

media-range - Used in the Accept, Content-Type, X-TAXII-Accept, and X-TAXII-Content-Type headers to indicate the format of an entity-body (in the case of Content-Type and X-TAXII-Content-Type) or the acceptable response format(s) of an entity-body (in the case of Accept and X-TAXII-Accept).

entity-body - The body of an HTTP Message before transfer and/or content encodings (if any) are applied. From HTTP/1.1.

DRAFT 1

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

message body -The body of an HTTP Message after transfer and/or content encodings (if any) are applied. From HTTP/1.1.

1.3 TAXII Protocol 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.

This specification defines two TAXII Protocol Version IDs, one for HTTP and one for HTTPS (aka HTTP Over TLS). The two Version IDs are provided in order to disambiguate between TAXII Services that are provided over HTTP and TAXII Services that are provided over HTTPS. This is discussed further in Section 9.2 HTTP Servers.

The TAXII Protocol Version IDs for the version of the TAXII HTTP Binding described in this specification are:

TAXII_HTTP_BINDING_1.0

and

TAXII_HTTPS_BINDING_1.0

2 TAXII Functional Units and Web Components

This section discusses TAXII Functional Units and common web components. A web component is any software that supports HTTP communications. Web browsers, web servers, application frameworks, and databases are all examples of web components. This section is informative in nature and is intended to enhance the understanding of the reader. This section does not define any requirements for TAXII Endpoints.

Though the concepts of TTA, TMH, and Back-end are suitable for discussing the capabilities required of a TAXII Endpoint, they are at a different level of abstraction than that of web components. A web system - a set of web components working in concert to support HTTP communications - may be comprised of a variety of web components: web servers, application frameworks, databases, firewalls, and more. Functionality of the TTA, TMH, and Back-end are not required to exist in any particular web component, nor are any web components specifically required.

DRAFT

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

This specification does not require or assume any particular set or configuration of web components. As long as the requirements for HTTP Requests and HTTP Responses are met, organizations are free to use any configuration of any number of web components.

2.1 Compliance with HTTP/1.1

In order to be compliant with this specification, an implementation MUST adhere to all requirements in the HTTP/1.1 specification in addition to the requirements in this document. Requirements in this document are restrictions and extensions of HTTP/1.1. This document attempts to re-use concepts and terms from HTTP/1.1 where possible and includes a reference to the relevant section of the specification when doing so.

3 TAXII Media Type

This section defines the TAXII Media Type. The TAXII Media Type is a restriction of the HTTP Media Type concept as defined in HTTP/1.1 "Section 3.7, Media Types":

HTTP uses Internet Media Types ... in order to provide open and extensible data typing and type negotiation.

```
media-type  =     type "/" subtype *( ";" parameter )
type        =     token
subtype     =     token
```

The TAXII Media Type is used in the X-TAXII-Content-Type and X-TAXII-Accept headers. The TAXII Media Type restricts the HTTP Media Type as follows:

1. type is restricted to TAXII Services Version IDs (e.g. TAXII_1.0)
2. subtype is restricted to TAXII Message Binding Version IDs (e.g. TAXII_XML_1.0).
3. parameter is not restricted by this specification.

It is worth noting that STIX version and binding information is not specified in the TAXII Media Type. For TAXII Messages that contain STIX, this information is conveyed using the Content Binding field in that TAXII Message.

4 TAXII HTTP Headers

This section defines the requirements for TAXII HTTP Headers. The term TAXII HTTP Headers refers to the set of five HTTP headers defined in this section. Some TAXII HTTP Headers are restrictions of existing HTTP Headers, while other TAXII HTTP Headers are X-Headers specifically for use in TAXII. Other HTTP Headers not mentioned in this section retain their original definitions and requirements from HTTP/1.1. Implementers must conform to the requirements in HTTP/1.1 except where this specification defines

DRAFT 1

explicit restrictions or extensions. This section focuses on the format of the header fields themselves. Their use in HTTP Requests and Responses is described in subsequent sections.

The following table, Table 1 - HTTP Headers, provides a listing of the TAXII HTTP Headers and a brief description of each.

Table 1 - HTTP Headers

Header	Required?	Description
Accept	No	Specifies which HTTP Media Types the requestor will accept in response.
Content-Type	Yes	Specifies which HTTP Media Type the entity body is formatted in.
X-TAXII-Accept	No	Specifies which TAXII Media Types the requestor will accept in response.
X-TAXII-Content-Type	Yes	Specifies which TAXII Media Type the entity body is formatted in.
X-TAXII-Protocol	Yes	Specifies which Protocol Binding is being used.

4.1.1 Accept

HTTP/1.1, Section 14.1 describes the Accept header:

The Accept request-header field can be used to specify certain media types which are acceptable for the response.

The Accept header field in HTTP Requests conforming to this specification follows the guidance in HTTP/1.1 with the following restrictions:

1. Only one media-range may be specified
2. The media-range MUST have a type of ‘application’
3. The media-range SHOULD have a subtype that is defined in the MIME Media Types IANA Table [5] as an application subtype. The selected subtype (e.g. ‘xml’) MUST reflect the acceptable TAXII Message Binding in the entity-body of the Response message.

This specification does not restrict other portions of the Accept header.

4.1.2 Content-Type

HTTP/1.1, Section 14.17 describes the Content-Type header:

HTTP/1.1, Section 14.1 describes the Content-Type header: The Content-Type entity-header field indicates the media type of the entity-body…

The Content-Type header field in Requests and Responses conforming to this specification follows the guidance in HTTP/1.1, with the following restrictions:

1. The media-range MUST have a type of ‘application’

DRAFT

2. The media-range SHOULD have a subtype that is defined in the MIME Media Types IANA Table [5] as an application subtype.
3. The selected subtype (e.g. 'xml') MUST reflect the TAXII Message Binding in the entity-body.

This specification does not restrict other portions of the Content-Type header.

4.1.3 X-TAXII-Accept

X-TAXII-Accept is similar to the Accept header in that it identifies acceptable content in the response, but instead of using the MIME Media Type table, this field uses the TAXII Media Type. Thus Accept identifies the acceptable MIME type of the response, using an IANA enumeration, while the X-TAXII-Accept message defines the acceptable TAXII version and message binding of the response.

The X-TAXII-Accept header follows the guidance in HTTP/1.1 Section 14.1, Accept, with the following restriction:

1. All media-types in the X-TAXII-Accept header MUST be valid TAXII Media Types.
2. All media-types in the X-TAXII-Accept header MUST be of the type identified by the Accept header (e.g. If the Accept header has a type/subtype of 'application/xml', all X-TAXII-Accept header values must identify XML bindings).

4.1.4 X-TAXII-Content-Type

X-TAXII-Content-Type is similar to the Content-Type header in that it identifies the format of the entity-body, but instead of using the MIME Media Type table, this field uses the TAXII Media Type. Thus Content-Type identifies the acceptable MIME type of the response, using an IANA enumeration, while the X-TAXII-Content-Type message defines the acceptable TAXII version and message binding of the response.

The X-TAXII-Content-Type header field follows the guidance in HTTP/1.1 Section 14.17 with the following restriction:

1. The media-type in the X-TAXII-Content-Type header MUST be a valid TAXII Media Type.
2. The media-type in the X-TAXII-Content-Type header MUST be of the type identified by the Content-Type header (e.g. If the Content-Type header has a type/subtype of 'application/xml', the X-TAXII-Content-Type header value must be an XML binding).

4.1.5 X-TAXII-Protocol

The X-TAXII-Protocol header is used to specify the TAXII Protocol Binding Version ID.

The value of the X-TAXII-Protocol MUST be a TAXII Protocol Binding Version ID defined in a TAXII Protocol Binding Specification. (This Protocol Binding Specification defines a Version ID of 'TAXII_HTTP_1.0').

The value of the X-TAXII-Protocol header indicates the TAXII Protocol Binding that the message sender is using.

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

DRAFT

5 HTTP Requests

This section defines the requirements for HTTP Requests.

5.1 TAXII Messages

This section defines requirements for the Request Method, Get Parameters (formally called the Query syntax component in Uniform Resource Identifier (URI): Generic Syntax [6]), and Entity Body of TAXII Messages that are sent as an HTTP Request.

This specification reserves the ‘message_type’ and ‘message_id’ get parameters for TAXII communications. The message_type parameter, if present, always indicates the type of TAXII Message being conveyed. The message_id parameter, if present, always indicates the message ID of the TAXII message.

All get parameters must be encoded in a manner agreed upon by both parties. While current standards do not require any specific encoding, common practice is to use a percent-encoding scheme. This specification does not formally define any requirements for encoding get parameters, it gently reminds implementers that there is a common practice that should be considered during development.

DRAFT

5.1.1 TAXII Discovery Request

This message does not use the Discovery Request message from any TAXII Message Binding Specification. Instead, this specification represents the Discovery Request message using HTTP mechanisms.

Request Method: GET
Get Parameters:

- message_type - MUST be ‘discovery_request’. This field is case insensitive.
- message_id - MUST be a string. This field is case sensitive.
- extended headers - These may be represented as any get parameter that is not ‘message_type’ or ‘message_id’.

Entity-Body: 0-length
Example:
http://taxii.example.com/DiscoveryService/?message_type=discovery_request&message_id=3

5.1.2 TAXII Feed Information Request

This message does not use the Feed Information Request message from any TAXII Message Binding Specification. Instead, this specification represents the Discovery Request message using HTTP mechanisms.

Request Method: GET
Get Parameters:

- message_type - MUST be ‘feed_information_request’. This field is case insensitive.

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

- message_id - MUST be a string. This field is case sensitive.
- extended headers - These may be represented as any get parameter that is not 'message_type' or 'message_id'.

Entity-Body: 0-length
Example:
http://taxii.example.com/FeedManagementService/?message_type=discovery_request&message_id=1

5.1.3 TAXII Manage Feed Subscription Request

Request Method: POST
Get Parameters: None
Entity-Body: Contains a valid TAXII Manage Feed Subscription Request message as defined by the TAXII Message Binding identified in the X-TAXII-Content-Type header.

5.1.4 TAXII Poll Request

While TAXII Message Specifications may define a TAXII Poll Request message, that definition is not used by this specification. Instead, this specification encodes the necessary Poll Request information into URL parameters.

Request Method: POST
Get Parameters: None

Entity-Body: Contains a valid TAXII Poll Request message as defined by the TAXII Message Binding identifies in the X-TAXII-Content-Type header.

5.1.5 TAXII STIX Message

Request Method: POST
Get Parameters: None
Entity-Body: Contains a valid TAXII STIX Message as defined by the TAXII Message Binding identified in the X-TAXII-Content-Type header.

5.2 Request Headers

This section defines usage requirements for TAXII HTTP Headers in HTTP Requests. TAXII HTTP Headers are defined in the TAXII HTTP Headers (Section 5). HTTP/1.1 Headers not mentioned here retain their original meaning and usage requirements.

1. The Accept header MAY be present in all HTTP Requests.
2. The Content-Type header SHOULD be present in all HTTP Requests that contain an entity-body.
3. The X-TAXII-Accept header MAY be present in all HTTP Requests.
4. The X-TAXII-Content-Type header SHOULD be present in all HTTP Requests that contain an entity-body.
5. The X-TAXII-Protocol header MUST be present in all HTTP Requests.

DRAFT

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

6 HTTP Responses

This section defines the requirements for HTTP Responses.

6.1 Response Headers

This section defines usage requirements for TAXII HTTP Headers in HTTP Responses. TAXII HTTP Headers are defined in the TAXII HTTP Headers section. HTTP/1.1 Headers not mentioned here retain their original meaning and usage requirements.

1. The Accept header MUST NOT be present in any HTTP Responses.
2. The Content-Type header SHOULD be present in all HTTP Responses that contain an entity-body.
3. The X-TAXII-Accept header MUST NOT be present in any HTTP Responses.
4. The X-TAXII-Content-Type header SHOULD be present in all HTTP Responses that contain an entity-body.
5. The X-TAXII- Protocol header MUST be present in all HTTP Responses.

6.2 Response Entity Body

The response entity body MUST conform to the requirements of the relevant TAXII Message Binding, as indicated by the Content-Type and X-TAXII-Content-Type headers.

7 HTTP Status Codes and TAXII Error Messages

This section describes common server states and the appropriate HTTP Status Code for that state.

HTTP 200 (OK) - This status code should be used to indicate that the TAXII Message in the HTTP Request was received, processed, and the HTTP Client should expect a TAXII Message in the HTTP Response body.

HTTP 400 (Bad Request) - This status code should be used to indicate that there was a problem with the request. This status code may indicate any number of problems with the HTTP Request, including a malformed TAXII Message.

HTTP 401 (Unauthorized) - This status code should only be used when the client should authenticate using the Authorization header field (per Section 14.8, Authorization in HTTP/1.1). For other authorizations failures, HTTP 403 (Forbidden) should be used.

HTTP 403 (Forbidden) - This status code should be used to indicate that the client does not have permission to access the TAXII Service. Alternatively, HTTP 404 (Not Found) may be used to conceal information.

HTTP 405 (Method Not Allowed) - This status code should be used to indicate that a client used an HTTP Method that is not allowed. Acceptable HTTP Methods are detailed in Section 5.1 TAXII Messages.

DRAFT

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

HTTP 406 (Not Acceptable) - This status code should be used to indicate that the server is only capable of generating a response that is not acceptable according to the Request's Accept and X-TAXII-Accept header fields (if present).

HTTP 415 (Unsupported Media Type) - This status code should be used when the Content-Type or X-TAXII-Content-Type header field specifies a Media Type or TAXII Media Type (respectively) that the server does not understand.

For states not covered in this section, the following rule of thumb should be applied: If an error is detectable by inspecting the HTTP Headers, parsing the entity-body, or validating the entity-body, an HTTP Status Code indicating that error should be returned. If an error is detectable by processing the TAXII Message, a TAXII Error Message should be returned.

For example, consider a Manage Feed Subscription Request. If the Manage Feed Subscription Request is not formatted correctly (this error is detectable by attempting to parse and/or validate the entity-body), the appropriate HTTP Status Code should be returned. If the message indicates a feed name that does not exist (this error is detectable by processing the TAXII Message), a TAXII Error Message should be returned.

8 Ports

Web Components that listen for TAXII messages SHOULD use port 80 when using HTTP and port 443 when using HTTP/TLS.

9 Security Mechanisms

When required, use HTTPS to provide an encrypted communication channel.

This section defines security mechanisms that an HTTP Clients and HTTP Servers may offer. In the context of this section, a security mechanism is something that establishes the identity of an endpoint, the encryption of the communication channel, or both.

This section lists a subset of security mechanisms covering the spectrum of common deployments. HTTP Clients and HTTP Servers SHOULD offer at least one of the mechanisms defined in this section.

9.1 HTTP Clients

This section defines security mechanisms that a client may offer to a server. If a server deems that the security mechanism offered by the client is insufficient, the server may terminate the connection. HTTP Client security mechanisms, at most, establish the identity of the Client. Regardless of the security mechanism offered by the Client, the Client may be able to participate in.

9.1.1 None

Clients choosing 'None' choose not to offer any security mechanism to the server.

DRAFT

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

9.1.2 HTTP Basic Authentication

Clients choosing HTTP Basic Authentication choose to offer credentials to the server in compliance with RFC 2617 [6]. Clients choosing this option SHOULD decline to send credentials over an unencrypted channel, as they are easily discoverable.

9.1.3 Client Certificates

Clients choosing Client Certificates choose to offer the server a Client Certificate for the purposes of authentication and authorization. Clients MUST do so in compliance with TLS 1.2 [7] or higher.

9.2 HTTP Servers

This section defines security mechanisms that a server may offer to a client.

9.2.1 None

Servers choosing 'None' choose not to offer any security mechanism to the client. The TAXII_HTTP_BINDING_1.0 Version ID MUST be used to indicate TAXII Services that are offered using HTTP.

9.2.2 HTTP Over TLS

Servers choosing HTTP/TLS choose to offer a Certificate to clients for the purpose of identification and transport encryption. Servers choosing HTTP Over TLS must do so in compliance with TLS 1.2 [7] or higher and HTTP Over TLS. The TAXII_HTTPS_BINDING_1.0 Version ID MUST be used to indicate TAXII Services that are offered using HTTP Over TLS.

DRAFT 1

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

10 Bibliography

[1] 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.

[2] E. Rescorla, "RFC 2818 - HTTP Over TLS," The Internet Engineering Task Force, 2000.

[3] M. Davidson and C. Schmidt, "TAXII Services Specification," The MITRE Corporation, 2012.

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

[5] Internet Assigned Numbers Authority, 2006. [Online]. Available: http://www.iana.org/assignments/media-types/application/index.html. [Accessed 2012].

[6] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen and L. Stewart, "RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication," The Internet Engineering Task Force, 1999.

[7] T. Dierks and E. Rescorla, "RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2," The Internet Engineering Task Force, 2008.

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

DRAFT

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