THE MITRE CORPORATION

The TAXII HTTP Protocol Binding Specification

Version 1.0 DRAFT

Mark Davidson, Charles Schmidt

4/24/2013

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 is a trademark 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 - 2013 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.

Table of Contents

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

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 at machine speed. TAXII is not an information sharing initiative or application and it does not attempt to define trust agreements, governance, or non-technical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats, and enables organizations to easily share the information they choose with the partners they choose. For more information on TAXII, see "Trusted Automated eXchange of Indicator Information (TAXII ™)" [1].

The TAXII HTTP Protocol Binding Specification defines the requirements for using HTTP/1.1 [2] or HTTP Over TLS [3]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 [4]. This specification defines requirements for HTTP Requests and Responses. It is recommended that the reader familiarize themself with the TAXII Services Specification as well as the HTTP/1.1 specification (RFC 2616) prior to reading this document.

1.1 TAXII Specifications

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

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

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

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

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

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

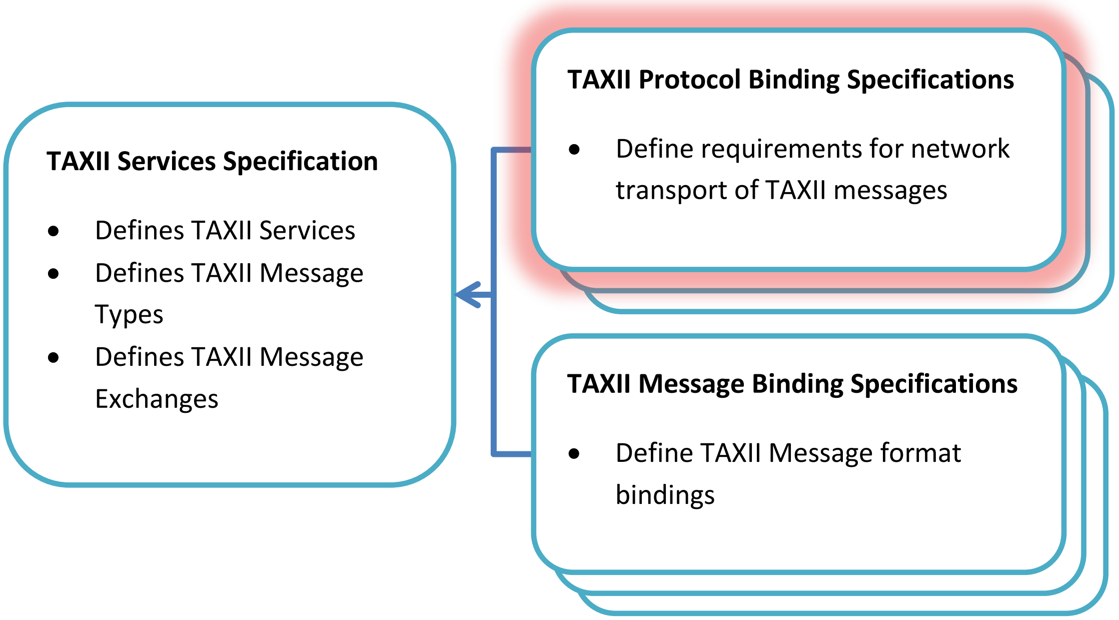
TAXII Services Specification
Defines TAXII Services
Defines TAXII Message Types
Defines TAXII Message Exchanges
TAXII Protocol Binding Specifications
Define requirements for network transport of TAXII messages
TAXII Message Binding Specifications
Define TAXII Message format bindings

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 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 The TAXII HTTP Protocol Binding Specification

This specification provides normative text on the transmission of TAXII Messages using HTTP and HTTPS. It does not provide details about how TAXII Messages are expressed, leaving that to a Message Binding Specification. The TAXII Services and TAXII Message Exchanges that these Messages support, as well as a detailed discussion of the meaning of message fields, are discussed in detail in the TAXII Services Specification.

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

1.1.1.1 TAXII Protocol Version ID for HTTP and HTTPS

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

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 **Error! Reference source not found.**.

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

TAXII_HTTP_BINDING_1.0

and

TAXII_HTTPS_BINDING_1.0

1.1.1.2 Specification Versioning

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

1.1.2 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. [5]

2 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

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

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 HTTP Protocol Binding Concepts

This section contains concepts and definitions for this specification.

3.1 TAXII Version-Binding Type

This section defines the TAXII Version-Binding Type. The TAXII Version-Binding Type is based on the format of the HTTP Media Type 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 Version-Binding Type is used in the X-TAXII-Content-Type and X-TAXII-Accept headers. The TAXII Version-Binding Type restricts the HTTP Media Type as follows:

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

It is worth noting that payload version and binding information is not specified in the TAXII Version-Binding Type. For TAXII Messages that contain payloads, this information is conveyed using the Payload 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. TAXII HTTP Headers are HTTP headers whose values are restricted by this specification, as well as HTTP X-Headers defined by this specification. HTTP Headers not mentioned in this section retain their original definitions and requirements from HTTP/1.1.

The Table 1 - HTTP Headers, provides a list 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 accepts in response.
X-TAXII-Accept	No	Specifies which TAXII Version-Binding Types the requestor

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

		accepts in response.
Content-Type	Yes, if there is an entity body. No otherwise.	Specifies HTTP Media Type in which the entity body is formatted.
X-TAXII-Content-Type	Yes, if there is an entity body. No otherwise.	Specifies TAXII Version-Binding Type in which the entity body is formatted.
X-TAXII-Protocol	Yes	Specifies which Protocol Binding is used in this exchange.

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. The media-range MUST have a type of ‘application’
2. The media-range SHOULD have a subtype that is defined in the MIME Media Types IANA Table [6] as an application subtype.
3. The selected subtype (e.g. ‘xml’) MUST agree with the X-TAXII-Accept header value (e.g., ‘TAXII_XML_BINDING_1.0’).

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:

The Content-Type entity-header field indicates the media type of the entity-body…

The Content-Type header field in HTTP Requests and HTTP 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’
2. The media-range SHOULD have a subtype that is defined in the MIME Media Types IANA Table [6] as an application subtype.
3. The selected subtype (e.g. ‘xml’) MUST agree with the X-TAXII-Content-Type header value (e.g., ‘TAXII_XML_BINDING_1.0’).

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

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

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 Version-Binding 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.

Note that the set of acceptable values indicate by the X-TAXII-Accept header may not include the value of the X-TAXII-Content-Type header of the HTTP Request. While this is discouraged in most cases, it is necessary for some HTTP Requests since the HTTP Protocol Binding expresses certain TAXII Messages using HTTP GET requests.

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

1. All media-types in the X-TAXII-Accept header MUST be valid TAXII Version-Binding 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 Version-Binding Type. Thus Content-Type identifies the acceptable MIME type of the response, using an IANA enumeration, while the X-TAXII-Content-Type provides a more specific definition of the format of the entity-body.

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 Version-Binding Type.
2. The media-type in the X-TAXII-Content-Type header MUST agree with 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 which protocol specification the HTTP Message conforms to.

The value of the X-TAXII-Protocol MUST be a TAXII Protocol Binding Version ID defined in a TAXII Protocol Binding Specification.

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.

5 HTTP Requests

This section defines the requirements for HTTP Requests.

5.1 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.

5.2 TAXII Messages

This section defines requirements for the Request Method, Query Parameters (formally called the Query syntax component in Uniform Resource Identifier (URI): Generic Syntax [7]), and Entity Body of TAXII Messages that are sent as an HTTP Request.

Where possible TAXII Messages are expressed using Query Parameters only, as this allows a GET request to be used. Where it is not possible to express a TAXII Message using only Query Parameters, a POST request is used. When a POST request is used, the request body POST is a TAXII Message from a TAXII Message Binding.

For TAXII Messages conveyed using GET requests, this specification defines the syntax for extended headers. For TAXII Messages conveyed using a GET request, extended headers MUST be represented using a Query Parameter that begins with ‘x_’ (e.g., ‘x_myExtendedHeader’). For TAXII Messages conveyed using a POST request, extended headers MUST be represented using the mechanism that the Message Binding defines.

Some strings may contain characters that are invalid in a URL. As such, query parameters should be encoded per Section 2.1 and Section 2.4 of Uniform Resource Identifier (URI): Generic Syntax [8].

Note that some TAXII Messages have example URLs. While the URLs use a ‘one URL per TAXII Service’ arrangement, this is not the only valid arrangement. It is possible (and completely valid) to offer multiple TAXII Services at the same URL.

5.2.1 TAXII Discovery Request

This specification represents the Discovery Request message using HTTP mechanisms. Other message bindings MUST NOT be used.

Request Method: GET
Query Parameters:

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

- message_type - Required. MUST be 'discovery_request'. This field is case insensitive.
- message_id - Required. MUST be a string. This field is case sensitive.

Note that because a GET request is used, the signature field is not present. This overrides the default behavior in TAXII.

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

5.2.2 TAXII Feed Information Request

This specification represents the Feed Information Request message using HTTP mechanisms. Other message bindings MUST NOT be used.

Request Method: GET
Query Parameters:

- message_type - Required. MUST be 'feed_information_request'. This field is case insensitive.
- message_id - Required. MUST be a string. This field is case sensitive.

Note that because a GET request is used, the signature field is not present. This overrides the default behavior in TAXII.

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

5.2.3 TAXII Manage Feed Subscription Request

Request Method: POST
Query 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.

5.2.4 TAXII Poll Request

Request Method: GET
Query Parameters:

- message_type - Required. MUST be 'poll_request'. This field is case insensitive.
- message_id - Required. MUST be a string. This field is case sensitive.
- feed_name - Required. MUST be a string. This field is case sensitive.
- exclusive_begin_timestamp -Optional. MUST be a Timestamp Label. Absence of this field indicates that there is no lower bound to the request.
- inclusive_end_timestamp - Optional. MUST be a Timestamp Label. Absence of this field indicates that there is no upper bound to the request.

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

- subscription_id - Optional. MUST be a string. This field is case sensitive.
- payload_binding - Optional. MUST be a single value or a comma-separated list of valid Payload Binding IDs. Absence of this field indicates that all payload bindings are accepted.
  Note: Recall that, per Section 2.1 of URI Generic Syntax, commas not used as delimiters must be percent encoded. (The RFC requires that values used as delimiters within a component must percent encoded.)

Note that because a GET request is used, the signature field is not present. This overrides the default behavior in TAXII.

Entity-Body: 0-length

5.2.5 TAXII Inbox Message

Request Method: POST
Query Parameters: None

Entity-Body: Contains a valid TAXII Inbox Message as defined by the TAXII Message Binding identified in the X-TAXII-Content-Type header.

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.

6.3 Status Codes

This section defines the usage of HTTP Status Codes in TAXII communications. HTTP status codes are used in accordance with HTTP/1.1; extensions and points of possible confusion are noted and clarified below.

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

HTTP 200 (OK) - This status code is 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. All responses that contain a TAXII Message (with the exception of TAXII Status Messages with a status other than 'Success') MUST use an HTTP 200 Status Code.

HTTP 406 (Not Acceptable) - In addition to the usage specified in HTTP/1.1, 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 X-TAXII-Accept header fields (if present).

HTTP 415 (Unsupported Media Type) - In addition to the usage specified in HTTP/1.1, this status code SHOULD be used when the X-TAXII-Content-Type header field specifies a TAXII Version-Binding Type that the server cannot process.

For HTTP Responses with a Status Code other than HTTP 200, a TAXII Status Message MAY be present in the message body. Clients receiving an HTTP Response with a Status Code other than 200 SHOULD attempt to process the response in the following manner:

1. If the X-TAXII-Content-Type header is present and contains a supported Message Binding Version ID, attempt to process the TAXII Message in the message body.
2. Otherwise, attempt to recover by creating a TAXII Status Message in a supported format with the following properties:
    - Status = Looked up from Table 2 - Status Code Mapping.
    - Message = All or part of the HTTP Response, escaped as necessary for the desired message binding. Implementations SHOULD include as must of the HTTP Response as possible.

Table 2 - Status Code Mapping

HTTP Status Code	TAXII Status Type
406 - Not Acceptable	Unsupported Message Binding
415 - Unsupported Media Type	Unsupported Message Binding
All other status codes	Failure

As an informational note, TAXII Clients should anticipate encountering any number of proxies, gateways, firewalls, and other internet infrastructure components that are not TAXII-aware and do not communicate in a TAXII conformant manner. Specifically, TLS handshakes will (for the foreseeable future) not provide TAXII Status Messages upon failure. Therefore, it is important for TAXII Clients to recover gracefully from communications with TAXII-unaware infrastructure.

7 Security Considerations

This section identifies scenarios that developers may wish to consider when developing TAXII Clients and Servers. Each scenario describes the security mechanisms used, as well as the information assurance properties of each. In the context of this section, a security mechanism is something that establishes the

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

identity of an endpoint, the encryption and/or integrity protection of the communication channel, or both.

When developing a TAXII Client or Server, it is recommended to support at least one of the scenarios listed in this section.

7.1 HTTP

In this scenario, there is no guarantee of information assurance. Information is not encrypted, and the client and server are not able to identify or authenticate each other. Clients and servers are unable to detect man in the middle attacks.

7.2 HTTP Authentication with HTTPS

In this scenario, the server TLS Certificate and associated TLS handshake convey the server's identity to the client. HTTP Authentication mechanisms (e.g., Digest) are used to convey credentials to the server, which can be used for authentication and authorization purposes.

7.3 TLS Mutual Authentication with HTTPS

In this scenario, the client and server TLS Certificates and associated TLS handshake provide identification and authentication credentials to each other.

8 Recommended Configurations

This section contains recommended configurations for use when deploying TAXII Services. Recommended configurations are not requirements, and implementers may choose whether or not to use them.

Recommended Discovery Service Location

TAXII Servers offering one or more Discovery Services are recommended to use http://example.com/TaxiiDiscoveryService/ (with example.com being replaced with your domain) to offer at least one of the Discovery Services.

Recommended Ports

TAXII Servers using HTTP are recommended to listen on port 80.
TAXII Servers using HTTPS are recommended to listen on port 443.

Recommended Security Consideration

TAXII Clients and Servers are recommended to be compatible with the scenario described in Section 7.3.

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

9 Development

TAXII and its component specifications are expected to continue to evolve based on user needs. Feedback, suggestions, and comments with regard to this or any of the other TAXII specifications are welcome. The TAXII web site (http://taxii.mitre.org/) contains the latest news and resources with regard to TAXII, including the latest version of all TAXII specifications. There is also a mailing list for the discussion of the specifications and where users can pose questions. Interested parties can sign up for this mailing list via the TAXII web site (http://taxii.mitre.org/community/registration.html). Finally, there is also a repository on GitHub.com (https://github.com/TAXIIProject/). This site will host code development efforts as well as modified versions of the TAXII specifications with changes that may be included in future releases of TAXII.

Users of TAXII are encouraged to make use of these resources, both to empower their own use of TAXII and to provide feedback that will help TAXII evolve to meet the needs of its users.

10 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] 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.

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

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

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

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

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

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

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

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

[10] 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.

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

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

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

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

[15] 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.