

THE MITRE CORPORATION

The TAXII HTTP Protocol Binding Specification

Version 1.0

Mark Davidson, Charles Schmidt

4/30/2013

The Trusted Automated eXchange of Indicator Information (TAXII™) specifies mechanisms for exchanging structured cyber threat information between parties over the network. This document describes how to use HTTP to convey TAXII Messages as part of a TAXII Message Exchange.

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

Feedback on this or any of the other TAXII specifications is welcome and can be sent to taxii-discussion-list@lists.mitre.org after signing up on the community registration page (<http://taxii.mitre.org/community/registration.html>).

Comments, questions, suggestions, and concerns are all appreciated.

Table of Contents

Trademark Information.....	1
Feedback	1
1 Introduction	3
1.1 The TAXII HTTP Protocol Binding Specification.....	3
1.1.1 Conformance to HTTP/1.1	3
1.1.2 TAXII Protocol Version ID for HTTP and HTTPS.....	3
1.2 Document Conventions	3
2 TAXII HTTP Headers.....	3
2.1.1 Accept	4
2.1.2 Content-Type	4
2.1.3 X-TAXII-Accept.....	5
2.1.4 X-TAXII-Content-Type.....	5
2.1.5 X-TAXII-Protocol	5
2.1.6 X-TAXII-Services.....	6
3 HTTP Requests	6
4 HTTP Responses.....	6
5 Handling Responses without TAXII Messages.....	7
5.1 HTTP Responses as TAXII Status Messages.....	7
5.2 TLS Alerts as TAXII Status Messages	7
6 Security Considerations	8
6.1 Server Authentication	8
6.2 Client Authentication	8
6.3 Encryption and Integrity Protection	9
7 Recommended Configurations	9
8 Bibliography	10

1 Introduction

The TAXII HTTP Protocol Binding Specification defines requirements for using HTTP/1.1 [1] or HTTP Over TLS [2] to participate in TAXII Message Exchanges (i.e., 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. Readers should familiarize themselves with the TAXII Services Specification and the HTTP/1.1 specification (RFC 2616) prior to reading this document.

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 TAXII Messages support are discussed in detail in the TAXII Services Specification [3].

1.1.1 Conformance to HTTP/1.1

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

1.1.2 TAXII Protocol Version ID for HTTP and HTTPS

This specification defines two TAXII Protocol Version IDs, one for HTTP and one for HTTPS (HTTP Over TLS). These two Version IDs are provided to disambiguate between TAXII Services that support HTTP and those that support HTTPS.

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

`urn:taxii.mitre.org:protocol:http:1.0`

and

`urn:taxii.mitre.org:protocol:https:1.0`

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. [4]

2 TAXII HTTP Headers

This section defines requirements for TAXII HTTP Headers. The term TAXII HTTP Headers refers to 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.

Table 1 provides a list of the TAXII HTTP Headers and a brief description of each.

Table 1 - HTTP Headers

Header	Description
Accept	Specifies which HTTP Media Types the requestor accepts in response.
Content-Type	Specifies the HTTP Media Type in which the entity body is formatted.
X-TAXII-Accept	Specifies which TAXII Message Bindings the requestor accepts in response.
X-TAXII-Content-Type	Specifies the TAXII Message Binding in which the entity body is formatted.
X-TAXII-Protocol	Specifies which TAXII Protocol Binding is used for this message.
X-TAXII-Services	Specifies the version of the TAXII Services Specification to which this message conforms.

2.1.1 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, if present, follows the guidance in HTTP/1.1 with the following restrictions:

1. All media-ranges MUST have a type of 'application'
2. All media-ranges SHOULD have a subtype that is defined in the MIME Media Types IANA Table [5] as an application subtype.
3. If the X-TAXII-Accept header (described in Section 2.1.3) is present, the subtype of each media-range MUST agree with at least one X-TAXII-Accept header value. For example, a subtype of 'xml' agrees with the X-TAXII-Accept value of 'urn:taxii.mitre.org:message:xml:1.0' (which indicates the TAXII XML Message Binding 1.0).

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

2.1.2 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, if present, 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 [5] as an application subtype.
3. If the X-TAXII-Content-Type (defined in Section 2.1.4) header is present, the media-range subtype MUST agree with the X-TAXII-Content-Type header value. For example, a subtype of 'xml' agrees with the X-TAXII-Content-Type of 'urn:taxii.mitre.org:message:xml:1.0' (which indicates the TAXII XML Message Binding 1.0).

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

2.1.3 X-TAXII-Accept

X-TAXII-Accept header is similar to the Accept header in that it identifies the acceptable formats of the response, but instead of using the MIME Media Type table this field identifies acceptable TAXII Message Bindings for responses to this message.

If the X-TAXII-Accept header is absent, it is assumed the client accepts all TAXII Message Bindings.

The X-TAXII-Accept header, if present, MUST contain one or more TAXII Message Binding Version IDs. The X-TAXII-Accept header MAY contain multiple Version IDs to indicate that multiple TAXII Message Bindings are acceptable. Multiple Version IDs are separated by a space (e.g., 'AcceptFormat1 AcceptFormat2').

TAXII Message Binding Version IDs are listed in order of preference with the leftmost TAXII Message Binding Version ID indicating the most preferred binding.

HTTP Requests sent as part of a TAXII Message Exchange SHOULD have an X-TAXII-Accept header. HTTP Responses sent as a part of a TAXII Message Exchange SHOULD NOT have an X-TAXII-Accept header. If an X-TAXII-Accept header is present in an HTTP Response, it SHOULD be ignored.

2.1.4 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 identifies the TAXII Message Binding of the contents of the entity-body.

The X-TAXII-Content-Type header MUST contain a valid TAXII Message Binding Version ID.

TAXII conformant senders MUST include the X-TAXII-Content-Type header when the entity body contains a TAXII Message. Conversely, if the X-TAXII-Content-Type header is not present in an HTTP Message, the recipient can assume that the message does not contain a TAXII Message.

2.1.5 X-TAXII-Protocol

The X-TAXII-Protocol header is used to specify to which TAXII Protocol Binding the HTTP Message conforms, indicating whether an HTTP or HTTPS Protocol Binding is being used as well as the version of that binding.

The value of the X-TAXII-Protocol header MUST be a TAXII Protocol Binding Version ID.

TAXII conformant senders MUST include the X-TAXII-Protocol header when the entity body contains a TAXII Message. Conversely, if the X-TAXII-Protocol header is not present in an HTTP Message, the recipient can assume that the message does not contain a TAXII Message.

The value of the X-TAXII-Protocol header MUST agree with the protocol being used. An example of the X-TAXII-Protocol header agreeing with the protocol being used is 'urn:taxii.mitre.org:protocol:https:1.0' being used with HTTPS.

2.1.6 X-TAXII-Services

The X-TAXII-Services header is used to specify the version of the TAXII Services Specification to which this HTTP Request conforms.

The value of the X-TAXII-Services header MUST be a TAXII Services Version ID.

TAXII conformant senders MUST include the X-TAXII-Services header when the entity body contains a TAXII Message. Conversely, if the X-TAXII-Services header is not present in an HTTP Message, the recipient can assume that the message does not contain a TAXII Message.

3 HTTP Requests

This section defines requirements for HTTP Requests that are sent as part of a TAXII Message Exchange.

HTTP Requests sent as part of a TAXII Message Exchange MUST:

1. Adhere to the requirements for TAXII HTTP Headers as described in Section 2.
2. Use a request method of POST.
3. Contain a TAXII Message in the entity body.

HTTP Requests sent as part of a TAXII Message Exchange MAY include URI Query Parameters . This specification does not govern the use of Query Parameters in TAXII Message Exchanges.

4 HTTP Responses

This section defines requirements for HTTP Responses that are sent as a part of a TAXII Message Exchange.

HTTP Responses sent from a TAXII conformant entity as a part of a TAXII Message Exchange MUST:

1. Adhere to the requirements for TAXII HTTP Headers as described in Section 2.
2. Contain a TAXII Message in the entity body whenever the HTTP Status Code is 200.

TAXII Architectures SHOULD respond to error conditions by using a TAXII Status Message with an appropriate Status Type whenever possible. In this case, the Status Message is returned to the requester in an HTTP Response with HTTP Status Code 200. In some cases it might be infeasible to express an error condition using a TAXII Status Message, either because the error condition occurs before the

involvement of TAXII-aware components of the Architecture or because TAXII Status Types do not reflect the error condition with sufficient accuracy. In these cases, it is acceptable for a TAXII Architecture to respond using an HTTP Status Code that reflects the error condition. If the HTTP Status Code is not 200, HTTP Responses sent as part of a TAXII Message Exchange MAY include a TAXII Status Message in order to provide additional detail to the recipient.

5 Handling Responses without TAXII Messages

In certain circumstances, TAXII clients might encounter responses that do not contain TAXII Messages. For example, an error might be generated by some non-TAXII aware component such as a web proxy. However, TAXII Architectures generally expect a TAXII Message in response to their requests. In order to ensure such expectations are met, this section outlines procedures for converting responses that do not contain a TAXII Message and mapping them to TAXII Messages. TAXII clients SHOULD be able to handle responses that do not contain a TAXII Message.

5.1 HTTP Responses as TAXII Status Messages

This section defines rules for interpreting an HTTP Response as a TAXII Status Message. Treat the HTTP Response as being equivalent to a TAXII Status Message with the following properties:

- Status = Use the appropriate TAXII Status Type as identified in Table 2.
- Message = The HTTP Response.

Table 2 - HTTP Status Code Mapping

HTTP Status Code	TAXII Status Type
400 - Bad Request	Bad Message
401 - Unauthorized	Unauthorized
403 - Forbidden	Unauthorized
406 - Not Acceptable	Unsupported Message Binding
407 - Proxy Authentication Required	Unauthorized
413 - Request Entity Too Large	Bad Message
415 - Unsupported Media Type	Unsupported Message Binding
All other Status Codes	Failure

Note that HTTP Status Codes are mapped from HTTP/1.1 Section 6.1.1.

5.2 TLS Alerts as TAXII Status Messages

If TLS is used, problems with the TLS handshake or connection are indicated using a TLS Alert Protocol Record. This section defines rules for interpreting a TLS Alert Protocol Record as a TAXII Status Message. Treat a TLS Alert Protocol Record as being equivalent to a TAXII Status Message with the following properties:

- Status = Use the appropriate TAXII Status Type as identified in Table 3.
- Message = The TLS Alert, represented as a hexadecimal string.

Table 3 - TLS Alert Type Mapping

TLS Alert Description	TAXII Status Type
40 - Handshake Failure	Unauthorized
41 - No Certificate	Unauthorized
42 - Bad Certificate	Unauthorized
43 - Unsupported Certificate	Unauthorized
48 - Unknown CA	Unauthorized
49 - Access Denied	Unauthorized
All other codes	Failure

Note that TLS Alert Levels are mapped from TLS 1.2 [6] Section 7.2.

6 Security Considerations

As noted in the TAXII Services Specification, TAXII Messages do not convey authentication information and instead rely upon protocols for this capability. In addition, while TAXII Messages support encryption of content, they rely on network-level encryption to protect the entire TAXII Message in transit.

Different communities might have different security requirements and capabilities. For this reason, this specification does not require the use of a particular authentication or encryption mechanism. Instead, this specification looks at the authentication and encryption mechanisms supported by HTTP and HTTPS, allowing individual enterprises to select the mechanism that best matches their needs and capabilities.

6.1 Server Authentication

Server authentication is not supported under the HTTP protocol.

Server authentication is supported by the HTTPS protocol. Specifically, as part of the TLS handshake that precedes the exchange of HTTP messages, the server supplies an identifying certificate. In order to authenticate the server, the client needs to verify that the certificate is intact, signed by a trusted party, and that it represents the intended server identity.

6.2 Client Authentication

Client authentication can be supported over both HTTP and HTTPS through the use of HTTP authentication mechanisms. There are many types of HTTP authentication mechanisms supported by modern web servers. It is important to note that sending authentication credentials over HTTP (rather than HTTPS) leaves those credentials open to compromise. As such, HTTP authentication using unencrypted HTTP messages is strongly discouraged. Servers can verify client identity by comparing the provided credentials against pre-populated values.

Client authentication can also be supported over HTTPS through TLS mutual authentication. In this case, the server requests that the client provide a cryptographic certificate identifying itself. The server can then use this certificate to authenticate the client using the same procedures described under server authentication.

6.3 Encryption and Integrity Protection

Encryption and integrity protection are not provided under the HTTP protocol.

Encryption and integrity protection are provided under HTTPS through the use of TLS. TLS can support a range of encryption suites - servers need to select appropriate cryptographic suites based on their security requirements.

7 Recommended Configurations

This section contains recommended configurations for use when deploying TAXII Services. These recommendations exist to promote interoperability between implementations.

Recommended Discovery Service Location

TAXII Servers offering one or more Discovery Services are recommended to use the following format to determine the location of at least one discovery service:

Discovery Service URL = "http://" + your domain + "/taxii-discovery-service/"

Example: `http://example.com/TaxiiDiscoveryService/`

Recommended Ports

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

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

8 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] The MITRE Corp., "The TAXII Services Specification 1.0," The MITRE Corp., 2013.
- [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] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," The Internet Engineering Task Force, 2008.