TAXII[™] Version 1.1.1. Part 3: HTTP Protocol Binding

Committee Specification Draft 01 / Public Review Draft 01

06 November 2015

Specification URIs

This version:

http://docs.oasis-open.org/cti/taxii/v1.1.1/csprd01/part3-http/taxii-v1.1.1-csprd01-part3-http.docx (Authoritative)
http://docs.oasis-open.org/cti/taxii/v1.1.1/csprd01/part3-http/taxii-v1.1.1-csprd01-part3-http.html
http://docs.oasis-open.org/cti/taxii/v1.1.1/csprd01/part3-http/taxii-v1.1.1-csprd01-part3-http.pdf

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part3-http.docx (Authoritative)
http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part3-http.html
http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part3-http.pdf

Technical Committee:

OASIS Cyber Threat Intelligence (CTI) TC

Chair:

Richard Struse (Richard.Struse@hq.dhs.gov), DHS Office of Cybersecurity and Communications (CS&C)

Editors:

Mark Davidson (mdavidson@mitre.org), MITRE Corporation
Charles Schmidt (cmschmidt@mitre.org), MITRE Corporation
Bret Jordan (bret.jordan@bluecoat.com), Blue Coat Systems, Inc.

Additional artifacts:

This prose specification is one component of a Work Product that also includes:

- *TAXII Version 1.1.1. Part 1: Overview*. http://docs.oasis-open.org/cti/taxii/v1.1.1/csprd01/part1-overview/taxii-v1.1.1-csprd01-part1-overview.html
- *TAXII Version 1.1.1. Part 2: Services*. http://docs.oasis-open.org/cti/taxii/v1.1.1/csprd01/part2-services/taxii-v1.1.1-csprd01-part2-services.html
- *TAXII Version 1.1.1. Part 3: HTTP Protocol Binding* (this document). http://docs.oasis-open.org/cti/taxii/v1.1.1/csprd01/part3-http/taxii-v1.1.1-csprd01-part3-http.html
- *TAXII Version 1.1.1. Part 4: XML Message Binding*. http://docs.oasis-open.org/cti/taxii/v1.1.1/csprd01/part4-xml/taxii-v1.1.1-csprd01-part4-xml.html
- *TAXII Version 1.1.1. Part 5: Default Query*. http://docs.oasis-open.org/cti/taxii/v1.1.1/csprd01/part5-query/taxii-v1.1.1-csprd01-part5-query.html
- XML schemas: http://docs.oasis-open.org/cti/taxii/v1.1.1/csprd01/schemas/

Related work:

This specification replaces or supersedes:

- *The TAXII HTTP Protocol Binding Specification Version 1.0*. http://taxiiproject.github.io/releases/1.0/TAXII_HTTPProtocolBinding_Specification.pdf.

This specification is related to:

- *TAXII Content Binding Reference.* http://taxiiproject.github.io/releases/1.1/TAXII_ContentBinding_Reference_v3.pdf

Declared XML namespaces:

- http://docs.oasis-open.org/cti/ns/taxii/xml/binding-1.1.1
- http://docs.oasis-open.org/cti/ns/taxii/default-query-1.1.1

Abstract:

This document describes HTTP Protocol Binding.

Status:

This document was last revised or approved by the OASIS Cyber Threat Intelligence (CTI) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti#technical.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://www.oasis-open.org/committees/cti/.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/cti/ipr.php).

Citation format:

When referencing this specification the following citation format should be used:

[TAXII-v1.1.1-HTTP]

TAXII[™] Version 1.1.1. Part 3: HTTP Protocol Binding. Edited by Mark Davidson, Charles Schmidt, and Bret Jordan. 06 November 2015. OASIS Committee Specification Draft 01 / Public Review Draft 01. http://docs.oasis-open.org/cti/taxii/v1.1.1/csprd01/part3-http/taxii-v1.1.1-csprd01-part3-http.html. Latest version: http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part3-http.html.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

STIX[™], TAXII[™], AND CybOX[™] (STANDARD OR STANDARDS) AND THEIR COMPONENT PARTS ARE PROVIDED “AS IS” WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY THAT THESE STANDARDS OR ANY OF THEIR COMPONENT PARTS WILL CONFORM TO SPECIFICATIONS, ANY

IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR FREEDOM FROM INFRINGEMENT, ANY WARRANTY THAT THE STANDARDS OR THEIR COMPONENT PARTS WILL BE ERROR FREE, OR ANY WARRANTY THAT THE DOCUMENTATION, IF PROVIDED, WILL CONFORM TO THE STANDARDS OR THEIR COMPONENT PARTS. IN NO EVENT SHALL THE UNITED STATES GOVERNMENT OR ITS CONTRACTORS OR SUBCONTRACTORS BE LIABLE FOR ANY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF, RESULTING FROM, OR IN ANY WAY CONNECTED WITH THESE STANDARDS OR THEIR COMPONENT PARTS OR ANY PROVIDED DOCUMENTATION, WHETHER OR NOT BASED UPON WARRANTY, CONTRACT, TORT, OR OTHERWISE, WHETHER OR NOT INJURY WAS SUSTAINED BY PERSONS OR PROPERTY OR OTHERWISE, AND WHETHER OR NOT LOSS WAS SUSTAINED FROM, OR AROSE OUT OF THE RESULTS OF, OR USE OF, THE STANDARDS, THEIR COMPONENT PARTS, AND ANY PROVIDED DOCUMENTATION. THE UNITED STATES GOVERNMENT DISCLAIMS ALL WARRANTIES AND LIABILITIES REGARDING THE STANDARDS OR THEIR COMPONENT PARTS ATTRIBUTABLE TO ANY THIRD PARTY, IF PRESENT IN THE STANDARDS OR THEIR COMPONENT PARTS AND DISTRIBUTES IT OR THEM “AS IS.”

Table of Contents

1 Introduction

The TAXII[™] HTTP Protocol Binding Specification defines requirements for using HTTP/1.1 or HTTP Over TLS **[RFC5246]** 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**[RFC2616]** 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.

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 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:oasis:cti:taxii:http:1.1.1`

and

`urn:oasis:cti:taxii:https:1.1.1`

1.2 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in **[RFC2119]**.

1.3 Normative References

[Fielding, 1999] 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.

[RFC2818] E. Rescorla, " HTTP Over TLS", RFC 2818, May 2000. https://tools.ietf.org/html/rfc2818

[RFC2616] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners-Lee, “Hypertext Transfer Protocol -- HTTP/1.1”, May 2000. https://www.ietf.org/rfc/rfc2616.txt

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

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

[RFC5246] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008. https://tools.ietf.org/html/rfc5246

2 TAXII[™] HTTP Header

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 (Internet Assigned Numbers Authority 2006) 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:oasis:cti:taxii:xml-1.1.1' (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 **[IANA, 2006]** 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:oasis:cti:taxii:xml-1.1.1' (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:oasis:cti:taxii:https:1.1.1' 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 **[RFC5246]** 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/taxii-discovery-service//

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 Conformance

Implementations have discretion over which parts of TAXII they implement (e.g., Discovery Service).

Conformant implementations must conform to all Normative Statements that apply to the portions of TAXII they implement (e.g., Implementers of the Discovery Service must conform to all Normative Statements regarding the Discovery Service).

Conformant implementations are free to ignore Normative Statements that do not apply to the portions of TAXII they implement (e.g., Non-implementers of the Discovery Service are free to ignore all Normative Statements regarding the Discovery Service).

The conformance section of this document is intentionally broad and attempts to reiterate what already exists in this document. The TAXII 1.1 Specifications, which this specification is based on, did not have a conformance section. Instead, the TAXII 1.1 Specifications relied on normative text. TAXII 1.1.1 represents a minimal change from TAXII 1.1, and in that spirit no new requirements have been defined in this document.

Appendix A. Acknowledgments

The individuals listed in this specification have participated in the creation of this specification and are gratefully acknowledged.

Authors of initial MITRE TAXII Specifications:

Mark Davidson, MITRE

Charles Schmidt, MITRE

Participants:

The following individuals were members of the OASIS CTI Technical Committee during the creation of this specification and their contributions are gratefully acknowledged:

- David Crawford, Aetna
- Joerg Eschweiler, Airbus Group SAS
- Marcos Orallo, Airbus Group SAS
- Roman Fiedler, AIT Austrian Institute of Technology
- Florian Skopik, AIT Austrian Institute of Technology
- Dean Thompson, Australia and New Zealand Banking Group (ANZ Bank)
- Alexander Foley, Bank of America
- Yogesh Mudgal, Bloomberg
- Owen Johnson, Blue Coat Systems, Inc.
- Bret Jordan, Blue Coat Systems, Inc.
- Adnan Baykal, Center for Internet Security (CIS)
- Ron Davidson, Check Point Software Technologies
- David McGrew, Cisco Systems
- Pavan Reddy, Cisco Systems
- Omar Santos, Cisco Systems
- Jyoti Verma, Cisco Systems
- Liron Schiff, Comilion (mobile) Ltd.
- Guy Wertheim, Comilion (mobile) Ltd.
- Doug DePeppe, Cyber Threat Intelligence Network, Inc. (CTIN)
- Jane Ginn, Cyber Threat Intelligence Network, Inc. (CTIN)
- Ben Othman, Cyber Threat Intelligence Network, Inc. (CTIN)
- Jeff Williams, Dell
- Richard Struse, DHS Office of Cybersecurity and Communications (CS&C)
- Marlon Taylor, DHS Office of Cybersecurity and Communications (CS&C)
- Dan Brown, DTCC
- Gordon Hundley, DTCC
- Chris Koutras, DTCC
- Robert Griffin, EMC
- Jeff Odom, EMC
- Ravi Sharda, EMC
- David Eilken, Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Sarah Brown, Fox-IT
- Ryusuke Masuoka, Fujitsu Limited
- Eric Burger, Georgetown University
- Peter Allor, IBM
- Eldan Ben-Haim, IBM
- Peter Clark, IBM
- Sandra Hernandez, IBM

- Jason Keirstead, IBM
- John Morris, IBM
- Arvid Van Essche, IBM
- Ron Williams, IBM
- Paul Martini, iboss, Inc.
- Chris Richardson, IID
- Jerome Athias, Individual
- Peter Brown, Individual
- Elysa Jones, Individual
- Sanjiv Kalkar, Individual
- Bar Lockwood, Individual
- Terry MacDonald, Individual
- Alex Pinto, Individual
- Michael Schwartz, Individual
- Patrick Maroney, Integrated Networking Technologies, Inc.
- Andres More, Intel Corporation
- Wouter Bolsterlee, Intelworks BV
- Marko Dragoljevic, Intelworks BV
- Joep Gommers, Intelworks BV
- Sergey Polzunov, Intelworks BV
- Rutger Prins, Intelworks BV
- Andrei Sîrghi, Intelworks BV
- Raymon van der Velde, Intelworks BV
- Niels van Dijk, Intelworks BV
- Robert Huber, iSIGHT Partners, Inc.
- Ben Huguenin, Johns Hopkins University Applied Physics Laboratory
- Mark Moss, Johns Hopkins University Applied Physics Laboratory
- Pamela Smith, Johns Hopkins University Applied Physics Laboratory
- Terrence Driscoll, JPMorgan Chase Bank, N.A.
- David Laurance, JPMorgan Chase Bank, N.A.
- Brandon Hoffman, Lumeta Corporation
- Jonathan Baker, Mitre Corporation
- Sean Barnum, Mitre Corporation
- Mark Davidson, Mitre Corporation
- Jasen Jacobsen, Mitre Corporation
- Ivan Kirillov, Mitre Corporation
- Jon Salwen, Mitre Corporation
- Charles Schmidt, Mitre Corporation
- John Wunder, Mitre Corporation
- James Cabral, MTG Management Consultants, LLC.
- Scott Algeier, National Council of ISACs (NCI)
- Denise Anderson, National Council of ISACs (NCI)
- Josh Poster, National Council of ISACs (NCI)
- Mike Boyle, National Security Agency
- Jessica Fitzgerald-McKay, National Security Agency
- Takahiro Kakumaru, NEC Corporation
- John-Mark Gurney, New Context Services, Inc.
- Christian Hunt, New Context Services, Inc.
- Daniel Riedel, New Context Services, Inc.
- Andrew Storms, New Context Services, Inc.
- Nat Sakimura, Nomura Research Institute, Ltd. (NRI)
- David Darnell, North American Energy Standards Board
- Cory Casanave, Object Management Group
- Don Thibeau, Open Identity Exchange

- Vishaal Hariprasad, Palo Alto Networks
- John Tolbert, Queralt, Inc.
- Daniel Wyschogrod, Raytheon Company-SAS
- Ted Julian, Resilient Systems, Inc..
- Brian Engle, Retail Cyber Intelligence Sharing Center (R-CISC)
- Igor Baikalov, Securonix
- Bernd Grobauer, Siemens AG
- John Anderson, Soltra
- Aishwarya Asok Kumar, Soltra
- Peter Ayasse, Soltra
- Jeff Beekman, Soltra
- Jonathan Bush, Soltra
- Michael Butt, Soltra
- Cynthia Camacho, Soltra
- Aharon Chernin, Soltra
- Mark Clancy, Soltra
- Brady Cotton, Soltra
- Trey Darley, Soltra
- Paul Dion, Soltra
- Daniel Dye, Soltra
- Brandon Hanes, Soltra
- Robert Hutto, Soltra
- Ali Khan, Soltra
- Chris Kiehl, Soltra
- Michael Pepin, Soltra
- Natalie Suarez, Soltra
- David Waters, Soltra
- Chip Wickenden, Soltra
- Benjamin Yates, Soltra
- Cedric LeRoux, Splunk Inc.
- Brian Luger, Splunk Inc.
- Kathy Wang, Splunk Inc.
- Curtis Kostrosky, Symantec Corp.
- Greg Reaume, TELUS
- Alan Steer, TELUS
- Crystal Hayes, The Boeing Company
- Tyron Miller, Threat Intelligence Pty Ltd
- Andrew van der Stock, Threat Intelligence Pty Ltd
- Andrew Pendergast, ThreatConnect, Inc.
- Jason Spies, ThreatConnect, Inc.
- Nick Keuning, ThreatQuotient, Inc.
- Wei Huang, ThreatStream
- Hugh Njemanze, ThreatStream
- Chris Roblee, TruSTAR Technology
- Mark Angel, U.S. Bank
- Brad Butts, U.S. Bank
- Mona Magathan, U.S. Bank
- Adam Cooper, United Kingdom Cabinet Office
- Mike McLellan, United Kingdom Cabinet Office
- Chris O'Brien, United Kingdom Cabinet Office
- James Penman, United Kingdom Cabinet Office
- Howard Staple, United Kingdom Cabinet Office
- Alastair Treharne, United Kingdom Cabinet Office
- Julian White, United Kingdom Cabinet Office

- Evette Maynard-Noel, US Department of Homeland Security
- Justin Stekervetz, US Department of Homeland Security
- Robert Coderre, VeriSign
- Kyle Maxwell, VeriSign
- Lee Chieffalo, ViaSat, Inc.
- Wilson Figueroa, ViaSat, Inc.
- Anthony Rutkowski, Yaana Technologies, LLC

Special Thanks:

A special thanks to the US Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC), and to Richard Struse, Chief Advanced Technology Officer of the DHS NCCIC. Without your sponsorship, vision, and relentless vigor, none of this would have been possible.

Appendix B. Revision History

Revision	Date	Editor	Changes Made
Working Draft 01	01 July 2015	Bret Jordan	Initial working draft based on MITRE specification