TAXII[™] Version 1.1.1. Part 1: Overview

Committee Specification Draft 01

06 November 2015

Specification URIs

This version:

http://docs.oasis-open.org/cti/taxii/v1.1.1/csd01/part1-overview/taxii-v1.1.1-csd01-part1-overview.docx (Authoritative)
http://docs.oasis-open.org/cti/taxii/v1.1.1/csd01/part1-overview/taxii-v1.1.1-csd01-part1-overview.html
http://docs.oasis-open.org/cti/taxii/v1.1.1/csd01/part1-overview/taxii-v1.1.1-csd01-part1-overview.pdf

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part1-overview.docx (Authoritative)
http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part1-overview.html
http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part1-overview.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* (this document). http://docs.oasis-open.org/cti/taxii/v1.1.1/csd01/part1-overview/taxii-v1.1.1-csd01-part1-overview.html
- *TAXII Version 1.1.1. Part 2: Services*. http://docs.oasis-open.org/cti/taxii/v1.1.1/csd01/part2-services/taxii-v1.1.1-csd01-part2-services.html
- *TAXII Version 1.1.1. Part 3: HTTP Protocol Binding*. http://docs.oasis-open.org/cti/taxii/v1.1.1/csd01/part3-http/taxii-v1.1.1-csd01-part3-http.html
- *TAXII Version 1.1.1. Part 4: XML Message Binding*. http://docs.oasis-open.org/cti/taxii/v1.1.1/csd01/part4-xml/taxii-v1.1.1-csd01-part4-xml.html
- *TAXII Version 1.1.1. Part 5: Default Query*. http://docs.oasis-open.org/cti/taxii/v1.1.1/csd01/part5-query/taxii-v1.1.1-csd01-part5-query.html
- XML schemas: http://docs.oasis-open.org/cti/taxii/v1.1.1/csd01/schemas/

Related work:

This specification replaces or supersedes:

- *TAXII Overview Version 1.1*. http://taxiiproject.github.io/releases/1.1/TAXII_Overview.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 provides an overview of TAXII.

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-Overview]

TAXII[™] Version 1.1.1. Part 1: Overview. Edited by Mark Davidson, Charles Schmidt, and Bret Jordan. 06 November 2015. OASIS Committee Specification Draft 01. http://docs.oasis-open.org/cti/taxii/v1.1.1/csd01/part1-overview/taxii-v1.1.1-csd01-part1-overview.html. Latest version: http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part1-overview.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

Trusted Automated eXchange of Indicator Information (TAXII [™]) defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols and messages to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not an information sharing initiative or application and 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.

1.1 Scope

This section describes the scope of TAXII by illustrating the spectrum of information sharing models TAXII supports. TAXII's scope includes, but is not limited to, the following information sharing models, as well as variants and combinations of the sharing models.

Hub and Spoke - In a hub and spoke information sharing architecture, one organization acts as a clearinghouse (the hub) for all sharing participants (the spokes). A spoke shares information with the hub, which then re-shares this information with all other spokes. The hub may perform analytics or filtering before re-sharing information. In this architecture, information may flow from spoke to hub and from hub to spoke.

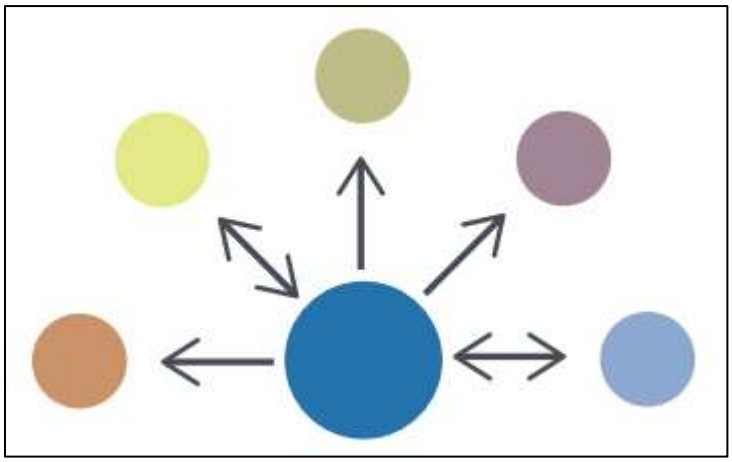

Figure 1 - Hub and Spoke Diagram

Source/Subscriber - In a source/subscriber information sharing architecture, one organization acts as a single source of information for all subscribers. In this architecture, information flows from the source to a subscriber.

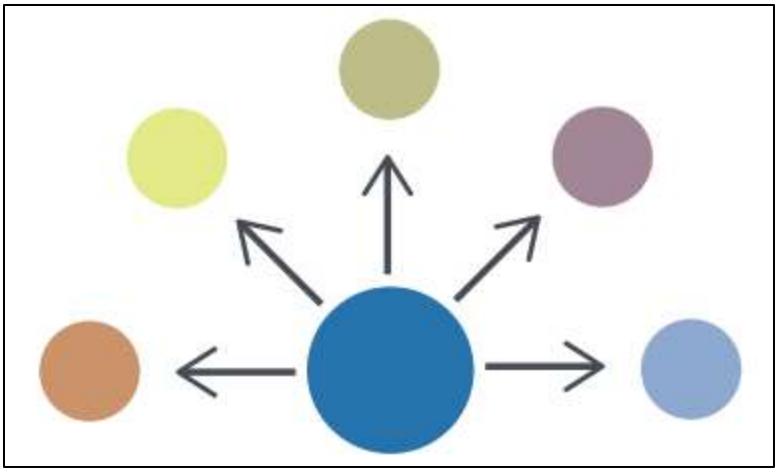

Figure 2 - Source/Subscriber Diagram

Peer to Peer - In the Peer to Peer information sharing architecture, any number of organizations act as both producers and consumers of information. In this architecture, information flows from one peer to another peer.

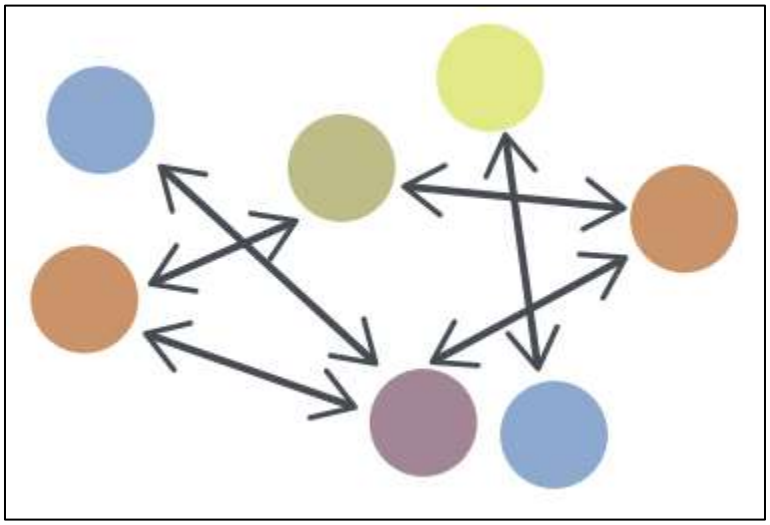

Figure 3 - Peer to Peer Diagram

1.2 TAXII[™] Documents

TAXII is defined by a collection of interrelated documents. This section describes those documents.

TAXII Overview - The TAXII Overview (this document) defines the primary concepts of TAXII, as well as the organization of TAXII component documents.

Services Specification - The Services Specification defines TAXII Services, as well as the information conveyed by TAXII Messages and TAXII Message Exchanges. It provides normative requirements that govern TAXII Services and Message Exchanges.

Message Binding Specification - A Message Binding Specification defines normative requirements for representing TAXII Messages in a particular format (e.g., XML). There may be multiple Message Binding Specifications created for TAXII where each Message Binding Specification defines a binding of TAXII Messages using a different format.

Protocol Binding Specification - A Protocol Binding Specification defines normative requirements for transporting TAXII Messages over some network protocol (e.g., HTTP). There may be multiple Protocol Binding Specifications created for TAXII where each Protocol Binding Specification defines requirements for transporting TAXII Messages using a different network protocol.

Query Format Specification - A Query Format Specification defines a query format that can be used to define query expressions that are used within TAXII Messages to provide characteristics against which content records are compared. Query Expressions allow requestors to collect only content that meets these criteria. A Query Format Specification my include how to express the given format in a particular Message Binding, or this may be handled by a separate Message Binding Specification.

Content Binding Reference - The Content Binding Reference is a non-normative document that lists Content Binding IDs for use within TAXII.

Figure 4 shows how these specifications relate to each other.

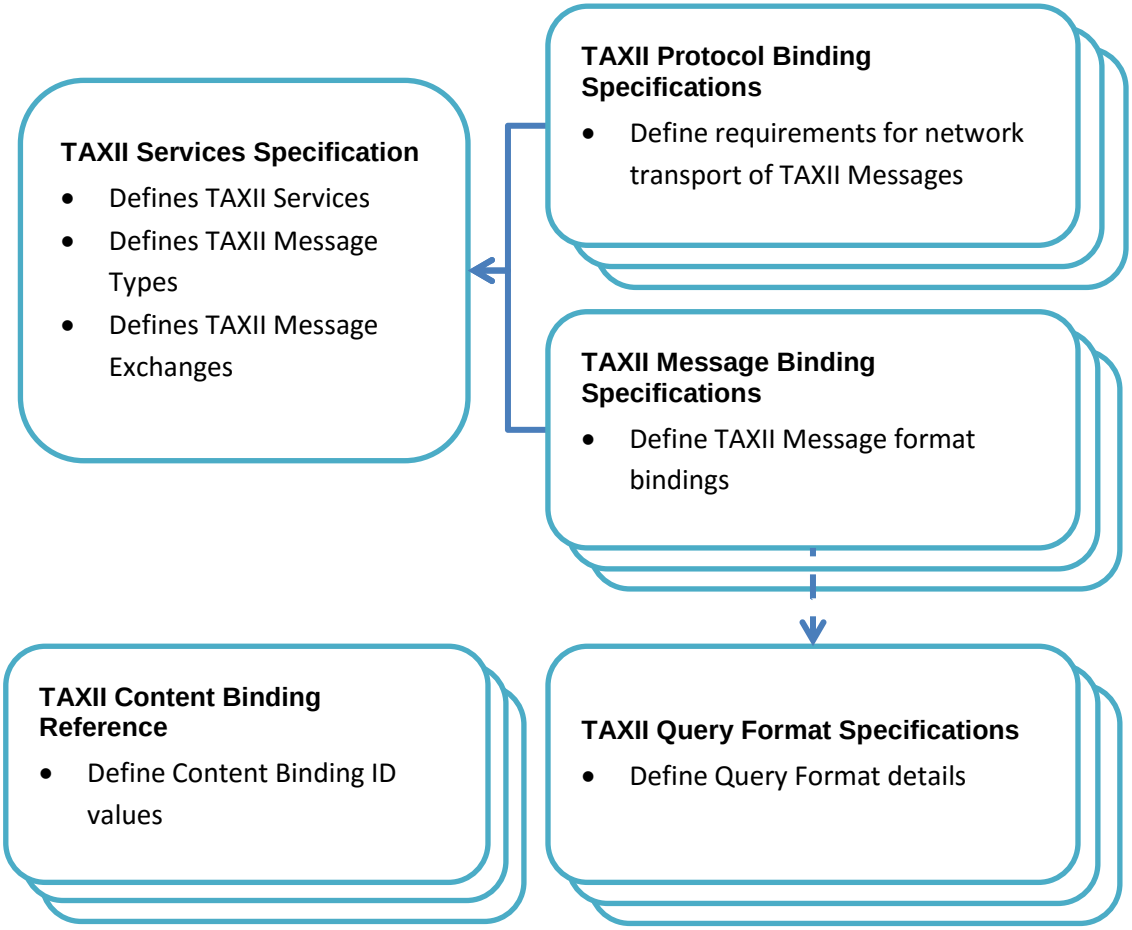

Figure 4 - TAXII[™] Specification Hierarchy

Separation of the TAXII Specifications exists to support flexibility as TAXII evolves. Threat information sharing communities often have specific constraints on the types of network protocols and message formats they are able to support, the types of content they can exchange, and the types of queries their infrastructure can support. Rather than tying TAXII to a specific mechanism that excludes portions of the community, TAXII's core concepts (i.e., its services and exchanges) are defined separately from the implementation details of those concepts. When there is a need for a new binding, it can be created, either as part of a new official release of TAXII or as a third-party extension for TAXII, without affecting TAXII's core components. Groups that use different protocol or message bindings for TAXII will not be able to communicate directly with each other, but because they are still using TAXII Messages and

Services at the core of their communications it is possible to create gateways that will allow interaction to occur.

1.2.1 Suggested Reading Order

For those wishing to become familiar with TAXII, this section suggests reading the TAXII documents in a specific order. The documents build on each other, so following the suggested reading order can make understanding TAXII easier:

1. The TAXII Overview (this document)
2. The TAXII Services Specification
3. Protocol and/or Message Binding Specifications based on requirements to support a given format or protocol
4. Query Format Specifications based on requirements to support a given query model

The Content Binding Reference can simply be consulted as needed to identify appropriate Content Binding ID values. The Content Binding Reference serves as a dictionary of Content Binding IDs and is generally not read beginning-to-end.

1.3 Specification Versioning

Changes to TAXII Specifications that impact content or tools are indicated by either a Major release or a Minor release.

Major release - A major release incorporates changes that require breaking backward compatibility with previous versions or represent fundamental changes to concepts. For a major release, the MAJOR version is incremented by one and the MINOR version is set to zero.

Minor release - A minor release incorporates changes that do not break backward compatibility with previous versions. For a minor release, the MINOR component is incremented by one.

1.4 Terms and Definitions

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

1.4.1 TAXII[™] Roles

TAXII Roles are used to denote participants in TAXII according to their high-level objectives in the use of TAXII Services.

Producer - An entity (e.g., a person, organization, agency, etc.) that is the source of structured cyber threat information.

Consumer - An entity that is the recipient of structured cyber threat information.

Note that these roles are not mutually exclusive - one entity might be both a Consumer and a Producer of structured cyber threat information.

1.4.2 TAXII[™] Functional Units

TAXII functional units represent discrete sets of functionality required to support TAXII. Note that this does not mean that separate software is needed for each functional unit - a single software application could encompass multiple functional units or multiple applications could cooperate to serve as a single functional unit. A functional unit simply represents some component with a well-defined role in TAXII.

TAXII Transfer Agent (TTA) - A network-connected functional unit that sends and/or receives TAXII Messages. A TTA interacts with other TTAs over the network and handles the details of the protocol requirements from one or more TAXII Protocol Binding Specifications. A TTA provides TAXII Messages to

a TAXII Message Handler (defined below) allowing the TAXII Message Handler to be agnostic to the utilized network protocol. By the same token, the TTA can be agnostic as to the content of TAXII Messages, leaving the handling of this information to the TAXII Message Handler.

TAXII Message Handler (TMH) - A functional unit that produces and consumes TAXII Messages. The TMH is responsible for parsing inbound TAXII Messages and constructing outbound TAXII Messages in conformance with one or more TAXII Message Binding Specifications. A TMH interacts with the TTA, which handles the details required to transmit those messages over the network. The TAXII Back-end interacts with the TMH to turn the information from the Back-end 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. This could cover data storage, subscription management, access control decisions, filtering of content prior to dissemination, and other activities. The TAXII specifications provide no requirements on how capabilities are implemented in a TAXII Back-end beyond noting that TAXII Back-ends need to be able to interact with a TMH. Individual implementers and organizations can decide which TAXII Back-end capabilities are necessary given the TAXII Services they wish to support and how they wish to provide this support.

TAXII Architecture - The term TAXII Architecture covers all functional units of a single Producer or Consumer's infrastructure that provide and/or utilize TAXII Services. A TAXII Architecture includes a TTA, a TMH, and a TAXII Back-end. As noted above, implementation details of a TAXII Back-end are outside of the scope of the TAXII specifications.

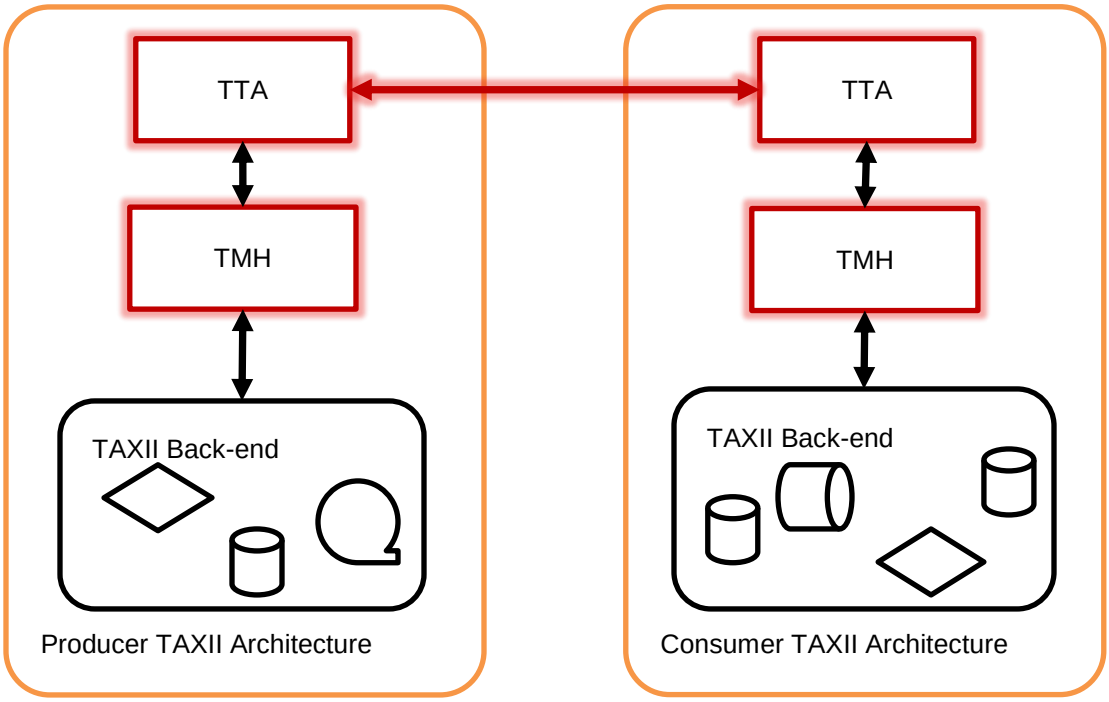

Figure 5 - The Interaction of TAXII[™] Functional Units

Figure 5 shows 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 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 Architectures 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 TAXII Back-ends.

2 TAXII[™] Capabilities

TAXII exists to provide specific capabilities for sharing structured cyber threat information. TAXII Capabilities are the highest level at which TAXII actions can be described. There are three Capabilities that the current version of TAXII supports: push messaging, pull messaging, and discovery.

2.1 Push Messaging

Structured cyber threat information can be pushed from a Producer to a Consumer. This can reflect a pre-existing relationship between the Producer and Consumer, where the Consumer has requested to receive periodic content pushes from the Producer. On the other end of the spectrum, push messaging can be used in a case where a Consumer is willing to accept contributions from any party and any Producer can volunteer content at any time without any pre-existing relationship. An example of the former is a Consumer who subscribed to a Producer's data feed, while an example of the latter is a Consumer that is acting as a repository of published information and allows anyone to volunteer data.

2.2 Pull Messaging

A Consumer can request to pull structured cyber threat information from a Producer. This not only allows the Consumer to control when it receives cyber threat data, but allows the Consumer to receive data without having to listen for incoming connections. As with push messaging, the Producer and Consumer can have an existing agreement for the Consumer to have access to the Producer's content. Alternately, a Producer can make its information available publicly and any Consumer can contact it requesting the data.

2.3 Discovery

TAXII implementers have a great deal of flexibility in choosing which TAXII Capabilities they support. As noted earlier, TAXII is bound to neither a particular network protocol nor to a particular message binding. In order to facilitate automated communication, TAXII includes the ability to discover the specific TAXII Services a TAXII user (or group of TAXII users) fields, as well as their network address and supported bindings. This does not remove the need for human involvement in the establishment of sharing agreements - sharing agreement negotiation is outside the scope of TAXII. Discovery does, however, allow for the automated exchange of information about which TAXII Capabilities a Producer might support and the technical mechanisms they employ in doing so.

2.4 Query

TAXII Consumers may wish to receive only content that match certain criteria (e.g., pertain to a particular event or mention some specific text). TAXII Query allows Consumers to define criteria that content must match in order to be sent from Producer to Consumer. TAXII Query capabilities are discoverable and can be used with both Push and Pull Messaging.

3 Conformance

In order to claim conformance with TAXII, products and software need to:

1. Be conformant with at least one version of the Services Specification.
2. Be conformant with at least one version of a Message Binding that is compatible with the Services Specification in #1.
3. Be conformant with at least one version of a Protocol Binding that is compatible with the Services Specification in #1.

In all cases either the Version ID associated with a TAXII Binding Specification or the title of the specification can be used to identify particular TAXII bindings when identifying an entity's TAXII conformance.

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