Technical Committee Charter Template

This is a draft proposal. It has not been submitted to or accepted by OASIS Open.

Your feedback is appreciated. Please identify yourself in any comments you add directly to this document (viewable by all) or send feedback privately to tc-admin@oasis-open.org.

Join. If you'd like to participate in this TC and be included as a Founder in the final version of this charter, please contact join@oasis-open.org. Details on TC membership are here.

Section 1: TC Charter

1.a. TC Name

Supply Chain Information Modeling (SCIM)

1.b. Statement of Purpose

The OASIS Supply Chain Information Modeling (SCIM) TC aims to standardize and promote information models about all aspects of supply chains.

An Information Model (IM) defines the essential content of messages used in computing, independently of how those messages are represented (i.e., serialized) for communication or storage. Information models are a means to understand and document the essential information content relevant to a system, application, or protocol exchange without regard to how that information is represented in actual implementations. Having a clear view of the information required provides clarity regarding the goals that the eventual implementation must satisfy.

1.c. Business Benefits

The establishment of information models and associated explanatory materials will benefit a wide array of stakeholders across the software and hardware industries. The key beneficiaries of this work can be broadly categorized into the following groups:

Software and Hardware Vendors: Standardized information models will provide clarity across supply chains reducing the confusion and inefficiencies that result from the various diverse implementations of data exchanges across participants in supply chains. It will help vendors plan their product updates, support, and discontinuation more effectively and transparently, thereby improving customer trust and satisfaction.

Open-Source Maintainers: Both hardware and software open-source maintainers will benefit from standardized supply chain information models, enabling them to make informed decisions about incorporating different software and hardware components into their projects.

End Users and Enterprises: Both individual end users and enterprises that rely heavily on technology for their operations will benefit significantly. They will receive timely and clear information about the products they use, helping them plan upgrades, replacements, or contingency plans in advance, thereby reducing vulnerabilities, disruptions, and potential security risks.

Technology Consultants and Service Providers: Consultants and service providers will be able to offer more accurate advice and support to their clients with access to standardized supply chain information.

Supply Chain Partners: The standardization would increase transparency and predictability in the supply chain, which can help reduce uncertainties and risks, leading to a more secure and resilient supply chain.

Government: Standardization can assist government agencies and regulatory bodies in overseeing the industry more effectively, ensuring that all players comply with the set guidelines, and promoting fair practices.

1.d. Scope

The OASIS Supply Chain Information Modeling (SCIM) TC will:

- Research and survey existing supply chain activities and share with the TC membership. Whenever possible, SCIM TC will reference and reuse existing work.
- Develop and maintain value propositions and use cases for supply chain information modeling.
- Develop and maintain supply chain information model standards about all aspects of supply chains, ensuring their relevance and applicability to current industry needs.
- Develop and maintain conformance supply chain information model standards

- Facilitate interoperability and compatibility across different platforms and industries.
- Promote the widespread adoption of these supply chain information model standards and ensure their broad application to hardware and software from both vendors and open-source maintainers.
- Provide technical expertise and guidance on the application and evolution of these supply chain information model standards.

1.e. Deliverables

The primary deliverables of the OASIS SCIM TC will be:

- Value propositions and use cases:
  - ○ Specifications or Committee Notes to explain why the models are needed and how they will be used
- Supply chain information model standards:
  - ○ One or more comprehensive specifications detailing the information models.
- Implementation Guide(s):
  - ○ One or more Committee Notes guiding stakeholders in implementing the information model(s).
- Open Source Software:
  - ○ One or more software repositories with software, tools, examples, FAQs, and other material supporting awareness and adoption of TC work products

1.f. IPR Mode

The OASIS Supply Chain Information Modeling (SCIM) TC will operate in the Non-Assertion Mode, as described in the OASIS IPR Policy.

1.g. Audience

The anticipated audience for this work includes, but is not limited, to:

- Software and hardware vendors
- Software and hardware open-source maintainers
- Technology consultants

- Business stakeholders reliant on technology products
- International, Federal, and local government organizations
- Regulatory bodies in the software and hardware industries

1.h. Language

The OASIS SCIM TC will conduct its business in English.

Section 2: Additional Information

2.a. Identification of Similar Work

The following are all activities that are adjacent to the proposed work but different from the information modeling of the OASIS SCIM TC.

- CISA SBOM
  o Much useful software supply chain information which will need to be reviewed for value propositions, use cases, and information to be modeled
  o https://www.cisa.gov/sbom

- Common Security Advisory Framework (CSAF)
  o CSAF is the definitive reference for the language which supports creation, update, and interoperable exchange of security advisories as structured information on products, vulnerabilities and the status of impact and remediation among interested parties.
  o SCIM may specify the underlying information model for CSAF. This model may be compared the underlying information model for similar items (e.g., OpenVex, CycloneDX).

- Computing Ecosystem Supply-Chain (CES)
  o CES define blockchain data schemas and ontologies, APIs, and smart contracts that go beyond the current integration with existing suppliers and customers (1 up & 1 down) allowing N-to-N
  o This is ongoing work to be monitored for opportunities for information modeling

- CycloneDX
  o CycloneDX specifies serializations for sharing SBOM and VEX information
  o SCIM may specify the underlying information model for CycloneDX. This model may be compared to the underlying information model for similar items (e.g., OpenVex, CSAF, SPDX).

- ISO/IEC/IEEE 12207:2017
  o Systems and software engineering — Software life cycle processes

- JSON Abstract Data Modeling (JADN)
  o JADN is an information modeling language that SCIM may utilize for specifying information models.

- NTIA Software Transparency
  o Much useful software supply chain information which will need to be reviewed for value propositions, use cases, and information to be modeled
  o https://www.ntia.gov/page/software-bill-materials

- OpenEoX
  o OpenEoX is an initiative aimed at standardizing the way End-of-Life (EOL) and End-of-Support (EOS) information is exchanged within the software and hardware industries.
  o SCIM may specify the underlying information model for OpenEoX.

- OpenVex
  o OpenVEX is an implementation of the Vulnerability Exploitability Exchange (VEX for short) that is designed to be minimal, compliant, interoperable, and embeddable.
  o SCIM may specify the underlying information model for OpenVex.
  o This model may be compared to the underlying information model for similar items (e.g., CSAF, CycloneDX).

- Static Analysis Results Interchange Format (SARIF)
  o SARIF defines a standard format for the output of static analysis tools
  SCIM may specify the underlying information model for SARIF.
  o This model may be compared with similar items, as well how SARIF ties in with other models (e.g. SBOM, VEX)

- System Package Data Exchange (SPDX)
  o SPDX is an implementation of SBOM (Software Bill of Materials) and VEX.
  o SCIM may specify the underlying information model for SPDX. This model may be compared the underlying information model for similar items (e.g., CycloneDX, CSAF, OpenVEX).

- X.st-ssc Security threats of software supply chain
  o ITU SG17 Q4
  o This is ongoing work to be monitored for opportunities for information modeling.

- X.sc-sscti Guidelines on Security Capabilities for Software Supply Chain in the Telecommunications Industry
  o ITU SG17 Q15
  o This is ongoing work to be monitored for opportunities for information modeling.

2.b. First TC Meeting

TBD

2.c. Ongoing Meeting Schedule

Monthly via TBD conferencing application

2.d. TC Proposers

- Altaz Valani, altazv@sonvirco.com
- Bret Jordan, bret.jordan.sdo@gmail.com
- Dave Kemp, NSA, d.kemp@cyber.nsa.gov
- Duncan Sparrell, sFractal Consulting, duncan@sfractal.com (Convenor)
- Jason Keirstead, Cyware, jason.keirstead@cyware.com
- Justin Murphy, CISA, justin.murphy@cisa.dhs.gov
- Jay White, Microsoft, jaywhite@microsoft.com
- Mike Rosa, NSA, mjrosa@cyber.nsa.gov
- Omar Santos, Cisco, osantos@cisco.com
- Vasileios Mavroeidis, University of Oslo, vasileim@ifi.uio.no

2.e. Anticipated Contributions

- https://supplychaininformationmodeling.github.io
- https://supplychaininformationmodeling.org
- https://github.com/oasis-open/openc2-jadn-software/tree/master/Schemas/CycloneDX
- https://github.com/oasis-open/openc2-jadn-software/tree/master/Schemas/Spdx

All of the material in section (2)(a)