

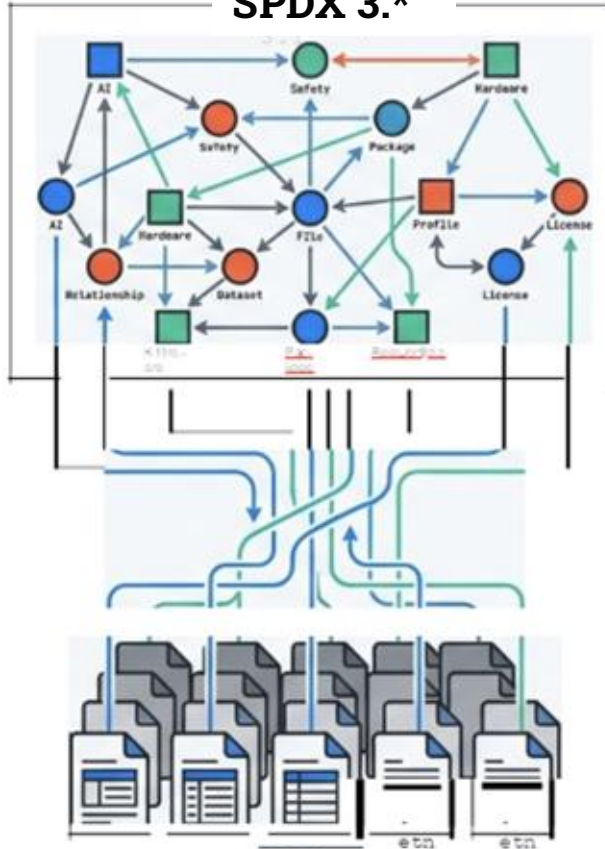
# What's new in SPDX 3.1: Supporting a Living Knowledge Graph

Karen Bennet

Co-chair SPDX AI/Dataset Profile  
AI Expert, Standards Council of Canada  
ISO A SC42, IEEE AI Committees  
30+ Years experience: OSS, AI/ML, Gen AI  
and Agentic AI systems.



## SPDX 3.\*



## SPDX 2.\*



# SPDX v3.1-RC1 Specification

<https://spdx.github.io/spdx-spec/v3.1-RC1/>

**Release Candidate (RC1) is intended for testing and validation.**

Expands beyond describing metadata on software for products, SPDX now supports a knowledge graph for full supply chain for products & systems in critical infrastructure

- **New Profiles:** Safety, Service, Hardware, Supply chain, and Operations
- **Updated Profiles:** Security, AI, Dataset, Software and Core
- **RelationshipType** has grown from 59 to 76 entries
- Introducing **SPDX Vetted Cryptography List** similar to SPDX License List



# Supply Chain behind a modern car ...

## Understanding and Managing SBOMs in Modern Automotive Vehicles: A Journey

Yuichi Kusakabe, Takashi Ninjouji, Honda Motor Co. Ltd.

Linux Foundation Member Summit @Naga 2025

### What is IVI (in-vehicle information) system ?

■ What is IVI (in-vehicle information) system ?  
An infotainment system that connects to the outside of the vehicle, adding communication functionality

The IVI system connects various things and provides "information" and "entertainment"

Linux Foundation Member Summit @Naga 2025

### Efforts in Managing SBOMs within the Supply Chain

#### Addressing resource constraints and workflow integration

Linux Foundation Member Summit @Naga 2025

### About use OSS(SBOM SPDX Lite)

■ We adopted OpenChain's SPOX Lite (Excel) to smoothly share OSS information between companies.

G.2 Format of SPOX Lite

Format: Annex of ISO/IEC 5962 (SPOX 2.2.1), SPOX 2.3

Elements: Annex of ISO/IEC 5962 (SPOX 2.2.1), SPOX 2.3

Component: Package Name, Package Version, Concluded License, Copyright Text, Other elements

Linux Foundation Member Summit @Naga 2025

### Scope of in-house software development

■ Honda: higher level than Hardware Abstraction Layer (HAL)

- Designs custom or new interfaces missing from the AOSP standard
- Minimize Customization to crucial Negative Legacy → Update failure

■ Tier1: HAL and hardware at Tier 1

Optimize division of labor to focus on application development  
Successfully developed an in-house IVI software platform based on AOS

Linux Foundation Member Summit @Naga 2025

### Honda IVI's OSS Usage

OSS Repository 58.9%(799/1,357)

Linux Foundation Member Summit @Naga 2025



**Actors:**

- Organizations
- People

Entire network of **organizations, people, activities, information, and resources** involved in the **life cycle of a product or service from creation to end-of-life.**

**From sourcing inputs and components, through manufacturing and assembly, to storage, distribution, and final delivery to the end user.**

**Lifecycle:**

Sourcing →

Manufacturing →

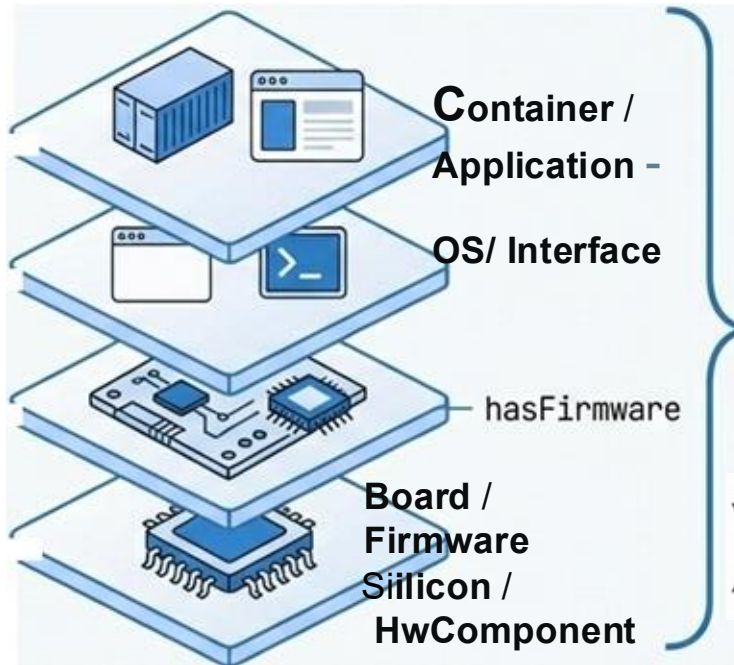
Distributors





**Hardware Bill of Materials (HBOM) and hardware-software co-dependencies.**

Extend SPDX to encompass physical components, their provenance, and their intricate relationships with firmware and software.



**Key Company Contributors**



**BOSCH**



Microsoft

**Honeywell**



.....

**Business context  
(technical and business  
operations) of the system  
such as Import / Export  
Control Classification  
Number and  
Assessments.**

**Key Company Contributors**

 **arm**

 **BOSCH**



 **Deloitte.**

Manage supply chain risks in **cloud-native environments** where traditional package-based SBOMs are insufficient.



- **Service Catalog** - Available services and features
- **Subscription Terms** - Licensing agreements
- **Deployment Config** - Infrastructure as Code (IaC)
- **Usage Metrics** - Resource consumption data
- **Security Posture** - Continuous security monitoring



**Standardized way of documenting and sharing information** about safety artifacts created, verified and maintained during lifecycle of system.

Set of concepts and data elements related to artifacts and their dependencies that are needed for **system's safety conformance documentation**.

**Enables automation of compliance with safety-critical industry standards** like automotive (ISO 26262), avionics (DO-178C), medical devices (IEC 62304), and industrial control (IEC 61508)



**SPDX**  
CRYPTOGRAPHY



## Standardizing Security: The Curated Cryptography List

SPDX 3.1 includes a new, vetted list of cryptographic algorithms to standardize how security mechanisms are documented in the same way it offers the SPDX License List.



# Existing Profiles Improvements

- **Consistency:** Field Naming / Metadata captured
- Improved Profile **descriptions, examples**
- Security: Clarify '**exploited**' property
- Additional information capture for:
  - **Regulatory Alignment:** such as EU AI Act Readiness, ISO 42001, IEEE 3119-2025
  - **Provenance**



# EU CRA Manufacturer Guidance

Work in progress: [SPDX-examples/conformance](#)

(SEBoK for Consumer Electronics) includes Stakeholder Needs and Stakeholder Requirements)

EU CRA Regulatory Knowledge Graph

Work in progress: [Mapping of SPDX fields to CRA clauses/appendix are captured in a spreadsheet](#)



Source: <https://openssf.org/blog/2025/10/22/sboms-in-the-era-of-the-cra-toward-a-unified-and-actionable-framework/>

# SPDX Tools

## SPDX Knowledge Graph Explorer



### IMPLEMENTING AI BILL OF MATERIALS (AI BOM) WITH SPDX 3.0

More than **60% of models** & **70% of datasets** on platforms like Hugging Face are **undocumented** [Oreamuno et al., 2023], rendering **effective auditing** of these assets **impossible**.



### From Hugging Face to GitHub: Tracing License Drift in the Open-Source AI Ecosystem

James Jewitt, Hao Li, Bram Adams, Gopi Krishnan Rajbahadur, Ahmed E. Hassan

School of Computing, Queen's University, Kingston, ON, Canada  
{james.jewitt, hao.li, bram.adams}@queensu.ca, grajbahadur@acm.org, ahmed@cs.queensu.ca

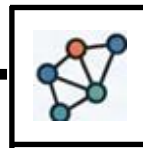
Source: <https://arxiv.org/pdf/2509.09873>



Whitepaper/Doc/Code

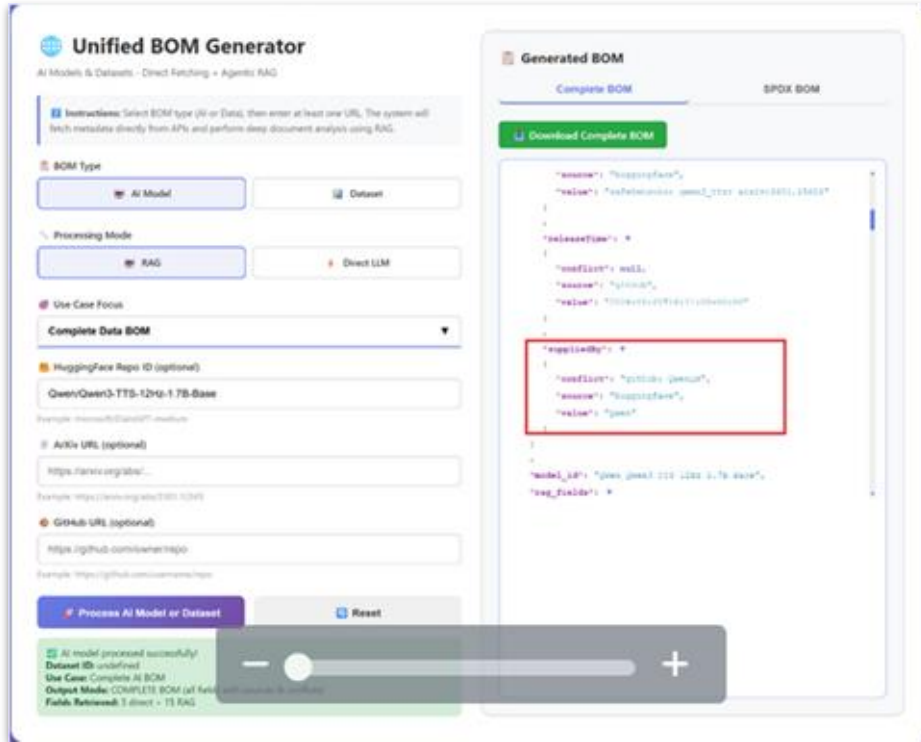


SPDX Knowledge  
Graph Tool



Graph Output

# SPDX Knowledge Graph Explorer



**Information Rich Knowledge Graph from multiple sources** (source, user guides, hugging face, github, etc ).

Generates AI and Dataset BOM that be **integrated into Supply Chain Graph**

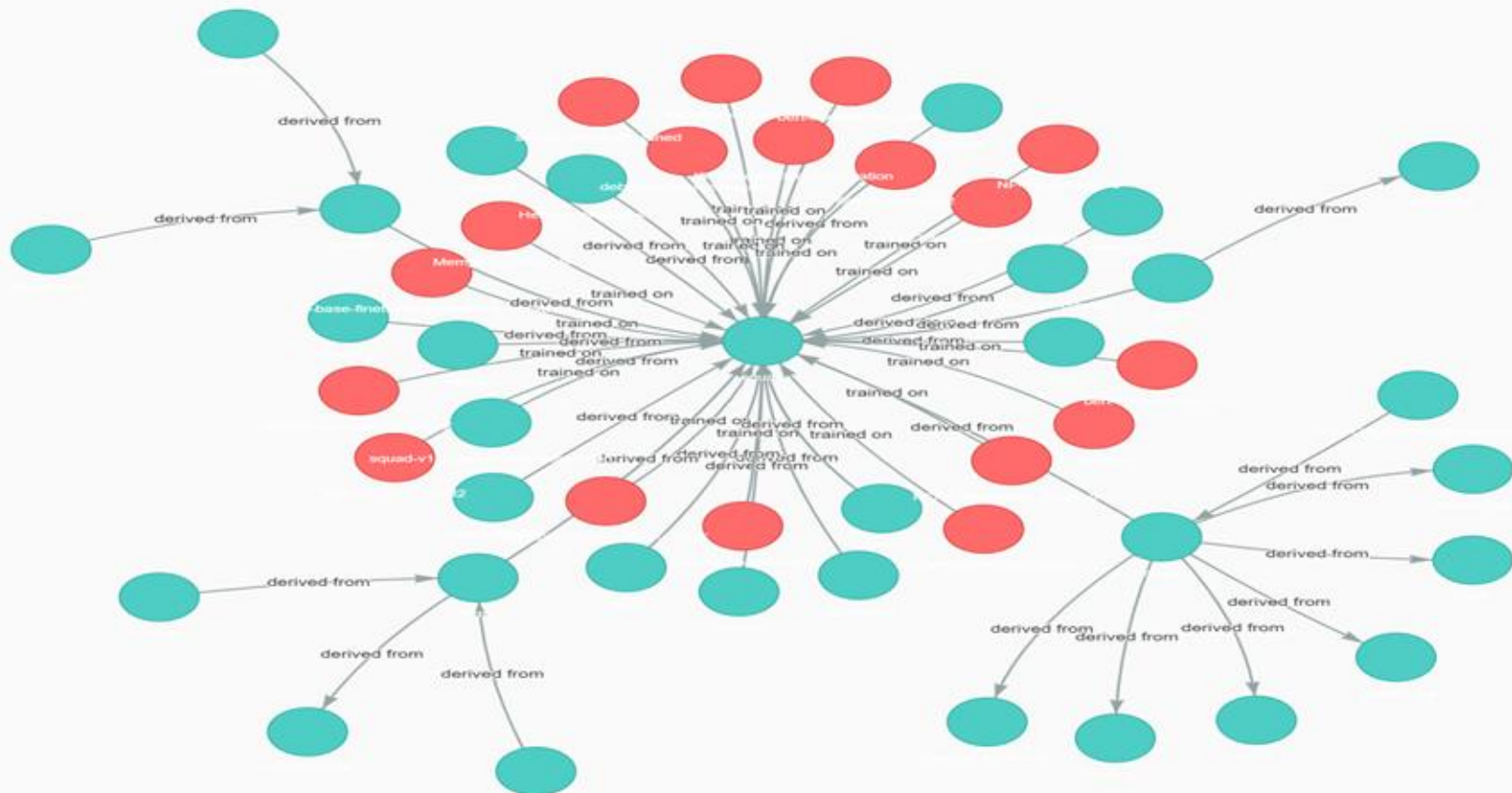
**Conflict Resolution / Confidence Checker** - checks metadata across multiple sources, identifies conflicts like licensing

**Demo version available upon request**



# Knowledge Graph Explorer

Neo4j Enhanced • 50 nodes • 55 edges



Found: **sg\_squad** (lmqg/sg\_squad) • Highlighted 2 parent node(s)

lmqg/sg\_squad

Type: Dataset  
 License: cc-by-4.0  
 Source: huggingface

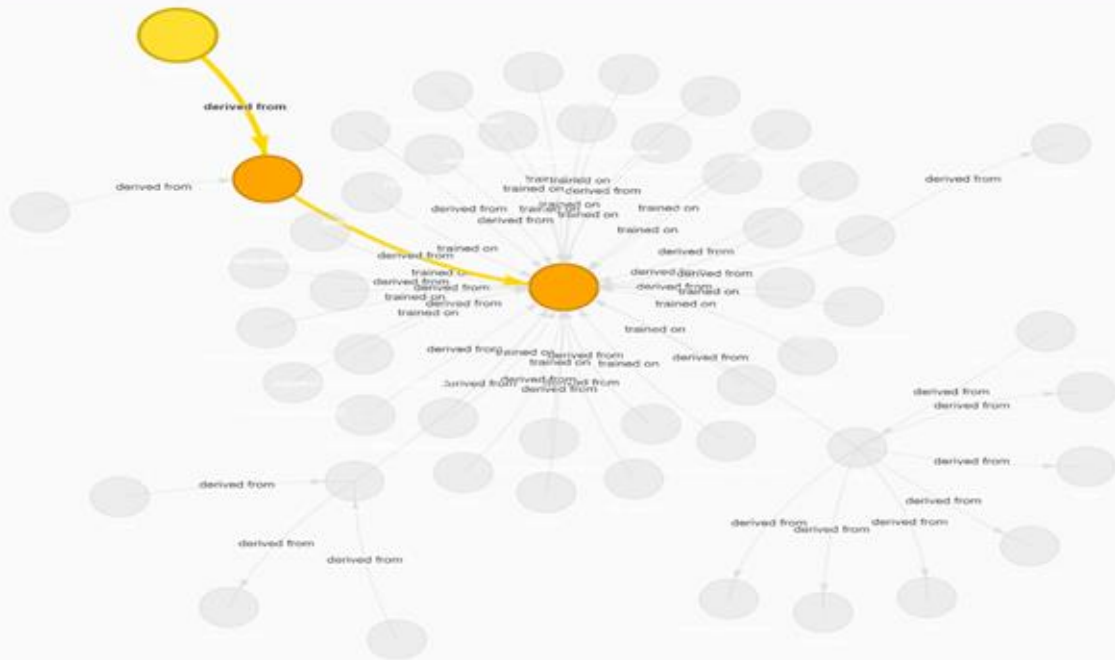
Ancestor Chain (2 nodes):

Parents:

- squad\_es
- **Compatible**
- License: cc-by-4.0
- Source uses permissive license - generally compatible

Grandparents:

- squad
- **Compatible**
- License: cc-by-4.0
- Source uses permissive license - generally compatible



# SPDX 3.1 Roadmap → RC2



## Community Feedback

Addressing community feedback

OWASP Feedback



## Strategic Integration

MITRE  
ATT&CK +  
D3FEND

With Threat  
and Controls  
Profile



## Scope

Agentic AI

Security

System  
Engineering



## Use Cases .

Continue to prepare  
Manufacturers for  
EU CRA

# SPDX 3.1 Roadmap → RC2

## Adding more Real World Examples



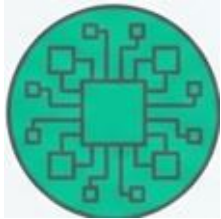
### Procurement & Auditing

Verifying software bills of materials before purchase.



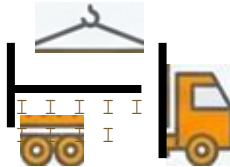
### Defense & Hardware

High-security hardware tracking for government contracts.



### Semiconductors

Anti-counterfeit tracking and supply chain verification.



### Logistics

Real-time monitoring of GPU Shipments.

# Come Join Us

## Key RC2 Weekly Working Groups



**Mondays:** Threats and Controls



**Tuesday:** Tech Team (between Profiles)



**Wednesdays:** AI / Dataset



**Friday:** Regulatory Compliance (CRA)  
& Functional Safety

## Resources



**SPDX Info:**

<https://github.com/spdx>



**Guide:** [OpenChain AI System BOM - Compliance Management Guide for the Supply Chain](#)  
[Wednesdays: AI / Dataset](#)



**Whitepaper:** [Implementing AI BOM with SPDX 3](#)

# SPDX 3.1 Takeaways:

- a **knowledge graph** not just a flat file (although it can export them)



The screenshot shows the homepage of the SPDX 3.1-RC1 specification. On the left is a navigation menu with categories: Home, Copyright, Introduction, 1. Scope, 2. References, 3. Symbols, 4. Terms and definitions, 5. Conformance, 6. Model and serializations, MODEL (with sub-items: Core, Software, Security, Licensing, SingleLicensing, ExpandedLicensing, Dataset, AI, Build, Like, Extension, Hardware, Service, SupplyChain, Operations, FunctionsSafety), and ANNEXES (with sub-items: A. RDF model definition and diagrams, B. SPDX license expressions). The main content area features the SPDX logo, the title 'The System Package Data Exchange™ (SPDX®) Specification Version 3.1-RC1', a copyright notice for 2010-2026, and a list of contributors with a thank-you message.

Home

Copyright  
Introduction  
1. Scope  
2. References  
3. Symbols  
4. Terms and definitions  
5. Conformance  
6. Model and serializations

MODEL

- Core
- Software
- Security
- Licensing
- SingleLicensing
- ExpandedLicensing
- Dataset
- AI
- Build
- Like
- Extension
- Hardware
- Service
- SupplyChain
- Operations
- FunctionsSafety

ANNEXES

- A. RDF model definition and diagrams
- B. SPDX license expressions

**SPDX** Home

## The System Package Data Exchange™ (SPDX®) Specification Version 3.1-RC1

Copyright © 2010-2026, The Linux Foundation and its Contributors, including SPDX Model contributors from DMG and its Contributors.

With thanks to Adam Cohn, Adolfo García Veytia, Alan Tse, Alexios Zavras, Alfred Strauch, Andrew Back, Ann Thornton, Armin Tänzer, Arthit Suriyawongkul, Ayumi Watanabe, Basil Peace, Bill Schineller, Bradlee Edmondson, Brandon Lunn, Bruno Correa, Claran Farrell, Daniel Geman, David Edelsohn, David Kemp, David A. Wheeler, Debra McGlade, Dennis Clark, Dick Brooks, Ed Wamicka, Elyas Rashno, Éran Strod, Eric Thoman, Esteban Rockett, Gary O'Neal, Gopi Krishnan Rajahadur, Guillaume Rousseau, Hassib Khanafar, Herik Birkholz, Hironyuki Fukuchi, Itaru Hosomi, Jack Manbeck, Jaime Garcia, Jeff Ucola, Jeff Latczak, Jeff Schult, Jillayne Lovejoy, John Ellis, Jonas Oberg, Joshua Watt, Kamsang Salima, Karen Bennet, Karri Copenhaver, Kate Stewart, Kevin Mitchell, Kim Weiss, Kirsten Newcomer, Kouki Hama, Kris Reeves, Liang Cao, Lon Holtberger, Marc-Etienne Vargenau, Mark Gisi, Marshall Clow, Martin Michlmayr, Martin von Willebrand, Mark Abwood, Matija Šušlje, Matt Gernonprez, Maximilian Huber, Meret Behrens, Michael J. Herzog, Michel Ruffin, Nicole Pappier, Nisha Kumar, Nobuyuki Tanaka, Norio Kobata, Nuno Brito, Oliver Fendt, Paul Madick, Peter Williams, Phil Robb, Philip Koltun, Philip Odencio, Philippe Ombredanne, Pierre Lapointe, Rana Rahaf, Robert Martin, Robin Gandhi, Rose Judge, Sam Ellis, Sameer Ahmed, Satoru Koizumi, Scott K Peterson, Scott Lamons, Scott Sterling, Sean Barmann, Sebastian Crane, Shane Coughlan, Steve Cropper, Steve Winslow, Steven Carbone, Stuart Hughes, Takashi Ninjouji, Thomas F. Inconrva, Thomas Steenberger, Tom Callaway, Tom Vidal, Toru Taima, Venkata Krishna, W. Trevor King, William Bartholomew, Yiv Bronshteyn, Yoshiko Ouchi, Yoshiyuki Ito, Yujii Nomura, Yumi Tomita, and Zachary McFarland for their contributions and assistance.

# SPDX 3.1 Takeaways:

- a **knowledge graph** not just a flat file (although it can export them)
- profiles capture the **full supply chain lifecycle**



The screenshot shows the home page of the SPDX 3.1-RC1 specification. On the left is a navigation menu with sections: Home, Copyright, Introduction, 1. Scope, 2. References, 3. Symbols, 4. Terms and definitions, 5. Conformance, 6. Model and serializations, MODEL, Core, Software, Security, Licensing, SingleLicensing, ExpandedLicensing, Dataset, AI, Build, Life, Extension, Hardware, Service, SupplyChain, Operations, FunctionsSafety, ANNEXES, A. RDF model definition and diagrams, B. SPDX license expressions. The main content area features the SPDX logo, the title 'The System Package Data Exchange™ (SPDX®) Specification Version 3.1-RC1', a copyright notice for 2010-2026, and a list of contributors with thanks.

# SPDX 3.1 Takeaways:

- a **knowledge graph** not just a flat file (although it can export them)
- profiles capture the **full supply chain lifecycle**
- provides **Evidence Traceability for Compliance**



# SPDX 3.1 Takeaways:

- a **knowledge graph** not just a flat file (although it can export them)
- profiles capture the **full supply chain lifecycle**
- provides **Evidence Traceability for Compliance**
- has more Tools to help with **automating the metadata capturing**



The screenshot shows the homepage of the SPDX 3.1-RC1 specification. On the left is a navigation menu with sections like 'Copyright', 'Introduction', '1. Scope', '2. References', '3. Symbols', '4. Terms and definitions', '5. Conformance', '6. Model and serializations', 'MODEL', 'Core', 'Software', 'Security', 'Licensing', 'SimpleLicensing', 'ExpandedLicensing', 'Dataset', 'AI', 'Build', 'Lite', 'Extension', 'Hardware', 'Service', 'SupplyChain', 'Operations', 'Functions/Safety', 'ANNEXES', 'A. RDF model definition and diagrams', and 'B. SPDX license expressions'. The main content area features the SPDX logo, the title 'The System Package Data Exchange™ (SPDX®) Specification Version 3.1-RC1', a copyright notice for 2010-2026, and a list of contributors.

Home

Copyright  
Introduction  
1. Scope  
2. References  
3. Symbols  
4. Terms and definitions  
5. Conformance  
6. Model and serializations

MODEL

- Core
- Software
- Security
- Licensing
- SimpleLicensing
- ExpandedLicensing
- Dataset
- AI
- Build
- Lite
- Extension
- Hardware
- Service
- SupplyChain
- Operations
- Functions/Safety

ANNEXES

- A. RDF model definition and diagrams
- B. SPDX license expressions

**SPDX** Home

## The System Package Data Exchange™ (SPDX®) Specification Version 3.1-RC1

Copyright © 2010-2026, The Linux Foundation and its Contributors, including SPDX Model contributions from DMG and its Contributors.

With thanks to Adam Cohn, Adolfo García Veytia, Alan Tse, Alexios Zavras, Alfred Strauch, Andrew Back, Ann Thornton, Armin Tünzer, Arthit Suriyawongkul, Ayumi Watanabe, Basil Peace, Bill Schineller, Bradlee Edmondson, Brandon Lunn, Bruno Correa, Claran Farrell, Daniel Geman, David Edelsohn, David Kemp, David A. Wheeler, Debra McGlade, Dennis Clark, Dick Brooks, Ed Wamicka, Elias Rashno, Éran Strod, Eric Thoman, Esteban Rockett, Gary O'Neal, Gopi Krishnan Rajbahadur, Guillaume Rousseau, Hassib Khanafar, Herik Birkholz, Hironyuki Fukuchi, Itaru Hosomi, Jack Manbeck, Jaime Garcia, Jeff Ugozia, Jeff Lutercz, Jeff Schutt, Jilaine Lovejoy, John Ellis, Jonas Oberg, Joshua Watt, Kamsang Salima, Karen Bennet, Karen Copenhaver, Kate Stewart, Kevin Mitchell, Kim Weims, Kirsten Newcomer, Kouki Hama, Kris Reeves, Liang Cao, Lon Holtberger, Marc-Etienne Vargenau, Mark Gisi, Marshall Clow, Martin Michlmayr, Martin von Willebrand, Mark Abwood, Matija Šušlje, Matt Gernonprez, Maximilian Huber, Meret Behrens, Michael J. Herzog, Michel Ruffin, Nicole Pappier, Nisha Kumar, Nobuyuki Tanaka, Norio Kobota, Nuno Brito, Oliver Fendt, Paul Madick, Peter Williams, Phil Robb, Philip Koltun, Philip Odence, Philippe Ombredanne, Pierre Lapointe, Rana Rahul, Robert Martin, Robin Gandhi, Rose Judge, Sam Ellis, Sameer Ahmed, Satoru Koizumi, Scott K Peterson, Scott Lamons, Scott Sterling, Sean Barmam, Sebastian Crane, Shane Coughlan, Steve Cropper, Steve Winslow, Steven Carino, Stuart Hughes, Takashi Ninjouji, Thomas F. Inconriva, Thomas Steenberger, Tom Callaway, Tom Vidal, Toru Taima, Venkata Krishna, W. Trevor King, William Bartholomew, Yiv Bronshteyn, Yoshiko Ouchi, Yoshiyuki Ito, Yujii Nomura, Yumi Tomita, and Zachary McFarland for their contributions and assistance.

# SPDX 3.1 Takeaways:

- a **knowledge graph** not just a flat file (although it can export them)
- profiles capture the **full supply chain lifecycle**
- provides **Evidence Traceability for Compliance**
- has more Tools to help with **automating the metadata capturing**
- providing more **guides & examples to Help Manufacturers for compliance** such as **EU CRA**



# Thank You!



## Any Questions?

