Home

SPDX Tech Team Home

← Please look at working meeting minutes for each week at the document tabs on the left pane

Meeting

Weekly on Tuesdays

at 12:00 US Eastern Time

(mind the daylight saving difference)

https://zoom.us/j/663426859

Approved meeting minutes

https://github.com/spdx/meetings/tree/main/tech

Past minutes waiting for approval

https://github.com/spdx/meetings/issues/592

https://github.com/spdx/meetings/labels/Tech

(if you attended the meeting, you can make an approval comment in the comment section)

Published specifications

- SPDX 2.2.1 / ISO/IEC 5962:2021
- SPDX 2.2.2
- SPDX 2.3 / JSON Schema
- SPDX 3.0 / OMG

In development

- SPDX 3.0 ISO version (spdx-spec, spdx-3-model)
- SPDX 2.3.1-dev
- SPDX 3.1-dev
- Hardware Profile
- Operations Profile
- Software-as-a-Service Profile
- Usage Profile

Backlog

- Backlog

Open issues & PRs

- meetings: Issues & PRs
- crypto-algorithms: Issues & PRs
- spdx-3-model: Issues & PRs
- spdx-spec: Issues & PRs
- spec-parser: Issues & PRs
- spdx-examples: Issues & PRs
- using: Issues & PRs

References

Minimum elements

- NTIA Minimum Elements (US, 2021)
- CISA Minimum Expected Baseline Attributes (US, 2024)
- BSI TR-03183 Part 2 (Germany, 2024)
- OpenChain Telco SBOM Guide Version 1.1 (2025)

Backlog

SPDX Tech Team Backlog

- Examples
  - Add `suppliedBy` and `verifiedUsing` (hash) for Dataset Example 01 https://github.com/spdx/spdx-examples/pull/120
- 3.1
  - New concept - `SoftwareComponent` https://github.com/spdx/spdx-3-model/pull/1044
  - Make 3.1 RDF URLs to work (have to do these in order):
    - 2) Setup RDF and schema URL directions https://github.com/spdx/spdx-spec/issues/1249
    - 3) Update example checks in CI https://github.com/spdx/spdx-spec/pull/1244
  - AI/Dataset
    - Add `AI/automationLevel` https://github.com/spdx/spdx-3-model/pull/1064
  - Hardware
    - Add Hardware profile to develop branch https://github.com/spdx/spdx-3-model/pull/1076
  - Update `from` and add `to` type of `hasConcludedLicense` and `hasDeclaredLicense` https://github.com/spdx/spdx-3-model/pull/1122
  - Clarify `hasDeclaredLicense` and `hasConcludedLicense` https://github.com/spdx/spdx-3-model/issues/1022
  - Move `inLanguage` to Core https://github.com/spdx/spdx-3-model/pull/1124
  - Add "known unknown" and "redacted" properties to elements for CISA minimum elements https://github.com/spdx/spdx-3-model/issues/1105
- 3.0 - ISO editorials
  - https://github.com/spdx/spdx-spec/issues?q=state%3Aopen%20label%3A%22ISO%20publication%22
  - The RDFs should only go to second-level version https://github.com/spdx/spdx-3-model/issues/1046
    - `https://spdx.org/rdf/3.0.1/terms/Core/Element` → `https://spdx.org/rdf/3.0/terms/Core/Element`
    - Need updates in documentation, tools and CI
  - Make 3.0 RDF URLs to work (have to do these in order):
    - 2) Setup RDF and schema URL directions https://github.com/spdx/spdx-spec/issues/1246
    - 3) Update example checks in CI https://github.com/spdx/spdx-spec/pull/1247
  - Do we need a patch release for possible ISO review changes? https://github.com/spdx/spdx-3-model/issues/996
- 3.0 issues

    - JSON-LD identifiers are not dereferenceable
      https://github.com/spdx/spdx-3-model/issues/1056
- 2.3 issues
    - Clarification Needed on SPDX File Relationships in Absence of Direct Mapping
      https://github.com/spdx/spdx-spec/issues/1227
    - SPDX 2.3.0 schema conflicts with documentation for Annotations
      https://github.com/spdx/spdx-spec/issues/1147
- 2.2.2 issues
    - Fix schema bug (Snippet "name" is not required in spec, but required in schema)
      https://github.com/spdx/spdx-spec/pull/1021 – fixed, need to republish
- General documentation/website
    - Subclass tree in spec website
      https://github.com/spdx/spec-parser/pull/184
    - “Using” Website vs Wiki
        - Use website (autogenerated from Markdown) (PR:
          https://github.com/spdx/using/pull/16 demo: https://bact.github.io/using/)
          or use GitHub wiki (to be setup)
    - Update SBOM SPDX Landscape
      https://landscape.spdx.dev/
      (Outreach?)
- Questions
    -

2025-11-11

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-11-11

PR: https://github.com/spdx/meetings/pull/996

Attendees

1. Alexios Zavras
2. Arthit Suriyawongkul
3. Bob Martin
4. Dick Brooks
5. Gale McCommons
6. Gary O'Neall
7. Greg Shue
8. Ilan Schifter
9. Jesse Porter
10. Joshua Watt
11. Karen Bennett
12. Kate Stewart
13. Luis Augenstein
14. Maximilian Huber
15. Nicole Pappler
16. Peter Monks
17. Steven Carbno

Agenda

- Approval of last week's minutes
- Glossary PR https://github.com/spdx/spdx-spec/pull/1294
- Examples update https://github.com/spdx/spdx-spec/pull/1299
- Add automationLevel for AI and non-AI automation (7-level enum) https://github.com/spdx/spdx-3-model/pull/1064
- Notifications:

    - FOSDEM Devroom open until Nov 30 https://hackmd.io/@spdx/FOSDEM-2026-CfP on Sunday afternoon ½ day
    - CRA in practice will be on Saturday 1/2 day
    - Hardware meeting taking point on mapping CRA requirements to SPDX properties/relationships.
    - Final stretch to ISO submission, Karen to pass on some feedback to Alexios.
    - OpenChain having a Friday Automotive Workshop, Alexios is presenting on SPDX; Also will be info on CycloneDX, Catema-X
    - CVE.org is collecting user stories to help guide the next version/implementation of the CVE reporting system: https://github.com/CVEProject/consumer-working-group/issues
    - To join #SBOM SIG: https://www.linkedin.com/groups/13274064/
- AI PRs
    - Prompt and AI Agent are close to ready, targeting 3.1; no good definition of context and prompting, so have to do extensive review, and building consensus.
    - RAG likely to go 3.2
    - Reviewing relationship types for 2 new classes.
- 3.1 Release
- Considerations for 3.1 (backlog)
    - Allow optional version parameter in media-type https://github.com/spdx/spdx-spec/issues/642
    - Purl for DownloadURL and DocumentNamespace tags https://github.com/spdx/spdx-spec/issues/372
    - How to handle symlinks in SPDX documents? https://github.com/spdx/spdx-spec/issues/610
    - Embedding SPDX into binaries https://github.com/spdx/spdx-spec/issues/739

Notes

- Minutes from last week approved.
- Notifications:
    - FOSDEM Devroom open until Nov 30 https://hackmd.io/@spdx/FOSDEM-2026-CfP on Sunday afternoon ½ day
    - CRA in practice will be on Saturday 1/2 day
    - Hardware meeting taking point on mapping CRA requirements to SPDX properties/relationships.
    - Final stretch to ISO submission, Karen to pass on some feedback to Alexios.
    - OpenChain having a Friday Automotive Workshop, Alexios is presenting on SPDX; Also will be info on CycloneDX, Catema-X
    - CVE.org is collecting user stories to help guide the next version/implementation of the CVE reporting system: https://github.com/CVEProject/consumer-working-group/issues
    - To join #SBOM SIG: https://www.linkedin.com/groups/13274064/

    - BSIDES Munich this coming weekend: https://2025.bsidesmunich.org/ SBOM generation workshop on Saturday info at: https://pretalx.com/bsides-munich-2025/talk/QLMT3U/
- PR# 1294 - agreed to merge, separate PR for adding to normative references
- PR# 1299 - agreed to merge, consider removing once CI flow is automated.
    - Joshua and Alexios to review example
    - Gary to work on PR to automatically create example file.
- Additional info for PR #1064 follows ISO/IEC 22989:2022 Artificial intelligence concepts and terminology, proposing 7-level enum:
    - 0) notAutomated
    - 1) assistiveAutomation
    - 2) partialAutomation
    - 3) conditionalAutomation
    - 4) highAutomation
    - 5) fullAutomation
    - 6) autonomous
    - This also aligned with J3016_202104 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles https://www.sae.org/standards/content/j3016_202104/ (SAE J3016 is now under ISO process as ISO/SAE CD TS 22736 Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles (Draft) https://www.iso.org/standard/87218.html)
- AI PRs
    - Prompt and AI Agent are close to ready; no good definition of context and prompting, so have does extensive review, and building consensus.
    - RAG likely to go 3.2
    - Reviewing relationship types for 2 new classes.
- 3.1 Release:
    - Close PR# 1061 - it's been replaced by PR# 1141.
    - Kate & Alexios to review PR# 1135.
    - Review which ones should be milestoned to 3.1
    - Gary & Kate to take a pass at pulling together the punch list.
    -

Backlog

- See backlog at **“Backlog”** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-11-04

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-11-04

PR: https://github.com/spdx/meetings/pull/994

Attendees

18. Gary O'Neall
19. Steven Carbno
20. Joshua Watt
21. Bob Martin
22. Alfred Strauch
23. Greg Shue
24. Ilan Schifter
25. Luis Augenstein
26. Maximilian Huber
27. Nicole Pappler
28. Ted Gauthier
29. Victor Lu
30. Dick Brooks
31. Arthit Suriyawongkul

Agenda

- Approval of last week's minutes
- [3.0/ISO] Update RDF IRIs (and tools/CIs) to use MAJOR.MINOR version (without patch point) "instead of `https://spdx.org/rdf/3.0.1/terms/Core/Element` they should simply be `https://spdx.org/rdf/3.0/terms/Core/Element`" https://github.com/spdx/spdx-3-model/issues/1046
- Glossary PR
- Examples update
- Considerations for 3.1 (backlog)
    - Allow optional version parameter in media-type https://github.com/spdx/spdx-spec/issues/642

    - Purl for DownloadURL and DocumentNamespace tags https://github.com/spdx/spdx-spec/issues/372
    - How to handle symlinks in SPDX documents? https://github.com/spdx/spdx-spec/issues/610
    - Embedding SPDX into binaries https://github.com/spdx/spdx-spec/issues/739
- Victor - OWASP AI update

Notes

- ISO - word document submitted to LF, being reviewed and plan to forward onto ISO soon along with other required information - hopefully this week
- RDF IRI's - issue closed, sufficient for ISO, but there is more work needed for the tooling and CI - reference https://github.com/spdx/spdx-spec/issues/1246
    - For the tooling context file and similar references, we'll address in the next patch release 3.0.2
- Glossary discussion updated in the PR https://github.com/spdx/spdx-spec/pull/1294
- in move from SPDX 2.x to 3.0 the glossary terms went from specific definitions to being a reference to ISO terminology. However there is a need to define SPDX's use of the terms since ISO has multiple definitions of many of the terms of interest to SPDX users.
    - Working to recreate glossary terms for SPDX 3.1. If ISO comes back with comments on the SPDX 3.0 submission we can bring the new glossary entries back to that version.

Future Meeting topics

- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Version series license families
- Clarify `hasDeclaredLicense` and `hasConcludedLicense` https://github.com/spdx/spdx-3-model/issues/1022
- Update `from` and add `to` type of `hasConcludedLicense` and `hasDeclaredLicense` https://github.com/spdx/spdx-3-model/pull/1122
- Add "known unknown" and "redacted" properties to elements for CISA minimum elements https://github.com/spdx/spdx-3-model/issues/1105

Backlog

- See backlog at **"Backlog"** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-10-28

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-10-28

PR: https://github.com/spdx/meetings/pull/992

Attendees

32. Alexios Zavras
33. Alfred Strauch
34. Arthit Suriyawongkul
35. Bob Martin
36. Dick Brooks
37. Gary O'Neall
38. Greg Shue
39. Jesse Porter
40. Joshua Watt
41. Kate Stewart
42. Peter Monks
43. Steven Carbno
44. Ummo Schwarting
45. Victor Lu

Agenda

- ISO Submission - new document (Alexios)
- Operations Profile (Ummo)
- Spec documentation feedback (Joshua)
- New profiles already updated in 3.1-dev website (Hardware and SupplyChain)

Notes

- ISO Submission
    - All issues raised by Rex have been addressed
    - New Word document produced by Friday and sent to Rex
    - Manual changes then submission

- Operations Profile
    - Going for minimum approach
    - Wanting to get ball rolling
    - Project information
    - Export control classification number and assessment artifacts.
    - PR being rebased. Merging in profile Operations branch, then merge to develop.
    - Limited set of folks looking into it. Focus on export control
    - Parent class of export class assessment.
    - Consider use of Annotation class in core to consider extending.
    - Have already consider security assessment
    - Consider calling it as export_assessment. Purposes beyond export control.
    - Looked into what safety was doing. Too complex for what looking for right now.
    - Targeting for PR for whole branch - this weekend.
- Spec document Feedback.
    - Garmin working on company wide compliance and reading on SPDX.
    - No examples in spec itself. Hard to understand what just do, from reading spec.
    - Add examples into our spec itself - see examples showing how to use.
    - Hard to translate. Security vuln assessment does this. Translate the abstract description into JSON.
    - Every class should have example - ideally on same page, but link to using repo would be ok.
    - Unclear how things map to concrete things.
    - Concern raised about abstract classes. Could do for those for non-abstract.
    - Generated solution - link to section in "using" to show context. Validate fragments of documents.
    - Two audiences: translating from another format; new content and starting in SPDX. Need to be clear about concepts and definitions of SPDX. How we expect fields and relationships to be used. Examples and fragments inline. Helping with encoding/decoding.
    - Fake example with everything, than cut/point to it?
    - RESOLUTION: Gary to look at extending the example; Joshua to work on translation to html.
- ..

Future Meeting topics

- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Version series license families
- Clarify `hasDeclaredLicense` and `hasConcludedLicense` https://github.com/spdx/spdx-3-model/issues/1022
- Update `from` and add `to` type of `hasConcludedLicense` and `hasDeclaredLicense` https://github.com/spdx/spdx-3-model/pull/1122

- Add "known unknown" and "redacted" properties to elements for CISA minimum elements https://github.com/spdx/spdx-3-model/issues/1105

Backlog

- See backlog at **“Backlog”** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-10-21

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-10-21

No meeting today – see you on 28 October 2025

Future Meeting topics

- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Version series license families
- Add Hardware profile to develop branch https://github.com/spdx/spdx-3-model/pull/1076
- Clarify `hasDeclaredLicense` and `hasConcludedLicense` https://github.com/spdx/spdx-3-model/issues/1022
- Update `from` and add `to` type of `hasConcludedLicense` and `hasDeclaredLicense` https://github.com/spdx/spdx-3-model/pull/1122
- Move `inLanguage` to Core https://github.com/spdx/spdx-3-model/pull/1124
- Add "known unknown" and "redacted" properties to elements for CISA minimum elements https://github.com/spdx/spdx-3-model/issues/1105

Backlog

- See backlog at **"Backlog"** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-10-14

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-10-14

PR: https://github.com/spdx/meetings/pull/971

Attendees

1. Alexios Zavras
2. Alfred Strauch
3. Arthit Suriyawongkul
4. Bob Martin
5. Dick Brooks
6. Gary O'Neall
7. Jesse Porter
8. Joshua Watt
9. Karen Bennet
10. Karsten Klein
11. Kate Stewart
12. Maximilian Huber
13. Raymond Sheh
14. Rose Judge
15. Steven Carbno
16. Victor Lu

Agenda

- Prioritize agenda
- Approve last week's minutes
- ISO Publication issues
  - https://github.com/spdx/spdx-spec/issues?q=is%3Aissue%20state%3Aopen%20label%3A%22ISO%20conformance%22
- Overview of Operations Profile
- Relationship Reviews Table (Art)
- Cleanup Update

    - 2.X PR Cleanup Update (Gary & Kate)
    - Merged A website for informative/non-normative documents/guides/howtos https://github.com/spdx/using/pull/16
- 2.x maintenance policy / deprecation notice of older specs
    - Need to be on https://spdx.dev/use/specifications/ page as well?
    - The CISA 2025 Minimum Elements draft document said "agencies should avoid accepting SBOMs for new software generated in ***deprecated versions*** of any format to maintain compatibility with SBOM consumption and management tools." -- Does SPDX have a process of deprecating an SPDX version? Where do we publish that information?
- Spec documentation feedback

Notes

- Request for each of profile teams to go through backlogs for profiles.
    - Mark those WIP as draft.
    - Flag those that need to be reviewed.
- ISO Publication
    - 1271 - see documentation in issue.
    - 1270 - need to create PR in Spec repo to add Intro. Parameter to spec parser, with mkdocs. Alexios will tackle. 8.3.1.2 in core profile. PR to model repo will be needed.
    - 1255 - will be closed, once Alexios finishes implementing in spec parser (and be consistent by default that way going forward)
    - 1236 - checking commit refs. Possibly squashed/refreshed. License Expression Annex. Need to do a search. Art will look for these.
    - 1235 - all references must have source in the text.
    - 1233 - handled at this point.
    - Reminder will need all PRS in 3.0 & dev at this point.
- Relationship Reviews
    - Art got to it before Kate did. Thanks Art!!!
    - See: https://github.com/spdx/spdx-3-model/issues/1114 and SPDX 3.1-dev RelationshipType
    - Highlighted hasConcludedLicense is missing type. Should be ok to add.
    - HasAddedFile, hasDataFile, hasDeletedFile - it may make sense to have restricted to File. Clarifying description of restriction is already there. Joshua thinks possibly should be Artifact, rather than specific file (which is software). Element to Artifact, bundle might be appropriate. Which is reason to leave as is. Leave as is, cause could be breaking change, but may want to update documentation. Typically a file or a bundle.
    - For licensing, agreement to expand out to allow hardware to be licensed. Not wanting to restrict until we've had joint discussion on this topic on compliance points with legal team.
- Operations Profile Review - moved to 28th.

- Cancelling next week's call.

Future Meeting topics

- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Version series license families

Backlog

- See backlog at **“Backlog”** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-10-07

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-10-07

PR: https://github.com/spdx/meetings/pull/946

Attendees

17. Alfred Strauch
18. Arthit Suriyawongkul
19. Bob Martin
20. Dick Brooks
21. Gary O'Neall
22. Greg Shue
23. Jesse Porter
24. Karen Bennet
25. Kate Stewart
26. Luis Augenstein
27. Maximillan Huber
28. Nicole Pappler
29. Peter Monks
30. Stanislav Pankevich
31. Steven Carbno
32. Victor Lu

Agenda

- Prioritize agenda
- Approve last week's minutes
- Hardware and Safety profile sync
- Continue discussion of feedback to CISA
    - All submitted comments: https://www.regulations.gov/document/CISA-2025-0007-0001/comment
- Archiving stale SPDX repos

    - Archive `tools` repo and send visitors to `tools-java`, https://github.com/spdx/tools/issues/318
    - Other repos?
- 2.x maintenance – most of these PRs have one review and wait for merging
    - Fix schema bug (Snippet "name" is not required in spec, but required in schema)
        - 2.2.2 https://github.com/spdx/spdx-spec/pull/1020
        - 2.3 https://github.com/spdx/spdx-spec/pull/1273
        - 2.3.1 https://github.com/spdx/spdx-spec/pull/1021
    - Fix spec cardinality typo (externalDocumentRef's Required = No, but cardinality is 1..*)
        - 2.3 https://github.com/spdx/spdx-spec/pull/1229
        - 2.3.1 https://github.com/spdx/spdx-spec/pull/1230
- 2.x maintenance policy / deprecation notice of older specs
    - Need to be on https://spdx.dev/use/specifications/ page as well?
    - The CISA 2025 Minimum Elements draft document said "agencies should avoid accepting SBOMs for new software generated in ***deprecated versions*** of any format to maintain compatibility with SBOM consumption and management tools." -- Does SPDX have a process of deprecating an SPDX version? Where do we publish that information?
- Outreach: A website for informative/non-normative documents/guides/howtos
    - https://github.com/spdx/using/pull/16

Notes

- Dick noted that There is a proposal to create an SBOM Implementers Manifesto modeled after the Agile Manifesto in the #SBOM SIG: https://www.linkedin.com/feed/update/urn:li:activity:7381068226174275584
- Stale PRs - Kate and Gary taking a pass on cleaning up backlog.
- Discussion between Safety & Hardware Profiles, and order for doing merge.
    - https://github.com/spdx/spdx-3-model/pull/1112/files https://github.com/spdx/spdx-3-model/pull/1109
        - The https://github.com/spdx/spdx-3-model/pull/1109 is about "intendedUse", if we like to put it in Core.
        - Discussion on where this belongs. Discussion of it being in Artifact, seems to be a consensus even though there are some optional fields that may not be relevant.
        - Supplier is one who interface to user.
        - Are tracking chain of custody or fabrication sequence. Each is important and distinctly different.
    - Fabrication sequence, had different suppliers as it is passed through the supply chain.
    - Software has multiple copies of same item. Hardware profile could make an item not usable.
    - Supply chain profile - can put info in wrong spot? Contradicting data.

    - Use case for supplier - who do I go to for something, party that delivered down the supply chain. Originator - who created.
    - IP(web address) is transport level, and shouldn't be considered a supplier.
    - Example: bought a new monitor, UPS delivered; bought through Amazon; Product is ASUS monitor. If got monitor and it was broken - contact Amazon or Asus? Warranty says ASUS, so supplier is ASUS, so they are the ones that should be providing an SBOM. Can go back to originator, but supplier is one with other contractual relationship with.
- Action is to clean up add into description of supplier that it is producer, and relate to supply chain.
- Movement of goods should be in supply chain. But need to know who have legal association with - that is the supplier. The fact that it went through multiple warehouses, and trucks between. It's the transport portion of a supply chain flow.
- What about virtual hardware? Containers? Everything is a buy/sell transaction; someone is providing / acquiring. Providing / acquiring is a set of terms. Supply chain - does the supplier field in artifact contradict the supply chain. Lack of clarity in the definition of supplier.
- Discussion of removing product agent from current draft.
- Issues: Product vs. Supply Chain. Products are made up of other products. "Your product is my component". Need to be clear about audience, and decomposition level.
- Nicole questioned where manufactured. People care, require supply chain profile. Screw from manufacturer, etc.
- Gary summarized AI:
    - Agree we need to review and update the definition of supplier (esp. From hardware team)
    - Supply chain should be a requirement in hardware profile.
    - Supplier and subclass artifact for hardware
    - If everyone agrees with above, then we move intendedUse to Artifact, and deprecate the dataset property.
    - Karen commented that they've discussed it in AI & Data and are fine with deprecating.
- Safety Profile converging on Hardware profile.
    - Once Steven updates 1119 (changing to artifact), and merges into hardware branch. What properties don't make sense in HW? Adding in commentary on optional fields that don't make sense (putting in as overrides). Put in as (0,0).
    - Another thing is to adjust definitions in artifact to be inclusive of hardware.
    - Please add Nicole as review so she gets notification
    - Nicole will review in context with Safety and comment if any outstanding issues.
- If Hardware team updates pull request, then it could be discussed on Safety profile.
- Stan has issues with Safety profile that should be discussed.
- Greg pointed out the EU CRA specifically describes who is responsible for white-labeled products (e.g., those that can be trivially re-branded).
- We need it worked out sooner than later, and but should work out these wrinkles.
    - Karen worried about AI & Data changes going forward.

    - Verification model, Operations may have comments.
- Verification method - possibly cross profile. Evidence of process being followed, etc.
- Special meeting to be called for Design assurance
- Karen recommends that all the profiles review the existing relationships.
    - Is a profile using relationship or not, are they comfortable with definition.
    - AI: Kate to set up table with relationships and checks for it.

Future Meeting topics

- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Version series license families

Backlog

- See backlog at **“Backlog”** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-09-30

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-09-30

PR: https://github.com/spdx/meetings/pull/940

Attendees

33. Alfred Strauch
34. Arthit Suriyawongkul
35. Greg Shue
36. Helio Chissini de Castro
37. Jesse Porter
38. Marc-Etienne Vargenau
39. Nicole pappler
40. Peter Monks
41. Rose Judge
42. Steven Carbno

Agenda

- Prioritize agenda
- Approve last week's minutes
- Continue discussion of feedback to CISA
- Archiving stale SPDX repos
    - Archive `tools` repo and send visitors to `tools-java`, https://github.com/spdx/tools/issues/318
    - Other repos?
- 2.x maintenance – most of these PRs have one review and wait for merging
    - Fix schema bug (Snippet "name" is not required in spec, but required in schema)
        - 2.2.2 https://github.com/spdx/spdx-spec/pull/1020
        - 2.3 https://github.com/spdx/spdx-spec/pull/1273
        - 2.3.1 https://github.com/spdx/spdx-spec/pull/1021
    - Fix spec cardinality typo (externalDocumentRef's Required = No, but cardinality is 1..*)

        - 2.3 https://github.com/spdx/spdx-spec/pull/1229
        - 2.3.1 https://github.com/spdx/spdx-spec/pull/1230
- 2.x maintenance policy / deprecation notice of older specs
    - Need to be on https://spdx.dev/use/specifications/ page as well?
    - The CISA 2025 Minimum Elements draft document said "agencies should avoid accepting SBOMs for new software generated in ***deprecated versions*** of any format to maintain compatibility with SBOM consumption and management tools." -- Does SPDX have a process of deprecating an SPDX version? Where we publish that information?

Notes

- Agreed to approve minutes
- Feedback to CISA
    - Briefly discussed the document that is proposed to be submitted - Art had some additional comments regarding the Appendix that he would like to see added. Rose will incorporate.
    - Should we deprecate older versions of SPDX? We haven't deprecated older versions as of now. Let's discuss more next week
- Redacted/known unknowns: https://github.com/spdx/spdx-3-model/issues/1105
    - The fact that something is redacted may also be redacted.
    - Is the non-existence of something enough?
    - If we want to put an explicit indicator for this it will probably need to be on the element.
    - This could also be done as an annotation - because this should be so rare, we could create annotation property
        - Could create annotation type known/unknown or redacted
    - If something is a known unknown we probably need a comment about how/why SBOM author came to that conclusion
    - Possible use case: When license is redacted but not the component – put known unknown/redacted on the nearest object
    - Use case: the entire document is redacted - how to handle?
    - Discussed some type of machine readable identifier in the annotation statement field to point to the known unknown or redacted element property.
- Threats and Management
    - Definitions of terms ("threats", "assets") - assuming definitions would end up in some level of glossary/definition and that approval of them needs to go through the tech team - is this the expectation?
    - There is a glossary: https://github.com/spdx/spdx-3-model/blob/develop/docs/glossary.md and a terms and definitions https://spdx.github.io/spdx-spec/v3.0.1/terms-and-definitions/
    - Proposal to update the glossary https://github.com/spdx/spdx-3-model/issues/1075

    - Open a PR or issue to bring discussion/additions to group
    -

Future Meeting topics

- Continue discussion of feedback to CISA
- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Version series license families

Backlog

- See backlog at **“Backlog”** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-09-23

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-09-23

PR: https://github.com/spdx/meetings/pull/939

Attendees

43. Alfred Strauch
44. Bob Martin
45. Dick Brooks
46. Gary O'Neall
47. Greg Shue
48. Helio Chissini de Castro
49. Jesse Porter
50. Joshua Watt
51. Karen Bennet
52. Luis Augenstein
53. Maximillian Huber
54. NISHANTH SANKARAN
55. Rose Judge
56. Steven Carbno
57. Victor Lu

Agenda

- Prioritize agenda
- Approve last week's minutes
- Continue discussion of feedback to CISA
- Merge in PR for hardware / supply chain
- Clarify on relationship for the 2.X release

Notes

- Agreed to approve minutes

- Feedback to CISA
    - Updated document: https://docs.google.com/document/d/1sLeKWOTUq-7ywv9iE22rxyEmTOMzlsuCMTVoYpMXomk/edit?tab=t.0#heading=h.m6m38593npz0
    - Discussion on whether hardware is in scope for the CISA document
        - Bob clarified that the scope is software
        - Agreed that SPDX should consider hardware in scope, but CISA scope is different
    -

Future Meeting topics

- Continue discussion of feedback to CISA
- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Version series license families

Backlog

- See backlog at **“Backlog”** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-09-16

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-09-16

PR: https://github.com/spdx/meetings/pull/935

Attendees

58. Alfred Strauch
59. Arthit Suriyawongkul
60. Dick Brooks
61. Elyas Rashno
62. Gary O'Neall
63. Gopi Krishnan Rajbahadur
64. Greg Shue
65. Helio Chissini de Castro
66. Joshua Watt
67. Karen Bennet
68. Karsten Klein
69. Kate Stewart
70. Marc-Etienne Vargenau
71. Maximillian Huber
72. Nicole Pappler
73. NISHANTH SANKARAN
74. Peter Monks
75. Rose Judge
76. Steven Carbno

Agenda

- Prioritize agenda
- Approve last week's minutes
- AI/Dataset Profiles 3.1 (fields about foundational model/RAG) - Gopi/Elyas/Kate
- Continue discussion of feedback to CISA
- 2.3 issues

- Clarification Needed on SPDX File Relationships in Absence of Direct Mapping https://github.com/spdx/spdx-spec/issues/1227
- SPDX 2.3.0 schema conflicts with documentation for Annotations https://github.com/spdx/spdx-spec/issues/1147

Notes

- Agreed to approve minutes
- Rearranged agenda
- Clarification Needed on SPDX File Relationships in Absence of Direct Mapping https://github.com/spdx/spdx-spec/issues/1227
    - We lack a relationship for describing the modified files to originating upstream. At a file to file level, we are coherent. But set of files modified from Upstream package.
    - Possibly consider derived from and contains. Also issue of which files are not present needs to be considered. Pick this up again next week. Looking for solution to use existing relationship, or consider adding one for upcoming version.
- AI/Dataset Profile 3.1 (Gopi/Elyas/Karen)
    - Gopi went through presentation, to explain the extensions for promptware vs agentware to interact with foundational models
    - Issue of sub-profiles, and dependencies between profiles may be needed for Agents and Prompts to be subprofiles of AI model. Since this was explicitly restricted before to only have dependencies on Software and Core. If we do this, we have to check that circular dependencies may not emerge. You should be able to definitely references, but have to be careful that no circular dependency emerge.
    - Max suggests this all just be part of AI profile, and there's classes for Prompt and Agent, rather than separate sub-profile. Steven showed a diagram with just classes, and there was general agreement that circular dependencies can emerge.
    - **Tentative decision:** ok to have class based dependencies between non core & software, and they do not create circular dependencies.
        - ACTION: Check with Alexios about Prompt class referencing Data & AI Profiles (we had it listed to the Software & Core profiles).
    - Subprofiles vs. Classes? We discussed this and it should be classes, based on the discussions. Art pointed out "This relaxation may slow the growth rate of Core profile too. As currently, sometimes we upgrade things to Core because of inter-profile limitations"
        - ACTION: look at moving recent additions to core should be moved back to more logical profiles.
- Brief question from Greg at very end on how prompts and requirements should be interacting. Kate pointed out that prompts are like operating a machine, and would trace back to requirements.

    - ACTION: Check we have a relationship to capture this dynamic between requirements class and prompts in the safety profile work.
- Next week: Focus on feedback to CISA response.
-

Future Meeting topics

- Continue discussion of feedback to CISA
- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Version series license families

Backlog

- See backlog at **“Backlog”** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-09-09

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-09-09

PR: https://github.com/spdx/meetings/pull/934

Attendees

77. Arthit Suriyawongkul
78. Helio Chissini
79. Joshua Watt
80. Kate Stewart
81. Marc-Etienne Vargenau
82. Nicole Pappler
83. Peter Monks
84. Rose Judge
85. Steven Carbno

Agenda

- Prioritize agenda
- Approve last week's minutes
- Response to CISA 2025 Minimum Elements

Notes

SPDX Feedback for CISA 2025 Minimum Elements

- 2025 Minimum Elements for a Software Bill of Materials (SBOM) https://www.cisa.gov/resources-tools/resources/2025-minimum-elements-software-bill-materials-sbom
- Public comments open until 3 October 2025
- Draft of response: SPDX Feedback to CISA (will be open for anyone to edit for few days)
- Review of the CISA 2025 Minimum Elements together

- We need JSON examples for each field
- **SBOM Author**
    - SBOM Author should be legal person or it can be a SoftwareAgent as well – currently per SPDX 3.0 spec, it can be a tool as well
    - We may need additional restriction to limit this to only legal person (Person or Organization)
    - We can have more than one SBOM Author
    - There should be at least one legal entity.
    - Tool (2.3) and SoftwareAgent (3.0) can be included but there should be at least one legal entity (one who runs the Tool or responsible for the SoftwareAgent)
- **Software Producer**
    - How can we know who is the true original?
    - “originatedBy” vs “suppliedBy”
    - In the open source context, the supplier maintains the software in the interest of their users. The originator does not matter in this context.
- **Component Name**
    - What is the usefulness of having multiple component names ?
    - The same software can have different names in different markets but PURL is better for identification.
        - Note that this is for human to read (“This field is distinct from the Software Identifiers field.” page 7)
    - Ask CISA for use cases on why this is useful?
- **Component Version**
    - What if there’s no previous version?
    - What is considered a component?
- **Component Hash**
    - What is the usefulness of component hash?
    - From people's experience, file hash is more useful.
- **License**
    - How to capture the difference that can already captured by SPDX 3.0 hasConcludedLicense and hasDeclaredLicense relationship types?
- **Dependency Relationship**
    - Potentially several relationship types (may need to consider the direction of the relationship to)
- *We finished up to **“Tool Name”**. We can continue offline and pick up at this point next week.*

Future Meeting topics

- AI/Dataset Profiles 3.1 (fields about foundational model) - Gopi
- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Version series license families

Backlog

- See backlog at **“Backlog”** tab
  https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-09-02

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-09-02

PR: https://github.com/spdx/meetings/pull/933

Attendees

86. Alexios Zavras
87. Alfred Strauch
88. Arthit Suriyawongkul
89. Bob Martin
90. Dick Brooks
91. Gary O'Neall
92. Greg Shue
93. Henk Birkholz
94. Ilan Schifter
95. Joshua Watt
96. Karsten Klein
97. Marc-Etienne Vargenau
98. Nicole Pappler
99. Nisha Kumar
100. Steven Carbno
101. Victor Lu

Agenda

- Prioritize agenda
- Approve last week's minutes
- JSON-LD identifiers are not dereferenceable https://github.com/spdx/spdx-spec/issues/1259
- Software component - proposal - include in 3.0
- Review of supply chain profile https://github.com/spdx/spdx-3-model/pull/1098
- Discussion on any overlaps between Operations, Hardware and Safety (e.g. Requirement model)
- 2025 NITA Minimum Elements RFC

Notes

- Tools update - Python tools have not been updated in a while, is it abandoned?
    - Not abandoned, some activity
    - Maybe we should do a release - more visible
    - Need more resources to support
    - We do have a python library that supports SPDX 3, lower level library, doesn't support SPDX 2
        - New version which supports any RDF graph model
- JSON-LD identifiers not dereferenceable
    - Ilan created a script that generates the redirects with the RDF model as input
        - Script generates redirect information that is directly uploaded to S3
        - Gary will try out the script
        - Ilan will update the issue with the script documentation
    - Issue covers machine readable - not just human readable
    - Look into other tools that can handle the content type redirects (Gary)
- Software component
    - Ilan raised concerns on if this may move to Core it would be a breaking change
    - Joshua, Bob, Gary, and Alexios is in favor of merging now
    - Discussion on relationship with hardware
    - We may want to introduce a Core abstract class above the software component
        - This would not be a breaking change
    - Continue discussion on the pull request - make a decision by the end of the week as to whether this can be merged in for 3.0: https://github.com/spdx/spdx-3-model/pull/1044

Future Meeting topics

- AI/Dataset Profiles 3.1 (fields about foundational model) - Gopi
- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Version series license families

Backlog

- See backlog at **"Backlog"** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-08-26

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-08-26

PR: https://github.com/spdx/meetings/pull/932

Attendees

102. Alexios Zavras
103. Alfred Strauch
104. Bob Martin
105. Gary O'Neall
106. Ilan Schifter
107. Karen Bennet
108. Nisha Kumar
109. Steven Carbno

Agenda

- Prioritize agenda
- "NONE" and "NOASSERTION" in license expression:
  - https://github.com/spdx/spdx-spec/pull/1262#discussion_r2285769285
  - https://github.com/spdx/spdx-spec/issues/49
  - https://github.com/spdx/spdx-spec/issues/50
- FYI: New draft proposal for minimum SBOM elements, links to relevant docs here:
- JSON-LD identifiers are not dereferenceable https://github.com/spdx/spdx-spec/issues/1259
- Make 3.0 RDF URLs to work (need this due to new version policy: MAJOR.MINOR):
  - 1) Update version in annotations.ttl https://github.com/spdx/spdx-spec/pull/1242
  - 2) Setup RDF and schema URL directions https://github.com/spdx/spdx-spec/issues/1246
  - 3) Update example checks in CI https://github.com/spdx/spdx-spec/pull/1247
- Make 3.1 RDF URLs to work (need this for testing 3.1-rc:
  - 1) Update version in annotations.ttl https://github.com/spdx/spdx-spec/pull/1243
  - 2) Setup RDF and schema URL directions https://github.com/spdx/spdx-spec/issues/1249

    - 3) Update example checks in CI https://github.com/spdx/spdx-spec/pull/1244
- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Version series license families
- Review of supply chain profile https://github.com/spdx/spdx-3-model/pull/1098
-

Notes

- "NONE" and "NOASSERTION" in license expression:
    - https://github.com/spdx/spdx-spec/pull/1262#discussion_r2285769285
    - https://github.com/spdx/spdx-spec/issues/49
    - https://github.com/spdx/spdx-spec/issues/50
    - Do we use quotes or backticks for operators?
        - Quotes may be easier and may show up betters in titles
        - Also more readable
        - Consensus - “Quotes”
    - NONE and NOASSERTION - should it be on the license list?
        - It would be a change to the RDF spec
        - The legal team may have concerns on adding it
        - Agreed to separate this out as a different issue and resolve in the future - leave it as is for now
- New draft proposal for minimum SBOM requirements
    - https://www.cisa.gov/resources-tools/resources/2025-minimum-elements-software-bill-materials-sbom
    - https://www.cisa.gov/sites/default/files/2025-08/2025_CISA_SBOM_Minimum_Elements.pdf
    - https://www.cisa.gov/sites/default/files/2024-10/SBOM%20Framing%20Software%20Component%20Transparency%202024.pdf
- Hardware supply chain separation
    - Please review: https://github.com/stevenc-stb/spdx-3-model/tree/stevenc-stb-patch-1/model/SupplyChain - this points to a pull request - once merged, it will be in the profile-hardware branch
    - Concern of the “package” being referred to but not defined
        - Wanted to capture both hardware and software
        - Similar to software “package”
        - Gary to create an issue for further discussion:
        - Hardware group will create a definition to be reviewed - not sure where we will end up with the actual definition - perhaps a glossary

Future Meeting topics

- Discussion on any overlaps between Operations, Hardware and Safety (e.g. Requirement model)
- AI/Dataset Profiles 3.1 (fields about foundational model) - Gopi

Backlog

- See backlog at **“Backlog”** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-08-19

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-08-19

PR: https://github.com/spdx/meetings/pull/931

Attendees

110. Alexios Zavras
111. Alfred Strauch
112. Arthit Suriyawongkul
113. Bob Martin
114. Dick Brooks
115. Gary O'Neall
116. Henk Birkholz
117. Joshua Watt
118. Karsten Klein
119. Maximilian Huber
120. Nicole Pappler
121. Peter Monks
122. Steven Carbno

Agenda

- Prioritize agenda
- License Expressions case insensitivity question [Alexios]
- Separating supply chain from the hardware bill of materials
- 3.1
    - Need approval - Update version number in RDF URLs https://github.com/spdx/spdx-3-model/pull/1052
    - Need approval - Update version number in model documentation https://github.com/spdx/spdx-3-model/pull/1048
- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065 - start with this next week
- JSON-LD identifiers are not dereferenceable https://github.com/spdx/spdx-spec/issues/1259

- AI team need feedback on AutomationLevel enum (borrowed from ISO/IEC 22989:2022) - Other non-AI profiles may use this?
    - https://github.com/spdx/spdx-3-model/pull/1064
- Version series license families

Notes

- License expression case insensitive question
    - Alexios has been reworking the annex
    - Should we just make license expressions case insensitive?
        - It would simplify the syntax
        - The only case-sensitive parts are now operators (allowed upper or lower case, but not mixed) and “LicenseRef”, “AdditionRef”, “DocumentRef” (allowed exactly as shown)
        - Are there any tools that look for case sensitive operators?
            - Peter’s tool has a “spec” option that does check for case sensitive
        - We should also include the DocumentRef and LicenseRef
        - Consensus - all agree complete case insensitivity
        - Would change operators, additionref, documentref and licenseref case sensitivity
        - Case sensitivity doesn’t include the DocumentRef in the Annex - Alexios will include the update
    - Alexios will update the PR #1262
    -
- ISO Formatting: ISO only accepts MS word, will include license expressions, working on transforming the headings and titles in the markdown to headings in the word document.
    - Targeting to send an update to Rex next week after all the content is finalized.
    - Some work will still need to be done with the word document manually after Alexios sends the update.
- Separating supply chain from the bill of materials
    - Suggest having the supply chain as a separate profile
    - The supply chain profile can apply to software
    - There is some overlap between supply chain and build profile
    - Build profile is designed to align with SLSA
        - SLSA has been updated and is no longer in sync
    - We could include important parts of the current build profile in the supply chain
    - Use case: ESP32 device with wifi and bluetooth - would this be one or 3 devices and which profile would we use?
        - One chip would be one piece of hardware - could contain different die components
        - 3 components would be capabilities
        - The die components would be more of a supply chain
        - Firmware would be a software profile with a relationship - runsOn or dependsOn

        - Build profile may not need to be replaced - slightly different than the complete software supply chain
            - Need to consider vulnerability traceability
            - Related to operations and threat profile
            - Current build profile supports traceability - would like to have the supply chain provide the same functionality
        - Build may be deprecated in the future
            - We'll work out the details in a future post 3.1 release
        - Supply chain will deal with general artifacts (both hardware and software)
        - Supply chain profile should be able to live without the hardware
        - Hardware group approved
        - Two requested followup:
            - Check for any hardware specifics in the supply chain profile
            - Check for any potential breaking changes if we do have supply chain profile cover the build profile functionality
        - Steven will create a pull request in the hardware branch
- Update version number in RDF URLs in develop branch 3.0.1 -> 3.1
    - https://github.com/spdx/spdx-3-model/pull/1052
    - approved
- Update version number in model documentation
    - https://github.com/spdx/spdx-3-model/pull/1048
    - Everything to be changed to "SPDX 3" - Art take this
- JSON-LD identifiers are not dereferenceable
    - https://github.com/spdx/spdx-spec/issues/1259
    - URLs should need at least major version in URL
    - Major-only version will point to latest published major.minor version
- AI team need feedback on AutomationLevel enum (borrowed from ISO/IEC 22989:2022)
    - https://github.com/spdx/spdx-3-model/pull/1064
    - People should read and comment on the issue

Future Meeting topics

- Discussion on any overlaps between Operations, Hardware and Safety (e.g. Requirement model)
- AI/Dataset Profiles 3.1 (fields about foundational model) - Gopi

Backlog

- See backlog at **"Backlog"** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-08-12

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-08-12

PR: https://github.com/spdx/meetings/pull/930

Attendees

123. Alexios Zavras
124. Alfred Strauch
125. Arthit Suriyawongkul
126. Bob Martin
127. Dick Brooks
128. Gary O'Neall
129. Greg Shue
130. Ilan Schifter
131. John Horan
132. Joshua Watt
133. Karen Bennet
134. Karsten Klein
135. Kate Stewart
136. Maximilian Huber
137. Michael J Herzog
138. Nicole Pappler
139. Nisha Kumar
140. Rose Judge
141. Steven Carbno

Agenda

- Any profiles ready for merge?
- License Expressions case insensitivity question [Alexios]
- PURL update
- Discussion on any overlaps between Operations, Hardware and Safety (e.g. Requirement model)

- Service profile (3.1-dev) is online now: https://spdx.github.io/spdx-spec/v3.1-dev/model/Service/Service/
    - Note that the IRI in metadata is wrong. Will be fixed by this PR https://github.com/spdx/spdx-3-model/pull/1052
- 3.1
    - Update versions in model documentation https://github.com/spdx/spdx-3-model/pull/1048
    - Update versions in RDF URLs https://github.com/spdx/spdx-3-model/pull/1052
- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Software component https://github.com/spdx/spdx-3-model/pull/1044
- AI/Dataset
    - Approved in AI/Dataset team, need review from Tech team for merge
        - Let DatasetPackage uses artifactSize instead https://github.com/spdx/spdx-3-model/pull/1069
        - Add Dataset/inLanguage https://github.com/spdx/spdx-3-model/pull/1066
    - Discussed in AI/Dataset team, need more input from Tech team
        - Revise Core/standardName and AI/standardCompliance descriptions to show their relationship https://github.com/spdx/spdx-3-model/pull/1067
        - Add automationLevel https://github.com/spdx/spdx-3-model/pull/1064

Notes

- Profiles ready for merge?
    - Merge Hardware profile
    - Diagram is not ready yet, will be in a separate PR later
    - There is a pending PR for FUSA to Hardware profile (#1073), which has to be merged before https://github.com/spdx/spdx-3-model/pull/1073 (merged)
- License Expressions case insensitivity question [Alexios]
    - Updating spdx-license-expressions annex based on last week joint tech / legal call
    - Currently, operators case sensitive (AND, OR,WITH)
    - Currently, license identifiers are case insensitive - but we should keep the canonical case
    - LicenseRef- is case sensitive and Addition-Ref, but what comes after are sensitive
    - Inconsistent with current Grammer
    - DocumentRef- not documented, but propose we keep consistent with LicenseRef- and AdditionRef-
        - No disagreement
    - NONE and NOASSERTION are now added to the expression syntax, what should be the case?

        - Case insensitive since most tooling will treat it as case insensitive
    - RDF section is out of date
        - We will remove this section
- Update from the PackageURL standardization - Michael Herzog
    - Slides
    - Plan to submit to ECMA on September 1, expected approval in December
    - Introduction of JSON Schemas
    - Shift focus from generic PURL component rules (7 components) to registered PURL Types
    - New PURL type for non-packaged software “scid” (Software Component IDentification) https://github.com/package-url/purl-spec/issues/516
    - PURL spec re-written in Markdown: https://github.com/package-url/purl-spec/pull/586
    - VERS specification for version range https://github.com/package-url/vers-spec/
    -

Future Meeting topics

- Discussion on any overlaps between Operations, Hardware and Safety (e.g. Requirement model)
- August 12 - PURL update from Michael Herzog

Backlog

- See backlog at **“Backlog”** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-08-05

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-08-05

PR: https://github.com/spdx/meetings/pull/926

Attendees

1. Alexios Zavras
2. Alfred Strauch
3. Arthit Suriyawongkul
4. Dick Brooks
5. Gary O'Neall
6. Greg Shue
7. Ilan Schifter
8. Joshua Watt
9. Karen Bennet
10. Karsten Klein
11. Kate Stewart
12. Matt Rutkowski
13. Maximilian Huber
14. Nicole Pappler
15. Rose Judge
16. Steven Carbno
17. Ummo Schwarting
18. Victor Lu

Agenda

- Safety Profile
- Discussion on any overlaps between Operations, Hardware and Safety (e.g. Requirement model)
- Service profile (3.1-dev) is online now: https://spdx.github.io/spdx-spec/v3.1-dev/model/Service/Service/
    - Note that the IRI in metadata is wrong. Will be fixed by this PR https://github.com/spdx/spdx-3-model/pull/1052

- 3.1
    - Update versions in model documentation https://github.com/spdx/spdx-3-model/pull/1048
    - Update versions in RDF URLs https://github.com/spdx/spdx-3-model/pull/1052
- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model: https://github.com/spdx/spdx-3-model/issues/1065
- Software component https://github.com/spdx/spdx-3-model/pull/1044
- Revise Core/standardName and AI/standardCompliance descriptions to show their relationship https://github.com/spdx/spdx-3-model/pull/1067
- Add Dataset/inLanguage https://github.com/spdx/spdx-3-model/pull/1066

Notes

- Translation of spec into word document - will send email to Rex tomorrow AM.
    - Some manual edit later is necessary
    - Bulk of things can be done automatically.
    - Language translations will pick up after word version for Rex is done.
- Safety Profile
    - Nicole did an overview of the classes planned for 3.1 and rationale behind new fields.
    - Question on verifiedUsing - slightly different semantic from the Artifact (Artifact includes the verification value in addition to the method)
    - Karsten - Threat modeling
        - Nicole - not currently included
        - Karsten is interested in including threat modeling
        - Greg noted it will be needed for CRA compliance issue
        - Steve - threat involves the operational environment, perhaps the operations team should be involved
        - Greg - needs to include information on where it is deployed (operations)
        - Karsten - threat model needs to include “controls”
        - Related - MITRE defend 3 - graph based thread modeling
        - There may already be standards out there
        - Proposal for a new profile “Threat Modeling”
        - Ummo - operations could be a place to include, but there are a lot of other cross-cutting issues - could be implemented in the operations profile
        - Nicole - threats are not that static - do we want to only model threats, or the complete threat analyzers
        - Karsten - different approaches to threat modeling - ad hoc or use existing patterns (e.g. CAPECS)

        - Karsten agree to lead, Nicole, Alfred, Kate, Greg, Steven are interested in contributing
- Component Proposal
    - PR https://github.com/spdx/spdx-3-model/pull/1044
    - Benefit - significant reduction in data
    - When producing an SBOM - you'll probably translate to packages similar to today
    - Greg - is sources used to build an executable part of the model?
        - Alexios - no necessarily executable, more the SPDX Package
        - The proposal is for more generic packages - can be used to associate sources
        - Would like to see the impact on Zephyr
    - Joshua
        - Would save a huge amount of space - generally in favor
        - Can we use a relationship between packages rather than a different Component class
            - Alexios - Package is an artifact, so somewhat different
    - Max - Could be complicated for consumers - will need to be implemented
        - Alexios - target is more for storage, not exchange
        - We could state that these should never appear in documents
    - Steven - is this part of a build - is this a bundle
        - Not a bundle since we're not combining the packages
        - Important to include the hierarchy rules
    - Karsten - Versions may have shared parts, but may diverge, +1 on the ability to reduce duplication and support grouping
    - Joshua - interested in using Components in documents
        - Alexios - may not need the complete hierarchy
        - Can be thought of as a way to group packages
    - Steven - impact on vulnerabilities - would the vulnerabilities be "grouped" through the components
        - Joshua - yes - this is a key use case
        - Would this actually save data - Joshua - yes for Yocto
    - Joshua - possibly flip the relationship direction
        - You'll want to have one component relate to multiple concrete packages
        - Propose use instanceOf relationship
        - Advantage of using fanout
        - Steven - since relationships are immutable, we can't add instances later, so we'll likely still have a large number of relationships
        - Different uses - if you mint during creation vs minting once you have the whole view
    - High level issues:
        - Direction of the relationship
        - Balance of exchanged document size vs. consumer implementation complexity

    - Is the relationshipship between packages and components the same as the relationship between component

Future Meeting topics

- Discussion on any overlaps between Operations, Hardware and Safety (e.g. Requirement model)
- August 12 - PURL update from Michael Herzog

Backlog

- See backlog at **“Backlog”** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-08-05 - Joint Tech/Legal

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech & Legal Team Meeting 2025-08-05

PR: https://github.com/spdx/meetings/pull/927

Attendees

19. Alexios Zavras
20. Bob Martin
21. Gary O'Neall
22. Karen Bennet
23. Kate Stewart
24. Ria Farrell
25. Steve Winslow
26. Victor Lu

Agenda

- Goals:
  - Close on the NOASSERTION / NONE license expression issue (several years old and many / most of the tools do not follow the spec)
  - Clean up the old issues in the repos – either decide we won't fix them or decide on a path to get them implemented
- Tentative topics:
  - adding NOASSERTION and possibly NONE to the license expressions: https://github.com/spdx/spdx-spec/issues/50
  - relationship between licenses: https://github.com/spdx/spdx-spec/issues/13
  - Closing out the older spec repo licensing issues: https://github.com/spdx/spdx-spec/issues?q=is%3Aissue%20state%3Aopen%20label%3A%22profile%3A%20licensing%22%20sort%3Acreated-asc
  - Closing out the older model repo licensing issues: https://github.com/spdx/spdx-3-model/issues?q=is%3Aissue%20state%3Aopen%20label%3AProfile%3ALicensing%20sort%3Acreated-asc

Notes

- Should we include NOASSERT & NONE in license values?
    - License expressions being combined between files; where there is NONE & NOASSERTION. By adding this it makes it easier to combine.
    - Consideration of use with "AND" only. NONE & NOASSERTION should be on their on their own. Semantically using AND conjunction is only one makes sense. OR doesn't make sense semantically.
    - For simple licensing, this is the case.
    - For expanded licensing, it's been added already to conjective license set.
    - Concern about it being a breaking change? No, only additive to RDF model. Target to 3.1
    - Gary - Concern is tooling allows for NONEs & NOASSERTIONs in AND/OR today due to the complexity. Make it clear in best practices guide what makes sense or not.
    - Discussion of handling in "WITH", NONE WITH exception for instance, doesn't make sense. So keep it to "AND" and "OR".
    - When used in an "AND" it makes sense, it is not coherent to use in "OR", but is syntax permitted.
    - Simple license expression will update syntax - Alexios will do PR and reference both issues (so will close issues)
    - Update Disjunctive documentation to be explicit they should not use NONE & NOASSERTION.
- https://github.com/spdx/spdx-spec/issues/13
    - How handling translations? Sets of related licenses.
    - Intent of Steward. Do we think of "separate" from matching guidelines, and have separate ones added to license list?
    - View from discussion is to put in in XML files for License list. All translations from steward should have language suffix but common name.
    - Remember: ported/unported are different license ids.
    - Next steps: Legal team to take a look through EUPL and decide what to propose. Steve to take this to legal team to discuss, and transfer issue to license list XML. Proposed schema change in license list XML issue.

2025-07-29

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-07-29

PR: https://github.com/spdx/meetings/pull/924

Recording:
https://zoom.us/rec/share/dS_CtUMyWJ4obyrYQnH-eprIjO30-Q0uRVXhL1Bv0C7moeDING8Hd_RGdkrCTnmp.SSGnZqSE7ktrJUv0

Attendees

1. Alexios Zavras
2. Alfred Strauch
3. Arthit Suriyawongkul
4. Bob Martin
5. Gary O'Neall
6. Greg Shue
7. Ilan Schifter
8. Joshua Watt
9. Karen Bennet
10. Karsten Klein
11. Matt Rutkowski
12. Nicole Pappler
13. Peter Monks
14. Steven Carbno
15. Ummo Schwarting
16. Victor Lu

Agenda

- Approve previous minutes
- Hardware Profile & Preliminary tooling (Alfred & Steven)
- Discussion on requirements - operation profile sync with other profiles

- SPDX GitHub Org Profile README is active: https://github.com/spdx .
  Changes can be made with a PR to https://github.com/spdx/.github.
  Please review and suggest changes
- 3.0 ISO submission
  - 3.0.2 milestone
    - spdx-3-model: https://github.com/spdx/spdx-3-model/milestone/8
    - spdx-spec: https://github.com/spdx/spdx-spec/milestone/13
- 3.1
  - Update spec-parser to generate MkDocs config for new profile
    https://github.com/spdx/spec-parser/pull/190
  - 3.1-rc milestone
    - spdx-3-model: https://github.com/spdx/spdx-3-model/milestone/7
    - spdx-spec: https://github.com/spdx/spdx-spec/milestone/12
  - Update versions in model documentation
    https://github.com/spdx/spdx-3-model/pull/1048
  - Update versions in RDF URLs
    https://github.com/spdx/spdx-3-model/pull/1052
- 3.0 OR 3.1: Introducing digital/cryptographic signatures to the model:
  https://github.com/spdx/spdx-3-model/issues/1065
- Software component https://github.com/spdx/spdx-3-model/pull/1044

Notes

- Hardware Profile discussion
  - Product definition & Supply chain definition
  - System and Organization Control (SOC)
  - SysAuditor tool that can on a hardware and creates an inventory of hardware and software on that hardware.
  - Get IDs of hardware and software. Identify roles.
  - This will also include compliance identification.
  - Demo. An SPDX SBOM JSON of a physical hardware produced by the tool.
  - Joshua noted dependsOn relationship should be a lifecycle scoped relationship - default runtime?
  - Discussion on how dictionary keys are defined to be unambiguous
    - Keys are defined in the specification referred to from the Hardware class
  - Can we get access to the tool?
    - Not an open source product - contact Steve and Alfred for access
  - Can you have bundles of bundles?
    - Yes
  - Important point - SPDX support both supply chain and H/S/BOM information
  - How does operations when you push out changes relate?
    - Good future discussion
  - Any possible overlaps in relationship types should be added as issues or pull requests on the hardware profile

- LF AI now has a security and compliance workgroup - see https://github.com/lfai/security-and-compliance
- ISO: 2 new milestones - 3.0.2 what we send to ISO, 3.0.3 is what is final ISO based on any feedback from ISO review
    - Updates are going into 3.0.1 - note that all changes need to be merged into the develop branch
        - Plan is to sync with develop after 3.0.2 is complete
    - Change the URI scheme to not include the patch level (e.g. 3.0 not 3.0.1)
        - Will we have one RDF file or one per patch
        - The RDF files will change per patch release - even just descriptions
        - OK to have updates to the patch release - they will not breaking changes
        - Publish both the 3 level and 2 level RDF file - have a 2 level that is always the latest
            - Terms have to be stable - IRIs will always be 2 levels
            - File names will be 3 level
            - Patch levels will be non-functional only
- Bob asked if tooling would be easier for upgrading from 3.0 to 3.1
    - Yes - consensus from all tooling providers who spoke up
    - Bob mentioned that some of the commercial tooling vendors are waiting for library support

Announcements

- SBOM for AI Use Cases 0.3 released https://github.com/aibom-squad/SBOM-for-AI-Tiger-Team/blob/main/SBOM-for-AI-Use-Cases/SBOM_for_AI_Use_Cases_(FinalDraft_v0.3).pdf

Future Meeting topics

- Nicole on Safety: Target Aug 5, 2025
- Licensing: Target August 5, 2025 - 1 hour earlier than Tech call.
- Discussion on any overlaps between Operations, Hardware and Safety (e.g. Requirement model)

Backlog

- See backlog at **“Backlog”** tab https://docs.google.com/document/d/1NdHYU_VZtLacD4bEmf2GiUVRTbrcev1beaJpq8s8-pU/edit?tab=t.4wfxhy2gdx3y

2025-07-22

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-07-22 | PR: https://github.com/spdx/meetings/pull/919

Attendees

17. Alfred Strauch
18. Bob Martin
19. Dick Brooks
20. Gary O'Neall
21. Greg Shue
22. Ilan Schifter
23. Joshua Watts
24. Kate Stewart
25. Matt Rutkowski
26. Nicole Pappler
27. Rose Judge
28. Steven Carbno
29. toscaliz

Agenda

- Approve previous minutes
- Operations Profile
- Re-org SPDX repo (add spdx-tools org and move tooling projects there)
- BSI TR-03183

Notes

- Operations Profile
  - Video of Ummo going through Operations Profile
  - Scope refined to be business operations & specific processes being addressed.
  - Adding examples
  - Ilan appreciates we're given the "why" of this and gap.
  - Metadata to help communicate operation components. Export Control, Cryptography, etc.

        - Discussion of shifting information, and consideration on using relationships.
        - When will there be a PR, for us to start to integrate?
            - Update branch needed ASAP
            - Resolve Lifecycle & Supply Chain. Hardware & Operation need to sync.
            - Anything that affects Core we want to get into RC1
            - Target Ummo & Marcel to be at the next meeting.
- Release Candidate initial criteria
    - Core should be solid
    - Hardware profile
    - Updates on Security, etc.
- Reorg SPDX github organization
    - Split into different organizations
    - What about a landing page?
    - A public repo called .github will show up as README for work. (Joshua to take pass)
        - https://github.com/spdx/.github/tree/main/profile
    - Request to Outreach to compose it. - Bob & Ilan to take it forward
    - Fix the old ones that haven't been touched as ATTIC?
    - Classify repos by TOPICs - appears under about - Ilan has seen ways here too.
    - CC0 or Community License for .github
    - Joshua and Ilan added as maintainers for the .github repo
    - Ilan will follow-up with the outreach team
- BSI TR-03183
    - Joshua spooling up on SBOMs CRAs
    - Version 2 published last Sept.
    - Architecture - issues in SPDX repo
    - BSI Extension - agreed to be added into repo.
    - Ask to add Joshua

Announcements

- Allan Friedman leaving CISA
    - CISA SBOM community meetings are TBD
    - Hardware focus

Future Meeting topics

- Alfred & Steven getting ready to give a demo of some tooling for SPDX 3.1 - to illustrate how to perceive the tools. Target: Jul 29, 2025
- Nicole on Safety: Target Aug 5, 2025
- Licensing: -- joint call to be scheduled.

2025-07-15

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-07-15 PR: https://github.com/spdx/meetings/pull/918

Attendees

- Alfred Strauch
- Arthit Suriyawongkul
- Bob Martin
- Dick Brooks
- Ilan Schifter
- Joshua Watts
- Max Huber
- Nicole Pappler
- Nisha Kumar
- Rose Judge
- Steven Carbno
- Victor Lu

Agenda

- Approve previous minutes
- Prioritize agenda
- ISO
    - The RDFs should only go to second-level version https://github.com/spdx/spdx-3-model/issues/1046
        - `https://spdx.org/rdf/3.0.1/terms/Core/Element` → `https://spdx.org/rdf/3.0/terms/Core/Element`
        - Need updates in documentation, tools and CI
- JSON-LD identifiers are not dereferenceable https://github.com/spdx/spdx-3-model/issues/1056
- 2.3 issues
    - Cardinality on external document references is wrong https://github.com/spdx/spdx-spec/issues/812

    - Fix broken Figure C.1 in Annex C
      https://github.com/spdx/spdx-spec/pull/1222
- ~~Logistics for 3.1-rc1~~
    - ~~Create GitHub Milestone “3.1-rc1” in both spdx-spec and spdx-3-model~~
    - ~~Update CI and/or spec-parser to allow new namespaces/profiles in 3.1 (and keep compatibility with 3.0) spec_parser/mkdocs.py~~
      ~~https://github.com/spdx/spdx-spec/issues/1231~~
- ~~Does an SPDX 3 require a Bom or an Sbom instance as a root element of SpdxDocument? https://github.com/spdx/ntia-conformance-checker/issues/268~~
- New concept - Software Component https://github.com/spdx/spdx-3-model/pull/1044 (want Alexios, Gary, Bob, Kate, Nicole, Ilan present)
- ~~1034 - Rose looking for review https://github.com/spdx/spdx-3-model/pull/1034 - AI: Kate~~
- Nisha: best practices for creating Relationship elements from package to license? https://github.com/spdx/spdx-spec/issues/1245

Notes

- Does an SPDX 3 require a Bom or an Sbom instance as a root element of SpdxDocument? https://github.com/spdx/ntia-conformance-checker/issues/268
    - Updated that BOM conformance should have root element, but SPDX document verifier does not require it. Have documented this in the issue.
- Logistics for 3.1-rc1
    - Create GitHub Milestone “3.1-rc1” in both spdx-spec and spdx-3-model - Kate to handle.
    - Update CI and/or spec-parser to allow new namespaces/profiles in 3.1 (and keep compatibility with 3.0) spec_parser/mkdocs.py - Art to take first pass, ask for review from Gary https://github.com/spdx/spdx-spec/issues/1231
    - Need Alexios to help with spec-parser.
- New concept - Software Component https://github.com/spdx/spdx-3-model/pull/1044 (want Alexios, Gary, Bob, Kate, Nicole, Ilan present)
- ISO update
    - Looking for contractor to make editorial changes in model/spec , and get it pushed out this month.
    - Template for translation from .pdf to word? Rex & Bob to get together.
- Nisha: need Steve Winslow or Alexios to provide input on how to use SPDX 3 to describe package license. File issue in spdx-spec repo.
- JSON-LD best practices - Ilan & Victor to discuss on Slack.

Announcements

- India SBOM Guidance:

    - CERT https://www.cert-in.org.in/PDF/TechnicalGuidelines-on-SBOM,QBOM&CBOM,AIBOM_and_HBOM_ver2.0.pdf
    - SEBI - https://www.sebi.gov.in/sebi_data/faqfiles/jun-2025/1749647139924.pdf
- AI area
    - TAIBOM from the UK is emerging with some interest. https://aibom.org/ - OpenID - Centralized vs Decentralized standards.
    - IBM released: IBM Risk Atlas Nexus 1.0.0 ontology https://github.com/IBM/risk-atlas-nexus

Future Meeting topics

- Nicole on Safety: Target Aug 5, 2025
- Alfred & Steven getting ready to give a demo of some tooling for SPDX 3.1 - to illustrate how to perceive the tools. Target: Jul 29, 2025

2025-07-08

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-07-08 PR: https://github.com/spdx/meetings/pull/917

Attendees

- Alfred Strauch
- Arthit Suriyawongkul
- Bob Martin
- Dick Brooks
- Gary O'Neall
- Henk Berkholz
- Ilan Schifter
- JC Ebersbach
- Jon Geater - Co-Chair SCITT
- Joshua Watts
- Max Huber
- Nicole Pappler
- Nisha Kumar
- Peter Monks
- Rose Judge
- Steven Carbno
- Victor Lu
-

Agenda

- Approve previous minutes
- Prioritize agenda
- SCITT
- 2.3 issues
    - Cardinality on external document references is wrong https://github.com/spdx/spdx-spec/issues/812
    - Fix broken Figure C.1 in Annex C https://github.com/spdx/spdx-spec/pull/1222
- Logistics for 3.1-rc1

    - Create GitHub Milestone “3.1-rc1” in both spdx-spec and spdx-3-model
    - Update CI and/or spec-parser to allow new namespaces/profiles in 3.1 (and keep compatibility with 3.0) spec_parser/mkdocs.py https://github.com/spdx/spdx-spec/issues/1231

Notes

- Minutes approved
- IETF SCITT presentation by Jonathan Geater
    - Supply Chain Integrity, Transparency and Trust
    - https://scitt.io/
    - https://datatracker.ietf.org/wg/scitt/about
    - https://github.com/ietf-scitt
    - Identity, Claim, Evidence, Artifact
    - Question on size of statement (output) - relatively small, can use hash of artifact
    - Question on input normalization - some implementations handle
- How to interoperate with SCITT
    - Henk suggested having a reference or example implementation that includes not only SBOMs but also VEXs and VDRs
    - Dick suggested that it would be very easy to register an SPDX SBOM in JSON format in SCITT
- Question on identities - how do I know who someone is?
    - Have to support multiple identity standards
    - API that abstracts the identity provider
    - [discussion on specific standards and what is supported currently and planned]
- Question - if want want to reference a proof inside an SPDX document, how would we use SCITT - can put a URI to the transparency data OR the complete receipt
- Question - relationship of SCITT to INTOTO - INTOTO is just another step in the lifecycle
- Currently - all known implementation of SCITT use lightweight ledgers (not blockchain)
- Does it make sense to have a SCITT integrity method to include SCITT in the SPDX documents?

2025-07-01

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-07-01PR: https://github.com/spdx/meetings/pull/915

Attendees

- Alfred Strauch
- Arthit Suriyawongkul
- Bob Martin
- Dick Brooks
- Gary O'Neall
- Joshua Watt
- Kate Stewart
- Marc-Etienne Vargenau
- Maximillian Huber
- Nicole Pappler
- Steven Carbno
- Victor Lu

Agenda

- Approve previous minutes
- Prioritize agenda
- Approve and merge translation https://github.com/spdx/spdx-3-model/pull/953
- ISO submission
- Schedule for 3.1 release candidate
- OpenJS
- OpenSSF OpenML SecOps paper
- Feedback from Open Source Summit - hallway track, etc.

Notes

- Approved minutes.

- ISO submission
    - Cover document ready from Bob
    - Request to have any last edits applied by Alexios & then Bob will regenerate word document. Want to keep one baseline.
        - 3.0.1 fixes since release are logged here: https://github.com/spdx/spdx-3-model/pull/1001
- Translations
    - Looking for a second Japanese reviewer to sign off on the text.
- 3.1
    - Each Profile Group need to report when ready to merge
        - Merge branches in to main
        - Need writeups from each profiles - website - what they are and how work together
    - There will be a 3.2 release
    - If Profiles are ready now, they can go into 3.1-rc1.
        - Services; Operations; Cryptology; Hardware; Safety; Security; AI&Data making progress.
    - Email to each of the profiles leads for when ready, response by next monday.
        - Tentative set date for 3 weeks from now.
        - If not, when ready for rc2
        - Identify changes for core
        - Gary to send email
        - Kate provides a set of lead emails to Gary.
- Outreach Liaison to OpenJS community
    - Comparison of use cases
    - Looking for volunteer to attend meeting
- Feedback from OSS NA
    - Gary, Kate, Joshua
    - Lot of SBOM presentations - with SPDX represented well
    - Tooling is still sore point - need more languages libraries
    - Dependency-Track not supporting SPDX; Cautions; should be able to get it merged.

2025-06-24

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-06-24 PR: https://github.com/spdx/meetings/pull/914

Attendees

- In alphabetical order
- Gary O'Neall
- Ilan Schifter
- Joshua Watt
- Kiyoshi Owada
- Nicole Pappler
- Norio Koboto
- Matthew Crawford
- Rose Judge
- Steven Carbno
- Bob Martin

Agenda

- Approve previous minutes
- Prioritize agenda
- General announcements
- spec-parser: exit(1) and print error messages at the end of program if there's an error https://github.com/spdx/spec-parser/pull/187
    - To address an issue with PR validation workflow reported by Steven during 2025-06-10 call

Backlog

- Clarify hasDeclaredLicense and hasConcludedLicense https://github.com/spdx/spdx-3-model/issues/1022
    - Call will be done with Legal to discuss this

- Post-3.0.1 Spec Update
    - Post-3.0.1 change log - PR: https://github.com/spdx/spdx-3-model/pull/1001
- Post-2.3 Spec update
    - [2.3] Fix broken Figure C.1 in Annex C - PR: https://github.com/spdx/spdx-spec/pull/1222
    - [2.3] Enable syntax highlighting for ABNF/XML - PR: https://github.com/spdx/spdx-spec/pull/1210
    - [2.3.1] Publish schema doc - PR: https://github.com/spdx/spdx-spec/pull/1220 (one for 2.3 is merged already)

Announcements

- BlackDuck supports 3.0
- SCITT presentation planned July 8, 2025

Notes

- Reviewed agenda no additions or changes
- Support for Dependency (by OWASP & Steve Springett) track will be accepted SPDX 3.0 - Gary working on script
- https://github.com/spdx/spec-parser/pull/187 will be dealt with by Joshua and Alexios
- Changes to 3.0.1 change log - keeping open may be part of ISO changes - no objections to merging
- Clean up of spec related to post 3 - new relationship
- Gary reviewed 2.3 PRs JASON issues
    - Dick has issues related to JASON and spec model differences - “describes” a package, subpackages - “contains” relationship, others “dependson
- Root element discussed - needs to be equivalent to 2.3 - Ilan has PR to be created - Should 2.3 issues be fixed for release or do we recommend moving to 3.0?
- Set a deadline for 2.3.1 pull requests first week of Sept. and schedule a release after

Actions

- Gary will deal with merge
- Provide a recommended migration date for 3.0 from 2.3 - 1-2 months

Future Meetings

- Security pull requests
- When will there be a formal release of the HW BOM and supply chain?
- General meeting on August or Sept. to go through Business Operations.

2025-06-17

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-06-17 PR: https://github.com/spdx/meetings/pull/913

Attendees

- Alfred Strauch
- Bob Martin
- Dick Brooks
- Gary O'Neall
- Ilan Schifter
- Joshua Watt
- Karen Bennet
- Kate Stewart
- Nicole Pappler
- Peter Monks
- Rose Judge
- Steven Carbno
- Victor Lu

Agenda

- Approve previous minutes
- Prioritize agenda
- General announcements
- hasSecurityContactPoint https://github.com/spdx/spdx-3-model/issues/861
    - Add phone and webpage as external identifier type? (Rose)
- Location and Event action data discussion - Steven
- Suggested changes for SoftwareService description https://github.com/spdx/spdx-3-model/issues/1013
    - PR: https://github.com/spdx/spdx-3-model/pull/1030
- Safety Profile Overview - Nicole

Backlog

- Clarify hasDeclaredLicense and hasConcludedLicense
  https://github.com/spdx/spdx-3-model/issues/1022
    - Call will be done with Legal to discuss this
- Post-3.0.1 Spec Update
    - Post-3.0.1 change log - PR: https://github.com/spdx/spdx-3-model/pull/1001
- Post-2.3 Spec update
    - New relationships in SPDX 2.3 spec? (Rose)
    - [2.3] Fix broken Figure C.1 in Annex C - PR:
      https://github.com/spdx/spdx-spec/pull/1222
    - [2.3] Enable syntax highlighting for ABNF/XML - PR:
      https://github.com/spdx/spdx-spec/pull/1210
    - [2.3.1] Publish schema doc - PR: https://github.com/spdx/spdx-spec/pull/1220
      (one for 2.3 is merged already)

Announcements

- SCITT registry for sharing disclosed materials is available and advancing to the standard. Use case around SBOMs and vulnerability reports. Link to SCITT proposed standard spec - see use case 2.2.1 for software supply chain and numerous references to SBOM artifacts as signed statements;
  https://datatracker.ietf.org/doc/draft-ietf-scitt-architecture/
    - Victor notes that in-Toto is for signed statement enterprise build process which in my understanding is for centralized identity. That is why I think DIF (distributed identity foundation) may play a role at the source or edge of the supply chain. I already discussed with DIF and Jan from DIF already joined SPDX slack workspace
- Security team has resumed meetings.

Notes

- Security contact point - relationship (Rose)
    - Discussed extending Contact point - with type of contact
    - hasContactPoint in relationshipTypes vocabulary in Core Profile and with contactType to be specific about security, regulatory, hardware, etc. Vocabulary.
    - Create subclass of relationship like assessmentRelationship, put in model/core/Classes.
    - Rose is working on PR for the next meeting.
    - Working on PR for website & phone number as own identifier types.
- Location
    - Recommendation is not to use creationtime - as it is not when the object is created.

    - Location - time; validity to location? This is what was known at a point in time. Timestamp rather that range is more appropriate. Hard to predict the future, so do what is known when it is "minted". Nicole agree. Steven to work on a PR
- Action Event Data
    - Not sure if we need it at this point in time. Preferring to use annotation instead. Static data related to actions. It was produced because of an action, will revisit if necessary.
- AI: Kate to review 1029 & 1027 on hardware branch needs reviews.
- Software Service - definition update needs a second reviewer: https://github.com/spdx/spdx-3-model/pull/1030 AI: Kate to add to queue to review and merge if ok.
- Safety Profile Overview (Nicole)
    - Walked through Functional Safety Case
    - Discussed Requirement Class Proposal; Requirement Context class.
    - Reuse Specification/Regulation from Hardware
    - Product Line Engineering example has been discussed as well (more generic property/behavior that is reused in different product lines)
    - verifiedUsing - Gary agrees just extending semantics. Thinks proposal should work.
    - Gary ok's with starting a branch for safety and start upstreaming. Profile-safety created.
    - Requirement will go to core profile (be used by hardware and safety)
- Next Week: Gary can be on the call, and those on site have lunch after.
    - Get Gary, Joshua, Kate, & Japanese contingent together for Lunch on Tuesday?
- Signing - SCITT & Intoto understanding.
    - Bob will work with Victor offline on SCITT.
    - SCITT - log of development environment (generic, any signed statement, inspection records from meat plant - trustworthy and provided by trusted party. Service's API)
    - SPDX is neutral to this. Any statement can be posted as a "signed" statement.
    - Minimum viable signing is X.509.
    - What are the partners that SPDX should work with SCITT, Intoto, DIF, … ? Not sure thing that there is anything for SPDX can do.
- COSINE Model Card extension and definition - June 25th - looking for someone to present.
    - Work with groups, how much can we capture in SPDX.
    - Need to see more use cases and examples out there.
    - Karen had Hugging Face discussions and is willing to talk to design phase and production; share experiences.
    - US needs - things not even thinking of that they should be.
    - ML Ops white paper, and define what needs to be included.
    - Mandatory lists being different. SPDX list is the framework, and we teach them how they map.
    - June 6 EO - NIST - bringing things together.

Future Meetings

- Open Source Summit is on June 24 -will be held..
- General meeting on July 3rd to go through Business Operations.

2025-06-10

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-06-10 PR: https://github.com/spdx/meetings/pull/910

Attendees

- Alfred Strauch
- Arthit Suriyawongkul
- Bob Martin
- Dick Brooks
- Jesse Porter (Qualcomm)
- Kate Stewart
- Nicole Pappler
- Peter Monks
- Steven Carbno
- Victor Lu

Agenda

- Approve previous minutes
- Prioritize agenda
- General announcements
- Validation for PR is not returning correct status - passes PR when spec parser returns ERRORS
    - https://github.com/spdx/spdx-3-model/actions/runs/15499592768/job/43644274069?pr=1029
- Attestation manifests and relation to SPDX.

Backlog

- Clarify hasDeclaredLicense and hasConcludedLicense https://github.com/spdx/spdx-3-model/issues/1022
    - Call will be done with Legal to discuss this

- Suggested changes for SoftwareService description https://github.com/spdx/spdx-3-model/issues/1013 ⇒ PR?
    - PR: https://github.com/spdx/spdx-3-model/pull/1030
- Post-3.0.1 Spec Update
    - Approve post-3.0.1 change log https://github.com/spdx/spdx-3-model/pull/1001
- Post-2.3 Spec update
    - New relationships in SPDX 2.3 spec? (Rose)
    - [2.3] Fix broken Figure C.1 in Annex C https://github.com/spdx/spdx-spec/pull/1222
    - [2.3] Enable syntax highlighting for ABNF/XML https://github.com/spdx/spdx-spec/pull/1210
    - [2.3.1] Publish schema doc https://github.com/spdx/spdx-spec/pull/1220

Notes

- Bob needs input on the draft cover letter.
- No concerns with last week's minutes - approved.
- Announcements:
    - SBOM Uses Cases - <insert link> until June 16th.
    - Dick EO puts NIST for secure software guidelines - OMD 2218 - secure by design and implementation. Removed concept of attestation form. CISA portal has be retained. Her eis the EO language: https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/
    - Here is an example of FUD about SBOM floating around; https://youtu.be/j9MB7oaq8aI?t=246
- Attestation topic
    - Role of SLSA for creating Attestation; Model signing is similar; C2PA is looking at this from a data perspective. In the Croissant meeting, thinking of capturing meta data for research papers. All these types of frameworks - centralized identity vs. distributed identities. How should we work with these different mechanisms?
    - Bob believes that an SBOM is an attestation, information about software, data & hardware.
    - Dick agrees it's an attestation from original software producer
    - https://docs.xygeni.io/xygeni-products/build-security/attestation-format
    - SPDX can vary from detailed level to high level. Lots of detail not captured by SPDX for data (compared to Croissant). Domain expertise questioned? If trying to get something to be automatically created by tooling - don't have to have everything in SPDX - should be able to point to things, and provide summaries.
    - Profiles in the ecosystem may be useful to provide multidimensional information for knowledge graphs. Figuring out how to point to other ecosystems may be the best way.
    - Ontologies for capturing information - want to be flexible.

    - In terms of tight integration - Kate believes we're there already, Steven agrees, but feels we need better tooling for helping individuals understand. Need better ways of describing relationship types.
    - Need to look at better descriptions of relationships.
    - Should we look at categories for relationship types.
    - PKO work from Bentley is adding some sophistication for hierarchical integration that may be of benefit - tighter way of defining beyond contains.
    - Relationships give tight integration, but fidelity of alternatives may be needed? Possibly different elements but related?
    - Victor defines the need for mapping of business controls to technical details. OSCAL is an example that needs to map to the technical controls. How to capture the information from SPDX info, and partner specifications.
    - Dick notes that well defined tree structure is important, but there's low hanging fruit around the content model for supplier names. Having guidance on what should be populated there. See: Link to Supplier Name guidance posted in the #SBOM SIG, https://www.linkedin.com/feed/update/urn:li:activity:7337945869616373760?utm_source=share&utm_medium=member_desktop&rcm=ACoAAABMsYcB3I6zhtjaqBqVcePEOQqxsZNzj5E
    - Victor points to https://arxiv.org/abs/2502.07223 - Distributed identity to be considered.
    - How can knowledge graphs be aligned for additional insights? Consider discussing this with Slava - detailed with source. More detailed in data profile in Croissant meetings.
- Validation Tooling
    - Firt reported from this PR https://github.com/spdx/spdx-3-model/actions/runs/15499592768/job/43644274069?pr=1029
    - Art can confirm the issue as well here: https://github.com/bact/spdx-3-model/actions/runs/15564791826/job/43826071759?pr=1 — the set -e still does not help because there's no non-zero exit.
    - We need non-zero exit from the spec-parser, so the GitHub workflow can know that there's something wrong. From spec-parser code, this line detect the error and log it: https://github.com/spdx/spec-parser/blob/014185824bc0d2080495b66fa1f923935737afaf/spec_parser/model.py#L100-L101
    - We may need to check the log after these following lines https://github.com/spdx/spec-parser/blob/014185824bc0d2080495b66fa1f923935737afaf/main.py#L11-L13
    - @Gary - can you aggregate intermediate results that are logged, and provide a final status update.
    - Steven to create an issue in spec-parser repo so validation workflow will function. Is this an old issue? So open issue https://github.com/spdx/spec-parser/issues/80
    - Proposed PR https://github.com/spdx/spec-parser/pull/187
- Victor
    - CD Foundation asserting that no one is using SBOM.
    - Can Art present to COSIGN? Possibly

- OASIS - COSIGN support - what should be in model card and datacard? Mandatory metrics, should they be revisited? Higher level info. Trying to get requirements from the field.

Future Meetings

- Business Operations Review - **target June 17th** - Ummo
- Open Source Summit is on June 24 - likely cancelled.
- General meeting on July 3rd to go through Business Operations.

2025-06-09 - Asia

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-06-09 - Asia

PR:https://github.com/spdx/meetings/pull/909

Attendees

- TAKASHI NINJOUJI (忍頂寺 毅)
- YOSHIYUKI ITO
- Kate Stewart

Agenda

- Prioritize agenda
- General announcements
- BOMops review
- Usage Profile - next steps
- Technical Operations Profile

Backlog

- Clarify hasDeclaredLicense and hasConcludedLicense https://github.com/spdx/spdx-3-model/issues/1022
    - Call will be done with Legal to discuss this
- Suggested changes for SoftwareService description https://github.com/spdx/spdx-3-model/issues/1013 ⇒ PR?
    - PR: https://github.com/spdx/spdx-3-model/pull/1030
- Post-3.0.1 Spec Update
    - Approve post-3.0.1 change log https://github.com/spdx/spdx-3-model/pull/1001
- 2.3 Spec update
    - New relationships in SPDX 2.3 spec? (Rose)
    - [2.3] Fix broken Figure C.1 in Annex C https://github.com/spdx/spdx-spec/pull/1222

- [2.3] Enable syntax highlighting for ABNF/XML https://github.com/spdx/spdx-spec/pull/1210
- [2.3.1] Publish schema doc https://github.com/spdx/spdx-spec/pull/1220

Notes

- **Operations is WIP,** sorting confusion
  - Business (export control, contractual, etc.) vs. Technical (config management & component management processes)
  - Technical operations is place holder term - need better name.
- **SPDX-Lite for 3.1** ?
  - Possible modifications ?
  - Further discussion of Industry profile common elements (telecom, auto, ??) for extending to SPDX-Lite
- **Service Profile** has been merged into 3.1 - some tweaking of terminology in process.
- Current new profiles for 3.1 are:
  - Functional Safety (FuSa) - Nicole
  - Hardware Profile - Steven & Alfred
  - Business Operations - Matthew
  - Services (merged) - Gary
  - AI & Data (being extended) - Gopi & Karen
  - Security (being extended) - Rose
  - Technical Operations - Kate?
    - Configuration management
    - Software Update
    - Product Line
  - Jasper - Software Update BOM ?
    - Will share information in future.
  - What next for Usage profile? Fold into TechOps?

Future Meetings

- Business Operations Review - target 17th; General meeting on July 3rd.

2025-09-08 - Asia

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-09-08 - Asia

Attendees

- TAKASHI NINJOUJI (忍頂寺 毅)
- Norio Kobota
- Nobuyuki Tanaka
- Yoshiyuki Ito
- Kate Stewart

Agenda

- Prioritize agenda
- General announcements
- CISA SBOM Mininum elements, feedback from SPDX.
- Openchain has SBOM study group → working group. Quality guide.

Backlog

Notes

- CISA minimum elements at: https://www.cisa.gov/sites/default/files/2025-08/2025_CISA_SBOM_Minimum_Elements.pdf
    - Draft concerns from SPDX review being collected at: SPDX Feedback to CISA
    - Discussing if OpenChain should formally submit it's own, or combine with SPDX or OpenSSF SBOM working group. Kobota-san to talk to Shane, and get back to Kate with plan.
- Openchain SBOM study group.
    - Started 6 months ago.
    - Some public and industry sector, defined guidelines & regulations.

- Private companies to generate and operate SBOM systems. Finding many issues in practice.
- Document: SBOM Document Quality Guide
- Disucssion of all the things that have seen going wrong. What is the best guidance for filling in the SBOM.
- Chapter 5 describes common issues, and recommended best practices.
- ACTION: Kate to share draft quality document with other SPDX community members for feedback in main tech call.
- Have covered SPDX light fields.

Future Meetings

2025-06-03

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-06-03 (PR: https://github.com/spdx/meetings/pull/893

Attendees

- Alfred Strauch
- Steven Carbno
- Nisha Kumar
- Joshua Watt
- Kate Stewart
- Ilan Schifter
- Victor Lu
- Dick Brooks
- Bob Martin

Agenda

- Approve previous minutes
- Prioritize agenda
- SPDX Examples question
- General announcements

Backlog:

- Clarify hasDeclaredLicense and hasConcludedLicense https://github.com/spdx/spdx-3-model/issues/1022
    - Call will be done with Legal to discuss this
- Suggested changes for SoftwareService description https://github.com/spdx/spdx-3-model/issues/1013 ⇒ PR?
- 3.0.1 Spec Update
    - Approve post-3.0.1 change log https://github.com/spdx/spdx-3-model/pull/1001
    -

- 2.3 Spec update
    - New relationships in SPDX 2.3 spec? (Rose)
    - [2.3] Fix broken Figure C.1 in Annex C https://github.com/spdx/spdx-spec/pull/1222
    - [2.3] Enable syntax highlighting for ABNF/XML https://github.com/spdx/spdx-spec/pull/1210
    - [2.3] Publish schema doc https://github.com/spdx/spdx-spec/pull/1221
    - [2.3.1] Fix broken Figure C.1 in Annex C https://github.com/spdx/spdx-spec/pull/1223
    - [2.3.1] Fix formatting/code highlight in Annex K https://github.com/spdx/spdx-spec/pull/1115
    - [2.3.1] Fix typos in schema descriptions https://github.com/spdx/spdx-spec/pull/1226
    - [2.3.1] Update version in front page https://github.com/spdx/spdx-spec/pull/1218
    - [2.3.1] Publish schema doc https://github.com/spdx/spdx-spec/pull/1220
-

Notes

- Add example 3 SPDX 3.0 files
    - https://github.com/spdx/spdx-examples/pull/106
    - Nisha looking human readable documentation for conversion and tool support.
    - Joshua pointed to "Using" repo - https://github.com/spdx/using
- News & Announcements:
    - SBOM use cases with minimum - document to be reviewed for publishing until June 16.
    - AI BOM use case document - open for freedback until June 4.
    - Microsoft sbom-tool now supports the generation and validation of SPDX 3.0 https://github.com/microsoft/sbom-tool/releases/tag/v4.0.3
    - Welcome to the hashtag#SBOM Special Interest Group (hashtag#SBOM SIG). This public group has been established to foster the respectful and collaborative free exchange of information to help people implement SPDX and CycloneDX SBOM in practice and use this information to monitor for software supply chain risks and vulnerabilities. Contributors are asked to post information that will help others with their SBOM journey to be successful. https://www.linkedin.com/groups/13274064/
        - Let SPDX outreach team know about it
        - Add links to SPDX implementers call for those working in that direction.
- Summary from each working group for monthly call
    - Send info to Rose.
    - Kate to figure out who's sending out request these days (Rose, Rob, ?)
- Joint meeting with legal has been penciled in for July <kate to fill in date>
    - Associated License? Any other mentions?
- Technical Operations Working Group

    - Operations Profile has been clarified to be "business operations" - nearing completion of original task.
    - Cross between group with Configuration.
    - Ramifications of topic is causing confusion.
        - Bulid, Configuration, …
        - Need to clarify what this group should define. Clarify perspective.
        - Need to set Goals & Objectives.
        - Need planned configuration vs. managing configurations over time.
        - Services doesn't need to be harmonized.
        - Build, Hardware, Data, AI, Safety, Risk Management (Policy) - need to be harmonized.
        - Operation controls - what should/needs to be considered.
        - Operations
        - Lifecycle is bigger concept. Datasets, models, hardware,
    - Configuration
        - Hardening guidance - Bob to provide linkage to work he's aware of
            - https://saf.mitre.org/
            - https://anchore.com/blog/automate-stig-compliance-with-mitre-saf/
        - Usage profile from Japanese had some overlap with this. - Kate to deep dive into history and find some of the prior work.
    - Lifecycle of SBOM type -
    - Operations draft from Alfred & Steven.
        - Files outside of Software?
        - New Relationships?
    - Discover if something is turned on or off while operating.
        - Gather info during operations and distribute.
    - In security space, Nisha has been encountering this. Don't care so much about what's there, but how are they operating and being used. Kernel Configurations & Kubernetes configurations are coming up in the wild. What they've asked the systems to do, is what the systems are doing.
    - Metrics gathered need to be exportable to central database. Common data exchange, what systems need to understand each other.
    - Bespoke schemas for data collection from different tools, need to be harmonized.
    - Level of abstraction & organizations able to define their key data elements appropriate to who they are.
    - We need to avoid to sliding into these vendors materials - Bob ok with linking and conveying strategic view.
        - Linkage and Relationships are ok.
    - Intel's hardware (or asset based approach) https://arxiv.org/abs/2502.19567 - some discussions with Santiago on this topic
- SHACL bug for Extension found (PR proposed) - need to decide about 3.0.1 inclusion https://github.com/spdx/spdx-3-model/issues/1017#issuecomment-2822649891 → 3.0.1
    - Bob joined, Ilan, Bob, Josh agreed to go forward with rerelease.

Future Meetings:

- Business Operations Review - target 17th; General meeting on July 3rd.

2025-05-27

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-05-27 PR: https://github.com/spdx/meetings/pull/892

Attendees

- Alfred Strauch
- Arthit Suriyawongkul
- Gary O'Neall
- Karsten Klein
- Kate Stewart
- Maximilian Huber
- Steven Carbno
- Ilan Schifter

Agenda

- Approve previous minutes
- Prioritize agenda
- Add taxonomy type for hardware
  https://github.com/spdx/spdx-3-model/pull/1027
- Adding Regulation class (continue)
  https://github.com/spdx/spdx-3-model/pull/1015
- Suggested changes for SoftwareService description
  https://github.com/spdx/spdx-3-model/issues/1013 ⇒ PR?
- Follow up spdx-examples fixes & merge approved PRs (Update and to be sorted offline)
  - Merge approved PRs https://github.com/spdx/spdx-examples/pulls
- SHACL bug for Extension found (PR proposed) - need to decide about 3.0.1 inclusion
  https://github.com/spdx/spdx-3-model/issues/1017#issuecomment-2822649891 → 3.0.1
- New relationships in SPDX 2.3 spec? (Rose)
- Clarify hasDeclaredLicense and hasConcludedLicense
  https://github.com/spdx/spdx-3-model/issues/1022
  - Call will be done with Legal to discuss this

Notes

- Minutes approved
- The need to communicate the status of ISO submission

“Taxonomy” class in Hardware Profile

- https://github.com/spdx/spdx-3-model/pull/1027
- “Taxonomy” class could also be used for the use case of different types of safety risk assessment in AI Profile, see https://github.com/spdx/spdx-3-model/issues/650
    - “high” in EU General Risk Assessment Methodology and “high” in EU AI Act mean different thing
- Rename “Taxonomy” to “DefinedType” and move to Core Profile
    - Core/DefinedType
- Hardware Profile WG will discuss within the group, update the diagram and make a PR
- Remove “DefinedHazard” type and replace with “DefinedType” - proposal to HW group
- Use the “DefinedType” rather than “Taxonomy” in future AI profile

Others

- Cryptographic algorithm list
- CycloneDX-SPDX mapping work from Bosch https://github.com/OpenChain-Project/SBOM-sg-SEPIA

2025-05-20

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-05-20 PR: https://github.com/spdx/meetings/pull/887

Attendees

- Alfred Strauch
- Arthit Suriyawongkul
- Bob Martin
- Dick Brook
- Ilan Schifter
- Kate Stewart
- Nicole Pappler
- Steven Carbno
- Victor Lu

Agenda (please add new topics to the end of the list)

- Approve previous minutes
- Prioritize agenda
- Adding Regulation class (continue) https://github.com/spdx/spdx-3-model/pull/1015
- Suggested changes for SoftwareService description https://github.com/spdx/spdx-3-model/issues/1013 ⇒ PR?
- Follow up spdx-examples fixes & merge approved PRs (Update and to be sorted offline)
    - Merge approved PRs https://github.com/spdx/spdx-examples/pulls
    - https://github.com/spdx/spdx-examples/pull/109 is ready to merge
- SHACL bug for Extension found (PR proposed) - need to decide about 3.0.1 inclusion https://github.com/spdx/spdx-3-model/issues/1017#issuecomment-2822649891 → 3.0.1
- New relationships in SPDX 2.3 spec? (Rose)
- Clarify hasDeclaredLicense and hasConcludedLicense https://github.com/spdx/spdx-3-model/issues/1022
    - Call will be done with Legal to discuss this

Notes

- Discussion of operations profile
    - Split into Business & Technical
    - Kate brought up prior work on "Usage" from Japanese team that should be considered https://github.com/spdx/spdx-3-model/tree/usage-profile
    - Next steps:
- Discussion on Hardware Profile
    - Outstanding PRS to be merged.
    - Add taxonomy type for hardware https://github.com/spdx/spdx-3-model/pull/1027 → Merged.
    - requirementsCatagory typo https://github.com/spdx/spdx-3-model/pull/1025 → Kate to review
    - Some concerns overlap with the primary purpose field that already exists. Many different ways that someone can categorize the same item. https://github.com/spdx/spdx-3-model/blob/develop/model/Software/Properties/primaryPurpose.md
    - Should this be core property? Software or systems?
- JDF - different formats may be needed. Next steps - Kate to follow up on thread.
    - Looking for spot that illustrates need. Can produce what necessary.
    - Transmittal paper needs drafting - planning on working on Thursday.
- OMG pages have been corrected.
- ELISA call - who to talk about Java tools.
- Microsoft generating SPDX 3.0 Core, Software & License profiles. Ameet is anxious for HBOM to be published.

2025-05-13

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-05-13 PR: https://github.com/spdx/meetings/pull/886

Attendees

- Joshua Watt
- Nicole Pappler
- Karen Bennet
- Steven Carbno
- Alfred Strauch
- Karsten Klein
- Dick Brooks
- Gary O'Niel
- Karen Bennet
- Ilan Schifter

Agenda (please add new topics to the end of the list)

- Approve previous minutes
- Prioritize agenda
- Adding Regulation class (continue) https://github.com/spdx/spdx-3-model/pull/1015
- Add naming convention and cardinality to Markdown doc https://github.com/spdx/spdx-3-model/pull/982
    - Approved
- Suggested changes for SoftwareService description https://github.com/spdx/spdx-3-model/issues/1013
    - Commented
- artifactSize is added post-3.0.1 but has 3.0.1 IRI https://spdx.github.io/spdx-spec/v3.1-dev/model/Software/Properties/artifactSize/ https://github.com/spdx/spdx-3-model/pull/966
    - I think this stems from some confusion about how the versioning of IRIs works; we've not bumped the version to 3.1 yet, so all the IRIs in the documentation say

    3.0.1. We don't know who added this to the agenda, so no discussion about this occurred.
- Follow up spdx-examples fixes & merge approved PRs (Update and to be sorted offline)
    - Merge approved PRs https://github.com/spdx/spdx-examples/pulls
    - https://github.com/spdx/spdx-examples/pull/109 is ready to merge
- SHACL bug for Extension found (PR proposed) - need to decide about 3.0.1 inclusion https://github.com/spdx/spdx-3-model/issues/1017#issuecomment-2822649891
    - Allow classes derived from Extension https://github.com/spdx/spec-parser/pull/186
- New relationships in SPDX 2.3 spec? (Rose)
- Clarify hasDeclaredLicense and hasConcludedLicense https://github.com/spdx/spdx-3-model/issues/1022
    - Call will be done with Legal to discuss this

Notes

-

2025-05-06

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-05-06 PR: https://github.com/spdx/meetings/pull/885

Attendees

- Alexios Zavras
- Alfred Strauch
- Arthit Suriyawongkul
- Bob Martin
- Colin McAllister
- Dick Brooks
- Gary O'Neall
- Joshua Watt
- Karsten Klein
- Maximilian Huber
- Nicole Pappler
- Nisha Kumar
- Rose Judge
- Steven Carbno
- Victor Lu

Agenda (please add new topics to the end of the list)

- Approve previous minutes
- Prioritize agenda
- Adding Regulation class (continue) https://github.com/spdx/spdx-3-model/pull/1015
- OMG specification published https://www.omg.org/spec/SPDX/3.0
- Add naming convention and cardinality to Markdown doc https://github.com/spdx/spdx-3-model/pull/982
- Suggested changes for SoftwareService description https://github.com/spdx/spdx-3-model/issues/1013

- artifactSize is added post-3.0.1 but has 3.0.1 IRI
  https://spdx.github.io/spdx-spec/v3.1-dev/model/Software/Properties/artifactSize/
  https://github.com/spdx/spdx-3-model/pull/966
- Follow up spdx-examples fixes & merge approved PRs (Update and to be sorted offline)
  - Merge approved PRs https://github.com/spdx/spdx-examples/pulls
- SHACL bug for Extension found (PR proposed) - need to decide about 3.0.1 inclusion
  https://github.com/spdx/spdx-3-model/issues/1017#issuecomment-2822649891
- [FYI] SBOM datasets (could be used for SPDX tests?)
  - A Dataset of Software Bill of Materials for Evaluating SBOM Consumption Tools
    - Dataset: https://zenodo.org/records/14233415
    - Paper: https://arxiv.org/abs/2504.06880
    - Focus on Java/Maven projects, SPDX Lite
  - Wild SBOMs: a Large-scale Dataset of Software Bills of Materials from Public Code
    - Dataset: https://zenodo.org/records/14250103
    - Paper: https://arxiv.org/abs/2503.15021
    - Has a stat of SBOM standards and formats found on public code (Software Heritage Archive)

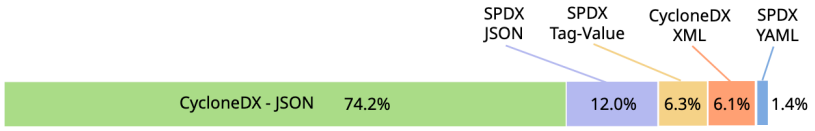

Fig. 3. Distribution of SBOM standards and file formats

- New relationships in SPDX 2.3 spec? (Rose)
- Clarify hasDeclaredLicense and hasConcludedLicense
  https://github.com/spdx/spdx-3-model/issues/1022
- Allow classes derived from Extension
  https://github.com/spdx/spec-parser/pull/186
-

Notes

- Previous minutes approved

Regulation

- Regulation class
  - Subclass of: Element? Artifact? Specification?
  - DECISION: Regulation subclass of Specification
- Regulation reference
  - Dick (from chat): Regulations are frequently cited using well defined citations, i.e. US CFR Title 18 Part 208.
- Regulation Conformance separate

        - conformsTo new value in RelationshipType vocabulary ?
        - Do we also need a governedBy new value ?
        - How to accommodate "self-conformance", as in the case of OpenChain
        - conforms vs the intent to conforms
        - conformsTo means fulfilling any conformance requirement
        - DECISION: add conformsTo new RelationshipType
    - Softer relationship: no actual conformance, but showing relevance
        - Need new subtype of Relationship to also include extra information
        - Not reusing RelationshipCompleteness to show how conformant something is
            - RelationshipCompleteness should be used for the completeness of the relationship itself. Not about the content quality of the relationship type.
        - Example of a Relationship with additional information https://spdx.github.io/spdx-spec/v3.0.1/model/Security/Classes/VulnAssessmentRelationship/
    -

New Relationship to 2.X spec

- Rose raised a question on possibility to add a new relationship to 2.3 spec
- Gary: No plan for 2.4 release yet
- To discuss more
- One way is to add the relationship to 3.X first and add back to 2.X

2025-04-29

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-04-29 PR: https://github.com/spdx/meetings/pull/884

Attendees

- Alfred Strauch
- Arthit Suriyawongkul
- Bob Martin (MITRE)
- Colin McAllister
- Dick Brooks (Business Cyber Guardian)
- Gary O'Neall
- Ilan Schifter
- Joshua Watt
- Karen Bennet (ISO)
- Karsten Klein
- Nicole Pappler
- Steven Carbno
- Sujal Bhor

Agenda

- Approve previous minutes
- Prioritize agenda
- Adding Regulation class https://github.com/spdx/spdx-3-model/pull/1015
- OMG specification published https://www.omg.org/spec/SPDX/3.0
- Add naming convention and cardinality to Markdown doc https://github.com/spdx/spdx-3-model/pull/982
- Suggested changes for SoftwareService description https://github.com/spdx/spdx-3-model/issues/1013
- artifactSize is added post-3.0.1 but has 3.0.1 IRI https://spdx.github.io/spdx-spec/v3.1-dev/model/Software/Properties/artifactSize/ https://github.com/spdx/spdx-3-model/pull/966

- Follow up spdx-examples fixes & merge approved PRs (Update and to be sorted offline)
    - Fix validation error in example 9 (Gary) https://github.com/spdx/spdx-examples/pull/118
    - Add lib definitions to example 6 bin.spdx file (Nisha & Gary) https://github.com/spdx/spdx-examples/pull/119
    - Merge approved PRs https://github.com/spdx/spdx-examples/pulls
- SHACL bug for Extension found (PR proposed) - need to decide about 3.0.1 inclusion https://github.com/spdx/spdx-3-model/issues/1017#issuecomment-2822649891
- [FYI] SBOM datasets (could be used for SPDX tests?)
    - A Dataset of Software Bill of Materials for Evaluating SBOM Consumption Tools
        - Dataset: https://zenodo.org/records/14233415
        - Paper: https://arxiv.org/abs/2504.06880
        - Focus on Java/Maven projects, SPDX Lite
    - Wild SBOMs: a Large-scale Dataset of Software Bills of Materials from Public Code
        - Dataset: https://zenodo.org/records/14250103
        - Paper: https://arxiv.org/abs/2503.15021
        - Has a stat of SBOM standards and formats found on public code (Software Heritage Archive)

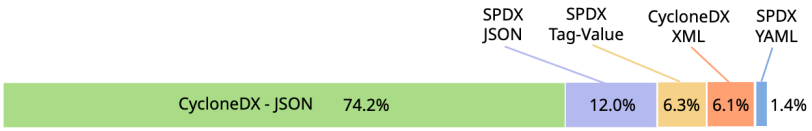

Fig. 3. Distribution of SBOM standards and file formats

Notes

Admin

- Approve Minutes of 2025-04-22 - approval agreed

OMG Update

- OMG update - already published at https://www.omg.org/spec/SPDX/3.0/

Regulation

- From the previous meeting, the meeting agreed that we should use relationship (instead of property) to link between two elements/artifacts. The pending discussion is about how to encode information like evidence and other documentation that support the conformance.
- Should there be a lifecycle-scoped relationship?
- Should there be a relationship to a relationship?

- The meeting discussed about class/subclass where the Regulation comes from.
    - Agreed that at least Regulation should be a subclass of Artifact.
    - A proposal is to have Regulation as a subclass of Specification as well (Artifact -> Specification -> Regulation)
- Discussing “Mandatory” property.
    - A comment that may not possible to say a regulation is “mandatory” or not in itself (depends on context)
    - But we can say if a Specification is formal or not
    - If it is still ambiguous, maybe we are not including it for now, until we have more experience we can decide to add this later.
- Discussing External Identifier and External Reference
    - Should these be required/mandatory fields (the fields are already in the superclass Artifact, but not mandatory)
    - Dick: There are purchase order standards for EDI ANSI X12
    - Arthit: In the case of EU regulations, we have ELI (European Legislation Identifier) https://data.europa.eu/data/datasets/eli-european-legislation-identifier-eurlex
    - “external” here is external in reference to SPDX specification. The external ID can come from inside the organization (“internally identified”).
    - If we can define URI schema for specification/standard from common bodies like IETF, W3C, BSI, ISO, JISC, IEEE, etc (“Package URL but for standards”) may be useful for ID too.
- Mandatory property or not: From Consumer / Producer perspectives
    - Gary: Consumers really like to have some of these information
    - Producers may have limitations finding some information
    - If forcing a mandatory property to a class, it means in a situation where the Producer cannot find information for the property, the Producer may have to omit the entire class (and other information it may contain).
    - Gary’s view: some information is better than no information
- Location/Jurisdiction
    - Karen: May need that for AI. Because some regulation is for a region. (EU AI Act is in general for EU region/market, for example)
    - Arthit: Export control is another use case for location/jurisdiction
- Version information
    - (From chat) Art: Versioning is another information that we may need for a standard/spec. So we can know that a spec A is an iteration of a spec B. And we may be able to imply as well that spec A is replacing or compatible with spec B. (If X conformsTo A, then X conformsTo B).
- Specification Type
    - To have Regulation a subclass of Specification (hierarchy)
    - OR to have just the “type” (with enum) inside Specification. It is an instance of a Specification class with type “Regulation”.
- Definitions
    - Dick: Regulations are defined in the US Code of Federal Regulations.

    - Karsten: For me regulations and specifications are siblings. What is a parent?
    - SPDX is a specification, not a regulation.
    - What is the difference between Specification and Regulation?
    - A law can specify an entity or an activity to follow a certain standard. In this case, a standard can be considered a regulation.
- Specification/Regulation at least has to be an Artifact because we need something we can point to.
    - Specification as subclass of Artifact
    - Regulation as subclass of Artifact
    - But not necessary that Specification as subclass of Regulation
- Discuss more next week on this topic of Regulation

2025-04-22

← Please look at working meeting minutes for each week at the document tabs on the left pane

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-04-22 PR: https://github.com/spdx/meetings/pull/883

Attendees

- Alfred Strauch
- Colin McAllister
- Dick Brooks
- Gary O'Neall
- Ilan Schiffer
- Joshua Watt
- Karen Bennet
- Karsten Klein
- Kate Stewart
- Nicole Pappler
- Nisha Kumar
- Peter Monks
- Steven Carbno
- Victor Lu

Agenda

- Live Minutes - moving from https://spdx.swinslow.net/p/spdx-tech-minutes
- PyPI Org update
    - FYI - PEP 770 – Improving measurability of Python packages with Software Bill-of-Materials https://peps.python.org/pep-0770/
- Implementation advice to make SPDX files work in a reproducible build environment https://github.com/spdx/spdx-maven-plugin/issues/177#issuecomment-2819658533
- Representing NOASSERTION and NONE in SPDX license expression (2.x and 3.1?) https://github.com/spdx/Spdx-Java-Library/pull/307#discussion_r2040195580 https://github.com/spdx/spdx-spec/issues/49

- Does the JSON schema support serialization of Extensions?
  https://github.com/spdx/spdx-3-model/issues/1017
- Add naming convention and cardinality to Markdown doc
  https://github.com/spdx/spdx-3-model/pull/982
- Suggested changes for SoftwareService description
  https://github.com/spdx/spdx-3-model/issues/1013
- artifactSize is added post-3.0.1 but has 3.0.1 IRI
  https://spdx.github.io/spdx-spec/v3.1-dev/model/Software/Properties/artifactSize/
  https://github.com/spdx/spdx-3-model/pull/966
- Follow up spdx-examples fixes & merge approved PRs (Update and to be sorted offline)
  - Fix validation error in example 9 (Gary)
    https://github.com/spdx/spdx-examples/pull/118
  - Add lib definitions to example 6 bin.spdx file (Nisha & Gary)
    https://github.com/spdx/spdx-examples/pull/119
  - Merge approved PRs https://github.com/spdx/spdx-examples/pulls
- Adding Regulation class
  https://github.com/spdx/spdx-3-model/pull/1015
-

Notes:

- Deprecating use of Etherpad platform; shifting to Google Docs for live recording. Final version will remain on GitHub.

- PyPI Organization for Python package publication
  - Need to have an email from the organization "spdx.dev".
  - Need to have an email.
  - Need to know which domain to use with an email address.
  - Need to point to as a member of the organization.

- Implementation advice to make SPDX files work in a reproducible build environment
  https://github.com/spdx/spdx-maven-plugin/issues/177#issuecomment-2819658533
  - Use of Epochs: https://reproducible-builds.org/docs/source-date-epoch/

- Representing NOASSERTION and NONE in SPDX license expression (2.x and 3.1?)
  https://github.com/spdx/Spdx-Java-Library/pull/307#discussion_r2040195580
  https://github.com/spdx/spdx-spec/issues/49
  - Use case for concluded - can we avoid special cases. Would it be possible to move NONE & NOASSERTION to License list? SPDX License Expressions are pulling this up.
  - Be able to take License expressions as strings as context and cut/paste is going to be key.
  - Can we vector use to NOLIMITS? May be special designations.
  - Resolved: we need to bring it up on legal call, so lawyers can weigh in.

- Does the JSON schema support serialization of Extensions?
  https://github.com/spdx/spdx-3-model/issues/1017
    - Java library implementations weren't passing validation. Some types of extensions with multiple properties, there's no way to validate.
    - Extension "extension" is abstract - so will fail there. You have to make your own type, and create your own validation. Extension "cycloneDX" should work, or own IRI, should be possible.
    - Any other IRI is a subclass of extension. Schema validation will allow any value that is not an existing known abstract class. If any issues, let Joshua know.
    - Gary still has questions with about JAVA, but will follow up offline
    - Discussion on creating a longform prose on how to get a validation of an extension. It's in the USING repo. Two examples are "getting started" and "cross-reference" ; so put another one there in the same style on how to form an extension.
    - There was validation when it was in spec itself, but it Joshua looking to moving validation to work under using repo - see: https://github.com/spdx/using/tree/main/docs
    - Nisha suggests that having a one day on SHACL for implementers call to know
    - Must use FULL IRI's as it is not in the context file.

- Adding Regulation class
  https://github.com/spdx/spdx-3-model/pull/1015
    - Discussion headed towards that Relationship type might be more appropriate to correlate to artifact for conformance.
    - Should it be a lifecycle type relationship?
    - An artifact claiming to be compliant, is different from evidence that is true.
    - WORKING CONCLUSION: Should be a relationship NOT a property of an artifact.
    - Now we need to handle the evidence
    - Some approaches to handle this:
        - Relationship to relationship; separating (enables evidence provided after for supporting artifact) - safety & build profile.
        - Property on relationship
        - Straight to/from relationship (safety: comply to standard, with linked report)
        - Pick this up first on agenda next week.
        - Restart discussion with pro's/con's of approach.

older notes

NOTES:

- MEETING MINUTES AND AGENDAS ARE MAINTAINED IN THE GITHUB REPOS.
- Past minutes archived at: https://github.com/spdx/meetings/tree/master/tech
- Past minutes waiting for approval at: https://github.com/spdx/meetings/labels/Tech

SPDX Tech Team Meeting 2025-04-15 PR: https://github.com/spdx/meetings/blob/main/tech/2025/2025-04-15.md

Attendees

- Alexios Zavras
- Alfred Strauch
- Arthit Suriyawongkul
- Colin McAllister
- Gary O'Neall
- Ilan Schifter
- Joshua Watt
- Karen Bennet
- Kate Stewart
- Nicole Pappler
- Peter Monks
- Sean Barnum
- Steven Carbno
- Victor Lu

Agenda

- Representing NOASSERTION and NONE in SPDX license expression (2.x and 3.1?)
  https://github.com/spdx/Spdx-Java-Library/pull/307#discussion_r2040195580
  https://github.com/spdx/spdx-spec/issues/49
- Use "SPDX 3 JSON" instead of "SPDX 3 JSON-LD"
  https://github.com/spdx/spdx-3-model/issues/1008
- Does the JSON schema support serialization of Extensions?
  https://github.com/spdx/spdx-3-model/issues/1017
- Add naming convention and cardinality to Markdown doc
  https://github.com/spdx/spdx-3-model/pull/982

- Suggested changes for SoftwareService description https://github.com/spdx/spdx-3-model/issues/1013
- artifactSize is added post-3.0.1 but has 3.0.1 IRI https://spdx.github.io/spdx-spec/v3.1-dev/model/Software/Properties/artifactSize/ https://github.com/spdx/spdx-3-model/pull/966
- Follow up spdx-examples fixes & merge approved PRs (Update and to be sorted offline)
    - Fix validation error in example 9 (Gary) https://github.com/spdx/spdx-examples/pull/118
    - Add lib definitions to example 6 bin.spdx file (Nisha & Gary) https://github.com/spdx/spdx-examples/pull/119
    - Merge approved PRs https://github.com/spdx/spdx-examples/pulls

Notes

spdx-3-model/issues/1008

- No disagreement raised on the revised wording. Discussion about documentation not being read, JSON-LD optimizations, etc. to remind them that there is a defined schema now.
- Confusion on #serialization/overiew; action:
    - Update description "SPDX 3 JSON";
    - How it fits into theoverall serialization.
    - Clarify that for people writing tools should implement the SPDX 3 JSON when they produce documents.
- Sean: Has a "shape" been defined? No, not yet. Possible to constrain how JSON LD is output to a specific "shape" to be investigated.
    - Sean - it is called "framing" - link: https://www.w3.org/TR/json-ld11-framing/
- 3 actions: on https://github.com/spdx/spdx-spec/blob/develop/docs/serializations.md
    - Update definition of SPDX 3 JSON per wording in issue - Art
    - Update Overview to describe the 3 sections - Alexios
    - Investigate JSON LD framing to see if it can help tooling - Joshua - see if we can emit it from SHALC2Code
    - Target 3.1 - due to potential impact to standards effort
    - Point to the 3.1 definitions for anyone actively development
- Peter - question on Cannonical - is it a reccomendation or requirement for SPDX spec?
    - Sean, Gary - Reccomendation
    - Suggestion that we create a linter

OpenJS - JavaScript

- Victor - no SBOM format - https://docs.google.com/document/d/1VmmOivNJeocns_5XN3ijcpR4BMmz4-mVoGjqvBmOnY8/edit?tab=t.0#heading=h.m9nc0aibj5z5
- Can SPDX be used?

- SPDX is generated from NPM today
- Action: all - review the above document to see if SPDX can be interoperable

Other items

- In email, Rose was going to restart the security working group

==========

SPDX ASIA Meeting 2025-04-14 PR: https://github.com/spdx/meetings/pull/882

Attendees

- Kate Stewart
- Nobuyuki Tanaka
- Norio Kobota
- Takashi Ninjouji

Notes

- Discussion of 3.0.1 vs 3.1.
- 3.1 will have multiple release candidate.
- Japanese translation meeting happening soon with Watanabe-san, leading effort.
- https://github.com/spdx/spdx-3-model/issues/1008 - discussion of the JSON & JSON-LD.
- Discussion of examples to be contributed to https://github.com/spdx/spdx-examples
- Gold reference examples of 3.0 are needed, as well as 2.3 examples.
- Japan SBOM study group, will implement JSON for other examples; across different versions.
- Interest in Automotive & SDV platform is growning. SPDX output from tool chain outputs from Yocto & Zephyr, (see https://zephyr-dashboard.renode.io/ for examples of 3 SBOM files).
- Discussion about CRA and impact on prjects
    - www.linuxfoundation.org/research/cra-readiness
    - https://www.enisa.europa.eu/sites/default/files/2024-11/Cyber%20Resilience%20Act%20Requirements%20Standards%20Mapping%20-%20final_with_identifiers_0.pdf
    - www.linuxfoundation.org/research/cra-compliance-best-practices

==========

SPDX Tech Team Meeting 2025-04-08 PR: https://github.com/spdx/meetings/pull/876

Attendees

- Alfred Strauch
- Arthit Suriyawongkul
- Bob Martin
- Dick Brooks
- Illan Schifter
- Joshua Watt
- Karsten Klein
- Kate Stewart
- Nisha Kumar
- Steven Carbno
- Victor Lu

Agenda

- Use "SPDX 3 JSON" instead of "SPDX 3 JSON-LD" https://github.com/spdx/spdx-3-model/issues/1008
- Include derived classes in Documentation https://github.com/spdx/spdx-spec/issues/1190
- Add Regulation class and conformsTo relationship https://github.com/spdx/spdx-3-model/pull/1015
- 3 SBOMs failed validation in spdx-examples
    - https://github.com/spdx/spdx-examples/issues/102 - PR ready - merged
    - https://github.com/spdx/spdx-examples/issues/116 - need PR - Gary to investigate - PR ready
    - https://github.com/spdx/spdx-examples/issues/117 - need PR - Nisha to investigate - PR ready

Notes

- Updates:
    - Ilan working on converting issues to PRs, planed for next week.

Include derived classes in Documentation

https://github.com/spdx/spdx-spec/issues/1190 - Illan willing to help this. Help would be needed in Spec class repo. - Art raised, what should be present in the web site, useful for part of spec? Examples were NAK'd by Alexios. - Link from documentation?

- Website is generated from spec parser. If not part of spec, doesn't get to website. Some partial examples are there already - see security & AI profiles have examples. Please see Alexious comments here https://github.com/spdx/spdx-3-model/issues/1012 - All the derived classes would make it overwhelming. If we limit it to one level; might be more tractiable. Using website technology to selective view. Illan has ideas on this.
- Need Alexios on discussion. - General agreement in the call first level down makes sense, and will be helpful.

Add Regulation class and conformsTo relationship

https://github.com/spdx/spdx-3-model/pull/1015

- Some discussion if regulation should be a specification type
- interpretation of regulation? More discussion.
- Regulatory Authority?
- ConformsTo - who does the check? How would exceptions be captured?
- Should conforms to be it's own relationship type?
- Operations & Safety folk may have opinions here as well..
- Standards compliance profile? Needing more discuaion.
- We may able to use hasDocumentation and hasEvidence relationship type for this?
- Ilan suggest we model this like we do licenses, with exceptions? Be able to use similar sort of expression logic.

SBOM Examples

- actually failing, but being marked as passed.
- Need change CI to fix the flow to mark failed properly again.
- Joshua to take a look at CI PR - https://github.com/spdx/spdx-examples/pull/115
    - https://github.com/spdx/spdx-examples/issues/102 - PR ready - Joshua reviewed.
    - https://github.com/spdx/spdx-examples/issues/116 - need PR - Gary to investigate
    - https://github.com/spdx/spdx-examples/issues/117 - need PR - Nisha to investigate

Round Table

- Security Profile restarting. Rose volunteered to lead. Ilan interested in participating, next step? Bob is also interested. Karsten Klein is interested as well. Doodle poll for time to meet?
- Others interested in helping with BSI mapping to SPDX - Ilan, Art & Karsten are willing to help.
- Art is working with John on NTIA conformance checker - will add BSI to this as well. V3 minimum expectations has been added. Note that commandline tool is called

SBOM-conformance- checker. Concerns over BSI overshooting for EU CRA act. https://docs.google.com/document/d/1pueRxlxoM9n1eG9g6AihjLvybEBTd77m22mRYBQltpg/edit?usp=drivesdk Our mapping of CISA Baseline Attributes. Can use this for BSI work.

- Karsten - have been looking at different levels of criteria in CRA. Organizing to different levels of validation of an SBOM? Looking to beyond the minimum attributes. Adding in contractual, and other terms. Going beyond the lower level characteristics. Heading towards semantics and integrity checks for consistency.
- Stable tooling in Python is still a gap for Dick. spdx-python-model is on PyPI now, and Nisha is using python tooling. Dick looking for to take to production. Nisha is finding it stable for generating them. Challenge on reading and processing them. Yocto has been using bindings for reading/writing for over a year. Joshua indicates its converting into python classes natively for serializing and deserializing. Vulnerability information needed to conform is there. Validates a subset of stuff. It doesn't do profile conformance validation. Enforces strict type, but not semantic per

Future Meetings

- need to get Operations Profile update.

==========

SPDX Tech Team Meeting 2025-04-01 PR: https://github.com/spdx/meetings/pull/873

Attendees

- Alfred Strauch
- Alexios Zavras
- Arthit Suriyawongkul
- Bob Martin
- Dick Brooks
- Ilan Schifter
- Joshua Watt
- Kate Stewart
- Nicole Pappler
- Peter Monks
- Sean Barnum
- Steven Carbno
- Victor Lu

Agenda

- Follow up on Actions from last week (Dead links, OMG status, etc)
- Tools: Need to have version supported be explicit (Gradle, Maven, Online Compare?)
- SHACL (Ilan) https://github.com/spdx/spdx-3-model/issues?q=is%3Aissue%20state%3Aopen%20label%3ARDF%2FOWL%2FSHACL
- Translations (Art, Alexios, etc.) https://github.com/spdx/spdx-spec/issues/1169
- Suggested Profile prefixes RDF (connected to SHACL too) https://github.com/spdx/spdx-3-model/issues/1010
- Documenting model naming convention https://github.com/spdx/spdx-3-model/pull/982

Notes

Follow up from Last week

- Dead links: Pending - Bob/Alexios to raise in upcoming meeting
- OMG submission - Moving forward, not on public web page.
- SPDX logo, trademarks - Kate to follow up with Alexios for spec gen & website version.
- Need list of documents to go to ISO - Alexios to start thread with Jorey, Seth cc: Bob, Gary, Kate

Tools

- Status of Go Bindings: low level is available. https://github.com/spdx/spdx-go-model
- Python bindings are available as well. https://pypi.org/project/spdx-python-model/
    - Can do basic type validations, but not advanced validations like those relationship-related
- Tools Python & Go - higher level still need to be updated to leverage low level bindings.
- Online Tool supports of SPDX 3.0
    - Compare tool
    - Validate: https://tools.spdx.org/app/validate/ supports 3.0
    - Convert: https://tools.spdx.org/app/convert/ supports “To 3.0” but not “From 3.0”
    - Visual Editor: https://tools.spdx.org/app/dots/ only works with SPDX 3.0
    - Conformance Checker: https://tools.spdx.org/app/ntia_checker/ does not support 3.0

SHACL

- Ilan went through several of the issues and discussed behavior for validation with Sean
    - NotAffected - https://github.com/spdx/spdx-3-model/issues/923,
        - VEX requirements for not affected are playing a role here: see: https://www.cisa.gov/sites/default/files/2023-04/minimum-requirements-for-vex-508c.pdf
    - Serveral others were walked through #987, #988, #981,

- Shifted discussion to where they should be placed. Separate file or not?
    - Sean recommends not separating unless clear reason why
    - Alexios asks about the end goal for publishing
    - Joshua we're already mixing the ontology and validation in a single file, so would like to see this continue.
    - Considering making a new section that the parser could understand in files already have, or new files? Easier to prevent them becoming lies, if they are where they are defined. For cross cutting, may want to have explicit reference.
    - Recommendation to go from issues to go to PRs.
- If it is a Profile-level conformance, put it on the Profile file
    - see: https://github.com/spdx/spdx-3-model/blob/develop/model/Build/Build.md#profile-conformance
    - maybe after the Profile Conformance section? Similarly licensing.
- If defined in one of properties or elements, it should go there.
- When apply multiple places, need to create a special box to put them in, and should be at the model level.
- Illan will create PRs to a section; and then the parser will need to be updated. Have implications on TTL.
- This is going to be targetted for 3.1 (or 3.1.1) not 3.0.1.
- Discussion on biasing towards the normal flow, and keep up the testing.
- Add "Validation" section into Markdown file, and spec-parser convert it to SHACL rules in TTL file

Translations

- Art did further research (https://github.com/spdx/spdx-spec/issues/1169) If files can be placed in specific folders, the plugin should be able to help us here.
- For the Spec, we don't have things merged yet, looking for an example. See 1141 (Japanese translation).

==========

SPDX Tech Team Meeting 2025-03-25 | PR: https://github.com/spdx/meetings/pull/870

Attendees

- Alfred Strauch
- Arthit Suriyawongkul
- Bob Martin
- Dick Brooks

- Joshua Watt
- Kate Stewart
- Nicole Pappler
- Steven Carbno
- Victor Lu

Agenda

- SHACL update (Ilan)
- Remove "schema files" from profileConformance
  https://github.com/spdx/spdx-3-model/issues/991
- Use "SPDX 3 JSON" instead of "SPDX 3 JSON-LD"
  https://github.com/spdx/spdx-3-model/issues/1008
- SPDX 3.0 in OMG (Bob)
- Dead links (Bob)
- Python and Golang bindings are now published. Someone needs to integrate them into spdx-tools (Gary)
  - https://github.com/spdx/spdx-python-model
  - https://github.com/spdx/spdx-go-model
- OpenJS problems (Victor - needs Gary)

Notes

SPDX 3.0 in OMG

- Formal OMG Spec at this point.
  - Will appear here https://www.omg.org/spec/SPDX
- ISO paperwork can commence
- Do we need a patch release for possible ISO review changes?
  https://github.com/spdx/spdx-3-model/issues/996
  - Yes, as a placeholder, but won't publish unless needed.

Dead Links

- Bob will take investigation to Outreach to review for website & sort it.
  - Link to v2.1 HTML version on spdx.dev is 404
    https://github.com/spdx/spdx-spec/issues/882
    https://github.com/spdx/spdx-spec/issues/1122
  - SPDX Schema URL in IANA media type registration entry is dead
    https://github.com/spdx/spdx-spec/issues/1158

Python binding

- Binding package moved to PyPI

    - https://pypi.org/project/spdx-python-model/
- The application for PyPI Organization (to be used as the package publisher) is on stale
    - https://docs.pypi.org/organization-accounts/
    - So using personal accounts as publishers until we can have the organization account
- Looking for multiple owners to support Joshua & Arthit - looking for backup owners.

CRA primer

- OpenSSF Zephyr readiness for EU Cyber Resilience Act
- Cyber Resilience Act (CRA) https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- Joshua: Similar vulnerability handling requirements in regulations regarding devices using radio frequency
- Vulnerability ID is required for reporting/database
- Dick (in chat):
    - SPDX V 2.3 already supports an SBOM with vulnerability reporting information - see appendx K.
    - IEC 29147:2018 is already a requirement for US Federal Government supply chain requirements and NIST Guidance: https://cisa.gov/sag
    - NIST NVD (National Vulnerability Database) is indeed improving https://nvd.nist.gov/
- Cyber Resilience Act Requirements Standards Mapping (from JRC & ENISA) https://www.enisa.europa.eu/sites/default/files/2024-11/Cyber%20Resilience%20Act%20Requirements%20Standards%20Mapping%20-%20final_with_identifiers_0.pdf
- There are classes of product
- This standard ISO 18031-1:2024 (Common security requirements for radio equipment - Part 1: Internet connected radio equipment) provides requirements looks similar to CRA
- Concerns on compliance for open source projects; Some of the open source repos are not the commercial products
- Need of badge/self-assessment
- Discussion on voluntary reporting requirements?
- What will be counted as a "open source steward"?
- SPDX 3.1 or 3.2 are expected to have fields to capture information for CRA, if not already in 3.0
- NTIA Minimum Requirements and CISA one look like a common baseline
- Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle https://cisa.gov/sag
- Secure Software Development Self-Attestation Resources and Knowledge https://www.nasa.gov/secure-software-development-self-attestation-resources-and-knowledge/

==========

SPDX Tech Team Meeting 2025-03-18 | PR: https://github.com/spdx/meetings/pull/871

SPDX Tech Team Meeting 2025-03-11 / PR https://github.com/spdx/meetings/pull/863

SPDX Asia Tech Team Meeting 2025-03-10 / PR https://github.com/spdx/meetings/pull/864