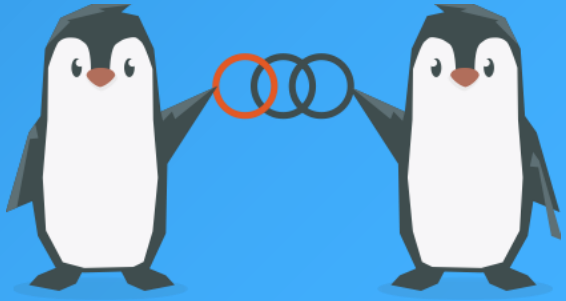
OpenChain SBOM Study Group Kickoff meeting

- Case Study: SPDX-Lite

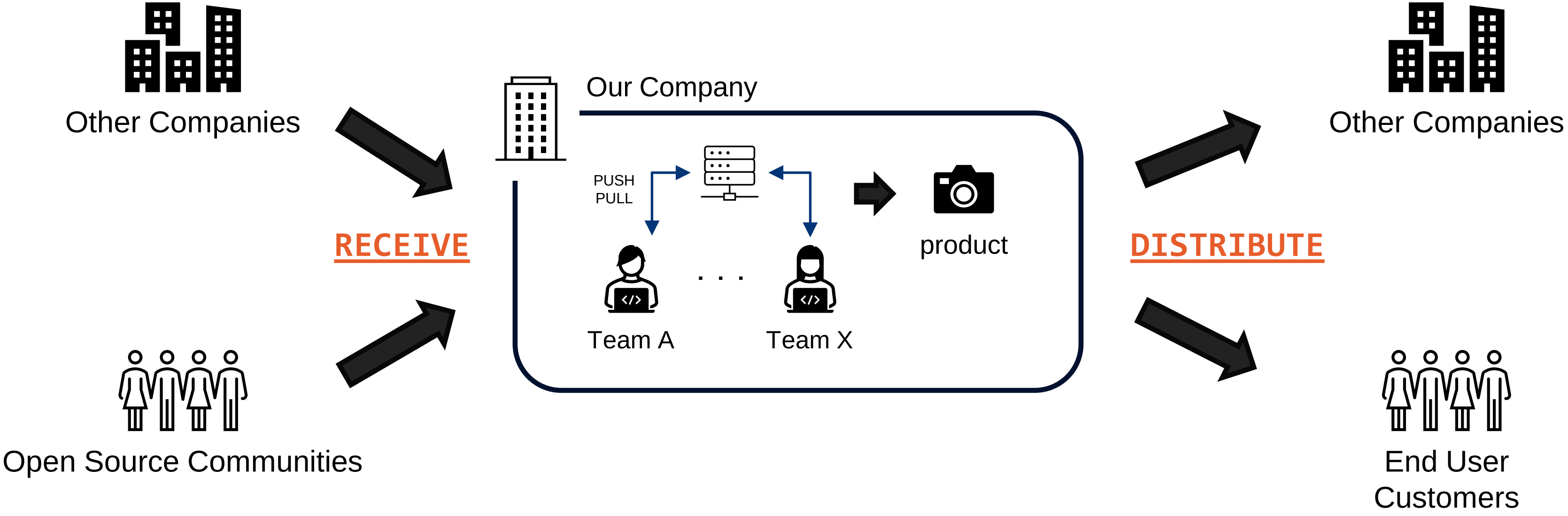
Norio Kobota, OpenChain Japan Working Group

THE LINUX FOUNDATION

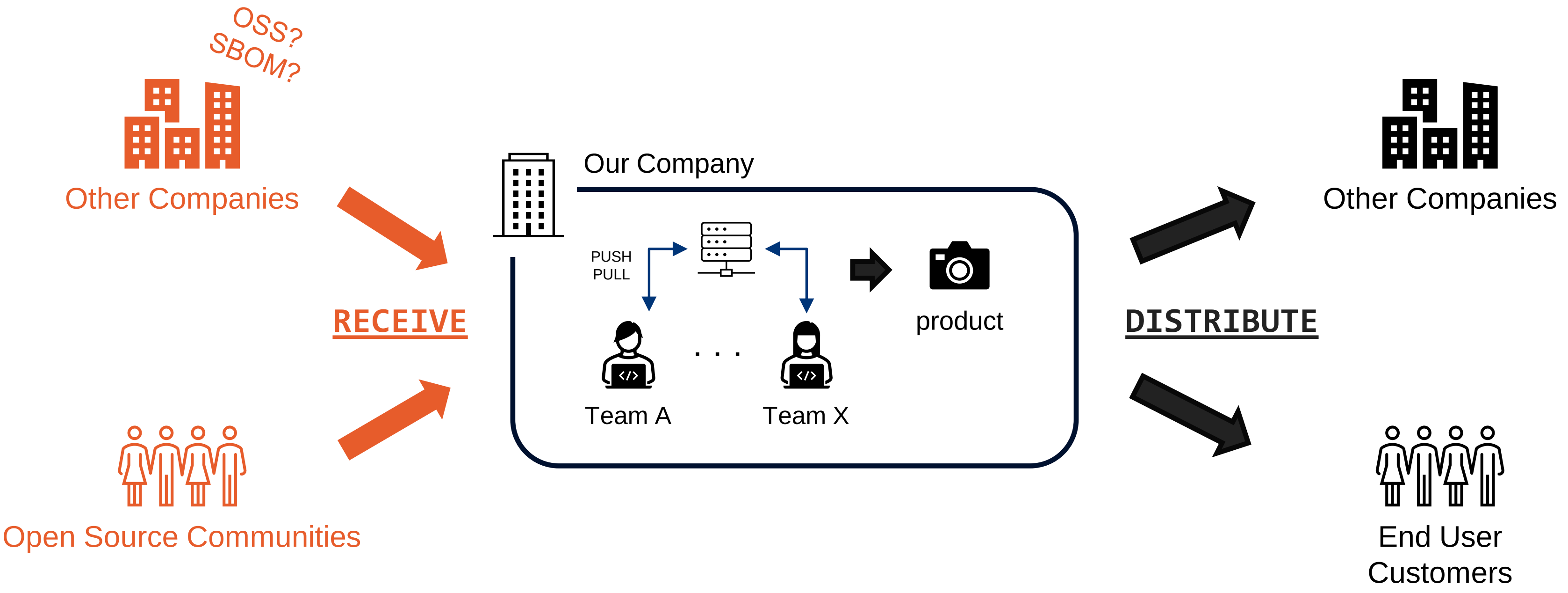
OPENCHAIN



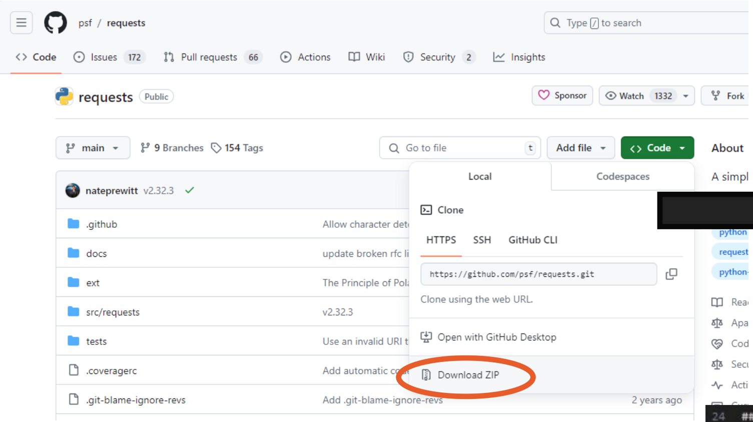
Focus Areas of SPDX Lite
Solving the Challenges of Software Exchange between External Parties.



Focus Areas of SPDX Lite
Solving the Challenges of SBOM Exchange between External Parties.



What Happens when software suppliers don’t understand?



psf / requests

Code · Issues 172 · Pull requests 66 · Actions · Wiki · Security 2 · Insights

requests Public

Sponsor · Watch 1332 · Fork

main · 9 Branches · 154 Tags · Go to file · Add file · Code

About

A simpl

nateprewitt v2.32.3 ✓		
.github	Allow character det	
docs	update broken rfc li	
ext	The Principle of Pol	
src/requests	v2.32.3	
tests	Use an invalid URI t	
.coveragerc	Add automatic co	
.git-blame-ignore-revs	Add .git-blame-ignore-revs	2 years ago

Local · Codespaces

Clone

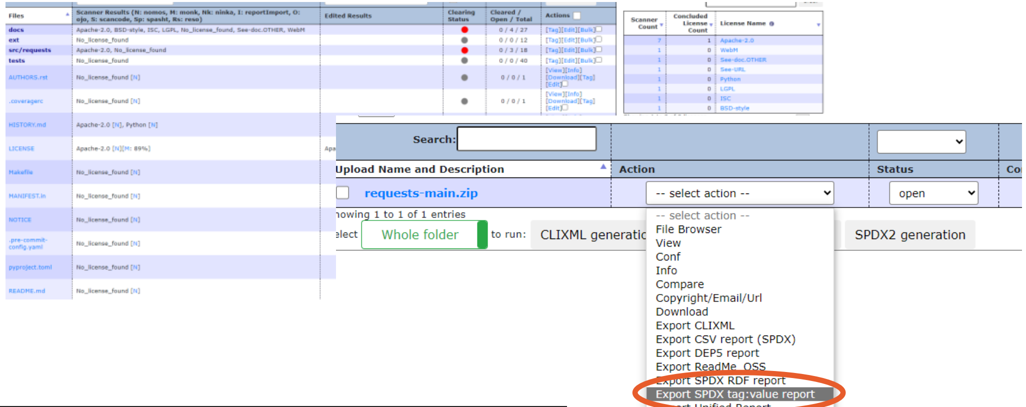
HTTPS · SSH · GitHub CLI

`https://github.com/psf/requests.git`

Clone using the web URL.

Open with GitHub Desktop

Download ZIP



Files	Scanner Results (N: nomos, M: monk, Nk: ninka, I: reportImport, O: ojo, S: scancode, Sp: spasht, Rs: reso)	Edited Results	Clearing Status	Cleared / Open / Total	Actions □
docs	Apache-2.0, BSD-style, ISC, LGPL, No_license_found, See-doc.OTHER, WebM		●	0 / 4 / 27	[Tag][Edit][Bulk]□
ext	No_license_found		●	0 / 0 / 12	[Tag][Edit][Bulk]□
src/requests	Apache-2.0, No_license_found		●	0 / 3 / 18	[Tag][Edit][Bulk]□
tests	No_license_found		●	0 / 0 / 40	[Tag][Edit][Bulk]□
AUTHORS.rst	No_license_found [N]		●	0 / 0 / 1	[View][Info] [Download][Tag] [Edit]□
.coveragerc	No_license_found [N]		●	0 / 0 / 1	[View][Info] [Download][Tag] [Edit]□
HISTORY.md	Apache-2.0 [N], Python [N]				
LICENSE	Apache-2.0 [N][M: 89%]	Apa			
Makefile	No_license_found [N]				
MANIFEST.in	No_license_found [N]				
NOTICE	No_license_found [N]				
.pre-commit-config.yaml	No_license_found [N]				
pyproject.toml	No_license_found [N]				
README.md	No_license_found [N]				

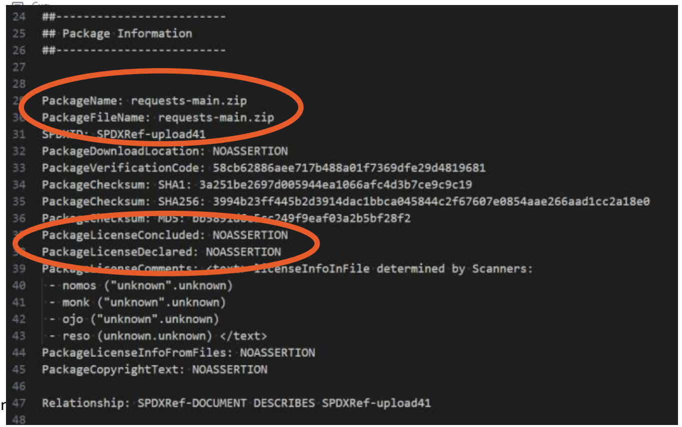
Scanner Count	Concluded License Count	License Name
7	1	Apache-2.0
1	0	WebM
1	0	See-doc.OTHER
1	0	See-URL
1	0	Python
1	0	LGPL
1	0	ISC
1	0	BSD-style

Search:

Upload Name and Description	Action	Status	Co
□ requests-main.zip	-- select action --	open	

howing 1 to 1 of 1 entries

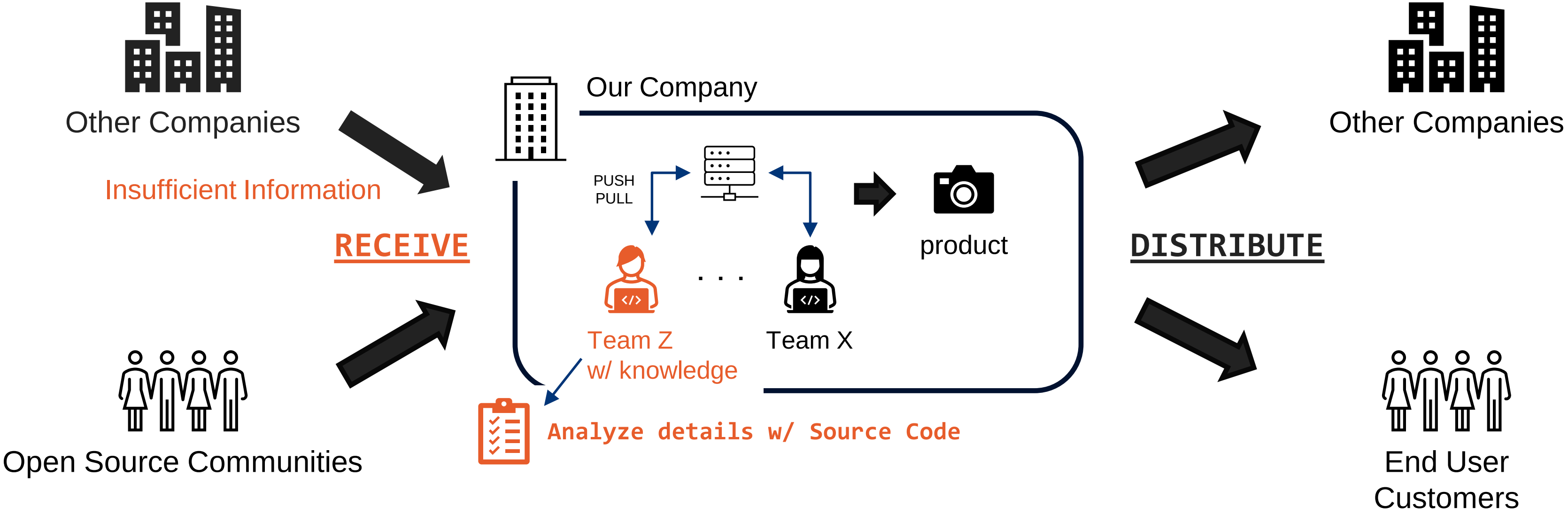
elect Whole folder to run: CLIXML generatio SPDX2 generation



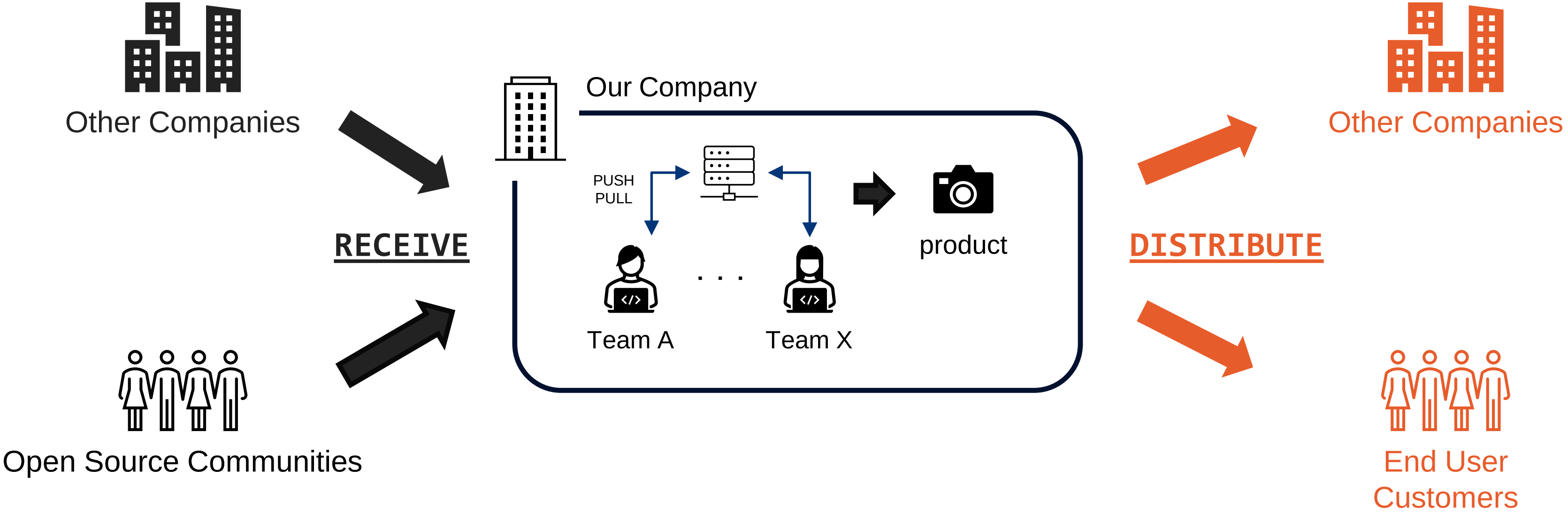
```
##------------------------
## Package Information
##------------------------


PackageName: requests-main.zip
PackageFileName: requests-main.zip
SPDXID: SPDXRef-upload41
PackageDownloadLocation: NOASSERTION
PackageVerificationCode: 58cb62886aee717b488a01f7369dfe29d4819681
PackageChecksum: SHA1: 3a251be2697d005944ea1066afc4d3b7ce9c9c19
PackageChecksum: SHA256: 3994b23ff445b2d3914dac1bbca045844c2f67607e0854aae266aad1cc2a18e0
PackageChecksum: MD5: bb5891d[illegible]5cc249f9eaf03a2b5bf28f2
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageLicenseComments: <text> LicenseInfoInFile determined by Scanners:
 - nomos ("unknown".unknown)
 - monk ("unknown".unknown)
 - ojo ("unknown".unknown)
 - reso (unknown.unknown) </text>
PackageLicenseInfoFromFiles: NOASSERTION
PackageCopyrightText: NOASSERTION

Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-upload41

```

licen

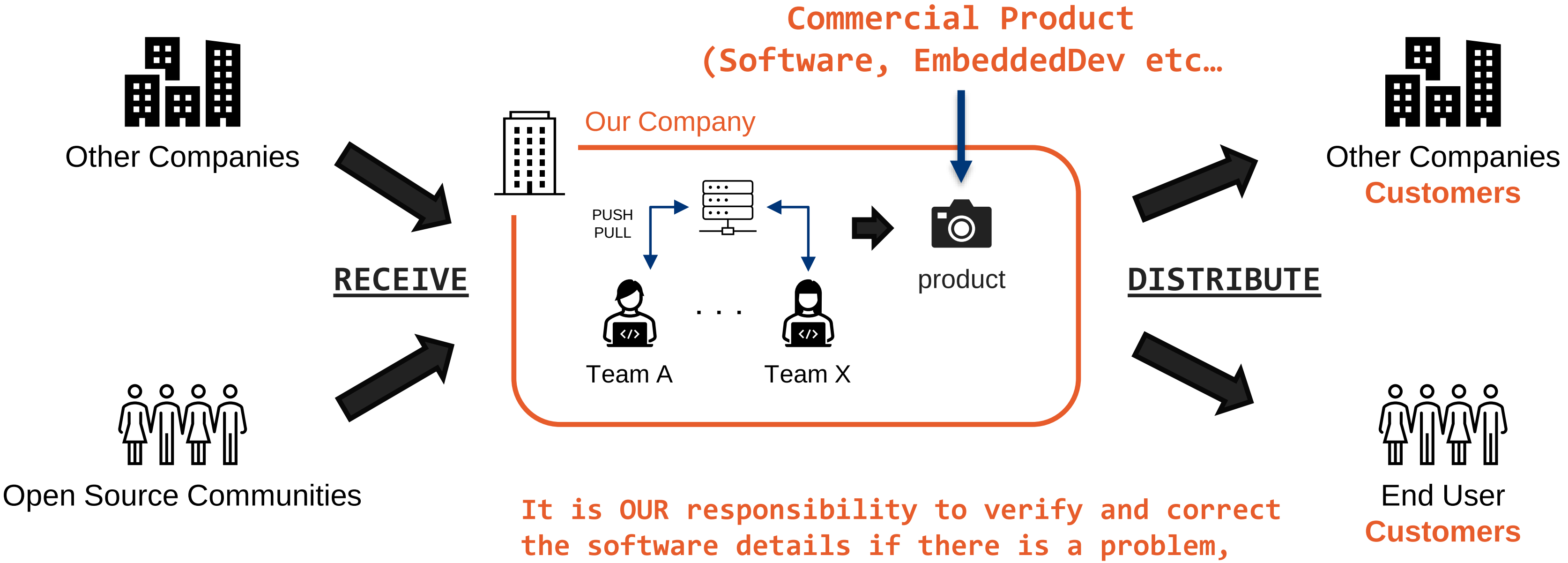
SBOM Supply Chain Reality
Knowledgeable team analyzes the details and manages configuration



Focus Areas of SPDX Lite
Solving the Challenges of SBOM Exchange between External Parties.

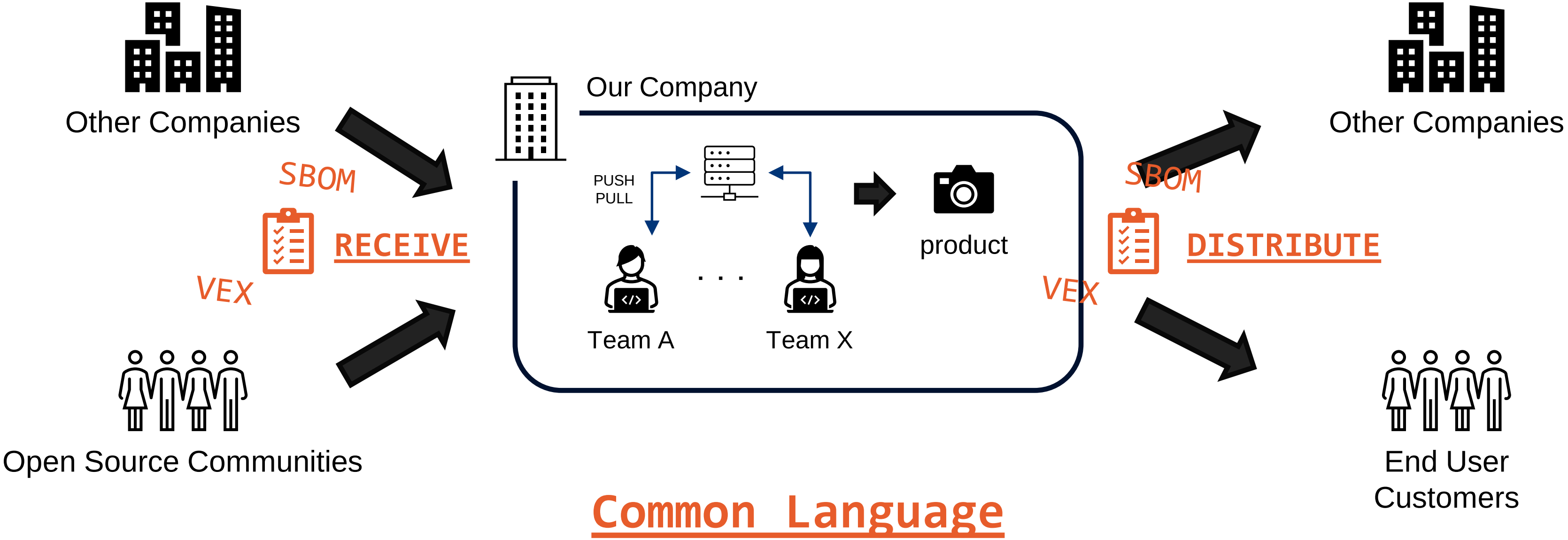


Who should know all the details of software?

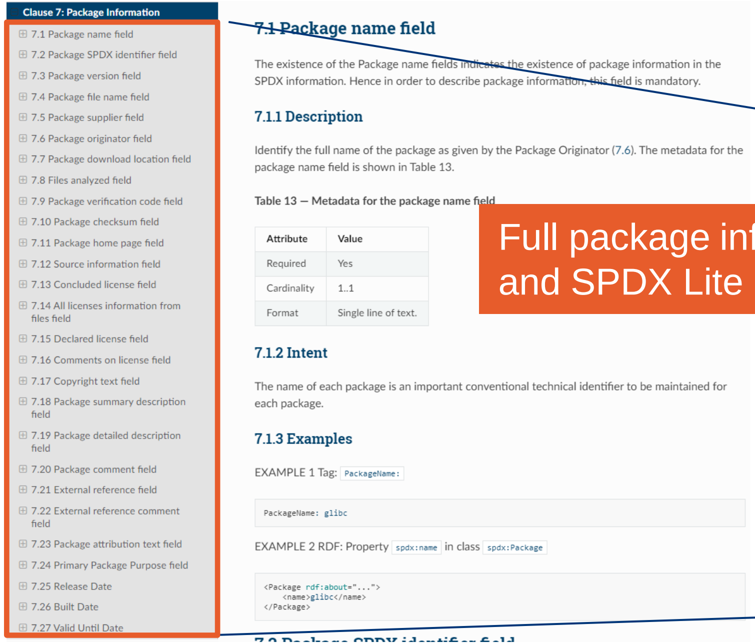


It is OUR responsibility to verify and correct the software details if there is a problem, not customers.

SBOM enables us to exchange information with anyone in a common format



Minimum clues needed for experts to investigate in detail.



Clause 7: Package Information

- 7.1 Package name field
- 7.2 Package SPDX identifier field
- 7.3 Package version field
- 7.4 Package file name field
- 7.5 Package supplier field
- 7.6 Package originator field
- 7.7 Package download location field
- 7.8 Files analyzed field
- 7.9 Package verification code field
- 7.10 Package checksum field
- 7.11 Package home page field
- 7.12 Source information field
- 7.13 Concluded license field
- 7.14 All licenses information from files field
- 7.15 Declared license field
- 7.16 Comments on license field
- 7.17 Copyright text field
- 7.18 Package summary description field
- 7.19 Package detailed description field
- 7.20 Package comment field
- 7.21 External reference field
- 7.22 External reference comment field
- 7.23 Package attribution text field
- 7.24 Primary Package Purpose field
- 7.25 Release Date
- 7.26 Built Date
- 7.27 Valid Until Date

7.1 Package name field

The existence of the Package name fields indicates the existence of package information in the SPDX information. Hence in order to describe package information, this field is mandatory.

7.1.1 Description

Identify the full name of the package as given by the Package Originator (7.6). The metadata for the package name field is shown in Table 13.

Table 13 — Metadata for the package name field

Attribute	Value
Required	Yes
Cardinality	1..1
Format	Single line of text.

7.1.2 Intent

The name of each package is an important conventional technical identifier to be maintained for each package.

7.1.3 Examples

EXAMPLE 1 Tag: `PackageName:`

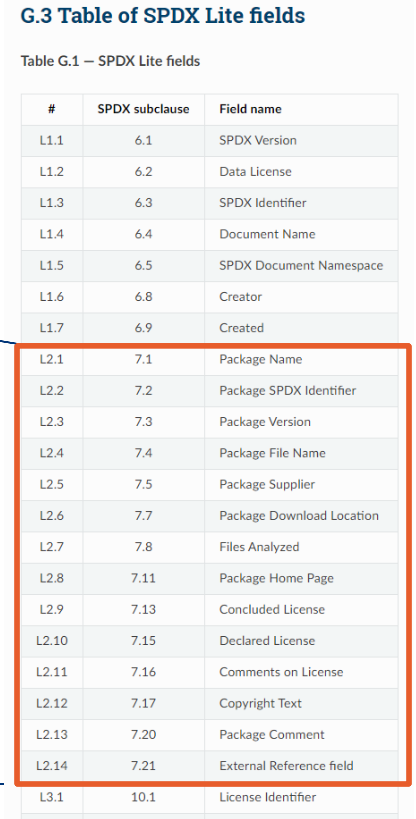
```
PackageName: glibc
```

EXAMPLE 2 RDF: Property `spdx:name` in class `spdx:Package`

```
<Package rdf:about="...">
    <name>glibc</name>
</Package>
```

7.2 Package SPDX identifier field

Full package info in SPDX v2.3 and SPDX Lite package info.



G.3 Table of SPDX Lite fields

Table G.1 — SPDX Lite fields

#	SPDX subclause	Field name
L1.1	6.1	SPDX Version
L1.2	6.2	Data License
L1.3	6.3	SPDX Identifier
L1.4	6.4	Document Name
L1.5	6.5	SPDX Document Namespace
L1.6	6.8	Creator
L1.7	6.9	Created
L2.1	7.1	Package Name
L2.2	7.2	Package SPDX Identifier
L2.3	7.3	Package Version
L2.4	7.4	Package File Name
L2.5	7.5	Package Supplier
L2.6	7.7	Package Download Location
L2.7	7.8	Files Analyzed
L2.8	7.11	Package Home Page
L2.9	7.13	Concluded License
L2.10	7.15	Declared License
L2.11	7.16	Comments on License
L2.12	7.17	Copyright Text
L2.13	7.20	Package Comment
L2.14	7.21	External Reference field
L3.1	10.1	License Identifier

https://spdx.github.io/spdx-spec/v2.3/package-information/

https://spdx.github.io/spdx-spec/v2.3/SPDX-Lite/

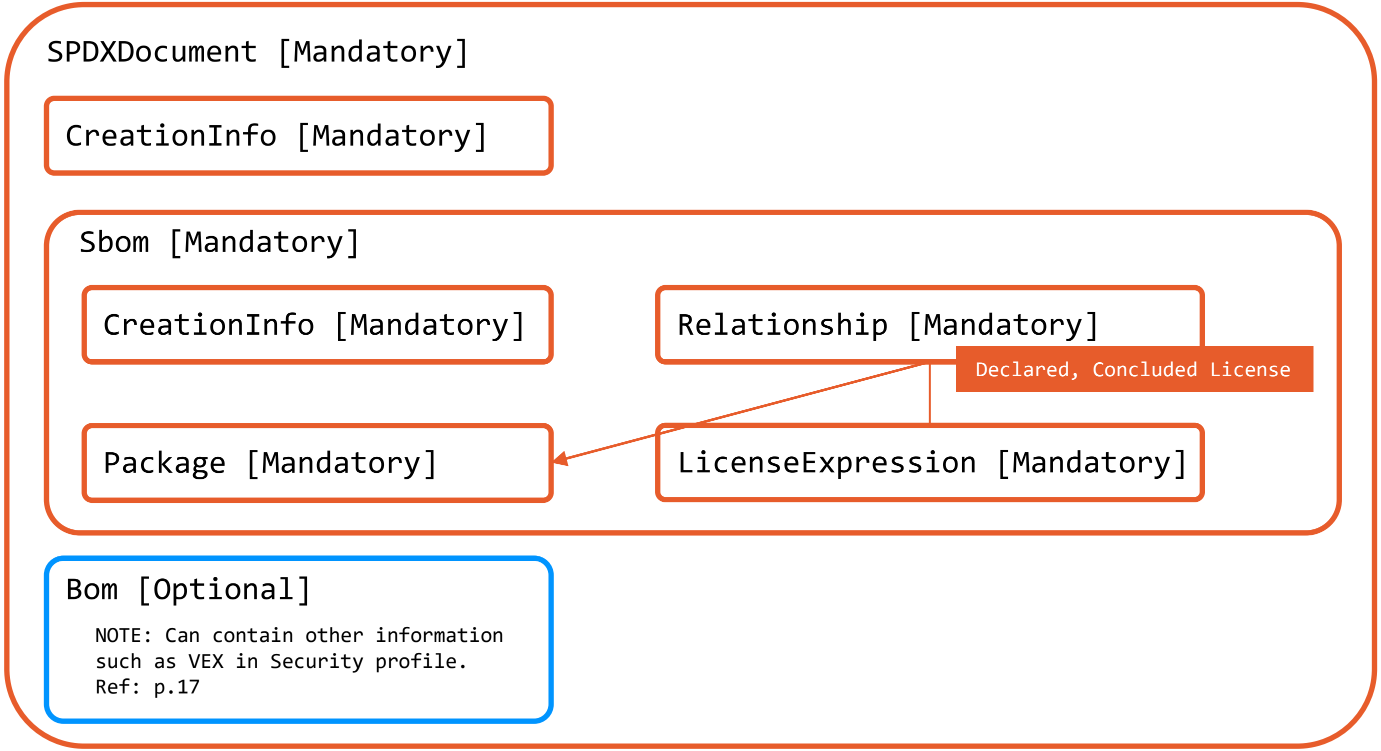
SPDX Lite (Lite profile) in SPDX v3.0

❑ SPDX Lite Design Principle

Because of its origins, SPDX Lite essentially considers the minimum information required to comply with Open Source License compliance.

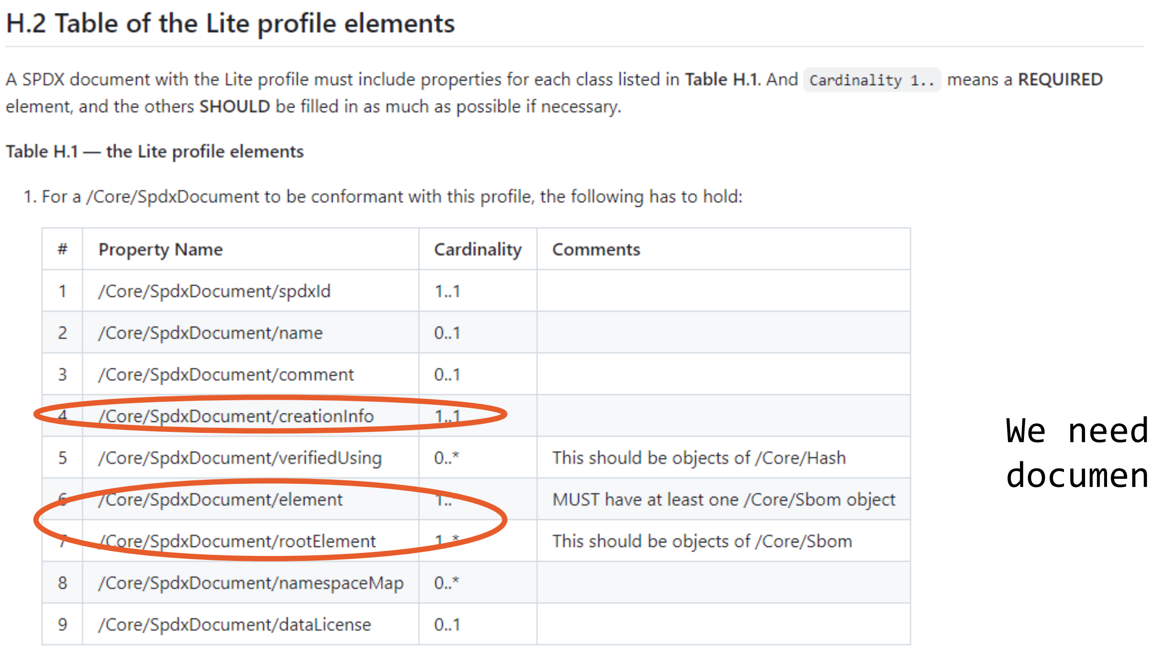
- ✓ Properties that are mandatory by the SPDX specification are also mandatory and are no different, but adding recommendations on what to write. [MANDATORY]
- ✓ Specify additional properties that must be provided for license compliance. [MANDATORY]
- ✓ Specify recommended properties for reducing the burden on the recipient. [RECOMMENDED]
- ✓ Everything else is optional. [OPTIONAL]

Overview of SPDX Data structure for Lite profile



NOTE: Can contain other information such as VEX in Security profile.
Ref: p.17

Deep dive into Lite profile in SPDX v3.0



H.2 Table of the Lite profile elements

A SPDX document with the Lite profile must include properties for each class listed in **Table H.1**. And `Cardinality 1..` means a **REQUIRED** element, and the others **SHOULD** be filled in as much as possible if necessary.

Table H.1 — the Lite profile elements

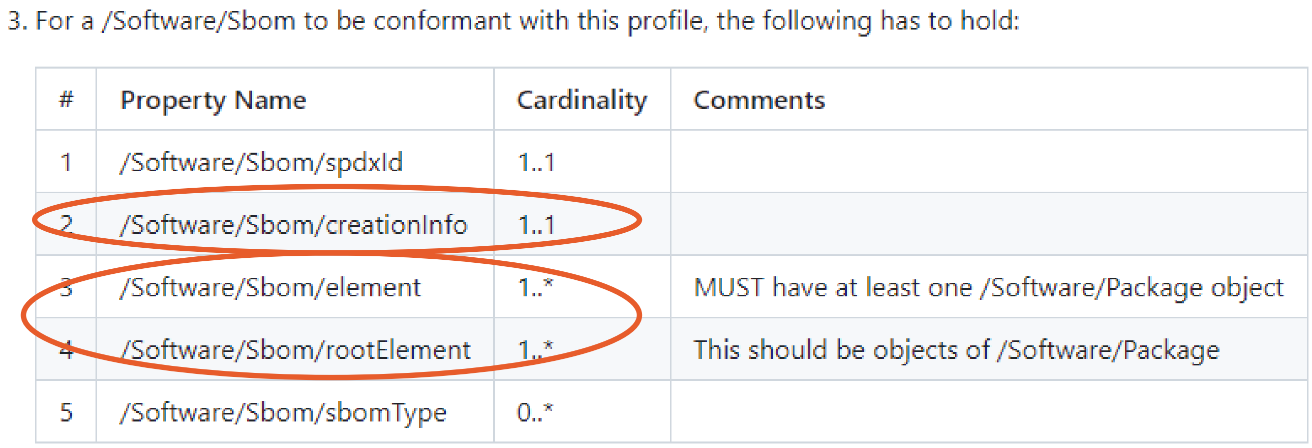
1. For a /Core/SpdxDocument to be conformant with this profile, the following has to hold:

#	Property Name	Cardinality	Comments
1	/Core/SpdxDocument/spdxId	1..1	
2	/Core/SpdxDocument/name	0..1	
3	/Core/SpdxDocument/comment	0..1	
4	/Core/SpdxDocument/creationInfo	1..1	
5	/Core/SpdxDocument/verifiedUsing	0..*	This should be objects of /Core/Hash
6	/Core/SpdxDocument/element	1..	MUST have at least one /Core/Sbom object
7	/Core/SpdxDocument/rootElement	1..*	This should be objects of /Core/Sbom
8	/Core/SpdxDocument/namespaceMap	0..*	
9	/Core/SpdxDocument/dataLicense	0..1	

https://github.com/spdx/spdx-spec/blob/development/v3.0.1/docs/annexes/SPDX-Lite.md

We need to know who created this document and what it contains.

Deep dive into Lite profile in SPDX v3.0

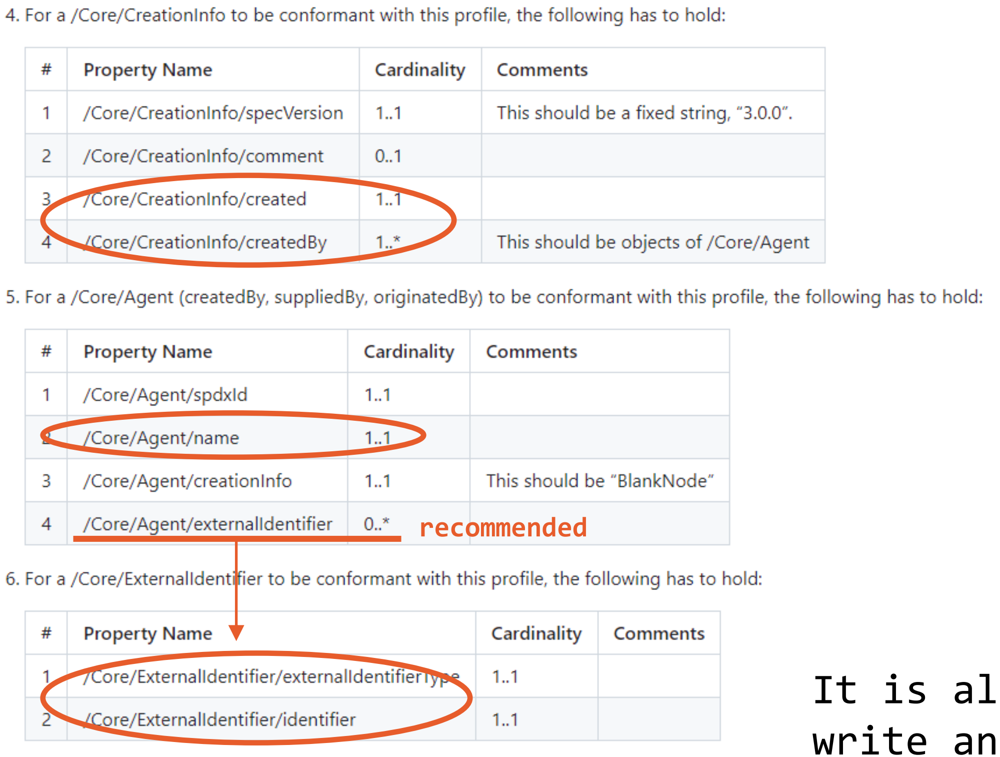


3. For a /Software/Sbom to be conformant with this profile, the following has to hold:

#	Property Name	Cardinality	Comments
1	/Software/Sbom/spdxId	1..1	
2	/Software/Sbom/creationInfo	1..1	
3	/Software/Sbom/element	1..*	MUST have at least one /Software/Package object
4	/Software/Sbom/rootElement	1..*	This should be objects of /Software/Package
5	/Software/Sbom/sbomType	0..*	

Similarly, it’s essential to know who created this SBOM and what it contains.

Deep dive into Lite profile in SPDX v3.0



4. For a /Core/CreationInfo to be conformant with this profile, the following has to hold:

#	Property Name	Cardinality	Comments
1	/Core/CreationInfo/specVersion	1..1	This should be a fixed string, “3.0.0”.
2	/Core/CreationInfo/comment	0..1	
3	/Core/CreationInfo/created	1..1	
4	/Core/CreationInfo/createdBy	1..*	This should be objects of /Core/Agent

5. For a /Core/Agent (createdBy, suppliedBy, originatedBy) to be conformant with this profile, the following has to hold:

#	Property Name	Cardinality	Comments
1	/Core/Agent/spdxId	1..1	
2	/Core/Agent/name	1..1	
3	/Core/Agent/creationInfo	1..1	This should be “BlankNode”
4	/Core/Agent/externalIdentifier	0..*	

recommended

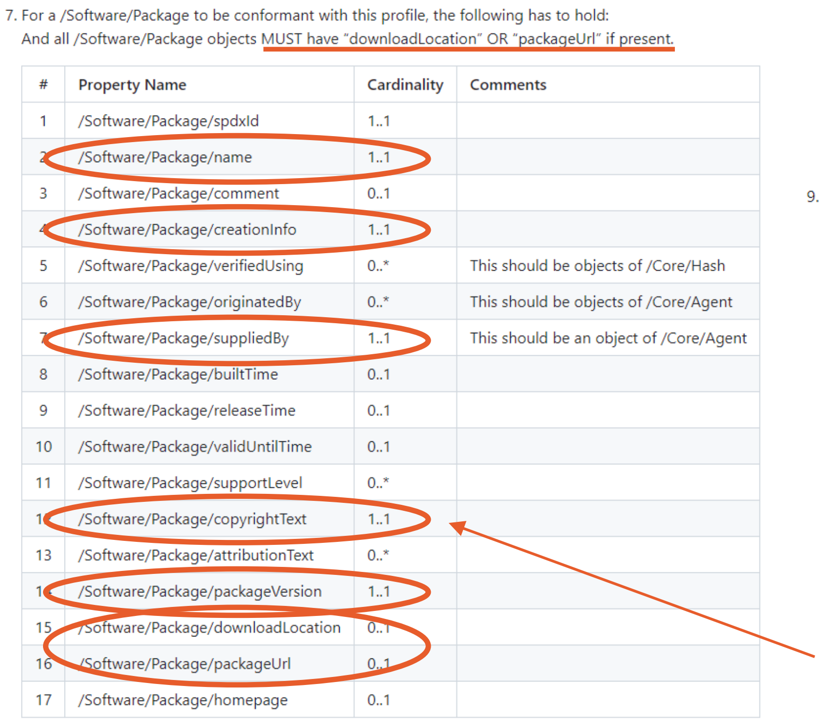
6. For a /Core/ExternalIdentifier to be conformant with this profile, the following has to hold:

#	Property Name	Cardinality	Comments
1	/Core/ExternalIdentifier/externalIdentifierType	1..1	
2	/Core/ExternalIdentifier/identifier	1..1	

It is essential to know who created it and when.

It is also recommended to write an email address etc. for the creator.

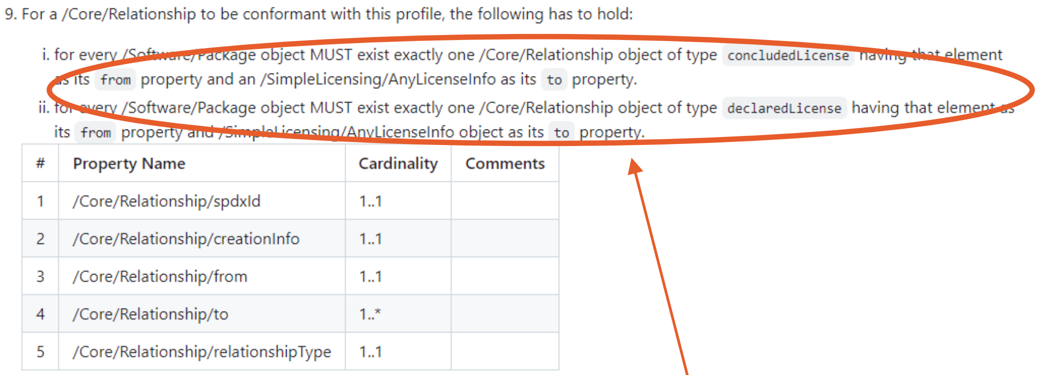
Deep dive into Lite profile in SPDX v3.0



7. For a /Software/Package to be conformant with this profile, the following has to hold:
   And all /Software/Package objects MUST have "downloadLocation" OR "packageUrl" if present.

#	Property Name	Cardinality	Comments
1	/Software/Package/spdxId	1..1	
2	/Software/Package/name	1..1	
3	/Software/Package/comment	0..1	
4	/Software/Package/creationInfo	1..1	
5	/Software/Package/verifiedUsing	0..*	This should be objects of /Core/Hash
6	/Software/Package/originatedBy	0..*	This should be objects of /Core/Agent
7	/Software/Package/suppliedBy	1..1	This should be an object of /Core/Agent
8	/Software/Package/builtTime	0..1	
9	/Software/Package/releaseTime	0..1	
10	/Software/Package/validUntilTime	0..1	
11	/Software/Package/supportLevel	0..*	
12	/Software/Package/copyrightText	1..1	
13	/Software/Package/attributionText	0..*	
14	/Software/Package/packageVersion	1..1	
15	/Software/Package/downloadLocation	0..1	
16	/Software/Package/packageUrl	0..1	
17	/Software/Package/homepage	0..1	

It's essential to have the package name and version, who created it, who provided it, and where it came from in Package information.



9. For a /Core/Relationship to be conformant with this profile, the following has to hold:

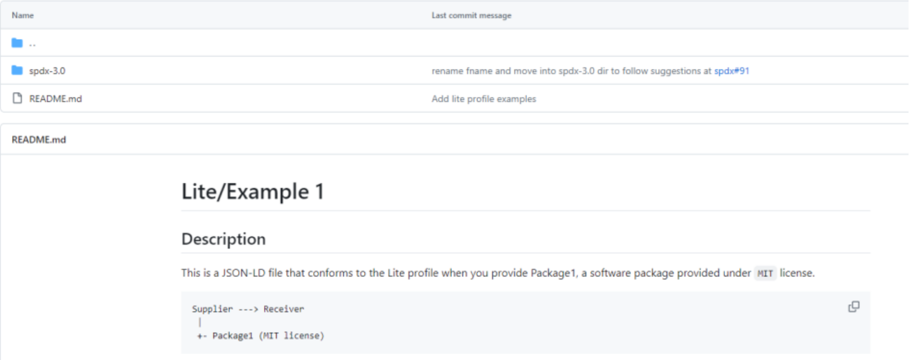
   i. for every /Software/Package object MUST exist exactly one /Core/Relationship object of type `concludedLicense` having that element as its `from` property and an /SimpleLicensing/AnyLicenseInfo as its `to` property.

   ii. for every /Software/Package object MUST exist exactly one /Core/Relationship object of type `declaredLicense` having that element as its `from` property and /SimpleLicensing/AnyLicenseInfo object as its `to` property.

#	Property Name	Cardinality	Comments
1	/Core/Relationship/spdxId	1..1	
2	/Core/Relationship/creationInfo	1..1	
3	/Core/Relationship/from	1..1	
4	/Core/Relationship/to	1..*	
5	/Core/Relationship/relationshipType	1..1	

For license compliance, it is mandatory to describe copyright text and associate with license information by using Relationship object.

Difficult to understand only with the specifications.



Name	Last commit message
..	
spdx-3.0	rename fname and move into spdx-3.0 dir to follow suggestions at spdx#91
README.md	Add lite profile examples

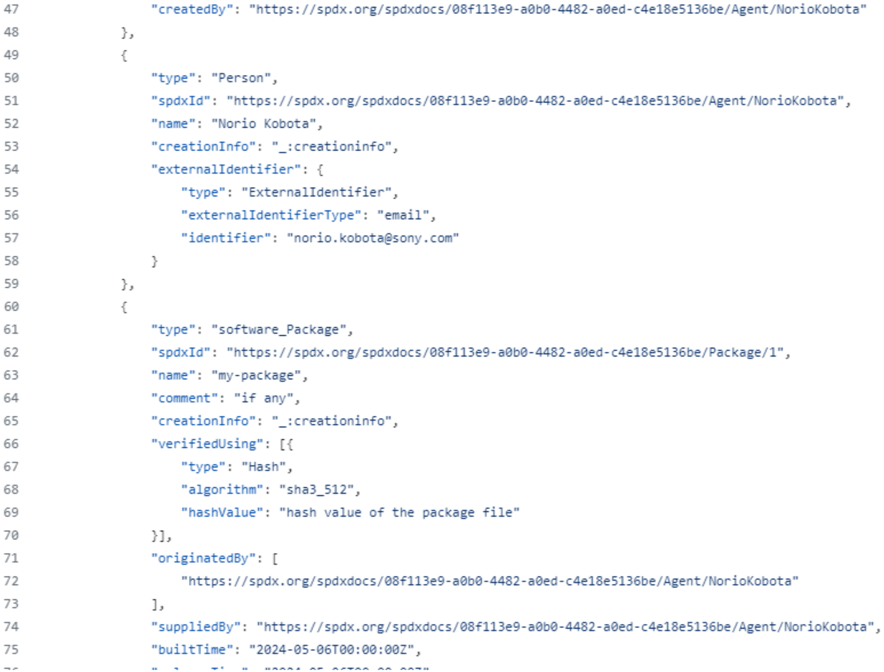
README.md

Lite/Example 1

Description

This is a JSON-LD file that conforms to the Lite profile when you provide Package1, a software package provided under `MIT` license.

```
Supplier ---> Receiver
 |
 +- Package1 (MIT license)
```

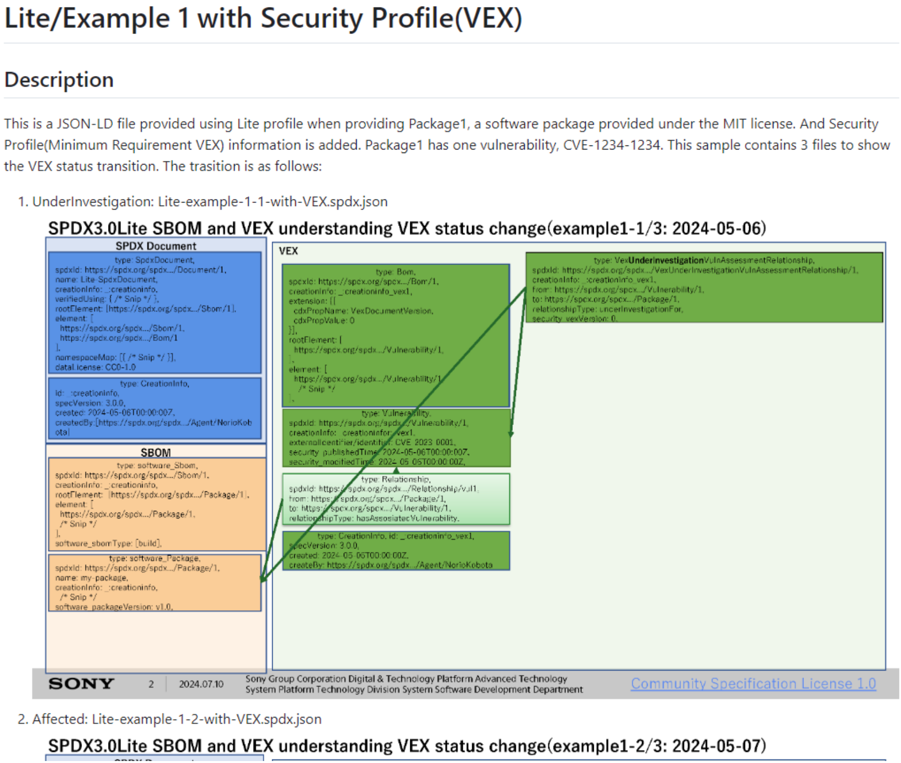


```
                "createdBy": "https://spdx.org/spdxdocs/08f113e9-a0b0-4482-a0ed-c4e18e5136be/Agent/NorioKobota"
            },
            {
                "type": "Person",
                "spdxId": "https://spdx.org/spdxdocs/08f113e9-a0b0-4482-a0ed-c4e18e5136be/Agent/NorioKobota",
                "name": "Norio Kobota",
                "creationInfo": "_:creationinfo",
                "externalIdentifier": {
                    "type": "ExternalIdentifier",
                    "externalIdentifierType": "email",
                    "identifier": "norio.kobota@sony.com"
                }
            },
            {
                "type": "software_Package",
                "spdxId": "https://spdx.org/spdxdocs/08f113e9-a0b0-4482-a0ed-c4e18e5136be/Package/1",
                "name": "my-package",
                "comment": "if any",
                "creationInfo": "_:creationinfo",
                "verifiedUsing": [{
                    "type": "Hash",
                    "algorithm": "sha3_512",
                    "hashValue": "hash value of the package file"
                }],
                "originatedBy": [
                    "https://spdx.org/spdxdocs/08f113e9-a0b0-4482-a0ed-c4e18e5136be/Agent/NorioKobota"
                ],
                "suppliedBy": "https://spdx.org/spdxdocs/08f113e9-a0b0-4482-a0ed-c4e18e5136be/Agent/NorioKobota",
                "builtTime": "2024-05-06T00:00:00Z",
```

We are creating and evaluating samples that are as simple as possible and fit our use cases.

https://github.com/NorioKobota/spdx-examples/tree/lite-profile/lite/example1

Verify if the Lite profile works well with VEX - Security profile



Lite/Example 1 with Security Profile(VEX)

Description

This is a JSON-LD file provided using Lite profile when providing Package1, a software package provided under the MIT license. And Security Profile(Minimum Requirement VEX) information is added. Package1 has one vulnerability, CVE-1234-1234. This sample contains 3 files to show the VEX status transition. The trasition is as follows:

1. UnderInvestigation: Lite-example-1-1-with-VEX.spdx.json

SPDX3.0Lite SBOM and VEX understanding VEX status change(example1-1/3: 2024-05-06)

SPDX Document

```
type: SpdxDocument,
spdxId: https://spdx.org/spdx.../Document/1,
name: Lite-SpdxDocument,
creationInfo: _:creationinfo,
verifiedUsing: { /* Snip */ },
rootElement: [https://spdx.org/spdx.../Sbom/1],
element: [
  https://spdx.org/spdx.../Sbom/1,
  https://spdx.org/spdx.../Bom/1
],
namespaceMap: [{ /* Snip */ }],
dataLicense: CC0-1.0
```

```
type: CreationInfo,
id: _:creationinfo,
specVersion: 3.0.0,
created: 2024-05-06T00:00:00Z,
createdBy:[https://spdx.org/spdx.../Agent/NorioKobota]
```

SBOM

```
type: software_Sbom,
spdxId: https://spdx.org/spdx.../Sbom/1,
creationInfo: _:creationinfo,
rootElement: [https://spdx.org/spdx.../Package/1],
element: [
  https://spdx.org/spdx.../Package/1,
  /* Snip */
],
software_sbomType: [build],
```

```
type: software_Package,
spdxId: https://spdx.org/spdx.../Package/1,
name: my-package,
creationInfo: _:creationinfo,
  /* Snip */
software_packageVersion: v1.0,
```

VEX

```
type: Bom,
spdxId: https://spdx.org/spdx.../Bom/1,
creationInfo: _:creationinfo_vex1,
extension: [{
  cdxPropName: VexDocumentVersion,
  cdxPropValue: 0
}],
rootElement: [
  https://spdx.org/spdx.../Vulnerability/1,
],
element: [
  https://spdx.org/spdx.../Vulnerability/1
    /* Snip */
],
```

```
type: Vulnerability,
spdxId: https://spdx.org/spdx.../Vulnerability/1,
creationInfo: _:creationinfo_vex1,
externalIdentifier/identifier: CVE-2023-0001,
security_publishedTime: 2024-05-06T00:00:00Z,
security_modifiedTime: 2024-05-06T00:00:00Z,
```

```
type: Relationship,
spdxId: https://spdx.org/spdx.../Relationship/vul1,
from: https://spdx.org/spdx.../Package/1,
to: https://spdx.org/spdx.../Vulnerability/1,
relationshipType: hasAssosiatedVulnerability,
```

```
type: CreationInfo, id: _:creationinfo_vex1,
specVersion: 3.0.0,
created: 2024-05-06T00:00:00Z,
createBy: https://spdx.org/spdx.../Agent/NorioKobota
```

```
type: VexUnderInvestigationVulnAssessmentRelationship,
spdxId: https://spdx.org/spdx.../VexUnderInvestigationVulnAssessmentRelationship/1,
creationInfo: _:creationinfo_vex1,
from: https://spdx.org/spdx.../Vulnerability/1,
to: https://spdx.org/spdx.../Package/1,
relationshipType: underInvestigationFor,
security_vexVersion: 0,
```

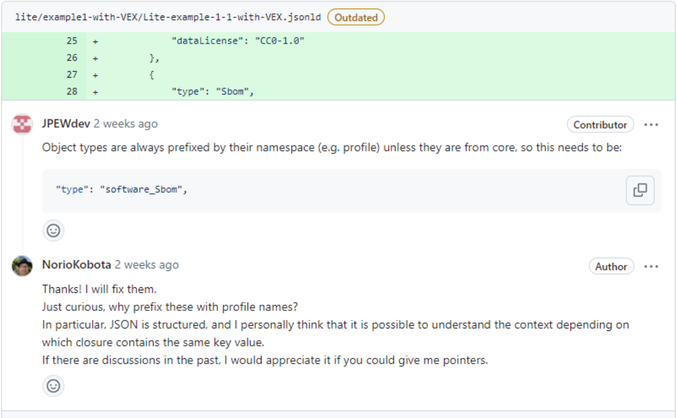
SONY 2 2024.07.10 Sony Group Corporation Digital & Technology Platform Advanced Technology System Platform Technology Division System Software Development Department Community Specification License 1.0

2. Affected: Lite-example-1-2-with-VEX.spdx.json

SPDX3.0Lite SBOM and VEX understanding VEX status change(example1-2/3: 2024-05-07)

Reviewed with SPDX community engineers.
Great Thanks to Josh!

https://github.com/spdx/spdx-examples/pull/91



lite/example1-with-VEX/Lite-example-1-1-with-VEX.jsonld Outdated

```
+              "dataLicense": "CC0-1.0"
+          },
+          {
+              "type": "Sbom",
```

JPEWdev 2 weeks ago Contributor

Object types are always prefixed by their namespace (e.g. profile) unless they are from core, so this needs to be:

```
"type": "software_Sbom",
```

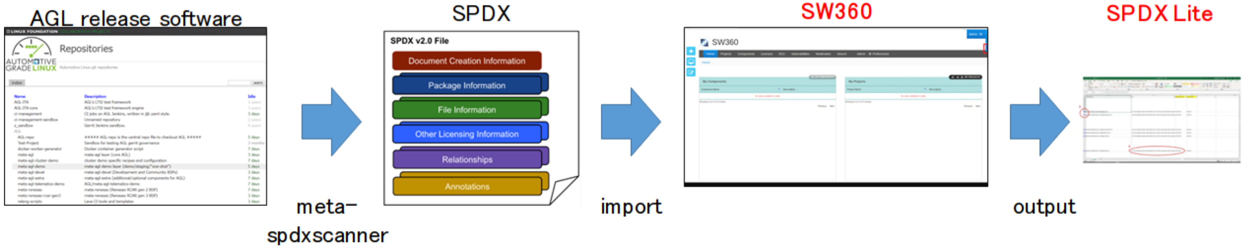
NorioKobota 2 weeks ago Author

Thanks! I will fix them.
Just curious, why prefix these with profile names?
In particular, JSON is structured, and I personally think that it is possible to understand the context depending on which closure contains the same key value.
If there are discussions in the past, I would appreciate it if you could give me pointers.

https://github.com/no-ta/spdx-examples/tree/merge-lite-example-1/lite/example1-with-VEX/spdx-3.0

SPDX Lite – Actually Used in Japan

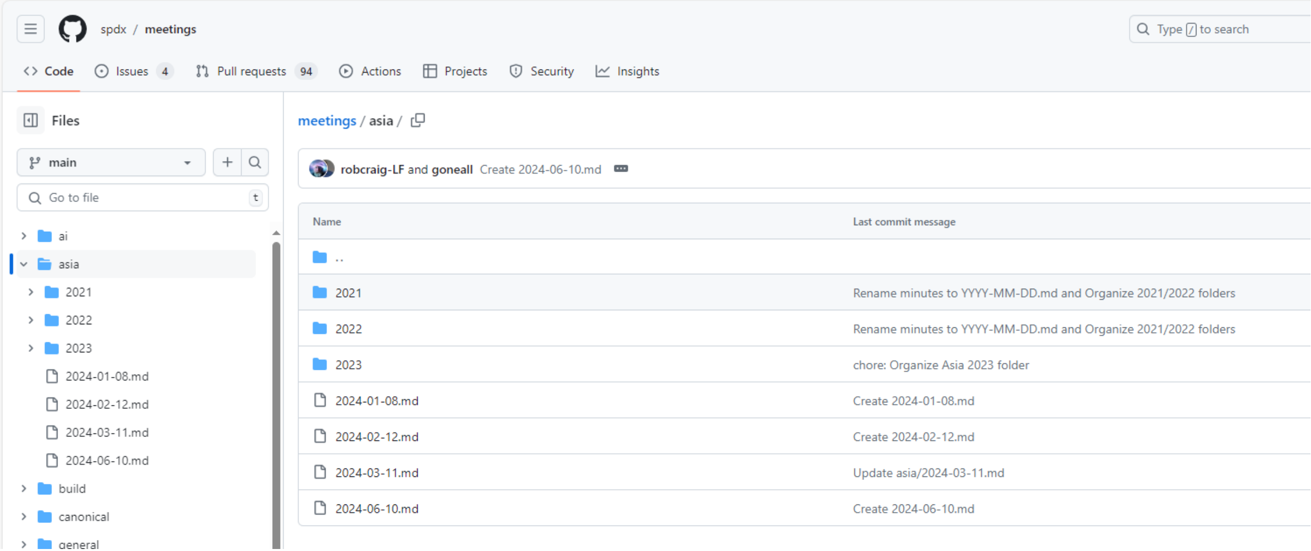
OpenChain and AGL Collaborate to Facilitate Open Source Compliance in Automotive Production



https://openchainproject.org/news/2019/12/05/openchain-and-agl-collaborate-to-facilitate-open-source-compliance-in-automotive-production

SPDX Lite (v2.x) - Since the number of properties that can be managed in a spreadsheet, so I heard that it is popular among legal and intellectual property professionals other than engineers in Japan.

Thanks to the SPDX project



meetings / asia /

robcraig-LF and goneall Create 2024-06-10.md

Name	Last commit message
..	
2021	Rename minutes to YYYY-MM-DD.md and Organize 2021/2022 folders
2022	Rename minutes to YYYY-MM-DD.md and Organize 2021/2022 folders
2023	chore: Organize Asia 2023 folder
2024-01-08.md	Create 2024-01-08.md
2024-02-12.md	Create 2024-02-12.md
2024-03-11.md	Update asia/2024-03-11.md
2024-06-10.md	Create 2024-06-10.md

The SPDX team set up an Asia Call once a month because it's hard to attend regular spdx-tech meetings due to time zones.

Thanks, Any Questions?