Annex E

SPDX Lite (Normative)

23 Explanation of the Lite profile

The Lite profile is designed to make it quick and easy to start a Software Bill of Materials in situations where a company may have limited capacity for introducing new items into their processes. The Lite profile captures the minimum set of information required for license compliance in the software supply chain. It contains information about the creation of the SBOM, package lists with licensing and other related information, and their relationships.

All elements in Lite profile are essential for complying with licenses. It is easy to use a SPDX document with the Lite profile for anyone who does not have enough knowledge about licensing information and easy to import license information from former versions of SPDX Lite format files. The Lite profile offers the flexibility to be used either alone or in combination with other SPDX profiles as a SPDX document in the software supply chain.

24 Mandatory and recommended properties

The Lite profile specifies that some properties MUST be present and some others SHOULD be present, as much as possible.

The following lists collect and present this information for every class present in the SPDX data, in a concise and easy-to-follow format. The lists of properties are in alphabetical order, for easy reference.

24.1 /Core/SpdxDocument

- Mandatory
    1. creationInfo
    2. element (may be multiple), MUST have at least one /Core/Sbom object
    3. rootElement (may be multiple), SHOULD be objects of type /Core/Sbom
    4. spdxId
- Recommended
    1. comment
    2. dataLicense
    3. name
    4. namespaceMap (may be multiple)
    5. verifiedUsing (may be multiple), SHOULD be objects of type /Core/Hash

24.2 /Software/Sbom

- Mandatory
    1. creationInfo
    2. element (may be multiple), MUST have at least one /Software/Package object

3. rootElement (may be multiple), SHOULD be objects of type /Software/Package
4. spdxId

- Recommended

1. sbomType (may be multiple)

24.3 /Software/Package

- Mandatory

1. copyrightText
2. creationInfo
3. name
4. packageVersion
5. spdxId
6. suppliedBy, SHOULD be an object of type /Core/Agent

- Recommended

1. attributionText (may be multiple)
2. builtTime
3. comment
4. downloadLocation
5. homepage
6. originatedBy (may be multiple), SHOULD be objects of type /Core/Agent
7. packageUrl
8. releaseTime
9. supportLevel (may be multiple)
10. validUntilTime
11. verifiedUsing (may be multiple), SHOULD be objects of type /Core/Hash

However, there MUST be at least a “downloadLocation” or “packageUrl” property.

Additionally:

1. 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.
2. 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.

24.4 /Core/Hash

- Mandatory

1. algorithm
2. hashValue

- Recommended

1. comment

24.5 /SimpleLicensing/LicenseExpression

- Mandatory
    1. creationInfo
    2. licenseExpression
    3. spdxId
- Recommended
    1. licenseListVersion

24.6 /SimpleLicensing/SimpleLicensingText

- Mandatory
    1. creationInfo
    2. licenseText
    3. spdxId
- Recommended
    1. comment

24.7 /Core/Agent (createdBy, suppliedBy, originatedBy)

- Mandatory
    1. creationInfo, SHOULD be “BlankNode”
    2. name
    3. spdxId
- Recommended
    1. externalIdentifier (may be multiple)

24.8 /Core/CreationInfo

- Mandatory
    1. created
    2. createdBy (may be multiple), SHOULD be objects of type /Core/Agent
    3. specVersion, MUST be a fixed string, “3.0.0”.
- Recommended
    1. comment

24.9 /Core/ExternalIdentifier

- Mandatory
    1. externalIdentifierType
    2. identifier

24.10 /Core/NameSpaceMap

- Mandatory
    1. namespace
    2. prefix

24.11 /Core/Relationship

- Mandatory

    1. creationInfo
    2. from
    3. relationshipType
    4. spdxId
    5. to (may be multiple)