ERICSSON

Supplier Software Bill of Material Specification

Specification

Abstract

This specification defines the recommended Software Bill of Material format that Ericsson suppliers and partners should adhere to. It states the mandatory attributes that are required to be populated along with their format and how to populate them. Suppliers and partners can provide additional information when deemed necessary.

Note that the supplier SBOM is to be shared with Ericsson operators and customers along with the Ericsson SBOM document when requested. The same access control policies that apply to Ericsson SBOM documents shall be applied to the supplier SBOM documents.

This document undergoes reviews regularly and will be updated from time to time.

Supplementary Documents

This is a list of documents that are required to get an understanding of this document.

[1] SPDX Specification v2.2.1

[2] SPDX License List

Table of Content

Background

To comply with operator requirements and government agencies, Ericsson requires suppliers and partners that provide software to Ericsson to deliver a Software Bill of Material (SBOM) document in addition to other required documentation. **Note** that the supplier SBOM is to be shared with Ericsson operators and customers along with the Ericsson SBOM document when requested. The same access control policies that apply to Ericsson SBOM documents shall be applied to the supplier SBOM documents.

Suppliers should provide SBOMs that meet the NTIA's Recommended Minimum Elements, including a list of the supplier's integrated open-source software and commercial components [3].

There are two widely used data formats that express the syntax of an SBOM: SPDX and CycloneDX.

Since SPDX is recognized as an international open standard (ISO/IEC 5962:2021); it is strongly recommended for Ericsson software suppliers and partners to provide an SBOM in SPDX format.

This document is based on the ISO/IEC 5962 Information technology — SPDX Specification V2.2.1 which is a publicly available standard [1] and compliant to the "Minimum Elements" for an SBOM that was released by the National Telecommunications and Information Administration (NTIA) [3] following the United States Executive Order 14028.

According to NTIA's "Minimum Elements for an SBOM", table 1 maps the mandatory attributes with the SPDX standard.

NTIA element name	SPDX 2.2.1 field name
Supplier Name	"supplier" (section 7.5 of ISO/IEC 5962)
Component Name	"name" (section 7.1 of ISO/IEC 5962)
Version of the Component	"versionInfo" (section 7.3 of ISO/IEC 5962)
Other Unique Identifiers	"documentNamespace", "SPDXID" (section 6.5, 7.2 of ISO/IEC 5962)
Dependency Relationship	"relationships" (section 11.1 of ISO/IEC 5962)
Author of SBOM Data	"creators" (section 6.8 of ISO/IEC 5962)
Timestamp	"created" (section 6.9 of ISO/IEC 5962)

Table 1

The following sections list the attribute JSON keys and format specified in table 1 in addition to mandatory attributes that are required to conform to the SPDX V2.2.1 specification.

1 SPDX document creation information section

1.1 SPDX version field

Refers to the SPDX specification version. For more information, please refer to section 6.1 of ISO/IEC 5962 [1].

Attribute	"spdxVersion"
Type	String
Cardinality	1..1
Format	SPDX-M.N where: • M is the major version • N is the minor version
Value	"SPDX-2.2"

1.2 Data license field

The intent of this field is to alleviate any concern that the content in an SPDX document is subject to any form of intellectual property right. For more information, please refer to section 6.2 of ISO/IEC 5962 [1].

Attribute	"dataLicense"
Type	String
Cardinality	1..1
Format	N/A
Value	"CC0-1.0"

1.3 SPDX identifier field

The intent of this field is to be able to identify the current SPDX document to other elements in the relationship section. For more information, please refer to section 6.3 of ISO/IEC 5962 [1].

Attribute	"SPDXID"
Type	String

Cardinality	1..1
Format	N/A
Value	"SPDXRef-DOCUMENT"

1.4 Document name field

The intent of this field is to identify the name of this document as designated by the creator, in this case the supplier or partner that is providing Ericsson with the software. For more information, please refer to section 6.4 of ISO/IEC 5962 [1].

Note that this is the package that the Software Bill of Material document describes.

Attribute	"name"
Type	String
Cardinality	1..1
Format	Single line of text
Recommended Value	Name and version of the software separated by a separator For example: "*glibc-v2.3*"

2 SPDX document namespace field

The intent of this field is to provide an SPDX document-specific namespace as a unique absolute identify URI. Note that there is no intention for this URI to represent an accessible endpoint. For more information, please refer to section 6.5 of ISO/IEC 5962 [1].

Note that this is the package that the Software Bill of Material document describes.

Attribute	"documentNamespace"
Type	String
Cardinality	1..1
Format	URI
Value	Please see section 2.1.1

2.1.1 Additional Information

This URI must be unique, shall follow RFC-3986, cannot contain a URI "part" (for example the # delimiter), and must contain a scheme (for example "https:").

This URI does not need to be accessible. It is only intended to provide a unique ID.

If the SPDX document is updated, thereby creating a new version, a new URI for the updated document shall be created. There can only be one URI for an SPDX document and only one SPDX document for a given URI.

2.2 External document references field

The intent of this field is to identify all external SPDX documents referenced within this SPDX document. A package within this document may be related to other packages that have an external SPDX document. For more information, please refer to section 6.6 of ISO/IEC 5962 [1].

Attribute	"externalDocumentRefs"
Type	Array
Cardinality	0..*
Format	"externalDocumentId" : please refer to section 2.2.1, "checksum" : please refer to section 2.2.2, "spdxDocument" : please refer to section 2.2.3
Value	N/A

2.2.1 External document ID field

The intent of this field is to provide a unique identifier to an external SPDX document within this document.

Attribute	"externalDocumentId"
Type	String
Cardinality	1..1
Format	DocumentRef-x where: x is a unique string containing letters, numbers, . , - and/or +

Value	Example: "*DocumentRef-1"*

2.2.2 Checksum field

The intent of this field is to provide the checksum of the external SPDX document.

Attribute	"checksum"
Type	Object
Cardinality	1..1
Format	"algorithm" : please refer to section 2.2.2.1, "checksumValue" : please refer to section 2.2.2.2
Value	N/A

2.2.2.1 Algorithm field

The intent of this field is to provide the algorithm used to produce the checksum of the external SPDX document. Note that currently the only supported algorithm in the ISO standard is SHA1.

Attribute	"algorithm"
Type	String
Cardinality	1..1
Format	Enum ["SHA256", "SHA1", "SHA384", "MD2", "MD4", "SHA512", "MD6", "MD5", "SHA224"]
Value	N/A

2.2.2.2 Checksum value field

The checksumValue property provides a lower case hexidecimal encoded digest value produced using a specific algorithm for the external SPDX document.

Attribute	"checksumValue"

Type	String
Cardinality	1..1
Format	Lowercase hexadecimal digits
Value	N/A

2.2.3 SPDX document field

The intent of this field is to provide the unique ID for the external document as defined in "documentNamespace" attribute of that external referenced SPDX document.

Attribute	"spdxDocument"
Type	string
Cardinality	1..1
Format	URI
Value	"documentNamespace" attribute in the external referenced SPDX document

2.3 Creation info field

The intent of this field is to provide the necessary information for forward and backward compatibility for processing tools.

Attribute	"creationInfo"
Type	Object
Cardinality	1..1
Format	"creators" : please refer to section 2.3.1 "created" : please refer to section 2.3.2 "comment" : please refer to section **Error! Reference source not found.**
Value	N/A

2.3.1 Creators field

The intent of this field is to identify the creators of this SPDX document, in this case the supplier or partner that is providing Ericsson with the software. If the SPDX document was created by an individual, indicate the person's name. If the SPDX document was created on behalf of a company or organization, indicate the entity name. If the SPDX document was created using a software tool, indicate the name and version for that tool. If multiple participants or tools were involved, use multiple instances of this field. For more information, please refer to section 6.8 of ISO/IEC 5962 [1].

Attribute	"creators"
Type	Array
Cardinality	1..*
Format	"Person: person name" "Organization: organization" "Tool: name of the tool-version"
Value	Example: "*Organization: Telefonaktiebolaget LM Ericsson*"

2.3.2 Created field

The intent of this field is to indicate when this SPDX document was originally created. For more information, please refer to section 6.9 of ISO/IEC 5962 [1].

Attribute	"created"
Type	String
Cardinality	1..1
Format	YYYY-MM-DDThh:mm:ssZ Please see section 2.3.2.1 for additional information
Value	Example: "*2024-06-05T09:19:06Z*"

2.3.2.1 Additional Information

The date is to be specified according to combined date and time in UTC format as specified in ISO 8601 standard.

3 Package information section

ISO/IEC 5962 defines a package as: "A Package refers to any unit of content that can be associated with a distribution of software. Typically, a Package is composed of one or more files. An SPDX document may, but is not required to, provide details about the individual files comprising a Package" [1].

In the context of this document, a "Package" is the software Product that the supplier or partner is providing to Ericsson. Note that the order in which each package is defined in the Software Bill of Material is not of importance. However, this document (SPDXRef-DOCUMENT) shall define at least one package: the "root" package.

Note that these are the required fields, however the supplier or partner can provide additional fields.

Attribute	"packages"
Type	Array
Cardinality	1..*
Format	"name" : please refer to section 3.1, "SPDXID" : please refer to section 3.2, "versionInfo" : please refer to section 3.3, "downloadLocation" : please refer to section 3.4, "licenseConcluded" : please refer to section 3.5, "licenseDeclared" : please refer to section 3.6, "copyrightText" : please refer to section 3.7, "supplier" : please refer to section 3.8
Value	N/A

3.1 Package name field

The intent of this field is to identify the full name of the package as given by the Package Originator. For more information, please refer to section 7.1 of ISO/IEC 5962 [1].

Attribute	"name"
Type	String

Cardinality	1..1
Format	Single line of text
Value	Example: "*log4j-jboss-logmanager*"

3.2 Package SPDX identifier field

The intent of this field is to uniquely identify each package referenced in the Software Bill of Material document. There may be several versions of the same package within an SPDX document. Each element needs to be uniquely referred so that relationships between elements can be clearly articulated. For more information, please refer to section 7.2 of ISO/IEC 5962 [1].

Attribute	"SPDXID"
Type	String
Cardinality	1..1
Format	SPDXRef-x where: x is a unique string containing letters, numbers, ., and/or –
Value	Example: "*SPDXRef-1*"

3.3 Package version field

The intent of this field is to identify the version of the package as given by the Package Originator. For more information, please refer to section 7.3 of ISO/IEC 5962 [1].

Attribute	"versionInfo"
Type	String
Cardinality	1..1
Format	Single line of text
Value	Example: "*2.6.9"*

3.4 Package download location field

The intent of this field is to indicate the download Universal Resource Locator (URL), or a specific location within a version control system (VCS) where the package was downloaded. For more information, please refer to section 7.7 of ISO/IEC 5962 [1].

Attribute	"downloadLocation"
Type	String
Cardinality	1..1
Format	Uniform resource locator | NOASSERTION | NONE | VCS location
Value	Example: "*https://github.com/log4js-node/log4js-node/archive/v6.3.0.zip"*

3.5 Concluded license field

The field contains the licenses the SPDX document creator has concluded as governing the package or alternative values if the governing license cannot be determined. For more information, please refer to section 7.13 of ISO/IEC 5962 [1].

Attribute	"licenseConcluded"
Type	String
Cardinality	1..1
Format	<SPDX License Expression> where: <SPDX License Expression> is a valid SPDX License Expression
Value	Example: "*BSD-3-Clause"*

3.6 Declared license field

The intent of this field is to list the licenses that have been declared by the authors of the package. Any license information that does not originate from the package authors, e.g. license information from a third-party repository, should not be included in this field. For more information, please refer to section 7.15 of ISO/IEC 5962 [1].

Attribute	"licenseDeclared"

Type	String
Cardinality	1..1
Format	<SPDX License Expression> where: <SPDX License Expression> is a valid SPDX License Expression
Value	Example: "*BSD-3-Clause"*

3.7 Copyright text field

The intent of this field is to record any copyright notices for the package. This will be a free form text field extracted from package information files. For more information, please refer to section 7.17 of ISO/IEC 5962 [1].

Attribute	"copyrightText"
Type	String
Cardinality	1..1
Format	Free form text that can span multiple lines | NOASSERTION
Value	Example: "*Copyright 2008-2010 John Smith"*

3.8 Package supplier field

The intent of this field is to identify the actual distribution source for the package identified in the SPDX document. This might or might not be different from the originating distribution source for the package. The name of the Package Supplier shall be an organization or recognized author and not a web site. For more information, please refer to section 7.5 of ISO/IEC 5962 [1].

Attribute	"supplier"
Type	String
Cardinality	1..1
Format	"Organization: organization" | "Person: person" | NOASSERTION
Value	Example: *"Organization: The Linux Foundation"*

4 Other licensing information detected section

4.1 Extracted license information field

The intent of this section is to provide information regarding licenses that are not found on the SPDX License List. For example, some FOSS or COTS might have their own licenses which is not part of the SPDX license. The following FOSS is an example of such a case:

https://github.com/matplotlib/matplotlib/

Attribute	"hasExtractedLicensingInfos"
Type	Array
Cardinality	0..*
Format	"licenseId" : please refer to section 4.1.1, "extractedText" : please refer to section 4.1.2 "name" : please refer to section 4.1.3
Value	N/A

4.1.1 License identifier field

The intent of this field is to provide a locally, unique identifier to refer to licenses that are not found on the SPDX License List. This unique identifier can then be used in the package sections of the SPDX document.

This identifier shall be unique within the SPDX document.

For more information, please refer to section 10.1 of ISO/IEC 5962 [1].

Attribute	"licenseId"
Type	String
Cardinality	1..1
Format	LicenseRef-x where:

	x is a unique string containing letters, numbers, . and/or -
Value	Example: *"LicenseRef-1"*

4.1.2 Extracted text field

The intent of this field is to provide a copy of the actual text of the license reference extracted from the package. For more information, please refer to section 10.2 of ISO/IEC 5962 [1].

Attribute	"extractedText"
Type	String
Cardinality	1..1
Format	Free form text field that may span multiple lines
Value	Example: "*License agreement for matplotlib versions 1.3.0 and later* ========== *1. This LICENSE AGREEMENT is between the Matplotlib Development Team* *("MDT"), and the Individual or Organization ("Licensee") accessing and* *otherwise using matplotlib software in source or binary form and its* *associated documentation ..."*

4.1.3 License Name field

The intent of this field is to provide a common name for the license that is not on the SPDX list. Use NOASSERTION if there is no common name or it is not known. For more information, please refer to section 10.3 of ISO/IEC 5962 [1].

Attribute	"name"
Type	String
Cardinality	1..1
Format	Single line of text | NOASSERTION

Value	N/A

5 Relationships between SPDX elements information section

This section provides information about the relationship between two SPDX elements. For example, you can represent a relationship between two different Files, between a Package and a File, between two Packages, or between one SPDXDocument and another SPDXDocument.

5.1 Relationship field

The intent of this field is to provide information about the relationship between two SPDX elements.

DESCRIBES relationship is a mandatory relationship. It shall be used to indicate that this document (SPDXRef-DOCUMENT) describes which "root" package.

CONTAINS relationship shall be used between the different packages.

For example:

```
{
  "spdxElementId": "SPDXRef-DOCUMENT",
  "relatedSpdxElement": "SPDXRef-PACKAGE-1",
  "relationshipType": "DESCRIBES"
},
{
  "spdxElementId": "SPDXRef-PACKAGE-1",
  "relatedSpdxElement": " SPDXRef-PACKAGE-2",
  "relationshipType": "CONTAINS"
}
```

For more information, please refer to section 11.1 of ISO/IEC 5962 [1].

Attribute	"relationships"
Type	Array

Cardinality	1..*
Format	"spdxElementId" : please refer to section 5.1.1, "relationshipType" : please refer to section 5.1.2, "relatedSpdxElement" : please refer to section 5.1.3
Value	N/A

5.1.1 SPDX ID field

The intent of this field is to provide the ID to which the SPDX element is related.

Attribute	"spdxElementId"
Type	String
Cardinality	1..1
Format	SPDXID where SPDXID is a string as described in 1.3 or 3.2
Value	Example: "*SPDXRef-PACKAGE-1"*

5.1.2 Relationship type field

The intent of this field is to provide information about the relationship between two SPDX elements.

Note that these are the mandatory relationship types, however the supplier or partner can provide additional relationship types.

Attribute	"relationshipType"
Type	String
Cardinality	1..1
Format	Enum ["DESCRIBES", "CONTAINS"]
Value	N/A

5.1.3 Related SPDX element field

The intent of this field is to provide the ID of the related SPDX element. Note that this field is either set to another package in this SPDX document or to an external SPDX document or to NOASSERTION when it is not clear if there are relationships that may apply or not or to NONE if there are NO other relationships.

Attribute	"relatedSpdxElement"
Type	String
Cardinality	1..1
Format	["DocumentRef-x:"]SPDXID | NOASSERTION | NONE where "DocumentRef-x:" is an optional reference to an external SPDX document as described in 2.2 where SPDXID is a string as described in 1.3 or 3.2 where NOASSERTION can be used to explicitly indicate it is not clear if there are relationships that may apply or not where NONE can be used to explicitly indicate there are NO other relationships
Value	N/A

6 Terminology

COTS	Commercial-Off-The-Shelf or Commercially available Off-The-Shelf products
FOSS	Free and Open Source Software
NTIA	National Telecommunications and Information Administration
SBOM	Software Bill of Material
SPDX	Software Packet Data Exchange
URL	Universal Resource Locator
VCS	Version Control System

7 References

[1] SPDX Specification v2.2.1

[2] SPDX License List

[3] The Minimum Elements For a Software Bill of Materials (SBOM)

