How to manage OSS license obligations and SBoM by SW360's new features

Presenters:
kouki1.hama@toshiba.co.jp,

CC-BY-SA-4.0
Introduce SW360 and New features

- SW360 in General
- License and Obligation Management
- Management SBOM by SPDX format

Who is Presenting?

- Kouki Hama (濵 功樹)
  Toshiba Corporation, Software Engineering & Technology Center
Overview

SW360 is a 3rd party software component catalogue that assigns 3rd party and own components to products or projects.

- **Goals and Benefits**
  - Reuse information about components
  - Coordinate product documentation process
  - Supports OSS license clearing
All 3rd party and own components come with one or more licenses

- License Information per Component
- For each component license information is captured
- As such, license information per product is available
OpenChain Specification

- OpenChain ISO/IEC 5230 is the International Standard for open source license compliance.
- OpenChain Spec refers to license obligations

3.1.5 License obligations
A process shall exist for reviewing the identified licenses to determine the obligations, restrictions and rights granted by each license.
Manage OSS license and obligations

OSS License

• All OSS have licenses
• SPDX websites provides summary of OSS license info
  • https://spdx.org/licenses/

OSS License Obligations

• Different licenses have different obligations
• Some obligations should be managed by your companies or departments
• OSDAL (Open Source Automation Development Lab) Provides License obligation info
  • https://www.osadl.org/Access-to-raw-data.oss-compliance-raw-data-access.0.html
Import and Add license Obligations

Import OSS license and Obligation info

- SW360 can import Licenses Data from SPDX through GUI
- SW360 can import Obligations Data from OSDAL through GUI

Add new obligation like OSDAL-like format

- Add new license obligations by yourself
- SW360 Supports to add license obligation by "input assistant function" or "elements of obligation"
Licenses and Resulting Obligations
BSD-3-Clause Simple License Example

Copyright <YEAR> <COPYRIGHT HOLDER>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE...

• USE CASE Source code delivery
  ○ YOU MUST Forward Copyright notices
  ○ YOU MUST Forward License text
  ○ YOU MUST Forward Warranty disclaimer
  ○ YOU MUST NOT Promote

• USE CASE Binary delivery
  ○ YOU MUST Provide Copyright notices In Documentation OR Distribution material
  ○ YOU MUST Provide License text In Documentation OR Distribution material
  ○ YOU MUST Provide Warranty disclaimer In Documentation OR Distribution material
  ○ YOU MUST NOT Promote
Import License Obligation from OSDAL

1. Import Licenses from SPDX
2. Import Licenses Obligations from OSDAL
License information in SW360

Example: BSD-3-Clause License text

This license text from SPDX

BSD 3-CLAUSE “NEW” OR “REVISED” LICENSE (BSD-3-CLAUSE)

License Text

Copyright (c) . All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
**Importing results of License Obligations**

---

### License Obligation from OSDAL

<table>
<thead>
<tr>
<th>USE CASE Source code delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>YOU MUST Forward Copyright notices</td>
</tr>
<tr>
<td>YOU MUST Forward License text</td>
</tr>
<tr>
<td>YOU MUST Forward Warranty disclaimer In Documentation OR Distribution material</td>
</tr>
<tr>
<td>YOU MUST NOT Promote</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>USE CASE Binary delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>YOU MUST Provide Copyright notices In Documentation OR Distribution material</td>
</tr>
<tr>
<td>YOU MUST Provide License text In Documentation OR Distribution material</td>
</tr>
<tr>
<td>YOU MUST Provide Warranty disclaimer In Documentation OR Distribution material</td>
</tr>
<tr>
<td>YOU MUST NOT Promote</td>
</tr>
</tbody>
</table>

---

License Obligation from OSDAL
OSDAL licenses obligation

Example: BSD-3-Clause

USE CASE Source code delivery
YOU MUST Forward Copyright notices
YOU MUST Forward License text
YOU MUST Forward Warranty disclaimer
YOU MUST NOT Promote

USE CASE Binary delivery
YOU MUST Provide Copyright notices In Documentation OR Distribution material
YOU MUST Provide License text In Documentation OR Distribution material
YOU MUST Provide Warranty disclaimer In Documentation OR Distribution material
YOU MUST NOT Promote

Obligations depends on USE CASES

List of obligation items

And more. Such as
• Patent hints
• COMPATIBILITY
• COPYLEFT CLAUSE

https://www.osadl.org/fileadmin/checklists/unreflicenses/BSD-3-Clause.txt
Add New License Obligation Like OSDAL format

And new obligations
- Assist to keep Structure by Preview
- Selects prediction candidates
Select Obligation Element

Being able to Select License Obligation Element
Manage Software Bill of Materials

Software Bill of Materials

- OpenChain Spec refers to the (Software) Bill of Materials

3.3.1 Bill of materials
A process shall exist for creating and managing a bill of materials that includes each open source component (and its identified licenses) from which the supplied software is comprised.

- Executive Order 14028

<table>
<thead>
<tr>
<th>Data Fields</th>
<th>Minimum Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation Support</td>
<td>Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.</td>
</tr>
<tr>
<td>Practices and Processes</td>
<td>Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.</td>
</tr>
</tbody>
</table>
Manage Software Bill of Materials

**SBoM Format**

- **Software Package Data exchange (SPDX)**
- CycloneDX
- Software Identification (SWID) tags

**SPDX**

- Software Package Data exchange
  - [https://spdx.dev/](https://spdx.dev/)
SPDX in SW360

SPDX Clause

Clause 1: Scope
Clause 2: Normative references
Clause 3: Terms and definitions
Clause 4: Conformance
Clause 5: Composition of an SPDX document
Clause 6: Document Creation Information
Clause 7: Package Information
Clause 8: File Information
Clause 9: Snippet Information
Clause 10: Other Licensing Information Detected
Clause 11: Relationship between SPDX Elements Information
Clause 12: Annotation Information
Clause 13: Review Information (deprecated)

Now SW360 Supports Clause 6, 7, 9, 10, 11, 12

Plan to Support Clause 8: file information
SPDX for Open Interconnectivity

Goals and Benefits

- Tool integration: exchange clearing information
- Open to partners
- Maximize reuse of available clearing information
The SPDX Lite profile defines a subset of the SPDX specification, from the point of view of use cases in some industries. SPDX Lite aims at the balance between the SPDX standard and actual workflows in some industries.

SPDX Lite has affinity with SPDX tools due to its containing the mandatory part of the Document Creation and Package Information in the SPDX Lite definition.

An SPDX Lite document can be used in parallel with SPDX documents in software supply chains.

https://spdx.github.io/spdx-spec/SPDX-Lite/
Edit SPDX in SW360

https://github.com/toshiba/sw360/commits/dev/feature-spdx_information_management
### Edit SPDX in SW360

#### Package Information

<table>
<thead>
<tr>
<th>Select Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add new Package</td>
</tr>
</tbody>
</table>

#### 7. Package name *
- **Enter package name**

#### 7.2 Package SPDX Identifier *
- **SPDXRef**
- **Enter package SPDX identifier**

#### 7.3 Package version
- **Enter package version**

#### 7.4 Package file name
- **Enter package file name**

#### 7.7 Package download location *
- **Enter package download location**
- **NONE**
- **NOASSERTION**

#### 7.8 Files analyzed
- **TRUE**
- **FALSE**

#### 7.11 Package home page
- **Enter package home page**
- **NONE**
- **NOASSERTION**

#### 7.13 Concluded license *
- **Enter concluded license**
- **NONE**
- **NOASSERTION**

#### 7.15 Declared license *
- **Enter declared license**
- **NONE**
- **NOASSERTION**

#### 7.16 Comments on license
- **Enter comments on license**
Export SPDX

Select format

Download SPDX file

SPDX Tag
RDF/XML
JSON
XLS
Import SPDX
Summary

• SW360 is Software BoM management tool

• Managing Software BoM management is important for OSS compliance and OpenChain Specification

• New SW360 supports License obligations and SPDX format
Thank you!

Useful Links

• CC-BY-SA 4.0
  https://creativecommons.org/licenses/by-sa/4.0/

• Internet
  https://www.eclipse.org/sw360

• GitHub
  https://www.github.com/eclipse/sw360
  https://www.github.com/sw360

• Further Links
  https://www.spdx.org