SBOM FORMATS & STANDARDS GROUP - REPORT OUT

CO-CHAIRS:
JC HERZ & KATE STEWART
Lifecycle of an SBOM

Information that goes into SBOMs can be best obtained from the tools and processes used in each stage of the software lifecycle:

1. Produce
2. Deliver
3. Update
4. Consume
Key Format: SPDX

The Software Package Data Exchange (SPDX®) specification provides a standard language for communicating licensing and components information (metadata) for software packages and related content with the aim of facilitating license and other policy compliance between companies and organizations.
Key Format: SWID

The Software Identification (SWID) Tags were designed to provide a transparent way for organizations to track the software installed on their managed devices. It was defined by ISO in 2012 and updated as ISO/IEC 19770-2:2015 in 2015. SWID Tag files contain descriptive information about a specific release of a software product.
# Translation & Harmonization Guidance for Mapping to Framing Baseline

<table>
<thead>
<tr>
<th>Baseline</th>
<th>SPDX</th>
<th>SWID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier Name</td>
<td>(3.5) PackageSupplier: &lt;Entity&gt; @role (softwareCreator/publisher), @name</td>
<td></td>
</tr>
<tr>
<td>Component Name</td>
<td>(3.1) ComponentName: &lt;softwareIdentity&gt; @name</td>
<td></td>
</tr>
<tr>
<td>Unique Identifier</td>
<td>(3.2) SPDXID: &lt;softwareIdentity&gt; @tagID</td>
<td></td>
</tr>
<tr>
<td>Version String</td>
<td>(3.5) PackageVersion: &lt;softwareIdentity&gt; @version</td>
<td></td>
</tr>
<tr>
<td>Component Hash</td>
<td>(3.10) PackageChecksum: &lt;Payload&gt;../&lt;File&gt; @[hash-algorithm]:hash</td>
<td></td>
</tr>
<tr>
<td>Relationship</td>
<td>(7.1) Relationship: CONTAINS</td>
<td>&lt;Link&gt; @rel, @href</td>
</tr>
<tr>
<td>Author Name</td>
<td>(2.5) Creator: &lt;Entity&gt; @role (tagCreator), @name</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Mapping baseline component information to existing formats
Related Formats Surveyed

- CoSWID Tag
- CPE
- Cyclone DX
- Grafeas
- in-toto
- Package-URL (purl)
- SEVA
- Software Heritage Index
- Sparts
- SPDX-Lite
Next Steps

Tooling Support and Quick Start Guides

Working with Key Format definition groups to improve handling of:

- Software Identifier Challenges
- Delivery and Distribution
- Component Modification
- Formats for Higher Trust and Provenance