Assembling a Group of Products

Software producers, such as product manufacturers and integrators, often need to assemble and test a set of products together before delivering to their customers. This set of products may contain components that undergo version changes over time and need to be tracked. This document[1] is a guide for creating the build SBOM for these kinds of assembled products.

Reference examples include: Embedded and Internet of Things (IoT) products, personal computers, servers, software releases with integrated components, etc.

Historically, the software engineering term that is used for describing these groups of products is a **software product line**.[2] For convenience in this document, the term "product line build SBOM" or "PLB-SBOM" will be used to refer to a collection of products. These terms can be tied to a specific version of hardware as well as being referenced standalone.

To describe a product line with a build SBOM, the following information is REQUIRED:

1. Determine an identifier to use;
2. Determine a versioning system to use with that identifier;
3. List all the product’s components that are being distributed together as a group;
4. Provide a version number for each component;
5. Provide a reference to the build SBOM that generated each component image included in the product group as part of the PLB-SBOM.

Additionally, the following information is RECOMMENDED:

1. Provide a hash of the artifact associated with each component as a cross check for drift. Examples could include tarball, zipfile, container image, install package, disc image, source file, etc., and may be machine specific - x86, arm, etc. It is recommended that the same type of hash be applied, but is not required;
2. Provide available identifiers (PURL, CPE, SWID tags) for the product component when appropriate;
3. The author of the PLB-SBOM data should be the entity that releases the product line.

The PLB-SBOM should be maintained, as updates to the product components are applied.

[1] This document was drafted by the SBOM Tooling & Implementation Working Group, a community-driven workstream. For more information see About this document.

[2] Wikipedia. Software product line. November 7, 2021. https://en.wikipedia.org/wiki/Software_product_line.

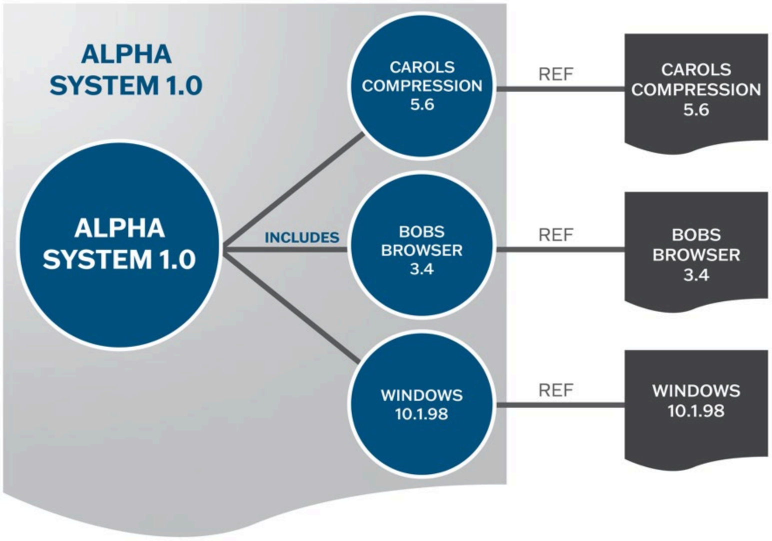

Figure 1: Sample graphical representation of a PLB-SBOM for “Alpha System 1.0”

Author of SBOM Data: Alpha System Manufacturer LLC.
Timestamp: 2023-10-11T11:04:51Z

Component Name: Alpha System
Version of the Component: 1.0
Supplier Name: Alpha System Manufacturer LLC.
Dependency Relationship: Bobs Browser 2.3
Dependency Relationship: Carols Compression 5.6
Dependency Relationship: Microsoft Windows 10.1
Hash: SHA256: c8b4ddea515dcd46933e981f74650286a6fa4873984cd9801972ec4f8612bdd0

Component Name: Bobs Browser
Version of the Component:2.3
Supplier Name: Bob Co, LTD
Hash: SHA256: 10faa5bad459d81ac9b6c33bcf41388ea86587fe5feee9b8d5dee4e10bc47e82
External/BOM Reference: pointer to build of Bobs Browser 2.3 that generated the image

Component Name: Carols Compression
Version: 5.6
Supplier: Compressions’r’us LTD.
Hash: SHA256: 535ad7562fd10ae4d2242d30b9af5a1bd1af1109bd625490dde39679c48356e8
External/BOM Reference: pointer to build of Carols Compression 5.6 that generated the image

Component Name: Windows
Version: 10.1
Supplier: Microsoft
Hash: SHA256: d862a9cac3bf7a619f997ecb23f610671b1b8b96192068955faf263d65dda5bb
External/BOM Reference: pointer to build SBOM of Windows 10.1 that generated the image