Ke, Jessica - Intern

From: Henk Birkholz <henk.birkholz@sit.fraunhofer.de>
Sent: Wednesday, June 16, 2021 5:00 PM
To: SBOM_RFC
Cc: Thomas Fossati; Ned Smith; Carsten Bormann; Henk Birkholz
Subject: Joint SBOM comments in response to document NTIA-2021-0001

This memo describes a set of requirements that we think is an essential and vital initial set of requirements for a minimal SBOM. We hope this response to the request for public comment from June 2nd, 2021 regarding Docket No. 210527-0117 "Software Bill of Materials Elements and Considerations" (document id NTIA-2021-0001) is of help to the current NTIA's task as outlined in the Executive Order on Improving the Nation's Cybersecurity. It would be great, if this input can initiate a continuous dialog on how to frame the set of (initial) minimal SBOM requirements. In support of our shared goal, we happily offer our contributions and are always available for feedback, questions and an exchange of thoughts.

Sincerely yours,

Henk Birkholz (Fraunhofer SIT)
Thomas Fossati (ARM)
Ned Smith (Intel)
Carsten Bormann (University Bremen TZI)

(1) An SBOM MUST contain an unique identifier to identify the exact SBOM so the SBOM can be referenced by other entities. The unique identifier MUST be intended to be unique in a given scope. An SBOM identifier SHOULD be a globally unique identifier. An identifier scope MUST be defined and included in the SBOM. A scope SHOULD be defined via a namespace mechanism that allows qualified identifiers (connotation of meaning to the identifier). A scope SHOULD be attributed to an authoritative entity that is responsible for assigning identifiers that are not reused and can be globally unique. The SBOM identifier MAY be expressed as an URI or a CRI.

(2) An SBOM MUST be associated with a product or description of a product to be considered valid. A product can be a device, a hardware component, a service, or an identifiable set of software packages. The reference to a product MUST either be a unique product instance identifier or a product class identifier. An SBOM MUST always be able to include a reference to the product it describes. If an SBOM does not explicitly reference to a product, it is expected that the product references its corresponding SBOM unambiguously and reliably. The reference MAY be expressed as an URI or a CRI. A unique product instance identifier SHOULD be bound to the product it describes. A unique product instance identifier can be a serial-number, software heritage identifier (SWHID), SWID/CoSWID tag, or distributed identity (DID). A unique product class identifier MUST reliably identify a set of identical products and SHOULD be a composite value that can be composed of name, type, model or version.

(3) Products can be compositions of products. For example, a product that is a service can be composed of-sub services. A software product can be composed of software components, such as software packages, libraries, or sub-modules. Hardware products can be composed of devices, hardware components, or sub-components. An SBOM MUST be able to express a product's composition and MUST align with the corresponding structure of software components that may include products from different suppliers.

(4) The authenticity and veracity of an SBOM MUST be verifiable.
Authenticity is achieved via cryptographic proof of an SBOM's issuer identity, signatures, and included hashes. The identity of the entity that is responsible for vouching for the authenticity of an SBOM and that associates the SBOM

unambiguously with a product description MUST be verifiable. One way to conduct that verification of the vouching entity (authenticating the SBOM issuer) is to check a certification path that is associated with a trust anchor (e.g., a certification authority associated with the vouching entity).