Software Component Transparency

Washington DC | April 11, 2019

Healthcare Proof of Concept

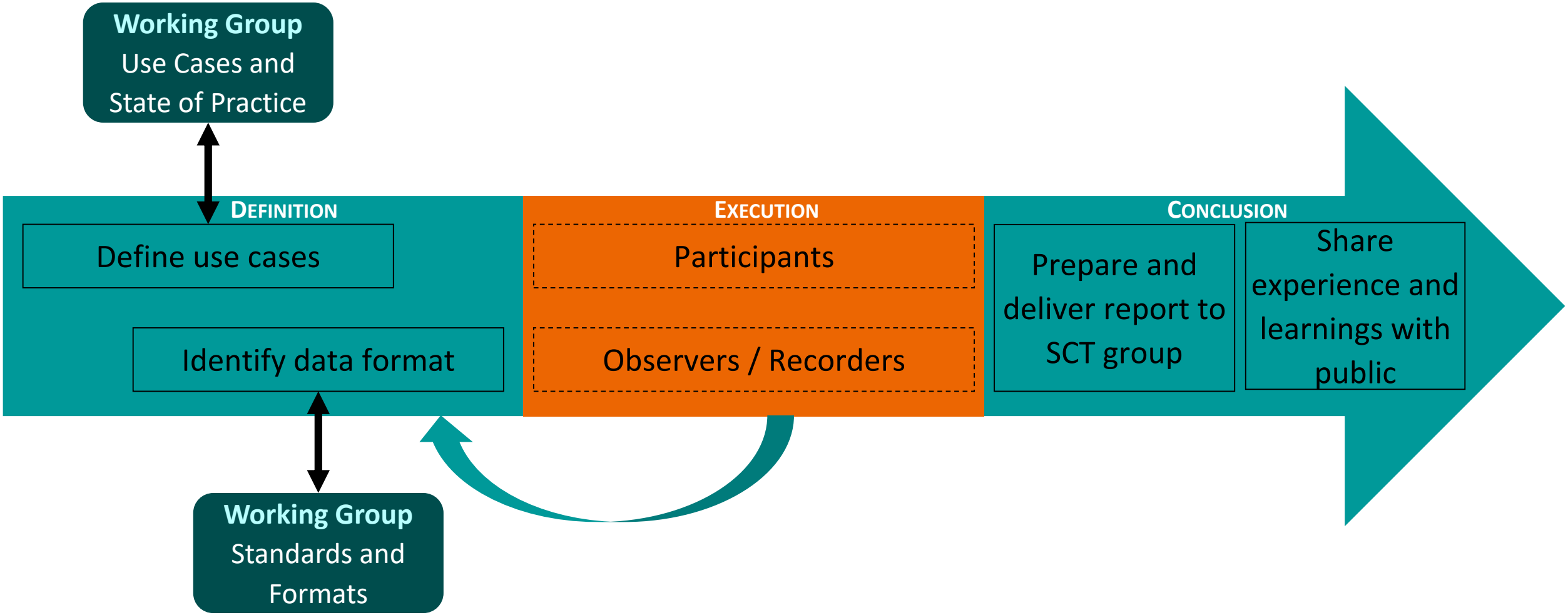
Updated 2019-04 - 09

Objective

This is a collaborative effort between healthcare delivery organizations (HDOs) and medical device manufacturers (MDMs) to employ a provisional SBOM format and exercise use cases for SBOM production and consumption.

The goal is to demonstrate successful use of SBOMs and relate to the overall cross-sector effort to establish standardized formats and processes.

Overview


Working Group
Use Cases and
State of Practice
DEFINITION
Define use cases
Identify data format
EXECUTION
Participants
Observers / Recorders
CONCLUSION
Prepare and deliver report to SCT group
Share experience and learnings with public
Working Group
Standards and
Formats

Currently Defined Details

Use Cases

- Procurement
- Asset Management
  - Risk Management
  - Vendor Management
  - Vulnerability Management

This is a very high level description. These use cases have been elaborated by a sub-group defining/detailing use cases and personas.

Participants

- Healthcare Delivery Organizations
  - New York Presbyterian
  - Cedars-Sinai
  - Christiana Health
  - Mayo
  - Mass General
- Medical Device Manufacturers
  - Abbott
  - Bayer
  - Philips
  - Siemens

Scope

Item	In	Out	Comment
CBOM vs. SBOM (inclusion of hardware components)		X	Minimum viable product, version 1, no clear line, let it be defined further outside the POC. Don't lose track of the issue. Parking lot.
Identifying a standard as the only acceptable format (canonization)		X	No endorsement
Conforming to a standard (as opposed to defining a bespoke format)	X		SWID and SPDX will both be used, but still not an endorsement
Inclusion of vulnerability information (front-end correlation)		X	Gets stale, initiates long conversation, may need its own working group, could interfere with the execution of the POC, let's get the 1.0 version right and continue the conversation
Dependencies – level 1	X		Best effort/optional*, may not contribute to POC
Dependencies – level n	X		Best effort/optional*, may not contribute to POC, can explode complexity
Globally unique & immutable component identifiers (one and only one)		X	Not in version 1.0, hard problem
Vendor name	X		
Version down to build number (as far as provided)	X		
Context ("yeah it's in here, but don't worry about it because…")	~~X~~	X	May not avoid further questions, worth a try to determine benefit Originally in scope, changed because of complexity
Delivery over the Internet (pull)	X		Subscribe to information, manufacturers will not have the option to do so from their suppliers, at least for the POC
API for data access	X		Could be a reference architecture/model for adoption
Machine readable format	X		

*Although not required for exercising the proof of concept, the final report should emphasize the importance of dependencies in the successful use of SBOMs.

Recent Activity

- NDA has been reviewed by HDO and MDM representatives and has been routed to their respective legal counsels, where required. Potential outstanding concerns will be discussed onsite.
- The initial draft of the Observation Collection form has been prepared; additional questions from the MDMs are being considered for inclusion in the final document.
- MDMs are developing an SBOM draft, with a completion date at the end of April. HDO studies will follow shortly thereafter, with an expected completion at the end of May.
- Finalize data format selection and develop product list for which SBOMS will be available.

Potential Concerns

- The POC may be well advanced before consensus is reached and work finalized by the other directly related working groups, especially “Standards and Formats.” The intent of the POC is not to choose winners, but to find a workable path to confirming the utility of medical device SBOMs to HDOs. Still, whatever format chosen could lend weight to that format.

- Participants may expect some degree of confidentiality concerning details of the exercise which would need to be respected amongst members of the working group and resolved prior to creating a public report.

- ~~The working group must establish a clearer definition of the roles of participants, as well as defining roles for those responsible for documenting the exercise and drafting the final report.~~
  (This was a concern in November, but this work has largely been accomplished).

- POC should be seen as just an exercise and not interfere with ongoing business relationships (e.g., no interaction with actual procurement or service activities).

Open Items

- How Software Of Unknown Provenance (SOUP) can/should be handled?
- Investigate better ways to avoid inconsistences in software component IDs in SBOM document.