1200 G Street, NW
Suite 500
Washington, DC 20005

P: +1 202-628-6380
W: www.atis.org

Guidelines for software integrity chains and provenance

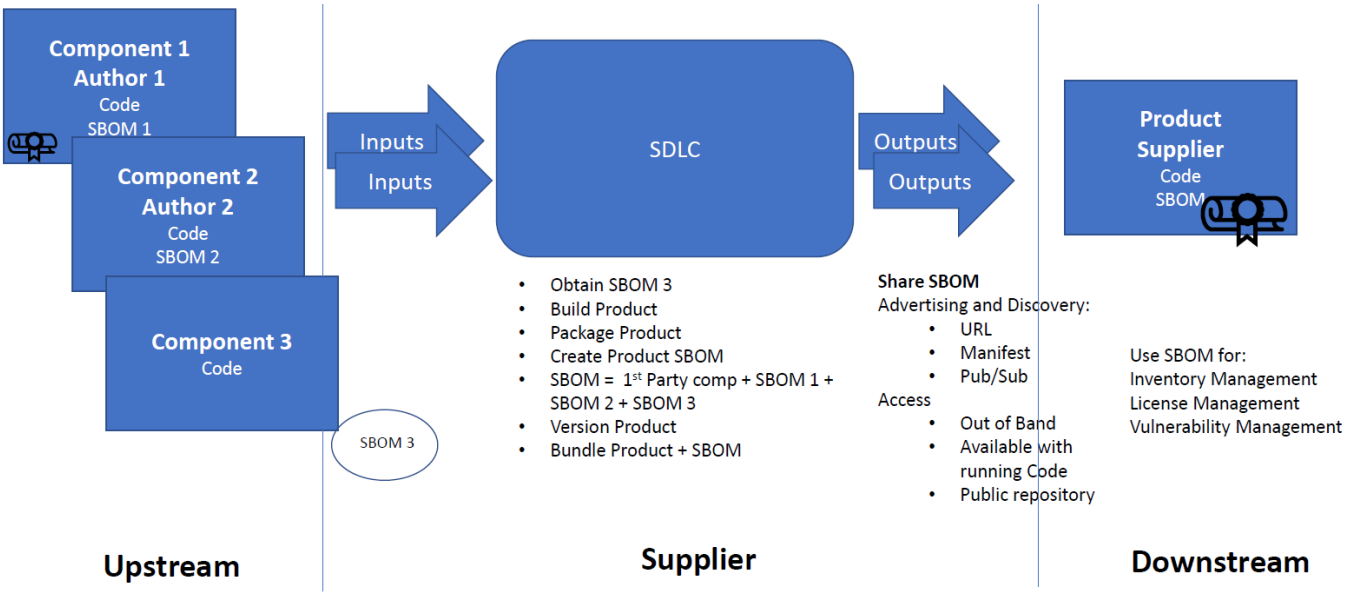
The ATIS 5G Supply Chain Working Group has undertaken development of a common a set of 5G supply chain requirements that encompasses integrated semiconductors, hardware and both proprietary and open source software.

5G networks are increasingly software driven due to virtualization and include significant proprietary as well as open source components. Since communication networks are critical infrastructure, dealing with vulnerabilities in a timely and effective way is essential. A Software Bill of Materials (SBOM) can help to uniquely identify software components and enable remediation to mitigate risks. However, identity of suppliers/authors as well as the actual components is a challenge. Going forward, we are working to define a framework and a set of requirements focused on the 5G ecosystem.

Vulnerabilities create threats that contribute to risk. Assurance is the process in which we quantify and manage contextual risks based on threat vectors exposed by vulnerabilities in process and data across the supply chain ecosystem.

One key element in assuring a secure software supply chain is to identify software components used within any system and track known vulnerabilities against the identified software to ensure that risk is managed and to enable both reactive and proactive actions.

SBOM provides a framework to implement vulnerability tracking. The primary purpose of an SBOM is to uniquely and unambiguously identify software components and their relationships to one another.



Typically, a software supplier executes a Software Development Life Cycle (SDLC) process which takes various software components as inputs and builds / packages an output software product which is then distributed to downstream systems. Each component used or created in this process involves the management of an associated SBOM.

Many organizations including NTIA (https://www.ntia.gov/SBOM) have done significant work in defining a common SBOM structure and process by offering a baseline of how software components are to be represented and created.

To be effective in vulnerability tracking, a software supplier should provide a complete list of all software in use (via an SBOM) including both proprietary and open source components.
The SBOM should include meta data such as supplier name, component name, unique identifier, version string, component hash, relationship and author name. The supplied SBOM file should be digitally signed by the supplier to ensure both the authenticity and integrity of the file. In addition, the supplier should provide an updated SBOM as part of every code release, each patch and/or update.

Unfortunately, one global authoritative source for naming and identifying software does not exist. This lack of clarity in component identity can make it difficult to map components to vulnerabilities.

Most open source components are managed in complex ecosystems that have authoritative systems for identification (e.g. package managers such as npm). However, this is not universally true. When authoritative upstream SBOMs are not available, suppliers must create “best effort” SBOMs on behalf of the original software author or obtain upstream components from alternative sources.

Ultimately, suppliers create SBOMs for their first party components, obtain SBOMs for the upstream components used in their product and provide assembled SBOM for their downstream users.

SBOMs can be obtained in a variety of ways. For supplier originated software, contractual terms can be used to ensure that SBOMs are properly delivered and managed with the associated software. In addition, Software Composition Analysis (SCA) tools can be used to determine all underlying components of a software system and identify at least the public known (open source) components. Where needed, SCA tools can also be used to generate an SBOM for custom developed code.

With an accurate and complete SBOM based inventory of software for a system, vulnerability management tools can then be used to map vulnerabilities to specific software components to assess risk and manage remediation.

Software composition and SBOM is just one piece of the larger industry challenge to assure the supply chain. The ATIS 5G Supply Chain Working Group is looking across the 5G ecosystem to create a model that identifies threats, controls and mitigations. This work is leveraging industry efforts and applying it to help ensure 5G network assurance.