Executive Order – NIST workshop position paper #5

(Guidelines for software integrity chains and provenance)

Microsoft Corporation

Focus Area

Guidelines for software integrity chains and provenance. See EO Sections 4(e)(ii, vi, and viii).

Microsoft Response and Recommendations

Microsoft has made significant investments in initiatives around supply chain security. We have reviewed and participated in open initiatives, including formats for Software Bill of Materials (SBOM); frameworks for supply chain integrity; data stores for supply chain evidence; and more. Based on these experiences, we propose addressing guidelines and practice areas outlined in Section 4(e) (ii, vi, and vii) by adopting existing open initiatives and evolving over time to a consistent, end-to-end model, referred to below as the **Supply Chain Integrity Model (SCIM)**. The below description of SCIM captures not only existing capabilities but also advancements that require further investment. SCIM would thus align with an iterative approach to developing and implementing supply chain integrity requirements, allowing for enhancements over time based on evolving threat models and practices. A phased roll out of requirements would also promote clarity for supplier planning and engineering and minimize disruptions to agencies.

SCIM supports the ongoing verification of artifacts, including hardware and software components, where the authenticity of entities, evidence, policy, and artifacts can be assured and the actions of entities can be guaranteed to be authorized, non-repudiable, immutable, and auditable. The proposed SCIM will be an industry standard specification, easing the path for uniform data flow across globally distributed supply chains.

SCIM Workflow and Example Application

The following diagram depicts the flow of artifacts between entities in the Supply Chain Integrity Model.

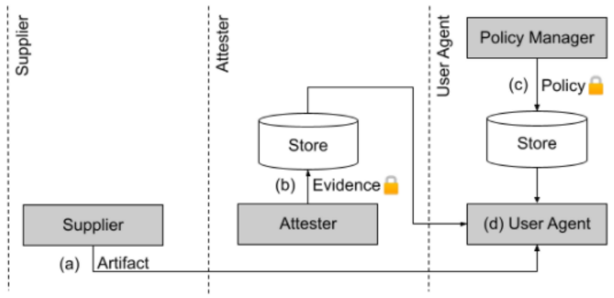

Figure 1 - Supply Chain Integrity Model - Overview

A Supplier creates an Artifact (a). An Attester creates Evidence (b) and submits to a Store for logging, query, and retrieval. The Supplier and Attester may be the same entity. A Policy Manager creates Policy (c) and submits to a Store where it is recorded and made available for query and retrieval. A User Agent receives an Artifact, retrieves Evidence and Policy, and verifies the Artifact (d).

The diagram below shows an example application of SCIM to the Software Development Lifecycle (SDLC).

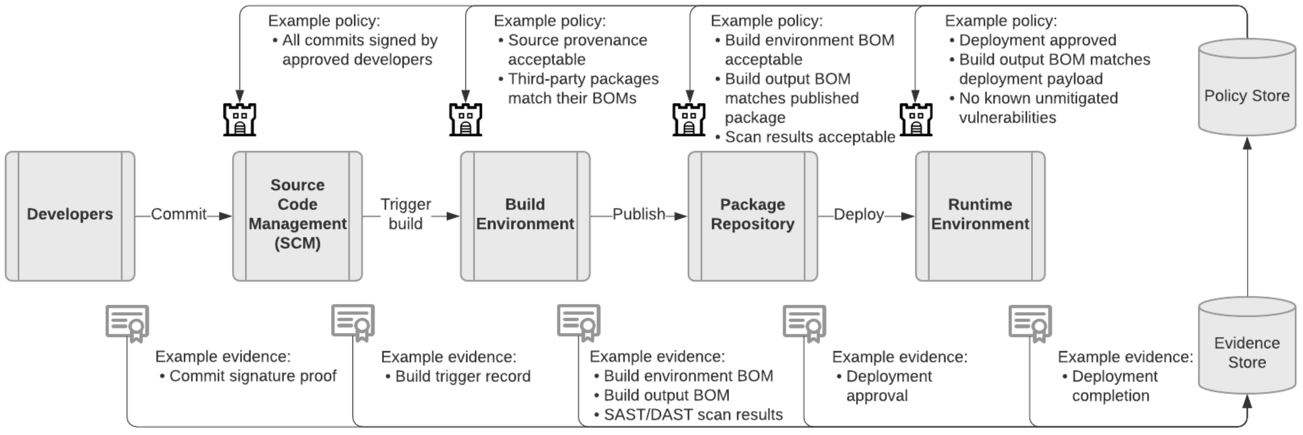

Figure 2 - Example SCIM Application to the Software Development Lifecycle (SDLC)

SCIM Specifications

The table below maps proposed SCIM specifications to existing industry specifications.

SCIM	Existing
The **SCIM-Evidence** specification defines an extensible data model and exchange format for providing all types of evidence (bills of materials, build information, configuration settings, security assurances, certifications, vulnerabilities, end of life information) for all types of artifacts (hardware, software, services, machine learning models, etc.).	SWID, SPDX, CycloneDX, in-toto, RATS, and others
The **SCIM-Policy** specification defines a data model and exchange format for providing policy for use in evaluating artifacts for a specified use.	in-toto, RATS, and others
The **SCIM-Store** specification defines a rich, graph-aware storage API that allows publishing and subscribing to Evidence and Policy.	DBOM, Grafeas, RATS, and others

Requirements Satisfied

The following table maps Section 4(e) requirements to the Supply Chain Integrity Model.

Executive Order Section 4 Practice	SCIM Mapping
4(e) (ii): generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the processes set forth in subsection (e)(i)	SCIM describes a general model for generating, discovering, and transmitting Evidence that demonstrates conformance to specified Policies.
4(e) (vi): maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis	The SCIM Store supports the ongoing, transparent, immutable, and non-repudiable logging of evidence, the audit of evidence using graph-aware query, and the enforcement of controls using Evidence and Policy.
4(e) (vii): providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website	SBOM is a class of Evidence which can be transmitted directly with a product or accessed from a SCIM Store.

Roadmap

Phase 1

- Organizations use existing tools and specifications to begin implementing Section 4 requirements, including SBOMs.
- SCIM community organized for the development of end-to-end standards.

Phase 2

- Organizations begin adopting SCIM specifications, which encompass and extend existing initiatives.
- SCIM specifications proposed to international standards bodies.

Phase 3

- SCIM specifications ratified by international standards bodies.
- Widespread adoption of end-to-end model across globally distributed supply chains.

Note: This paper describes principles and a proposed model and system for conveying evidence. It does not address what evidence or information for attestation of conformity must be conveyed - as referenced in the context of other parts of EO Section 4.

Conclusion

Organizations should begin using existing specifications and standards today while at the same time participating in the development and adoption of future SCIM standards. SCIM encompasses and extends existing initiatives to create an end-to-end, globally distributed system with strong guarantees of integrity.