Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie TR-03183: Cyber-Resilienz-Anforderungen an Hersteller und Produkte

Teil 2: Software Bill of Materials (SBOM)

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	2023-07-12	Fassung der TR-03183-2 zur Erstveröffentlichung

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: TR03183@bsi.bund.de
Internet: https://bsi.bund.de/dok/TR-03183

Inhalt

1 Einleitung

Diese Technische Richtlinie beschreibt die Anforderungen an eine „Software Bill of Materials (SBOM)“. Eine SBOM ist ein maschinenverarbeitbares Dokument und entspricht einer elektronischen Stück- / Teileliste. Sie inventarisiert eine Codebasis und enthält somit Informationen zu allen verwendeten Komponenten einer Software. Diese Informationen können in unterschiedlicher Breite und Tiefe dargestellt sein und reichen von einer groben Struktur bis zu einer feingranularen Aufschlüsselung von Produkten und Software-Komponenten. Zur Darstellung und Übertragung einer SBOM existieren unterschiedliche Formate.

Eine SBOM sollte bei jedem Software-Ersteller und -Anbieter vorhanden sein, um Software-Komplexität transparent darstellen zu können und um zu wissen, welche Bestandteile (z. B. Bibliotheken) eingesetzt werden, da fast immer eine Vielzahl unterschiedlicher Quellen und Komponenten genutzt wird. Dieses Wissen ist für Software-Managementprozesse, insbesondere für einen kontinuierlichen IT-Sicherheitsprozess und das Lebenszyklus-Management von Software unabdingbar und gilt daher als „Best Practice“ einer sicheren Software-Lieferkette. Eine SBOM kann öffentlich oder nicht öffentlich sein und auf unterschiedlichen Verteilungswegen verbreitet werden. In der Regel verwendet ein Ersteller einer Software ein oder mehrere Komponenten Dritter. Er erzeugt und verwaltet die SBOMs der eigenen Software; ebenso nimmt er die Konsumentenrolle der SBOMs der eingebundenen Komponenten ein. Die Fülle an SBOM-Informationen und die möglichen Unterschiede in der Struktur von SBOMs bedeuten einen hohen Aufwand für jeden Ersteller, dem nur mit Automatisierung effektiv zu begegnen ist.

Mit Hilfe von SBOM-Informationen kann geprüft werden, ob ein Produkt potenziell von einer Schwachstelle betroffen ist, indem dessen Komponentenliste mit den in den Schwachstelleninformationen aufgeführten Software-Komponenten abgeglichen wird. Eine SBOM enthält jedoch keine Aussage zu Schwachstellen oder deren Ausnutzbarkeit. Ob und in welchem Maße durch eine Schwachstelle einer verwendeten Software-Komponente ein Risiko für das Produkt besteht, welches die SBOM beschreibt, geht aus ihr ebenfalls nicht hervor. Hierzu sind weitere Informationen über die konkrete Schwachstelle erforderlich, wie beispielsweise mittels Security Advisories oder VEX[1] (Vulnerability Exploitability Exchange).

Um eine Betroffenheit oder Nicht-Betroffenheit durch eine Schwachstelle für ein Produkt zu bestätigen, bedarf es einerseits eines Abgleichs der SBOM des Produktes mit Schwachstelleninformationen, wie beispielsweise den CVE (Common Vulnerabilites and Exposures) oder Security Advisories der Komponentenersteller oder -anbieter. Andererseits ist eine Analyse der Software selbst notwendig, um festzustellen, wie deren potentiell betroffene Subkomponenten verwendet werden, und damit, ob und wie die eigene Software betroffen ist. Diese ist im Rahmen des Schwachstellenmanagements für das Produkt durchzuführen. Das Ergebnis dieser Analyse wird den Nutzern der Software dann als Security Advisory oder VEX für das Produkt bereitgestellt.

Die Erstellung einer SBOM ist im aktuellen Entwurf des Cyber Resilience Act (CRA) verpflichtend[2]. Beim CRA handelt es sich um eine Marktzugangsregulierung der EU für Produkte mit digitalen Elementen, die deren Anbieter verpflichtet, ein Schwachstellenmanagement zu betreiben und Informationen zu ihren Produkten in transparenter und verständlicher Form zu kommunizieren. Im US-amerikanischen Raum wird die SBOM durch die US Executive Order 14028 vom Mai 2021[3] bereits für Anwendungen im behördlichen Umfeld gefordert und seitens der FDA (Food and Drug Administration) muss für Medizinprodukte bereits seit März 2023 eine SBOM bei der Zulassung zwingend vorgelegt werden[4].

[1] https://ntia.gov/files/ntia/publications/vex_one-page_summary.pdf
[2] https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2022)454&lang=de
[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ Abschnitt 4
[4] https://www.congress.gov/117/bills/hr2617/BILLS-117hr2617enr.pdf Abschnitt 3305

2 Formalia

Die in diesem Dokument verwendeten Schlüsselwörter sind auf Basis der folgenden Übersetzungstabelle gemäß RFC 2119 zu interpretieren.

Tabelle 2: Übersetzungstabelle der Schlüsselwörter gemäß RFC 2119

Deutsch	***Englisch***
MUSS / MÜSSEN	MUST / SHALL
DARF NICHT / DÜRFEN NICHT / DARF KEIN(EN) / DÜRFEN KEIN(EN) / KANN NICHT / KÖNNEN NICHT / KANN KEIN(EN) / KÖNNEN KEIN(EN)	MUST NOT / SHALL NOT
VORAUSGESETZT	REQUIRED
SOLLTE / SOLLTEN	SHOULD
SOLLTE NICHT / SOLLTEN NICHT	SHOULD NOT
EMPFOHLEN	RECOMMENDED
KANN / KÖNNEN / DARF / DÜRFEN	MAY
MUSS NICHT / MÜSSEN NICHT	MAY NOT
OPTIONAL	OPTIONAL

3 Grundlagen

3.1 Definition SBOM

Eine „Software Bill of Materials“ (SBOM, dt.: Software-Stückliste / -Teileliste) ist eine maschinenverarbeitbare Datei, die Details und Lieferkettenverhältnisse der in einer Software genutzten Komponenten enthält.

Sie unterstützt die automatisierte Verarbeitung von Informationen zu Software-Komponenten, sowohl der sogenannten „Primärkomponente“ (englisch: Primary Component) als auch der von ihr eingebundenen (Dritt-)Komponenten.

Eine SBOM MUSS gewisse Mindestangaben enthalten (siehe Kapitel 5), KANN aber nahezu beliebig erweitert und detaillierter gestaltet werden.

Für jede Softwareversion MUSS eine neue, eigene SBOM erzeugt werden. Eine neue Version der SBOM zu einer gegebenen Softwareversion MUSS genau dann erzeugt werden, wenn mehr Informationen zu den eingebundenen Software-Komponenten zur Verfügung gestellt werden oder Fehler in den SBOM-Daten korrigiert werden.

Eine SBOM enthält keine Informationen zu Schwachstellen. Obwohl die Formate zur Beschreibung einer SBOM die Möglichkeit bieten, zusätzlich Schwachstelleninformationen aufzunehmen, ist dies nicht sinnvoll.

3.2 Verwendete Begriffe

Eine „Software-Komponente“ im Sinne dieser Technischen Richtlinie MUSS einer einzelnen, ausführbaren Datei[5] entsprechen.

In dieser Technischen Richtlinie wird zwischen „Anbieter“ (englisch: „Vendor“; alternativ, aber im Gegensatz dazu nicht notwendigerweise mit kommerziellem Hintergrund: „Lieferant“, englisch: „Supplier“) und „Ersteller“ (englisch: „Creators“; alternativ „Autoren“, englisch: „Authors“) differenziert, da „Hersteller“ diese beiden Rollen im Sinne von „Anbieter einer selbst-erstellten Software“ zusammenführt.

[5] siehe u. a. https://de.wikipedia.org/wiki/Ausführbare_Datei

4 SBOM-Formate

Eine SBOM MUSS in einem Format vorliegen, das eine der folgenden Spezifikationen in einer der angegebenen Versionen erfüllt.

- CycloneDX[6] in der Version 1.4 oder höher
- Software Package Data eXchange (SPDX)[7] in der Version 2.3 oder höher

[6] https://cyclonedx.org/specification/overview/
[7] https://spdx.dev/specifications/

5 Inhaltliche Anforderungen

5.1 Detaillierungsgrad

Für eine SBOM, die konform zu dieser Technischen Richtlinie ist, MUSS zumindest für jede zum Lieferumfang gehörende Komponente die rekursive Auflösung von Abhängigkeiten auf jedem Pfad mindestens bis einschließlich der ersten Komponente, die nicht mehr zum Lieferumfang gehört, durchgeführt werden (siehe Abschnitt 6.1.4). Diese SBOM MUSS als Teil des Build-Prozesses erstellt werden (Build SBOM, siehe Abschnitt 6.2.3).

5.2 Notwendige Datenfelder

5.2.1 Notwendige Datenfelder zur SBOM selbst

Jede SBOM MUSS mindestens die folgenden Informationen beinhalten:

Tabelle 3: Notwendige Datenfelder zur SBOM selbst

Datenfeld	***Beschreibung***
Ersteller der SBOM	„Uniform Resource Identifier (URI)“, der die E-Mail-Adresse der Entität enthalten MUSS, die diese SBOM erstellt hat
Zeitstempel	Datum und Uhrzeit des Zeitpunkts der SBOM-Daten-Zusammenstellung gemäß der Spezifikation der Formate (siehe Kapitel 4)

5.2.2 Notwendige Datenfelder zu jeder Komponente

Zu jeder Komponente, die in einer SBOM enthalten ist, MÜSSEN mindestens die folgenden Informationen angegeben werden[8]:

Tabelle 4: Notwendige Datenfelder zu jeder Komponente

Datenfeld	***Beschreibung***
Ersteller der Komponente	„Uniform Resource Identifier (URI)“, der die E-Mail-Adresse der Entität enthalten SOLLTE, die die jeweilige Software-Komponente erstellt hat und ggf. aktualisiert
Komponentenname	Bezeichnung, die der Software-Komponente vom ursprünglichen Ersteller zugewiesen wurde
Version der Komponente	Bezeichner, der vom Ersteller genutzt wird, um Änderungen in der Software-Komponente zu einer zuvor erstellten Version zu signalisieren. Es SOLLTEN Bezeichner entsprechend Semantic Versioning[9] verwendet werden, aber vorhandene Bezeichner DÜRFEN NICHT dafür verändert werden.
Abhängigkeiten von anderen Komponenten	Aufzählung aller Komponenten, von denen diese Komponente unmittelbar abhängig ist, entsprechend der Anforderungen im Abschnitt 5.1

[8] vgl. https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf Abschnitte IV und V sowie https://www.ntia.gov/sites/default/files/publications/ntia_sbom_framing_2nd_edition_20211021_0.pdf Abschnitt 2.2 und https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_formats_energy_brief_2021.pdf Seite 5.

[9] https://semver.org

Datenfeld	*Beschreibung*
Lizenz	Effektive Lizenz der Komponente. Wenn diese einem „SPDX-License-Identifier (SPDX-ID)“[10] zuordenbar ist, MUSS dieser verwendet werden. Andernfalls MUSS als Wert „Proprietary“ oder ein zwischen Anbieter und Kunde vereinbarter, der Struktur der SPDX-IDs entsprechender, eindeutiger Lizenzbezeichner verwendet werden, siehe dazu „Annex D: SPDX License Expressions“ der SPDX-Spezifikation[11].
Hashwert der ausführbaren Komponente	Kryptografisch sichere Prüfsumme (Hashwert) der Komponente in ihrer ausführbaren Form (d. h. als die einzelne, ausführbare Datei auf einem Massenspeicher) als SHA-256

5.3 Zusätzliche Datenfelder

5.3.1 Zusätzliche Datenfelder zur SBOM selbst

Jede SBOM MUSS zusätzlich die folgenden Informationen beinhalten, soweit sie existieren und ihre Voraussetzungen vorliegen:

Tabelle 5: Zusätzliche Datenfelder zur SBOM selbst

Datenfeld	*Beschreibung*
SBOM-URI	„Uniform Resource Identifier (URI)“ dieser SBOM

5.3.2 Zusätzliche Datenfelder zu jeder Komponente

Zu jeder Komponente, die in einer SBOM enthalten ist, MÜSSEN zusätzlich die folgenden Informationen angegeben werden, soweit sie existieren und ihre Voraussetzungen vorliegen:

Tabelle 6: Zusätzliche Datenfelder zu jeder Komponente

Datenfeld	*Beschreibung*
Quelltext-URI	„Uniform Resource Identifier (URI)“, des Quelltexts der Komponente, z. B. von einem ein Source Code Repository
URI der ausführbaren Form der Komponente	„Uniform Resource Identifier (URI)“, der direkt auf die ausführbare Form der Komponente zeigt
Hashwert des Quelltexts der Komponente	Kryptografisch sichere Prüfsumme (Hashwert) des Quelltexts[12] der Komponente als SHA-256
Andere eindeutige Bezeichner	Weitere Bezeichner, die genutzt werden können, um die Komponente zu identifizieren oder in einschlägigen Datenbanken nachzuschlagen, wie z. B. Common Platform Enumeration (CPE) oder Package URL (purl)

[10] https://spdx.org/licenses
[11] https://spdx.github.io/spdx-spec/v2.3/SPDX-license-expressions/
[12] Wie der Hashwert des Quelltexts berechnet wird, ist momentan nicht festgelegt.

6 Anhang

Die in diesem Anhang aufgeführten Informationen dienen lediglich zur Orientierung, d. h. sie haben keinen bindenden Charakter.

6.1 Detaillierungsgrad

Eine SBOM kann in unterschiedlicher Tiefe erstellt werden, z. B. entsprechend der folgenden Klassifizierung.

6.1.1 Top-Level-SBOM

Die SBOM beinhaltet neben den Informationen zur Primärkomponente Informationen zu allen Komponenten, die direkt (unmittelbar) durch die Primärkomponente eingebunden sind. Die SBOM wird auch als „SBOM der obersten Ebene“ bezeichnet.

6.1.2 *n*-Level-SBOM

Die SBOM beinhaltet neben den Informationen zur Primärkomponente Informationen zu allen Komponenten, die direkt (unmittelbar) oder transitiv über *n* Ebenen durch die Primärkomponente eingebunden werden. D. h. die rekursive Auflösung der transitiven Abhängigkeiten wird auf *n* Schritte in der Tiefe begrenzt. Der Parameter *n* wird nur dann unterschritten, wenn auf einem Pfad keine weiteren Komponenten mehr eingebunden sind.

6.1.3 Transitive SBOM

Die SBOM beinhaltet neben den Informationen zur Primärkomponente Informationen zumindest zu allen Komponenten, die direkt (unmittelbar) oder transitiv durch die Primärkomponente eingebunden sind. Die rekursive Auflösung der Komponenten und deren Abhängigkeiten wird auf jedem Pfad mindestens bis einschließlich der ersten externen Komponente (d. h. Komponente eines Drittanbieters) durchgeführt. Auch diese Komponente muss vollständig beschrieben werden, wobei die darunterliegenden Teilbäume nicht aufgelöst werden müssen.

6.1.4 Liefergegenstands-SBOM

Die SBOM beinhaltet neben den Informationen zur Primärkomponente Informationen zumindest zu allen zum Lieferumfang gehörenden eingebundenen Komponenten, die direkt (unmittelbar) oder transitiv durch die Primärkomponente eingebunden sind. Dabei wird die rekursive Auflösung von Abhängigkeiten auf jedem Pfad mindestens bis einschließlich der ersten Komponente, die nicht mehr zum Lieferumfang gehört, durchgeführt.

6.1.5 Vollständige SBOM

Die SBOM beinhaltet neben den Informationen zur Primärkomponente Informationen zu allen Komponenten, die direkt (unmittelbar) oder transitiv durch die Primärkomponente eingebunden werden. Die rekursive Auflösung der Komponenten und deren Abhängigkeiten wird vollständig durchgeführt.

6.2 SBOM-Typen

Je nach Art und Weise bzw. Zeitpunkt der Erstellung einer SBOM im Rahmen des Entwicklungs-, Auslieferungs-, Installations- und Ausführungsprozesses einer Softwarekomponente und der dadurch verfügbaren Daten unterscheiden sich die in der SBOM erfassbaren Informationen. Eine übliche Klassifikation ist, zwischen den folgenden SBOM-Typen zu unterscheiden[13].

6.2.1 Design SBOM

Die SBOM wird anhand der geplanten Zusammenstellung enthaltener Komponenten erstellt. Die Komponenten müssen nicht bereits existieren.

6.2.2 Source SBOM

Die SBOM wird aus der Entwicklungsumgebung, dem Quellcode und den enthaltenen Abhängigkeiten erstellt.

6.2.3 Build SBOM

Die SBOM wird als Teil des Build-Prozesses auf Basis von z. B. Quellcode, Abhängigkeitsinformationen, bereits erstellten Komponenten, flüchtigen Build-Prozessdaten und anderen SBOMs erstellt.

Hinweise:

1. Um auch bereits erstellte, ausführbare Komponenten erfassen zu können, steht bei übersetztem Code der Linker-Lauf im Fokus der Erstellung einer Build SBOM, nicht der Compiler-Lauf.
2. Bei interpretiertem Code existiert nur der Quelltext. Der Interpreter ist, soweit sinnvoll möglich, als Abhängigkeit anzugeben.

6.2.4 Analyzed SBOM

Die SBOM wird nach dem Build-Prozess durch Analyse von Artefakten wie ausführbaren Dateien, Paketen, Containern und Abbildern virtueller Maschinen erstellt. Dieser Typ wird auch als „3rd Party SBOM“ bezeichnet.

6.2.5 Deployed SBOM

Die SBOM liefert ein Inventar der Software auf einem System. Das kann eine Zusammenstellung anderer SBOMs sein, die Konfigurationsoptionen und die Untersuchung des Ausführungsverhaltens in einer (ggf. simulierten) Deployment-Umgebung mit einbezieht.

6.2.6 Runtime SBOM

Die SBOM wird mit Hilfe des die Software ausführenden Systems erstellt, um ablaufende (d. h. in Ausführung befindliche) Software-Komponenten sowie deren externe Aufrufe und dynamisch geladenen Komponenten ausschließlich zur Laufzeit (d. h. im Arbeitsspeicher) zu erfassen.

[13] Quelle: https://www.cisa.gov/resources-tools/resources/types-software-bill-materials-sbom

6.3 Weiterführende Informationen

6.3.1 Informationen der NTIA

Die „National Telecommunications and Information Administration (NTIA)“ des „United States Department of Commerce” bietet zahlreiche weiterführende Informationen zum Thema SBOM unter https://ntia.gov/sbom an.

6.3.2 Informationen der CISA

Auch die „Cybersecurity and Infrastructure Security Agency (CISA)“ des „United States Department of Homeland Security” bietet weiterführende Informationen zum Thema SBOM unter https://cisa.gov/sbom an.