Federal Office
for Information Security

Germany's work on SBOM in the context of EU's CRA

SBOM-a-Rama, 29.02.2024

Outline

EU’s Cyber Resilience Act

Technical Guideline on SBOM
by BSI

What is the Cyber Resilience Act (CRA)?

- Market access regulation
  - for all products with digital elements
  - Extends the requirements of the CE Mark from safety to security
- Requirements:
  - Secure by design, secure by default,
  - Vulnerability management,
  - Security updates throughout product‘s lifetime, …
  - SBOM:
    - Has to be maintained and used internally for vulnerability management
    - Does not have to be published
    - Has to be conveyed to the market surveillance authority on their request

Current status of the CRA

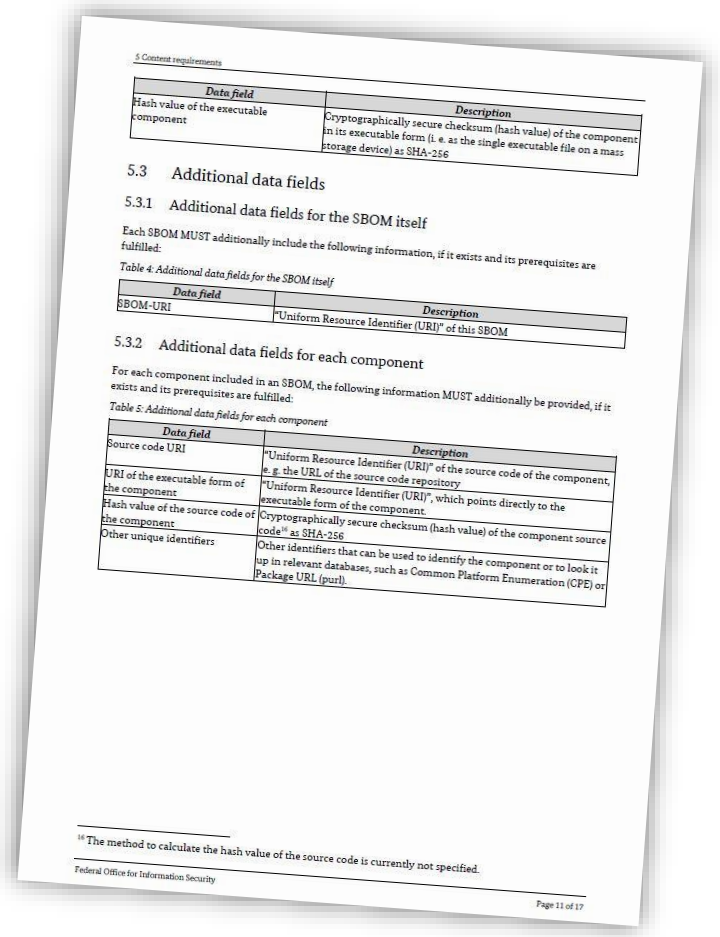
- Negotiations finished, all technical details fixed
- Legal/language polishing still needed
- Expected to be passed by EU Parliament before June 2024 (Elections of EU Parliament)
- Entry into force 36 months after publication

Technical Guideline on SBOM

- BSI published a Technical Guideline on SBOM
- Recommendation for manufacturers and basis for discussion in the EU and internationally
  - Recommended, not obligatory
  - Recognized in industry
- Requirements on content, scope, and format of an SBOM
- https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2.pdf

Technical Guideline on SBOM

- Requirements on content, scope, and format of an SBOM
  - Build SBOM
  - Delivery item SBOM
  - SPDX or CycloneDX



5 Content requirements

Data field	Description
Hash value of the executable component	Cryptographically secure checksum (hash value) of the component in its executable form (i. e. as the single executable file on a mass storage device) as SHA-256

5.3 Additional data fields

5.3.1 Additional data fields for the SBOM itself

Each SBOM MUST additionally include the following information, if it exists and its prerequisites are fulfilled:

Table 4: Additional data fields for the SBOM itself

Data field	Description
SBOM-URI	"Uniform Resource Identifier (URI)" of this SBOM

5.3.2 Additional data fields for each component

For each component included in an SBOM, the following information MUST additionally be provided, if it exists and its prerequisites are fulfilled:

Table 5: Additional data fields for each component

Data field	Description
Source code URI	"Uniform Resource Identifier (URI)" of the source code of the component, e. g. the URL of the source code repository
URI of the executable form of the component	"Uniform Resource Identifier (URI)", which points directly to the executable form of the component.
Hash value of the source code of the component	Cryptographically secure checksum (hash value) of the component source code[16] as SHA-256
Other unique identifiers	Other identifiers that can be used to identify the component or to look it up in relevant databases, such as Common Platform Enumeration (CPE) or Package URL (purl).

[16] The method to calculate the hash value of the source code is currently not specified.

Federal Office for Information Security

Page 11 of 17

Federal Office for Information Security

Technical Guideline on SBOM

- Work in progress
  - Version 1.1 (English) published in January 2024
  - Currently working on version 2.0
- Expert feedback sessions with organizations
  - Open Source Business Alliance (OSBA)
  - Other industry organizations
  - SBOM specification maintainers (SPDX, CycloneDX)
- Feedback welcome
  - Send us your feedback to tr03183@bsi.bund.de

Thank you for your attention!

Contact

Anna Thurm
Policy Officer Market Surveillance

anna.thurm@bsi.bund.de
Tel. +49 (0) 228 9582 8117

Federal Office for Information Security (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de

Federal Office
for Information Security