Fabasoft

White Paper

Software Bill of Materials (SBOM)

2026 October Release

Contents

1 Introduction

Every container image distributed via the public registry is signed with a `cosign` signature and includes a Software Bill of Materials (SBOM) in CycloneDX format as an attestation. The SBOM lists all software components contained in the image, their versions, and the associated dependencies.

The image's signature can be verified using the provided public key. The SBOM can then be downloaded and viewed locally. This ensures that the components of every image are fully traceable.

2 Prerequisites

The following items are required to download and verify the SBOM:

- `cosign` (CLI)
  To verify the signature and download the SBOM attestation.
  Tool: https://github.com/sigstore/cosign/releases
  Installation guidelines: https://docs.sigstore.dev/cosign/system_config/installation/
- `jq`
  To read and format the JSON data.
  Tool: https://jqlang.org/download/
- `OCI-COSIGN-KEY-Fabasoft-RD-2023`
  https://download.fabasoft.com/keys/
- Registry access
  Username and password for read access to the public registry.

3 Process

The process consists of three steps:

- Verify the image's signature
  Checks whether the image is correctly signed.
- Download the SBOM attestation
  The `cosign` attestation is retrieved from the registry and saved locally.
- Decode the SBOM
  The JSON content (Base64-encoded) is decoded and converted into a readable format.

3.1 Verify the Image's Signature

The image's signature can be verified with the following command.

Command

```
cosign verify \
  --private-infrastructure \
  --key OCI-COSIGN-KEY-Fabasoft-RD-2023 \
```

```
  --signature-digest-algorithm=sha512 \
  --registry-username "<user name>" \
  --registry-password "<password>" \
  <registry URL>/<product name>/<image name>@<image digest>
```

Example

```
cosign verify \
  --private-infrastructure \
  --key OCI-COSIGN-KEY-Fabasoft-RD-2023 \
  --signature-digest-algorithm=sha512 \
  --registry-username "test-user" \
  --registry-password "*****" \
  registry.fabasoft.com/fabasoft/appducx-lsp@sha256:0664...128e
```

3.2 Download the SBOM Attestation

The SBOM attestation can be downloaded with the following command.

Command

```
cosign verify-attestation \
  --type cyclonedx \
  --private-infrastructure \
  --key OCI-COSIGN-KEY-Fabasoft-RD-2023 \
  --signature-digest-algorithm=sha512 \
  --registry-username "<user name>" \
  --registry-password "<password>" \
  <registry URL>/<product name>/<image name>@<image digest> \
  > sbom_attestation.json
```

Example

```
cosign verify-attestation \
  --type cyclonedx \
  --private-infrastructure \
  --key OCI-COSIGN-KEY-Fabasoft-RD-2023.pub \
  --signature-digest-algorithm=sha512 \
  --registry-username "test-user" \
  --registry-password "*****" \
  registry.fabasoft.com/fabasoft/appducx-lsp@sha256:0664...128e \
  > sbom_attestation.json
```

3.3 Decode the SBOM

The SBOM can be decoded with the following command.

Command

```
jq -r '.payload' sbom_attestation.json | base64 -d | jq . > sbom-decoded.json
```

Example

```
jq -r '.payload' sbom_attestation.json | base64 -d | jq . > sbom_decoded.json
cat sbom_decoded.json
```

The result is a complete CycloneDX BOM in JSON format. The file can be opened in a text editor or imported into a common SBOM viewer or vulnerability scanner (e.g., Snyk, Grype, Trivy).