OpenChain Specification

Version 1.1

Contents

This is an official translation from the OpenChain Project. It has been translated from the original English text. In the event there is confusion between this translation and the English version, The English text shall take precedence.

Der vorliegende Text beinhaltet eine offizielle Übersetzung aus dem OpenChain Projekt. Bei Unklarheiten oder Mehrdeutigkeiten im Rahmen einer Auslegung hat der englische Text Vorrang.

1) Einleitung

Die OpenChain Initiative wurde im Jahr 2013 ins Leben gerufen, nachdem eine Gruppe von Open-Source-Anwendern zwei wiederkehrende Muster in Open-Source-Software-Lieferketten beobachtet hatte:

1) die für den Umgang mit Open Source Software definierten Prozesse wiesen bei Organisationen mit ausgereiften Open-Source-Compliance-Programmen erhebliche Ähnlichkeiten auf; und

2) es gab noch eine große Anzahl von Organisationen, die Software im Rahmen weniger weit entwickelter Programme austauschte.

Diese Erkenntnis führte dazu, dass der Konsistenz und Qualität der Compliance-Artefakte, die mit zugelieferter Software zur Verfügung gestellt werden, meist nur geringes Vertrauen entgegengebracht wird. Folglich führen auf jeder Stufe der Lieferkette Organisationen Compliance-Arbeit erneut durch, auch wenn sie bereits von Zulieferern ausgeführt wurde.

Es wurde daher zunächst eine Forschungs- und Arbeitsgemeinschaft gebildet, um zu prüfen, ob gemeinsame Standard-Spezifikationen für Compliance-Programme identifiziert und definiert werden könnten, die: i) zu einer verbesserten Qualität und Konsistenz der Open-Source-Compliance-Informationen führen, die in der gesamten Industrie geteilt werden; und ii) die hohen Transaktionskosten im Zusammenhang mit Open Source Software reduzieren, die sich aus der Wiederholung von Compliance-Arbeit ergeben. Die Forschungsgemeinschaft entwickelte sich dann zu einem Arbeitskreis, der schließlich im April 2016 offiziell als Kooperationsprojekt der Linux Foundation eingerichtet wurde.

Die OpenChain Initiative basiert auf folgender Vision und Mission:

- Vision: Eine Software Supply Chain, in der Freie und Open Source Software (FOSS) mit vertrauenswürdigen und konsistenten Compliance-Informationen zugeliefert wird.

- Mission: Etablieren von Anforderungen an einen effektiven Umgang mit Freier und Open-Source-Software (FOSS) durch Mitglieder der Software Supply Chain, so dass die Anforderungen und die damit verbundenen Sicherheiten gemeinsam und offen von Vertretern der Software Supply Chain, Open Source Community und Hochschulen entwickelt werden.

In Übereinstimmung mit der Vision und der Mission definiert diese Spezifikation eine Reihe von Anforderungen, die, wenn sie erfüllt werden, die Wahrscheinlichkeit erhöhen, dass ein Open-Source-Compliance-Programm ein ausreichendes Maß an Qualität, Konsistenz und Vollständigkeit erreicht hat, auch wenn ein Programm, das alle Anforderungen der Spezifikation erfüllt, keine vollständige Compliance garantiert. Die definierten Anforderungen stellen einen Katalog von grundlegenden (Minimal-) Anforderungen auf, die ein Programm erfüllen muss, um als “OpenChain Conforming” anerkannt zu werden. Die Spezifikation konzentriert sich auf die "Was" und "Warum" -Beschaffenheit eines Compliance-Programms, statt "Wie" und "Wenn" -Überlegungen anzustellen. So wird ein praktisches Maß an Flexibilität sichergestellt, welches es Organisationen aller Art ermöglicht, ihre Richtlinien und Prozesse optimal an ihre Ziele anzupassen.

Im folgenden Abschnitt 2 werden zunächst Definitionen von Schlüsselbegriffen eingeführt, die in der gesamten Spezifikation verwendet werden. Abschnitt 3 enthält die Anforderungen der Spezifikation. Jeder Anforderung ist eine Liste von einem oder mehreren sogenannten Verifikationsartefakten zugeordnet. Sie stellen die Nachweise dar, die vorhanden sein müssen, damit eine bestimmte Anforderung als erfüllt angesehen werden kann. Wenn ein bestimmtes Programm alle Anforderungen erfüllt, gilt es als “OpenChain Conforming” gemäß Version 1.1 der Spezifikation. Es ist nicht beabsichtigt, dass die jeweiligen Verifikationsartefakte öffentlich zugänglich sein müssen. Sie können vielmehr im Rahmen einer Verschwiegenheitsvereinbarung offen gelegt werden oder auf individuelle Anfrage von der OpenChain Initiative zur Bestätigung der Konformität bereitgestellt werden.

2) Definitionen

FOSS (Free und Open Source Software) - Software, die einer oder mehreren Lizenzen unterliegt, die den Anforderungen der Open Source Definition der Open Source Initiative (OpenSource.org) oder der Free Software Definition der Free Software Foundation entsprechen.

FOSS Liaison - eine konkrete Person, die für den Erhalt externer FOSS Anfragen bestimmt wird.

Identifizierte Lizenzen - eine Reihe von FOSS-Lizenzen, die aufgrund einer geeigneten Methode zur Identifizierung solcher Lizenzen identifiziert wurden.

OpenChain Conforming - ein Programm, das alle Anforderungen dieser Spezifikation erfüllt.

Software-Mitarbeiter - jeder Mitarbeiter oder Auftragnehmer, der die Vorgaben für zugelieferte Software festlegt, zu ihr beiträgt oder für ihre Vorbereitung verantwortlich ist. Je nach Organisation sind dies insbesondere Software-Entwickler, Release-Ingenieure, Qualitätsprüfer, Produkt-Marketing und Produkt-Management.

SPDX oder Software Package Data Exchange - der von der SPDX-Arbeitsgruppe erstellte Format-Standard für den Austausch von Lizenz- und Urheberrechtsinformationen für ein bestimmtes Softwarepaket. Eine Beschreibung der SPDX-Spezifikation finden Sie unter www.spdx.org.

Zugelieferte Software - Software, die eine Organisation an Dritte weitergibt (z. B. andere Organisationen oder Einzelpersonen).

Verifikationsartefakte - Nachweise, die vorhanden sein müssen, damit eine bestimmte Anforderung als erfüllt angesehen werden kann.

3) Anforderungen

G1: Erkennen und verstehen Sie Ihre Verpflichtungen bei der Nutzung von FOSS

1.1 Es existiert eine schriftliche FOSS-Richtlinie, in der die Anforderungen an die FOSS-Lizenz-Compliance innerhalb der Supplied Software Distribution geregelt ist. Die Richtlinie muss innerhalb des Unternehmens kommuniziert werden.

Verifikationsartefakt(e):

1.1.1 Es existiert eine schriftlich dokumentierte FOSS-Richtlinie.

1.1.2 Es existiert ein dokumentiertes Verfahren, das alle Software-Mitarbeiter auf die Existenz der FOSS-Richtlinie aufmerksam macht (z. B. über Training, internes Wiki oder eine andere im Unternehmen relevante Kommunikationsmethode).

Begründung:
Stellen Sie sicher, dass die notwendigen Schritte unternommen wurden, um Software-Mitarbeiter auf die Existenz der FOSS-Richtlinie hinzuweisen. Obwohl an dieser Stelle keine inhaltlichen Vorgaben an die FOSS-Richtlinie gestellt werden, können solche inhaltliche Vorgaben an anderer Stelle dieser Spezifikation genannt werden.

1.2 Zwingend vorgeschriebene FOSS-Schulungen für alle Software-Mitarbeiter

- **Die Schulung umfasst mindestens folgende Themen:**
  - FOSS-Richtlinie der Organisation und wo man eine Kopie findet;
  - Grundlagen zu gesetzlichen Vorgaben im Bereich Intellectual Property in Bezug auf FOSS und FOSS-Lizenzen;
  - FOSS-Lizenzkonzepte (einschließlich der Konzepte von permissive und copyleft-Lizenzen);
  - Lizenzmodelle für FOSS Projekte;
  - Rollenverteilung und Verantwortlichkeiten der Software-Mitarbeiter im Zusammenhang mit der FOSS-Richtlinie im Allgemeinen und FOSS-Compliance im Besonderen; und
  - Verfahren zur Identifizierung, Dokumentation und / oder Nachverfolgung von FOSS-Komponenten, die in der mitgelieferten Software enthalten sind**.**
- **Alle Software-Mitarbeiter müssen in den vergangenen 24 Monaten eine FOSS-Schulung absolviert haben (damit die FOSS Schulung als "aktuell" angesehen werden kann). Um die Anforderungen an die FOSS-Schulung zu erfüllen, kann ein Test zu absolvieren.**

Verifikationsartefakt(e):
1.2.1 Es existieren entsprechende FOSS-Schulungsunterlagen, die die oben genannten Themen abdecken (z. B. Präsentationen, Online-Kurse oder andere Schulungsunterlagen).

1.2.2 Es besteht ein Verfahren zur Nachverfolgung der Schulungsteilnahme für alle Software-Mitarbeiter.

1.2.3 Mindestens 85% der Software-Mitarbeiter haben eine aktuelle Schulung nach der oben genannten Definition erfolgreich absolviert.

Begründung:
Stellen Sie sicher, dass die Software-Mitarbeiter zeitnah an einer FOSS-Schulung teilgenommen haben und dass die Schwerpunkte der relevanten FOSS-Themen abgedeckt wurden. Ziel ist es, sicherzustellen, dass alle Schwerpunkte relevanter FOSS-Themen abgedeckt sind, wobei die einzelnen Schulungsprogramme wahrscheinlich sehr viel umfassender ausfallen als hier gefordert.

1.3 Es besteht ein Verfahren zur Überprüfung der Identifizierten Lizenzen um die jeweiligen Rechte, Einschränkungen und Verpflichtungen zu erkennen.

Verifikationsartefakt(e):

1.3.1 Es existiert ein dokumentiertes Verfahren zur Überprüfung und Dokumentation der Rechte, Beschränkungen und Verpflichtungen, die durch die jeweiligen Identifizierten Lizenzen an der bzw. in Bezug auf die gelieferte Software bestehen.

Begründung:
Es muss sichergestellt werden, dass ein Prozess besteht, in dem die Lizenzpflichten für die verschiedenen Anwendungsfälle geprüft und identifiziert werden.

G2: Weisen Sie die Verantwortung für die Erfüllung der License Compliance zu

2.1 Identifikation einer FOSS-Ansprechpartner-Funktion ("FOSS Liaison").

- Ernennung einer oder mehrerer Einzelpersonen, die für die Entgegennahme und Bearbeitung externer FOSS-Anfragen verantwortlich sind;

- Die FOSS Liaison muss kommerziell vernünftige Anstrengungen unternehmen, um auf FOSS-Compliance-Anfragen zu reagieren; und öffentlich den Kommunikationskanal bekannt machen, über den er/sie kontaktiert werden kann**.**

Verifikationsartefakt(e):
2.1.1 Machen Sie die FOSS-Liaison öffentlich bekannt (z. B. durch Veröffentlichen einer Kontakt-E-Mail-Adresse oder Aufnahme in das Open Compliance-Verzeichnis der Linux Foundation).

2.1.2 Es existiert ein intern dokumentiertes Verfahren, das die Verantwortung für den Empfang und die Bearbeitung von FOSS-Compliance-Anfragen zuweist.

Begründung:
Stellen Sie sicher, dass es für Dritte eine angemessene Möglichkeit gibt, sich mit Ihnen in Bezug auf FOSS-Compliance-Anfragen in Verbindung zu setzen und dass die Verantwortung zur Bearbeitung entsprechender Anfragen effektiv zugeordnet wird.

2.2 Identifikation der internen FOSS-Compliance Rolle(n).

- Zuweisen der Verantwortung zur Verwaltung und zum Management der internen FOSS-Compliance an individuelle Mitarbeiter. Die FOSS-Compliance-Verantwortlichen und die FOSS-Liaison können dieselben Personen sein.
- FOSS-Compliance-Management-Aktivitäten verfügen über ausreichende Ressourcen:
  - Weisen Sie angemessene Zeit für die Ausführung der Rolle zu; und
  - Weisen Sie ein angemessenes Budget zu.
- Zuweisen der Verantwortlichkeiten zur Entwicklung und Pflege von FOSS-Compliance-Richtlinie und -Prozessen;
- Gewährleisten, dass juristische Expertise in Bezug auf die FOSS-Compliance vorhanden und für die FOSS-Compliance-Verantwortlichen (intern oder extern) zugänglich ist; und
- Sicherstellen, dass eine Eskalationsmöglichkeit für die Lösung von FOSS-Compliance-Problemen zur Verfügung steht.

Verifikationsartefakt(e):
2.2.1 Name der Personen, Gruppe oder Funktionen des/der FOSS-Compliance-Verantwortliche (n) sind intern identifiziert.

2.2.2 Benennung der juristischen Expertise, die dem/den FOSS-Compliance-Verantwortlichen intern oder extern zur Verfügung steht.

2.2.3 Es existiert ein dokumentiertes Verfahren, das interne Verantwortlichkeiten für die FOSS-Compliance zuweist.

2.2.4 Es existiert ein dokumentiertes Verfahren zur Prüfung und Behebung von Fällen von Nicht-erfüllung der FOSS-Compliance-Anforderungen

Begründung:

Stellen Sie sicher, dass einzelnen Mitarbeitern konkrete FOSS-Verantwortlichkeiten verbindlich zugewiesen wurden.

G3: Überprüfen und genehmigen Sie FOSS Content

3.1 Es existiert ein Prozess zum Erstellen und Verwalten einer Bill of Materials der FOSS-Komponenten, die jede Komponente (und ihre Identifizierten Lizenzen) einer Version Zugelieferter Software enthält.

Verifikationsartefakt(e):
3.1.1 Es existiert ein dokumentiertes Verfahren zur Identifizierung, Nachverfolgung und Archivierung von Informationen über die Zusammensetzung von FOSS-Komponenten, aus denen eine Version Zugelieferter Software besteht.

3.1.2 Für jede Version Zugelieferter Software existiert eine Aufzeichnung, die nachweist, dass die dokumentierte Prozedur ordnungsgemäß befolgt wurde.

Begründung:
Stellen Sie sicher, dass ein Prozess zum Erstellen und Verwalten einer Bill of Materials der FOSS-Komponenten existiert, anhand dessen die Zugelieferte Software erstellt wird. Die Bill of Materials ist erforderlich, um systematisch die Lizenzbedingungen jeder Komponente mit dem Ziel zu überprüfen, die Lizenzpflichten und -bedingungen mit Blick auf die Verbreitung der Zugelieferten Software zu ermitteln.

3.2 Das FOSS-Programm muss es ermöglichen, die üblichen Anwendungsfälle von FOSS-Lizenzen in Zugelieferter Software abzudecken. Zu den üblichen Fällen zählen dabei insbesondere (beachten Sie allerdings, dass die Liste weder erschöpfend ist, noch alle Anwendungsfälle auf Sie Anwendung finden müssen):

- Verbreitung in Binärform;
- Verbreitung in Source Code Form;
- Integration mit anderer FOSS, so dass die Voraussetzungen des Copyleft vorliegen können;
- Enthält bearbeitete FOSS;
- Enthält FOSS oder andere Software unter einer inkompatiblen Lizenz, die mit anderen Komponenten innerhalb der Zugelieferten Software interagiert; und / oder
- Enthält FOSS mit Attributionsanforderungen

Verifikationsartefakt(e):
3.2.1 Ein Verfahren ist implementiert, das es ermöglicht die üblichen Anwendungsfälle von FOSS-Lizenzen in Zugelieferter Software für die FOSS-Komponenten jeder Version Zugelieferter Software abzudecken.

Begründung:
Stellen Sie sicher, dass das FOSS-Management-Programm ausreichend robust ist, um die üblichen Anwendungsfälle von FOSS-Lizenzen einer Organisation zu behandeln. Gewährleisten Sie, dass ein Verfahren zur Unterstützung dieser Tätigkeit besteht und dass die vorgesehene Prozedur befolgt wird.

G4: Stellen Sie FOSS-Inhaltsdokumentation und Artefakte bereit

4.1 Zusammenstellen der Artefakte, die nach Maßgabe des Programms zur FOSS-Überprüfung mit jeder Version Zugelieferter Software zur Verfügung gestellt werden müssen. Die Menge der Artefakte wird gemeinsam als Compliance-Artefakte bezeichnet. Sie können eine oder mehrere der folgenden Artefakte enthalten: Quellcode, Benennung des Autors, Urheberrechtshinweise, Kopien der Lizenzbedingungen, Bearbeitungshinweise, schriftliche Angebote, SPDX-Dokumente etc.

Verifikationsartefakt(e):
4.1.1 Es steht ein dokumentiertes Verfahren zur Verfügung, das sicherstellt, dass die Compliance-Artefakte mit jeder Version Zugelieferter Software entsprechend den Anforderungen der Identifizierten Lizenzen zusammengestellt und verteilt werden.

4.1.2 Kopien der Compliance-Artefakte der Version Zugelieferter Software werden archiviert und sind einfach wiederauffindbar, und es ist geplant, dass das Archiv mindestens so lange besteht, wie die Zugelieferte Software angeboten wird oder wie es die Identifizierten Lizenzen verlangen (je nachdem, welcher Zeitraum länger ist).

Begründung:
Stellen Sie sicher, dass die vollständigen Compliance-Artefakte entsprechend den Anforderungen der Identifizierten Lizenzen, sowie sonstige Berichte, die während der FOSS-Überprüfung erstellt wurden, mit jeder Version der Zugelieferten Software ausgeliefert werden.

G5: Verstehen Sie FOSS Community Engagement

5.1 Es gibt eine schriftliche Richtlinie, die die Beiträge zu FOSS-Projekten durch die Organisation regelt. Die Richtlinie muss intern kommuniziert werden.

Verifikationsartefakt(e):
5.1.1 Es existiert eine dokumentierte Richtlinie für Beiträge zu FOSS;

5.1.2 Es existiert ein dokumentiertes Verfahren, dass alle Software-Mitarbeiter auf die Existenz der Richtlinie für Beiträge zu FOSS aufmerksam macht (z. B. mittels Training, ein internes Wiki oder andere praktische Kommunikationsmethode).

Begründung:
Stellen Sie sicher, dass die Organisation der Entwicklung einer Richtlinie für öffentliche Beiträge zu FOSS eine ausreichende Beachtung geschenkt hat. Die Richtlinie für Beiträge zu FOSS kann Teil einer übergreifenden FOSS-Richtlinie oder eine eigene separate Richtlinie sein. In dem Fall, dass Beiträge zu FOSS überhaupt nicht erlaubt sind, sollte es eine Richtlinie geben, die diese Haltung klarstellt.

5.2 Wenn eine Organisation Beiträge zu FOSS-Projekten zulässt, muss ein Prozess existieren, der die in Abschnitt 5.1 skizzierte Richtlinie für Beiträge zu FOSS umsetzt.

Verifikationsartefakt(e):
5.2.1 Wenn die Richtlinie Beiträge zu FOSS zulässt, muss ein dokumentiertes Verfahren existieren, anhand dessen Beiträge zu FOSS erfolgen.

Begründung:
Stellen Sie sicher, dass eine Organisation einen dokumentierten Prozess hat, wie sie öffentlich zu FOSS beiträgt. Es kann eine Richtlinie dergestalt bestehen, dass Beiträge gar nicht gestattet sind. Aus dieser Situation folgt zwingend, dass kein Verfahren existieren kann und, dass diese Anforderung auch ohne Verfahren erfüllt werden würde.

G6: Zertifizieren der OpenChain-Anforderungen

6.1 Damit eine Organisation OpenChain Conforming ist, muss sie bestätigen, dass sie ein FOSS-Programm hat, das die in dieser OpenChain-Spezifikation Version 1.1 beschriebenen Kriterien erfüllt.

Verifikationsartefakt(e):
6.1.1 Die Organisation bestätigt, dass ein Programm existiert, das alle Anforderungen dieser OpenChain Spezifikation Version 1.1 erfüllt.

Begründung:
Es muss sichergestellt werden, dass ein FOSS-Programm alle Anforderungen dieser Spezifikation erfüllt, wenn eine Organisation angibt, ihr Programm sei OpenChain Conforming. Lediglich Teile der Anforderungen zu erfüllen, wird nicht als ausreichend angesehen, um ein Programm als OpenChain Conforming einzustufen.

6.2 Die Übereinstimmung mit dieser Version der Spezifikation ist ab dem Datum der Validierung der Zertifizierung für 18 Monate gültig. Die Anforderungen der Validierung der Zertifizierung finden Sie auf der Website des OpenChain-Projekts.

Verifikationsartefakt(e):
6.2.1 Die Organisation bestätigt, dass ein FOSS-Compliance-Programm existiert, das alle Anforderungen dieser OpenChain Spezifikation Version 1.1 während der vergangenen 18 Monate seit Erreichen der Validierung der Konformität erfüllt.

Begründung:
Es ist wichtig, dass die Organisation auf einem aktuellen Stand bezüglich der Spezifikation bleibt, wenn sie die Zertifizierung auf Dauer behaupten will. Diese Anforderung stellt sicher, dass die die Zertifizierung unterstützenden Prozesse und Kontrollen des Programms nicht abgeschwächt werden, wenn sie auf Dauer weiterhin die Übereinstimmung mit den Anforderungen der Spezifikation behaupten wollen.

Anhang I: Sprachübersetzungen

Um die globale Anwendung und Verbreitung zu erleichtern, begrüßen wir die Bemühungen, die Spezifikation in mehrere Sprachen zu übersetzen. Da auch die OpenChain Initiative wie ein Open Source Projekt aufgesetzt ist, werden Übersetzungen durch diejenigen gesteuert, die bereit sind, ihre Zeit und ihr Fachwissen zu Übersetzungen unter den Bedingungen der CC-BY 4.0-Lizenz und der Richtlinie des Projekts für Übersetzungen beizutragen. Die Details der Richtlinien und der verfügbaren Übersetzungen finden Sie auf der Spezifikations-Webseite des OpenChain-Projekts.