OpenChain Spezifikation
Version 2.1

Diese Spezifikation ist funktional identisch mit:

- **OpenChain Specification 2.0**
- **ISO/IEC PRF 5230**

Erfahren Sie mehr: www.openchainproject.org

Inhalt

Einleitung

Dieses Dokument definiert die wichtigsten Anforderungen an ein Qualitätsprogramm zur Einhaltung von Open Source-Lizenzen. Ziel ist es, einen Maßstab zur Stützung des Vertrauens bereitzustellen zwischen Organisationen, die Softwarelösungen aus Open Source austauschen. Die Spezifikationskonformität bietet die Sicherheit, dass ein Programm entwickelt wurde, um die erforderlichen Konformitätsartefakte (d. h. rechtliche Hinweise, Quellcode usw.) für jede Softwarelösung zu erzeugen. Dieses Dokument konzentriert sich eher auf die Aspekte „Was“ und „Warum“ eines Programms als auf das „Wie“ und „Wann“. Dies gewährleistet Flexibilität für verschiedene Organisationen unterschiedlicher Größe in verschiedenen Märkten, um spezifische Richtlinien- und Prozessinhalte auszuwählen, die zu ihrer Größe, ihren Zielen und ihrem Umfang passen. Beispielsweise kann ein OpenChain-konformes Programm eine einzelne Produktlinie oder die gesamte Organisation ansprechen.

Diese Einführung bietet den Kontext für alle potenziellen Benutzer. In Abschnitt 2 werden die in diesem Dokument verwendeten Schlüsselbegriffe definiert. Abschnitt 3 definiert die Anforderungen, die ein Programm erfüllen muss, um Konformität zu erreichen. Eine Anforderung besteht aus einem oder mehreren Verifizierungsmaterialien (d. h. Aufzeichnungen), die erstellt werden müssen, um die Anforderung zu erfüllen. Überprüfungsmaterialien müssen nicht veröffentlicht werden, obwohl eine Organisation sie anderen zur Verfügung stellen darf, möglicherweise verbunden mit einer Geheimhaltungsvereinbarung (NDA).

Dieses Dokument wurde als offene Initiative mit Rückmeldungen von mehr als 200 Mitwirkenden entwickelt. Einblicke in die historische Entwicklung erhalten Sie in der Mailingliste für Spezifikationen und in den häufig gestellten Fragen (FAQs).

Informatik — OpenChain Spezifikation

1 Geltungsbereich

In diesem Dokument werden die wichtigsten Anforderungen an ein Qualitätsprogramm zur Einhaltung von Open Source-Lizenzen aufgeführt, um einen Maßstab zur Stärkung des Vertrauens zwischen Organisationen bereitzustellen, die aus Open Source-Software bestehende Softwarelösungen austauschen.

2 Begriffe und Definitionen

Für die Zwecke dieses Dokuments gelten die folgenden Begriffe und Definitionen:

2.1
Compliance-Artefakte
Eine Sammlung von Artefakten, die die Ausgabe eines Compliance-Programms darstellen und der mitgelieferten Software beiliegen.

Hinweis: Die Sammlung kann eine oder mehrere der folgenden Komponenten enthalten (ist jedoch nicht darauf beschränkt): Zuordnungshinweise, Quellcode, Erstellungs- und Installationsskripte, Kopie von Lizenzen, Urheberrechtshinweise, Änderungsbenachrichtigungen, schriftliche Angebote, Stückliste für Open-Source-Komponenten und SPDX-Dokumente.

2.2
Identifizierte Lizenzen
Eine Reihe von Open-Source-Softwarelizenzen, die als Ergebnis der Befolgung einer geeigneten Methode zur Identifizierung von Open-Source-Komponenten identifiziert wurden, aus denen die gelieferte Software besteht

2.3
OpenChain-konform
Ein Programm, das alle Anforderungen dieses Dokuments erfüllt.

2.4
Open Source
Software, die einer oder mehreren Lizenzen unterliegt, die der von der Open Source Initiative veröffentlichten Open Source Definition (siehe opensource.org/osd) oder der von der Free Software Foundation veröffentlichten Open Software Definition (siehe gnu.org/philosophy/free-sw.html), oder einer ähnlichen Lizenz entsprechen.

2.5
Programm
Die Richtlinien, Prozesse und Mitarbeiter, aus denen die Open Source-Lizenzkonformitätsaktivitäten eines Unternehmens bestehen.

2.6
Programmteilnehmer
Jeder Mitarbeiter oder Auftragnehmer einer Organisation, der die bereitgestellte Software definiert, dazu beiträgt oder dafür verantwortlich ist.

Hinweis: Je nach Organisation kann dies auch (jedoch nicht darauf beschränkt) Softwareentwickler, Release-Ingenieure, Qualitätsprüfer, Mitarbeiter in Produktmarketing und Produktmanagement einschließen.

2.7
SPDX
Der von der SPDX-Arbeitsgruppe (Software Package Data Exchange) der Linux Foundation erstellte Formatstandard für den Austausch von Stücklisten für ein bestimmtes Softwarepaket, einschließlich der zugehörigen Lizenz- und Copyright-Informationen (siehe spdx.org).

2.8
Mitgelieferte Software
Software, die eine Organisation an Dritte (z. B. andere Organisationen oder Einzelpersonen) liefert.

2.9
Prüfungsmaterialien
Materialien, die nachweisen, dass eine bestimmte Anforderung der Spezifikation erfüllt ist.

ISO und IEC unterhalten terminologische Datenbanken zur Verwendung bei der Normung unter folgenden Adressen:

— ISO Online browsing platform: unter https://www.iso.org/obp

— IEC Electropedia: unter http://www.electropedia.org/

3 Anforderungen

3.1 Programmgrundlage

3.1.1 Richtlinie

Es muss eine schriftliche Open-Source-Richtlinie existieren, die die Einhaltung der Open-Source-Lizenz der gelieferten Software regelt. Die Richtlinie wird intern kommuniziert.

Prüfungsmaterial:

3.1.1.1 Eine dokumentierte Open Source-Richtlinie.
3.1.1.2 Ein dokumentiertes Verfahren, das Programmteilnehmer auf die Existenz der Open Source-Richtlinie aufmerksam macht (z. B. durch Schulungen, internes Wiki oder eine andere gängige Kommunikationsmethode).

Begründung:

Es soll sichergestellt werden, dass die notwendigen Schritte unternommen wurden, um eine Open-Source-Richtlinie zu erstellen, festzulegen und Software-Mitarbeiter auf deren Existenz hinzuweisen. Obwohl an dieser Stelle keine inhaltlichen Vorgaben an die Open-Source-Richtlinie gestellt werden, können diese durch andere Abschnitte dieser Spezifikation auferlegt werden.

3.1.2 Zuständigkeiten

Die Organization

- bestimmt die Aufgaben und deren entsprechende Verantwortlichkeiten, die sich auf die Leistung und Effektivität des Programms auswirken;
- bestimmt die erforderliche Fachkompetenz der Programmteilnehmer, die die jeweilige Aufgabe erfüllen;
- stellt sicher, dass die Programmteilnehmer auf der Grundlage einer angemessenen Ausbildung, Schulung und / oder Erfahrung Fachkompetenz besitzen;
- ergreift gegebenenfalls Maßnahmen, um die erforderliche Fachkompetenz zu erwerben; und
- bewahrt geeignete dokumentierte Informationen als Kompetenznachweis auf.

Prüfungsmaterial:

3.1.2.1 Eine dokumentierte Liste von Aufgaben mit entsprechenden Verantwortlichkeiten für die verschiedenen Programmteilnehmer.
3.1.2.2 Dokumentation der erforderlichen Fachkompetenzen für jede Aufgabe.
3.1.2.3 Dokumentierter Nachweis von erworbener Fachkompetenz für jeden Programmteilnehmer.

Begründung:

Es soll sichergestellt werden, dass die Programmteilnehmer ein ausreichendes Maß an Fachkompetenz für ihre jeweiligen Aufgaben und Verantwortlichkeiten erworben haben.

3.1.3 Beachtung

Die Organisation stellt sicher, dass die Programmteilnehmer davon Kenntnis haben:

- die Open Source-Richtlinie;
- relevante Open Source-Ziele;
- ihren Beitrag zur Wirksamkeit des Programms; und
- die Auswirkungen der Nichteinhaltung der Programmanforderungen.

Prüfungsmaterial:

3.1.3.1 Dokumentierter Nachweis der Kenntnisnahme der Programmteilnehmer insbesondere der Programmziele, ihres Beitrags innerhalb des Programms und der Auswirkungen von Programmkonformitäten.

Begründung:

Es soll sichergestellt werden, dass die Programmteilnehmer ein ausreichendes Bewusstsein für ihre jeweiligen Aufgaben und Verantwortlichkeiten innerhalb des Programms erhalten haben.

3.1.4 Programmumfang

Unterschiedliche Programme können für unterschiedliche Umfangsebenen definiert werden. Ein Programm kann beispielsweise eine einzelne Produktlinie, eine gesamte Abteilung oder eine gesamte Organisation umfassen. Die Bereichsbezeichnung muss für jedes Programm definiert werden.

Prüfungsmaterial:

3.1.4.1 Eine schriftliche Erklärung, die den Umfang und die Grenzen des Programms klar definiert.

Begründung:

Bereitstellung der Flexibilität, ein Programm zu erstellen, das den Anforderungen eines Unternehmens am besten entspricht. Einige Organisationen könnten sich dafür entscheiden, ein Programm für eine bestimmte Produktlinie zu verwalten, während andere ein Programm implementieren könnten, um die mitgelieferte Software der gesamten Organisation zu steuern.

3.1.5 Lizenzpflichten

Es muss ein Verfahren zur Überprüfung der identifizierten Lizenzen vorhanden sein, um die von jeder Lizenz gewährten Pflichten, Einschränkungen und Rechte zu ermitteln.

Prüfungsmaterial:

3.1.5.1 Ein dokumentiertes Verfahren zur Überprüfung und Dokumentation der Pflichten, Einschränkungen und Rechte, die von jeder identifizierten Lizenz gewährt werden.

Begründung:

Es soll sichergestellt werden, dass ein Prozess zum Überprüfen und Identifizieren der Lizenzverpflichtungen für jede identifizierte Lizenz für die verschiedenen Anwendungsfälle, auf die eine Organisation stoßen kann, vorhanden ist (wie in §3.3.2 definiert).

3.2 Definition und Unterstützung relevanter Aufgaben

3.2.1 Zugriff

Erstellung und Aufrechterhaltung eines Prozesses, um auf Open-Source-Anfragen von außerhalb der Organisation wirkungsvoll zu reagieren. Veröffentlichung einer Schnittstelle, über die Dritte Open-Source-Compliance-Anfragen absetzen können.

Prüfungsmaterial:

3.2.1.1 Öffentlich sichtbare Methode, mit der Dritte eine Open-Source-Lizenzkonformitätsanfrage stellen können (z. B. über eine veröffentlichte Kontakt-E-Mail-Adresse oder das Open-Compliance-Verzeichnis der Linux Foundation).
3.2.1.2 Ein internes dokumentiertes Verfahren zur Beantwortung von Open-Source-Lizenzkonformitätsanfragen von Drittanbietern.

Begründung:

Es soll sichergestellt werden, dass Dritte in Bezug auf Open-Source-Compliance-Anfragen eine angemessene Möglichkeit haben, sich an die Organisation zu wenden, und dass die Organisation bereit ist, effektiv zu reagieren.

3.2.2 Effektive Ausstattung

Definition der Aufgaben des Programms und deren Ausstattung:

- Zuweisung von Verantwortlichkeit, um die erfolgreiche Ausführung von Programmaufgaben sicherzustellen.
- Die Programmaufgaben sind ausreichend ausgestattet:
  - Die Zeit zur Ausführung der Aufgaben wurde zugewiesen; und
  - Es wurden angemessene Mittel bereitgestellt.
- Es gibt einen Prozess zum Überprüfen und Aktualisieren der Richtlinie und der unterstützenden Aufgaben;

- Das juristische Fachwissen in Bezug auf die Einhaltung von Open Source-Lizenzen ist für diejenigen zugänglich, die solche Leitlinien benötigen; und
- Es gibt einen Prozess zur Lösung von Open Source-Lizenzkonformitätsproblemen.

Prüfungsmaterial:

3.2.2.1 Dokument mit dem Namen der Personen, Gruppen oder Funktionen in den identifizierten Programmaufgaben.
3.2.2.2 Die identifizierten Programmaufgaben wurden ordnungsgemäß besetzt und mit angemessenen Mitteln ausgestattet.
3.2.2.3 Ermittlung des verfügbaren juristischen Fachwissens zur Behandlung von Open-Source-Lizenzkonformitätsfragen, die intern oder extern sein können.
3.2.2.4 Ein dokumentiertes Verfahren, das interne Verantwortlichkeiten für die Open Source-Konformität zuweist.
3.2.2.5 Ein dokumentiertes Verfahren zur Behandlung der Überprüfung und Behebung nicht konformer Fälle.

Begründung:

Es soll sichergestellt sein, dass i) Programm-Verantwortlichkeiten tatsächlich unterstützt und mit ausreichenden Ressourcen ausgestattet sind und ii) Richtlinien und unterstützende Prozesse regelmäßig aktualisiert werden, um Änderungen in den Best Practices für Open Source-Compliance zu berücksichtigen.

3.3 Überprüfung und Genehmigung von Open-Source-Inhalten

3.3.1 Komponentenstückliste

Es muss ein Prozess zum Erstellen und Verwalten einer Stückliste vorhanden sein, der jede Open Source-Komponente (und ihre identifizierten Lizenzen) enthält, aus der die gelieferte Software besteht.

Prüfungsmaterial:

3.3.1.1 Ein dokumentiertes Verfahren zum Identifizieren, Verfolgen, Überprüfen, Genehmigen und Archivieren von Informationen über die Sammlung von Open Source-Komponenten, aus denen die gelieferte Software besteht.
3.3.1.2 Eine Aufzeichnung der Komponenten von gelieferter Open-Source-Software, welche nachweist, dass das dokumentierte Verfahren ordnungsgemäß befolgt wurde.

Begründung:

Es soll sichergestellt sein, dass ein Prozess zum Erstellen und Verwalten einer Stückliste der mitgelieferten Komponenten der Open-Source-Software vorhanden ist. Eine Stückliste ist erforderlich, um die Lizenzbedingungen jeder Komponente systematisch zu überprüfen und genehmigen und die Pflichten und Einschränkungen zu verstehen, die für die gelieferte Software gelten.

3.3.2 Lizenzkonformität

Das Programm muss in der Lage sein, allgemeine Open-Source-Lizenzanwendungsfälle zu verwalten, auf die Programmteilnehmer für die bereitgestellte Software stoßen, einschließlich der folgenden Anwendungsfälle (beachten Sie, dass die Liste weder vollständig ist, noch alle Beispiele zutreffen müssen):

- Verbreitung in binärer Form;

- Verbreitung in Sourcecode-Form;
- Integriert in andere Open Source-Systeme, sodass zusätzliche Lizenzverpflichtungen entstehen;
- Enthält modifizierte Open Source-Software;
- Enthält Open Source oder andere Software unter einer inkompatiblen Lizenz, die mit anderen Komponenten der mitgelieferten Software interagiert; und/oder
- Enthält Open Source mit Forderungen zur Nennung der Urheberschaft.

Prüfungsmaterial:

3.3.2.1 Ein dokumentiertes Verfahren zur Behandlung der gängigen Open Source-Lizenzanwendungsfälle für die Open Source-Komponenten der mitgelieferten Software.

Begründung:

Es soll sichergestellt sein, dass das Programm robust genug ist, um die gängigen Open Source-Lizenzanwendungsfälle eines Unternehmens zu behandeln. Es soll sichergestellt sein, dass ein Verfahren zur Unterstützung dieser Aktivität vorhanden ist und dass das Verfahren befolgt wird.

3.4 Erstellung und Bereitstellung von Compliance-Artefakten

3.4.1 Compliance-Artefakte

Es muss ein Prozess zum Erstellen der Konformitätsartefakte für die mitgelieferte Software vorhanden sein.

Prüfungsmaterial:

3.4.1.1 Ein dokumentiertes Verfahren, das den Prozess beschreibt, unter dem die Compliance-Artefakte mit der mitgelieferten Software gemäß den Anforderungen der identifizierten Lizenzen erstellt und verteilt werden.

3.4.1.2 Ein dokumentiertes Verfahren zum Archivieren von Kopien der Konformitätsartefakte der gelieferten Software - wobei das Archiv für einen angemessenen Zeitraum[1] seit dem letzten Angebot der gelieferten Software vorhanden sein soll; oder wie von den identifizierten Lizenzen gefordert (je nachdem, welcher Zeitraum länger ist). Es gibt Aufzeichnungen, aus denen hervorgeht, dass das Verfahren ordnungsgemäß befolgt wurde.

Begründung:

Es soll sichergestellt werden, dass angemessene kommerzielle Anstrengungen zur Erstellung der Compliance-Artefakte, die der mitgelieferten Software beiliegen, unternommen werden, wie dies in den angegebenen Lizenzen vorgeschrieben ist.

3.5 Verstehen des Engagements gegenüber der Open Source Community

3.5.1 Beiträge

Wenn eine Organisation Beiträge zu Open Source-Projekten berücksichtigt, dann

- gibt es eine schriftliche Richtlinie, die Beiträge zu Open Source-Projekten regelt;
- muss diese Richtlinie intern kommuniziert werden; und es

[1] Bestimmt durch Domain, Gerichtsstand und / oder Kundenverträge

- muss ein Prozess existieren, der diese Richtlinie umsetzt.

Prüfungsmaterial:

Wenn eine Organisation Beiträge zu Open Source-Projekten zulässt, muss Folgendes vorhanden sein:

3.5.1.1 Eine dokumentierte Open Source-Beitragsrichtlinie;
3.5.1.2 Ein dokumentiertes Verfahren, das Open Source-Beiträge regelt; und
3.5.1.3 Ein dokumentiertes Verfahren, das alle Programmteilnehmer auf die Existenz der Open-Source-Beitragsrichtlinie aufmerksam macht (z. B. über Schulungen, internes Wiki oder eine andere gängige Kommunikationsmethode).

Begründung:

Wenn eine Organisation Beiträge zu Open-Source-Projekten erlaubt, soll sichergestellt werden, dass die Organisation der Entwicklung und Umsetzung einer Richtlinie für Beiträge ausreichende Beachtung geschenkt hat. Die Richtlinie für Beiträge zu Open Source kann Teil einer übergreifenden Open-Source-Richtlinie oder eine eigene separate Richtlinie sein.

3.6 Einhaltung der Spezifikationsanforderungen

3.6.1 Konformität

Wenn ein Programm als OpenChain-konform eingestuft werden soll, muss die Organisation bestätigen, dass das Programm die in diesem Dokument aufgeführten Anforderungen erfüllt.

Prüfungsmaterial:

3.6.1.1 Ein Dokument, das das in §3.1.4 angegebene Programm bestätigt, erfüllt alle Anforderungen dieses Dokuments.

Begründung:

Um sicherzustellen, dass eine Organisation, die erklärt, dass sie ein OpenChain-konformes Programm hat, alle Anforderungen dieses Dokuments erfüllt. Die bloße Erfüllung einer Teilmenge dieser Anforderungen wird nicht als ausreichend angesehen.

3.6.2 Dauer

Ein Programm, das OpenChain-konform mit dieser Version der Spezifikation ist, muss 18 Monate ab dem Datum der Konformitätsvalidierung gültig sein. Das Registrierungsverfahren für die Konformitätsvalidierung finden Sie auf der Website des OpenChain-Projekts.

Prüfungsmaterial:

3.6.2.1 Ein Dokument, das das Programm bestätigt, erfüllt alle Anforderungen dieses Dokuments innerhalb der letzten 18 Monate nach Erhalt der Konformitätsvalidierung.

Begründung:

Es ist wichtig, dass ein Programm mit der Spezifikation auf dem neuesten Stand bleibt, wenn ihre Programmkonformität auf Dauer behaupten möchte. Diese Anforderung stellt sicher, dass die unterstützenden Prozesse und Kontrollen des Programms nicht beeinträchtigt werden, wenn eine Organisation die Programmkonformität über den angegebenen Zeitraum hinaus geltend machen will.

Anhang A
(informativ)

Übersetzungen dieser Spezifikation in Fremdsprachen

Um die weltweite Akzeptanz zu erleichtern, sind Bemühungen zur Übersetzung der Spezifikation in verschiedene Sprachen sehr willkommen. Da OpenChain als Open-Source-Projekt fungiert, werden Übersetzungen von denjenigen erstellt, die bereit sind, ihre Zeit und ihr Fachwissen für die Durchführung der Übersetzungen einzubringen. Übersetzungen werden i) unter den Bedingungen der CC-BY-4.0-Lizenz angeboten und ii) im Einklang mit den Übersetzungsrichtlinien des Projekts. Die Details der Richtlinie und die verfügbaren Übersetzungen finden Sie im Wiki des OpenChain-Projekts.