

Contents

1) Wprowadzenie

2) Definicje

3) Wymagania

G1: Poznaj swoje obowiązki związane z FOSS

G2: *Przypisanie odpowiedzialności za Osiągnięcie Zgodności*

G3: Przeglądanie i zatwierdzanie treści FOSS

G4: Dostarczanie dokumentacji treści FOSS i jej poszczególnych elementów

G5: Zrozumienie istoty zaangażowania społeczności FOSS

G6: Poświadczenie zgodności z wymaganiami OpenChain

Dodatek I: tłumaczenia językowe

Copyright © 2016-2017 Linux Foundation. Ten dokument jest licencjonowany na licencji uznanie autorstwa (the Creative Commons Attribution) wersja 4.0 International (CC-BY 4.0). Kopię tej licencji można znaleźć pod adresem :<https://creativecommons.org/licenses/by/4.0/>.

OpenChain Specification 1.1

OpenChain Sepecyfikacja wersja 1.1

WPROWADZENIE

Inicjatywa OpenChain miała swój początek w 2013 roku, kiedy to grupa praktyków z obszaru łańcucha dostaw otwartego oprogramowania zaobserwowała dwa nowe wzorce: 1) istnienie znaczących podobieństw procesowych pomiędzy organizacjami o rozwiniętych programach typu compliance w zakresie oprogramowania open source; i 2) nadal istnieją organizacje zajmujące się wymianą oprogramowania z mniej programami. Ta ostatnia obserwacja zaskutkowała brakiem zaufania do jakości i spójności zgodności elementów towarzyszących wymianie oprogramowania. W konsekwencji, na każdym poziomie łańcucha dostaw, organizacje niższego szczebla często powtarzały prace w zakresie zgodności, które były już wykonywane przez inne jednostki wyższego szczebla. Powołano grupę studyjną do rozważenia, czy można stworzyć standardową specyfikację programu, która będzie: i) ułatwiać udostępnianie większej jakości i spójności informacji dotyczących zgodności otwartego oprogramowania udostępnianego w przemyśle; oraz ii) obniżyć wysokie koszty transakcji związane z otwartym oprogramowaniem w zakresie ponownej oceny zgodności. Grupa studyjna przekształciła się w grupę roboczą i kwietniu 2016 r. formalnie zorganizowała projekt jako Fundacja Linux. Wizja i misja Inicjatywy OpenChain są następujące:

- 1) **Wizja:** Sieć dostaw oprogramowania, w którym dostarcza się wolne / otwarte oprogramowanie (FOSS) z wiarygodnymi i spójnymi informacjami o jego zgodności.
- 2) **Misja:** Ustanowienie wymagań w celu skutecznego zarządzania wolnym / otwartym oprogramowaniem (FOSS) dla uczestników łańcucha dostaw, tak aby wymagania i powiązane zabezpieczenia zostały opracowane wspólnie i otwarcie przez przedstawicieli łańcucha dostaw oprogramowania, społeczności skupionej wokół otwartego oprogramowania i środowiska akademickiego.

Zgodnie z wizją i misją niniejsza specyfikacja definiuje zestaw wymagań, które jeżeli zostaną spełnione, znacznie zwiększą prawdopodobieństwo, że program zgodności z otwartą siecią osiągnie wystarczający poziom jakości, spójności i kompletności; Jednakże program, który spełnia wszystkie wymagania zawarte w specyfikacji, nie gwarantuje pełnej zgodności. Owe wymagania stanowią podstawowy poziom (minimalny) zestawu wymagań jakie program

musi spełniać, aby był rozważany za zgodny z OpenChain. Specyfikacja skupia się na cechach takich jak "co" i "dlaczego" programu zgodności, zamiast na "jak" i "kiedy". Zapewnia to pewien poziom elastyczności, który umożliwia różnym organizacjom dostosowywanie ich polityk i procesów do osiągnięcia zamierzonych celów.. Sekcja 2 wprowadza definicje kluczowych haseł używanych w specyfikacji. W sekcji 3 przedstawiono wymogi dotyczące specyfikacji, w których każdy zawiera listę jednego lub więcej elementów weryfikacyjnych. Są to przesłanki, które muszą zostać spełnione, aby można było uznać określony wymóg za zrealizowany. Jeśli wszystkie wymagania dla danego programu zostały spełnione, można uznać, że OpenChain jest zgodny z wersją 1.1 specyfikacji. Poszczególne elementy do weryfikacji nie zostaną upublicznione, ale mogą być dostarczone w ramach NDA(klauzuli o zachowaniu poufności) lub na prywatne żądanie organizacji OpenChain w celu potwierdzenia zgodności.

DEFINICJE

FOSS (Wolne/Otwarte Oprogramowanie) - oprogramowanie podlegające jednej lub więcej licencji, które spełniają definicję Open Source opublikowaną przez Inicjatywę Open Source (OpenSource.org) lub Definicję Wolnego Oprogramowania (opublikowaną przez Free Software Foundation) lub podobną licencję.

FOSS Liaison (Łącznik FOSS) - wyznaczona osoba otrzymująca zewnętrzne zapytania dotyczące FOSS

Zidentyfikowane Licencje - zestaw licencji FOSS zidentyfikowanych w wyniku zastosowania odpowiedniej metody identyfikacji takich licencji.

Zgodny z OpenChain - program, który spełnia wszystkie wymagania niniejszej specyfikacji.

Pracownicy oprogramowania - każdy pracownik lub wykonawca, który określa, przyczynia się lub jest odpowiedzialny za przygotowanie dostarczonego oprogramowania. W zależności od organizacji, która może obejmować (ale nie ogranicza się do) programistów, inżynierów odpowiadających za publikację, inżynierów wysokiej jakości, marketingu produktów i zarządzania produktami.

SPDX (Software Package Data Exchange) - standardowy format utworzony przez Grupę Roboczą SPDX w celu wymiany informacji o licencjach i prawach autorskich dla danego pakietu oprogramowania. Opis specyfikacji SPDX można znaleźć pod adresem www.spdx.org.

Dostarczane oprogramowanie- oprogramowanie, które jest dostarczane przez organizację osobą trzecim (np. inne organizacje, osoby prywatne)

Przesłanki weryfikacyjne – elementy, które muszą istnieć aby dany wymóg został spełniony

WYMAGANIA

G1: poznaj swoje obowiązki związane z FOSS

- 1.1 Istnienie pisemnej polityki FOSS, regulującej zgodność licencji oprogramowania FOSS podlegającego dystrybucji. Polityka ta musi być wewnętrznie zintegrowana.

Przesłanki weryfikacyjne:

1.1.1 Istnienie udokumentowanej polityki FOSS

1.1.2 Istnienie udokumentowanej procedury, która sprawia, że wszyscy pracownicy oprogramowania wiedzą o istnieniu polityki FOSS (np. Poprzez szkolenia, komunikację wewnętrzną lub inną metodę komunikacji praktycznej).

Uzasadnienie:

Upewnij się, że podjęto kroki w celu tworzenia, rejestrowania i informowania personelu oprogramowania o istnieniu polityki FOSS. Mimo tego, że nie ma żadnych sprecyzowanych wymogów dotyczących tego, co powinno być zawarte w polityce, inne działy specyfikacji mogą nakładać wymagania dotyczące tej polityki.

- Obowiązkowe szkolenie FOSS dla wszystkich pracowników oprogramowania przedstawia się następująco:
- Szkolenie obejmuje co najmniej tematy takie jak :
 - ◆ Polityka firmy FOSS i gdzie należy odszukać kopię zapasową ;
 - ◆ Podstawy prawa własności intelektualnej dotyczące licencji FOSS i FOSS;
 - ◆ Koncepcje licencjonowania oprogramowania FOSS (w tym pojęcia związane z dopuszczalnością i nadaniem oprogramowaniu statusu wolnego oprogramowania));
 - ◆ Modele licencjonowania projektów FOSS;
 - ◆ Rola personelu związanego oprogramowaniem i obowiązki związane z FOSS w szczególności i ogólnie z polityką FOSS;
 - ◆ Proces identyfikacji, zapisu i / lub śledzenia komponentów oprogramowania FOSS zawartych w dostarczonym oprogramowaniu.
- Pracownicy oprogramowania muszą ukończyć szkolenie w zakresie oprogramowania FOSS w ciągu ostatnich 24 miesięcy (należy to uznać za bieżący). Osiągnięcie celów szkolenia może być sprawdzone za pomocą testu.

Przesłanki weryfikacyjne:

1.1.1 Istnienie materiałów szkoleniowych FOSS dotyczących powyższych tematów (np. pokazy slajdów, kursy online lub inne materiały szkoleniowe);

1.1.2 Możliwość śledzenia postępów szkolenia do momentu jego ukończenia, dla wszystkich pracowników związanych z oprogramowaniem

1.1.3 Co najmniej 85% pracowników związanych z oprogramowaniem jest obecnych na szkoleniu, zgodnie z definicją w powyższym punkcie.

Uzasadnienie

Upewnij się, że pracownicy oprogramowania odbyli niedawno szkolenie w zakresie oprogramowania FOSS i że wszystkie najistotniejsze tematy zostały na nim poruszone. Istotą tego jest stworzenie podstawy tematów omawianych na szkoleniu, tak aby program szkoleniowy, rozwijał poszczególne kwestie niniejszej specyfikacji.

1.3 Istnienie możliwości sprawdzenia identyfikowanych licencji w celu określenia obowiązków, ograniczeń i praw przyznanych przez każdą licencję.

Przesłanki weryfikacyjne

1.3.1 Istnienie udokumentowanej procedury w celu sprawdzenia i udokumentowania obowiązków, ograniczeń i praw przyznanych przez każdą identyfikowaną licencję zawartą w dostarczonym oprogramowaniu.

Uzasadnienie

Celem jest zapewnienie istnienia procedury sprawdzającej i identyfikacyjnej obowiązków licencyjnych dla każdej zidentyfikowanych licencji w różnych przypadkach użytkowania.

G2: Przypisanie Odpowiedzialności za Osiągnięcie Zgodności

2.1 Identyfikacja funkcji łącznikowej FOSS ("Łącznik FOSS")

- Wyznaczenie osób (osoby) odpowiedzialnych za obieranie i odpowiadanie na zapytania z zewnątrz, które dotyczą FOSS
- Łącznik FOSS musi podejmować uzasadnione komercyjnie działania, aby odpowiednio reagować na zapytania dotyczące zgodności z FOSS.
- Podanie do publicznej wiadomości sposobu, za pomocą którego można się skontaktować z przedstawicielem FOSS.

Przesłanki weryfikacyjne :

2.1.1 Funkcja łączności z FOSS jest publicznie dostępna (np. Za pośrednictwem opublikowanego adresu e-mail kontaktowego lub katalogu Open Compliance Linux Foundation).

2.1.2 Istnieje wewnętrzna udokumentowana procedura, która wyznacza odpowiedzialność za otrzymywane pytania o zgodność z systemem FOSS.

Uzasadnienie

Zapewnienie sprawnego sposobu kontaktowania osobą trzecimi z organizacją w odniesieniu do pytań o zgodność z systemem FOSS i efektywne sprawowania tej odpowiedzialności.

2.2 Identyfikacja wewnętrznej roli Zgodności z systemem FOSS

- Wyznaczenie osób (osoby) odpowiedzialnych za zarządzanie wewnętrzną zgodnością z FOSS. Zarządzanie zgodnością z systemem FOSS i kontakty z FOSS mogą być wykonywane przez tą samą osobę.
- Działalność w zakresie zarządzania zgodnością z przepisami FOSS jest wystarczająco sfinansowana.
 - Przydzielono odpowiedni czas na realizację tego zadania .
 - Przydzielono rozsądny budżet w potrzebnym zakresie.
- Wyznaczenie zakresu odpowiedzialności za opracowanie i utrzymanie po i procesów zgodnych z FOSS.
- Znajomość prawna dotycząca zgodności z FOSS jest dostępna dla obszaru Zgodność z systemem FOSS (np. Może być wewnętrzna lub zewnętrzna).
- Istnienie procesu umożliwiającego rozwiązywanie problemów związanych z FOSS.

Przesłanki weryfikacyjne :

2.2.1 Nazwa osoby, grupy lub funkcji w obszarze Zgodności z oprogramowaniem FOSS zidentyfikowanych wewnętrznie.

2.2.2 Identyfikacja źródła analizy prawnej dostępnej dla obszaru Zgodność z przepisami FOSS, która może być wewnętrzna lub zewnętrzna.

2.2.3 Istnienie udokumentowanej procedury, która przypisuje wewnętrzną odpowiedzialność za zgodność z systemem FOSS.

2.2.4 Udostępniono udokumentowaną procedurę zajmującą się sprawdzeniem i ewentualnym wprowadzeniem procedury naprawczej, gdy jakieś wymogi nie zostały spełnione

Uzasadnienie :

Należy upewnić się, że określone obowiązki związane z FOSS zostały właściwie przypisane.

G3: Przeglądanie i zatwierdzanie treści FOSS

3.1 Istnienie procesu tworzenia i zarządzania zbiorem elementów FOSS, który uwzględnia każdą jego część (i jego zidentyfikowane licencje) w wydaniu dostarczonym z oprogramowaniem.

Przesłanki weryfikacyjne :

3.1.1 Istnienie udokumentowanej procedury umożliwiającej identyfikację, śledzenie i archiwizację informacji dotyczących gromadzenia elementów FOSS, z których składa się pakiet dostarczonego oprogramowania

3.1.2 Rejestry poszczególnych elementów FOSS istnieją dla każdego dostarczonego oprogramowania, wskazują na istnienie udokumentowanej procedury, która została poprawnie przeprowadzona.

Celem jest zapewnienie istnienia procesu tworzenia i zarządzania zastawieniem materiałów wykorzystywanych do konstruowania dostarczonego oprogramowania FOSS. Potrzebny jest zestaw materiałów niezbędnych do systematycznego przeglądu wszystkich postanowień licencyjnych każdego elementu w celu poznania obowiązków i ograniczeń dotyczących dystrybucji dostarczonego oprogramowania.

3.2 Program zarządzania FOSS musi być zdolny do obsługi wspólnych przypadków wykorzystania licencji oprogramowania FOSS, napotkanych przez personel oprogramowania dostarczony w ramach oprogramowania, które mogą obejmować następujące przypadki użycia (należy pamiętać, że lista nie jest wyczerpująca ani nie dotyczy wszystkich przypadków użycia):

- Rozpowszechniane w formie binarnej.
- Rozpowszechniane w formie źródłowej.
- Zintegrowane z innym oprogramowaniem FOSS, które może powodować powstanie obowiązków związanych z kopiowaniem,
- Zawiera zmodyfikowany FOSS.
- Zawiera oprogramowanie FOSS lub inne oprogramowanie na licencji niezgodnej z interakcją z innymi składnikami dostarczonego oprogramowania.
- Zawiera FOSS z wymaganiami atrybucji.

Przesłanki weryfikacyjne :

Wdrożono procedurę odpowiadającą za wspólne przypadki użycia licencji oprogramowania FOSS, we wszystkich jego wydaniach.

Uzasadnienie :

Zapewnienie, że program jest dostatecznie odporny, aby obsługiwać często używane przez organizację licencje na oprogramowanie FOSS oraz że istnieje procedura wspierania tej działalności i przestrzegania tej procedury.

G4: Dostarczanie dokumentacji treści FOSS i poszczególnych elementów

4.1 Przygotowanie zestawu elementów, które stanowią wynik programu zarządzania FOSS dla każdego wydania oprogramowania, które zostało dostarczone. Zestaw ten określa się jako elementy zgodności, które mogą obejmować (ale nie ograniczają do nich) co najmniej jeden z następujących elementów: kod źródłowy, uwagi o przypisaniu, powiadomienia o prawach autorskich, kopie licencji, powiadomienia o modyfikacjach, pisemne oferty, dokumenty SPDX itd.

Przesłanki weryfikacyjne :

4.1.1 Istnienie udokumentowanej procedury zapewniającej, że elementy zgodności są przygotowywane i dystrybuowane wraz z dostarczonym oprogramowaniem wraz z odpowiednimi licencjami.

4.1.2. Kopie elementów zgodności dostarczonych wersji oprogramowania są archiwizowane i łatwe do odszukania. Istnienie archiwum powinno być zaplanowane przynajmniej na czas, gdy dostarczane oprogramowanie jest oferowane lub wymagane przez określone licencje (w zależności od tego, który termin jest dłuższy).

Uzasadnienie :

Należy się upewnić, że kompletne zbiory elementów zgodności są dołączone do dostarczonego oprogramowania zgodnie z wymaganiami określonych przez Licencje, które to wymagania regulują Dostarczone Oprogramowanie wraz z innymi raportami tworzonymi w ramach procesu przeglądu FOSS.

G5: zrozumienie istoty zaangażowania społeczności FOSS

5.1 Istnienie polityki pisemnej, regulującej wkład do organizacji FOSS w projekty FOSS. Polityka ta musi być wewnętrznie skomunikowana.

Przesłanki weryfikacyjne :

5.1.1 Istnienie udokumentowanej polityki wkładu na rzecz FOSS. 5.1.2 Istnienie udokumentowanej procedury, która sprawia, że wszyscy pracownicy oprogramowania zdają sobie sprawę z istnienia polityki wkładu na rzecz FOSS (np. Poprzez szkolenia, wewnętrzną komunikację lub inną praktyczną metodę komunikacji).

Uzasadnienie:

Należy się upewnić, że organizacja rozsądnie rozważyła opracowanie polityki dotyczącej publicznego udziału w FOSS. Polityka wkładu FOSS może zostać włączona do ogólnej polityki FOSS organizacji lub być odrębną polityką. W sytuacji, w której wkład jest w ogóle niedozwolony, powinna istnieć polityka, która jasno o tym stanowi.

5.2 Jeśli organizacja zezwala na wkładna projekty FOSS, musi istnieć jakiś proces, który implementuje politykę wkładu FOSS opisaną w sekcji 5.1.

5.2.1 Zapewnienie istnienia polityki wkładu FOSS, regulującej kwestie składek na rzecz FOSS i istnienie udokumentowanej procedury regulującej te składki.

Uzasadnienie :

Upewnij się, że organizacja posiada udokumentowany proces tego, w jaki sposób organizacje publiczne uczestniczą w programie FOSS. Może istnieć taka polityka, która w ogóle nie zezwala na wkład . W tej sytuacji rozumie się, że żadna procedura nie istnieje i wymóg ten został spełniony.

G6: poświadczenie zgodności z wymaganiami OpenChain

6.1 Aby organizacja uzyskała certyfikat OpenChain, musi potwierdzić, że posiada program zarządzania FOSS, który spełnia kryteria opisane w niniejszej specyfikacji OpenChain w wersji 1.1.

Przesłanki weryfikacyjne :

6.1.1 Organizacja potwierdza istnienie programu zarządzania FOSS, który spełnia wszystkie wymagania niniejszej specyfikacji OpenChain w wersji 1.1

Uzasadnienie:

Aby zapewnić, że organizacja posiada program zgodny z OpenChain oświadcza, że program ten spełnia wszystkie wymagania specyfikacji. Spełnienie jedynie niektórych wymogów potrzebnych do uznania programu za OpenChain nie jest wystarczające do uznania programu za OpenChain.

6.2 Zgodność z tą wersją specyfikacji trwa 18 miesięcy od daty zatwierdzenia zgodności. Wymagania walidacji zgodności można znaleźć na stronie internetowej projektu OpenChain.

Przesłanki weryfikacyjne :

6.2.1 Organizacja potwierdza istnienie programu zarządzania FOSS, który spełnia wszystkie wymagania niniejszej specyfikacji OpenChain w wersji 1.1 w ciągu ostatnich 18 miesięcy od momentu zatwierdzenia zgodności.

Uzasadnienie:

Ważne jest, aby organizacja pamiętała o aktualizacji wdrożonych rozwiązań w stosunku do specyfikacji, jeśli chce uzyskać nadmiarowość w programie. Spełnienie tego wymogu zapewnia, że procesy wspomagające i sterowanie programem nie ulegają zniszczeniu, jeżeli chcą kontynuować zgodność z danymi nadmiarowymi .

Dodatek I: Tłumaczenia językowe

Aby ułatwić globalne przyjęcie, zapraszamy do podjęcia wysiłku i przetłumaczenia specyfikacji na wiele języków. Ponieważ OpenChain działa jako projekt Open Source, tłumaczenia są realizowane przez tych, którzy chcą poświęcić swój czas i wiedzę ekspercką, aby wykonać tłumaczenia zgodnie z licencją CC-BY 4.0 i polityką tłumaczeń projektu. Szczegóły dotyczące polityki i dostępne tłumaczenia można znaleźć na stronie internetowej projektu OpenChain.