OPENCHAIN

Spécifications OpenChain

Version 1.1

Table des matières

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.

Le présent document est la traduction officielle du projet OpenChain à partir du texte anglais original. En cas de contradiction entre cette traduction et la version anglaise, le texte original fait foi.

1) Introduction

L'Initiative OpenChain a débuté en 2013 quand un groupe de professionnels de l'open source a observé deux tendances émergentes : 1) des similarités significatives existent entre les processus d'organisations ayant un programme de conformité open source mâture ; et 2) il existe encore un grand nombre d'organisations échangeant du logiciel ayant des programmes de conformité moins développés. Cette dernière observation a entraîné un manque de confiance dans la cohérence et la qualité des livrables de conformité accompagnant le logiciel échangé. En conséquence, à chaque maillon de la chaîne d'approvisionnement, les organisations en aval refaisaient régulièrement le travail de conformité déjà réalisé par les organisations en amont.

Un groupe d'étude fût formé pour évaluer si une spécification d'un programme standard pourrait être créée qui permettrait de : i) faciliter une meilleure qualité et cohérence des informations de conformité open source partagées au travers de l'industrie ; et ii) diminuer les coûts transactionnels élevés associés à l'open source résultant de la nécessité de revoir la conformité. Le groupe d'étude a évolué en un groupe de travail, et en avril 2016, organisé formellement en tant que projet collaboratif de la Fondation Linux.

La Vision et la Mission de l'initiative OpenChain sont les suivantes :

- **Vision :** Une chaîne d'approvisionnement logicielle dans laquelle le logiciel libre et/ou open source est fourni avec des informations de conformité fiables et cohérentes.
- **Mission :** Établir les exigences pour atteindre une gestion efficace des logiciels libre et/ou open source pour les participants de la chaîne d'approvisionnement logicielle, afin que les exigences et garanties associées soient développées collaborativement et ouvertement par les représentants de la chaîne d'approvisionnement logicielle, la communauté open source, et le monde académique.

En accord avec la Vision et la Mission, cette spécification définit un jeu d'exigences qui, si satisfaites, améliorera significativement la probabilité qu'un programme de conformité open source ait achevé un niveau suffisant de qualité, cohérence et complétude ; bien qu'un programme qui satisfasse toutes les exigences de la spécification ne garantisse pas une conformité complète. Les exigences représentent un jeu d'exigences de base (minimum) qu'un programme doit satisfaire pour être considéré Conforme à OpenChain. La spécification se concentre sur les qualités des "quoi" et "pourquoi" d'un programme de conformité et non aux considérations des "comment" et "quand". Ceci assure un niveau --réaliste-- de flexibilité qui permet aux différentes organisations d'adapter leurs politiques et processus pour mieux atteindre leurs objectifs.

La section 2 introduit les définitions et termes clés utilisés tout au long de la spécification. La section 3 présente les exigences de la spécification avec pour chacune une liste d'un ou plusieurs Points de Vérification. Ils représentent la preuve qui doit exister pour considérer une exigence donnée satisfaite. Si toutes les exigences ont été satisfaites pour un programme donné, il sera considéré Conforme à OpenChain en accord avec la version 1.1 de cette spécification. Les Points de Vérification ne sont pas destinés à être

publics, mais pourraient être fournis sous Accord de Confidentialité ou sur demande privée de l'organisation OpenChain pour valider la conformité.

2) Définitions

FOSS (Free and Open Source Software, logiciel libre et/ou open source) - logiciel soumis à une ou plusieurs licences qui respecte l'Open Source Definition publiée par l'Open Source Initiative (OpenSource.org) ou la Free Software Definition (publiée par la Free Software Foundation) ou licence similaire.

Correspondant FOSS - une personne chargée de recevoir les demandes externes de renseignement sur les FOSS.

Licences Identifiées - un ensemble de licences FOSS identifiées comme résultat d'une méthode appropriée d'identification de telles licences.

Conforme à OpenChain - un programme qui satisfait toutes les exigences de cette spécification.

Équipe Logiciel - tout employé ou consultant qui définit, contribue à, ou est responsable de préparer, le Logiciel Fourni. En fonction des organisations, ceci peut inclure (mais n'est pas limité à) les développeurs logiciel, les ingénieurs de version, les ingénieurs qualité, les responsables produit et marketing produit.

SPDX ou Software Package Data Exchange (Echange de Données de Paquet Logiciel) - le format standard créé par le Groupe de Travail SPDX pour les informations de licence et de droits d'auteur pour un paquet logiciel donné. Une description de la spécification SPDX peut être trouvée sur le site www.spdx.org.

Logiciel Fourni - logiciel qu'une organisation fournit à des tierces parties (i.e., personnes morales et/ou physiques).

Points de Vérification - preuve qui doit exister pour qu'une exigence puisse être considérée comme satisfaite.

3) Exigences

G1: Connaître vos responsabilités vis-à-vis des FOSS

1.1 Il existe une politique formelle relative aux FOSS qui régit la conformité aux licences FOSS pour la distribution du Logiciel Fourni. Cette politique doit être communiquée en interne.

Point(s) de vérification :

• 1.1.1 Il existe une politique FOSS documentée.

• 1.1.2 Il existe une procédure documentée informant l'Équipe Logiciel de l'existence d'une politique FOSS (par exemple, via formation, wiki interne, ou autre moyen de communication).

Raison :

S'assurer que l'Équipe Logiciel ait été informée de l'existence d'une politique FOSS. Bien qu'aucune exigence ne soit fournie ici sur ce que la politique devrait contenir, d'autres sections peuvent définir des exigences sur son contenu..

1.2 Il existe une formation sur le FOSS, obligatoire pour l'Équipe Logiciel, qui :

- Au minimum, couvre les sujets suivants :
  - La politique FOSS et où en trouver une copie ;
  - Les bases de la Propriété Intellectuelle en relation avec le FOSS et les licences FOSS ;
  - Les concepts des licences FOSS (y compris les concepts de licence permissive et copyleft) ;
  - Les modèles de licences de projet FOSS ;
  - Les rôles et responsabilités de l'Équipe Logiciel vis-à-vis de la politique FOSS en général et de la conformité FOSS en particulier ; et
  - Les processus pour identifier, enregistrer et tracer les composants FOSS contenus dans le Logiciel Fourni.
- L'Équipe Logiciel doit avoir reçu cette formation FOSS dans les derniers 24 mois (pour être considérée valide). Un test peut être utilisé pour permettre à l'Équipe Logiciel de satisfaire cette exigence de formation.

Point(s) de vérification :

• 1.2.1 Il existe un support de formation au FOSS couvrant les sujets mentionnés ci-dessus (par exemple, diapositives de présentation, cours en ligne, ou autre support de formation).

• 1.2.2 Méthode de suivi de la participation à la formation par l'Équipe Logiciel.

• 1.2.3 Au moins 85% de l'Équipe Logiciel est à jour, tel que défini ci-dessus.

Raison :

S'assurer que l'Équipe Logiciel a récemment participé à la formation FOSS et qu'un ensemble clé des sujets liés au FOSS est couvert. L'intention est d'assurer qu'un ensemble clé de sujets de base est couvert mais un programme typique de formation serait susceptible d'être plus complet que ce qui est requis ici.

1.3 Il existe un processus pour revoir les Licences Identifiées pour déterminer leurs obligations, restrictions et droits accordés par chacune des licences.

Point(s) de vérification :

• 1.3.1 Il existe une procédure documentée pour contrôler et décrire les obligations, restrictions et droits accordés par chacune des Licences Identifiées gouvernant le Logiciel Fourni.

Raison :

S'assurer qu'il existe un processus pour contrôler et identifier les obligations des licences pour les cas d'usage donnés pour chaque Licence Identifiée.

G2: Attribuer les responsabilités pour atteindre la conformité

2.1 Créer un rôle de Correspondant FOSS ("Correspondant FOSS").

Attribuer à une ou plusieurs personne la responsabilité de traiter les demandes FOSS externes ;

Le Correspondant FOSS doit s'appliquer, dans une limite raisonnable d'un point de vue commercial, à traiter correctement les demandes de conformité FOSS ; et

Indiquer publiquement un moyen simple de joindre le Correspondant FOSS.

Point(s) de vérification :

• 2.1.1 Le Correspondant FOSS est identifiable publiquement (ex.: par une adresse email de contact publique ou via l'annuaire Open Compliance Directory de la Linux Foundation).

• 2.1.2 Il existe une procédure interne documentée qui attribue la responsabilité de traiter les demandes de conformité FOSS.

Raison :

S'assurer qu'il soit raisonnablement facile à un tiers de contacter l'entité pour lui adresser ses demandes relatives à la conformité FOSS et que la responsabilité de les traiter a bien été attribuée.

2.2 Créer le(s) rôle(s) de responsable de la conformité FOSS interne.

Attribuer à une ou plusieurs personnes la responsabilité de la gestion de la conformité FOSS en interne. Les rôles de responsable de la conformité FOSS et celui de Correspondant FOSS peuvent être assumés par la même personne.

L'activité de conformité FOSS doit disposer de ressources suffisantes :

Suffisamment de temps a été alloué pour effectuer les tâches du rôle ;

Un budget raisonnable du point de vue commercial lui est consacré.

Attribuer les responsabilités pour définir et tenir à jour la politique et les processus de conformité FOSS ;

Le ou les responsables de la conformité FOSS doivent avoir accès à l'expertise juridique nécessaire (elle peut être interne ou externe); et

Un processus est en place pour résoudre les problèmes de conformité FOSS.

Point(s) de vérification :

- 2.2.1 Il existe une liste de personnes en charge de la gestion de la conformité FOSS en interne.
- 2.2.2 L'expertise juridique, interne ou externe, accessible aux responsables de la conformité FOSS, a été identifiée.
- 2.2.3 Il existe une procédure documentée pour attribuer les responsabilités internes pour la gestion de la conformité FOSS.
- 2.2.4 Il existe une procédure documentée pour la vérification de la conformité et le traitement des cas de non-conformité.

Raison :

S'assurer que les responsabilités pour la gestion de la conformité FOSS ont bien été attribuées.

G3: Contrôler et valider le contenu FOSS

3.1 Il existe une procédure pour créer et gérer une liste exhaustive des composants FOSS et de leurs licences associées ("bill of materials") pour chaque version du Logiciel Fourni.

Point(s) de vérification :

• 3.1.1 Il existe une procédure documentée pour identifier, tracer et archiver les informations sur l'ensemble des composants FOSS inclus dans chaque version publiée du Logiciel fourni.

• 3.1.2 Il existe des documents relatifs aux composants FOSS pour chacune des version publiée du Logiciel fourni, montrant que la procédure documentée a été suivie correctement.

Raison :

S'assurer qu'il existe une procédure pour créer et gérer une liste des composants FOSS ayant servi à la réalisation du Logiciel fourni. Cette liste est nécessaire au contrôle systématique des termes des licences des composants afin d'appréhender correctement l'ensemble des obligations et restrictions qui en découlent dans le cadre de la distribution du Logiciel fourni.

3.2 Le programme de gestion des questions FOSS doit être en mesure de gérer les cas d'usage courants de licences FOSS auxquels peut être confrontée l'Équipe Logiciel pour le Logiciel fourni, qui peuvent être notamment les suivants (cette liste n'est pas exhaustive et certains exemples peuvent ne pas s'appliquer à votre contexte) :

- distribution sous forme de binaire;
- distribution sous forme de code source;
- intégration avec d'autres logiciels FOSS qui peuvent déclencher des obligations liées au copyleft;
- inclusion de logiciels FOSS modifiés;
- inclusion de logiciels FOSS ou propriétaires diffusés sous des licences incompatibles dans le cadre de leur interaction au sein du Logiciel fourni; et/ou
- inclusion de composants FOSS portant des obligations de mentions de paternité.

Point(s) de vérification :

• 3.2.1 Une procédure a été mise en place pour traiter les cas courants d'usage des licences FOSS pour les composants FOSS de toutes les versions du Logiciel fourni.

Raison :

S'assurer que le programme est suffisamment complet pour traiter les cas d'usage de licences FOSS couramment rencontrés par l'entité, qu'il existe une procédure pour mettre en œuvre cette activité et que cette procédure est suivie.

G4: Fourniture des documentations et livrables FOSS

4.1 Préparer l'ensemble des livrables qui représente la sortie du programme de gestion des FOSS pour chacune des versions du Logiciel Fourni. Cet ensemble correspond aux Livrables de Conformité qui peuvent inclure (mais ne sont pas limités à) un ou plusieurs des éléments suivants : code source, notices d'attribution, notices de droits d'auteur, copie des licences, notifications de modifications, offres écrites, documents SPDX et ainsi de suite.

Point(s) de vérification :

• 4.1.1 Il existe une procédure documentée qui assure que les Livrables de Conformité sont préparés et distribués avec les versions du Logiciel Fourni comme requis par les Licences Identifiées.

• 4.1.2 Des copies des Livrables de Conformité de la version du Logiciel Fourni sont archivées et facilement accessibles, et une archive est planifiée pour être disponible tant que le Logiciel Fourni est proposé ou que celle-ci est requise par les Licences Identifiées (le plus long des deux).

Raison :

S'assurer qu'une collection complète des Livrables de Conformité ainsi que les rapports créés dans le cadre du processus de revue des FOSS accompagnent le Logiciel Fourni comme requis par les Licences Identifiées qui gouvernent le Logiciel Fourni.

G5: Comprendre l'implication dans les communautés FOSS

5.1 Il existe une politique formelle pour cadrer les contributions de l'entité aux projets FOSS. Cette politique doit être communiquée en interne.

Point(s) de vérification :

• 5.1.1 Il existe une politique de contribution FOSS documentée;

• 5.1.2 Il existe une procédure documentée informant l'Équipe Logiciel de l'existence d'une politique de contribution FOSS (par exemple, via formation, wiki interne, ou tout autre moyen de communication).

Raison :

S'assurer que l'entité a suffisamment pris en compte la question de la contribution publique aux projets FOSS et a élaboré une politique à ce sujet. Cette politique de contribution FOSS peut faire partie de la politique FOSS générale ou constituer un document distinct. Pour les cas où les contributions sont systématiquement interdites, une politique doit expliciter cette position.

5.2 Si l'entité autorise les contributions aux projets FOSS, elle doit mettre en place les processus pour implémenter la politique de contribution FOSS mentionnée à la Section 5.1.

Point(s) de vérification :

• 5.2.1 Si la politique de contribution FOSS autorise les contributions, elle doit s'accompagner de processus documentés précisant les modalités de celles-ci.

Raison :

S'assurer que l'entité dispose de processus documentés pour contribuer publiquement aux projets FOSS. Il se peut que la politique en la matière soit d'interdire toute contribution. Dans de tels cas, l'absence de processus dédiés est légitime et la présente exigence sera considérée comme respectée.

G6: Attester sa conformité aux exigences OpenChain

6.1 Pour être certifiée OpenChain, une entité doit attester disposer d'un programme de gestion des logiciels FOSS qui réponde aux critères énoncés dans la présente version 1.1 de la spécification OpenChain.

Point(s) de vérification :

• 6.1.1 L'entité atteste qu'elle dispose d'un programme de gestion des logiciels FOSS répondant à l'ensemble des exigences de la version 1.1 de la spécification OpenChain.

Raison :

S'assurer, que, si une entité déclare disposer d'un programme conforme à OpenChain, ce programme réponde effectivement à l'ensemble des exigences de la présente spécification. La simple observation d'un sous-ensemble de ces exigences est insuffisante pour attribuer la certification OpenChain à un programme.

6.2 La conformité avec cette version de la spécification dure 18 mois à partir de la date de la validation de cette conformité. Les critères de validation de la conformité sont disponibles sur le site Web du projet OpenChain.

Point(s) de vérification :

• 6.2.1 L'entité atteste disposer d'un programme de gestion des logiciels FOSS qui répond à l'ensemble des exigences de la spécification OpenChain dans sa version 1.1 au cours des 18 mois précédant la date de validation.

Raison :

Il est important que l'entité reste en phase avec la spécification si elle souhaite continuer à pouvoir afficher sa conformité. Cette exigence permet de garantir que les processus implémentant le programme de conformité et leur vérification ne se dégradent pas avec le temps.

Annexe I : Traductions

Afin de faciliter l'adoption d'OpenChain au niveau mondial, nous encourageons la traduction des spécifications en différentes langues. OpenChain fonctionne comme un projet Open Source : les traductions sont assurées par des volontaires souhaitant y consacrer leur temps et leur expertise et placer le résultat sous licence CC-BY 4.0, selon la politique de traduction du projet. Les détails de la politique et ses traductions sont disponibles sur le site Web de la spécification OpenChain.