SPÉCIFICATIONS OPENCHAIN

Version 2.0

Renforcer la confiance dans les logiciels Open Source sur lesquels reposent vos solutions

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

Ces spécifications définissent les exigences fondamentales pour un Programme de conformité Open Source de qualité. L'objectif est de fournir un point de repère à même de renforcer la confiance entre organisations échangeant des logiciels contenant des composants Open Source. Le respect de ces Spécifications assure qu'un Programme a été mis en œuvre pour produire les livrables de conformité (ex : notices juridiques, code source, etc.) pour chacun des logiciels. Les spécifications Open Chain se concentrent plus sur le "quoi" et le "pourquoi" d'un programme de conformité que sur le "comment" et "quand" Cela permet d'offrir à des organisations de tailles différentes, opérant dans des marchés différents, une flexibilité suffisante pour choisir des politiques et des processus qui soient adaptés à leurs tailles et objectifs spécifiques ainsi qu'aux périmètres qu'elles visent. Par exemple, un Programme conforme à OpenChain peut porter sur une seule gamme de produits ou sur l'ensemble de l'organisation.

Cette introduction présente le contexte pour l'ensemble des utilisateurs potentiels. La section 2 définit les termes clés utilisés dans le cadre de la présente Spécification. La section 3 définit les exigences requises pour qu'un Programme soit considéré comme conforme. Chaque exigence est constituée d'un ou plusieurs Éléments de vérification ex. : documents spécifiques) qui doivent être produits pour qu'elle soit considérée comme satisfaite. Il n'est pas nécessaire que les Éléments de vérification soient rendus public, mais il est possible qu'une organisation choisisse de les communiquer à des tiers, éventuellement sous un accord de confidentialité (NDA).

La présente Spécification a été élaborée de manière ouverte et collaborative, grâce à la participation de plus de 150 contributeurs. La liste de diffusion et la FAQ de la Spécification offrent un bon aperçu de l'historique de son développement.

2) Définitions

« Livrables de conformité » - un ensemble de Livrables qui constituent la matérialisation du Programme pour le Logiciel Fourni. . Cet ensemble peut notamment comprendre : des code source, des notices d'attribution, des notices de droits d'auteur, des copies des licences, des notifications de modifications, des offres écrites de mise à disposition, une liste des composants Open Source (BOM) et des documents SPDX.

« Licences Identifiées » - Un ensemble de licences Open Source identifiées graĉe à une méthode pertinente pour identifier les composants Open Source intégrés au Logiciel Fourni.

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

« Open Source » - qualifie un 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.

« Programme » – Un ensemble de politiques, de processus et d'acteurs qui gèrent les activités de conformité aux licences Open Source au sein d'une organisation.

« Équipe Logiciel » - tout employé ou consultant qui définit, contribue à, ou est responsable de préparer, le Logiciel Fourni. En fonction des organisations, ceci peut notamment inclure les développeurs logiciel, les "relase managers", les ingénieurs qualité, les responsables produit et des intervenants du marketing.

« SPDX » - le format standard créé par le groupe de travail SPDX (Software Package Data Exchange) de la Linux Foundation pour l'échange de données de licences et de droits d'auteur pour un paquet logiciel donné.. Une description de la spécification SPDX est disponible sur le site www.spdx.org.

« Logiciel Fourni » - Logiciel qu'une organisation fournit à des tierces parties (personnes morales ou physiques).

« Éléménts de vérification » - éléments qui doivent exister pour qu'une exigence puisse être considérée comme satisfaite.

3) Exigences

1.0 Fondamentaux du Programme

1.1 Politique Open Source

Il existe une politique formelle pour cadrer la conformité aux licences Open Source contenues dans les Logiciels Fournis. Cette politique doit être communiquée en interne.

Élément(s) de vérification :

□ 1.1.1 Une politique Open Source documentée.

□ 1.1.2 Une procédure documentée informant l'Équipe Logiciel de l'existence de la politique Open Source (par exemple, via des formations, un wiki interne ou tout autre moyen de communication).

Raison :
S'assurer que les mesures ont été prises pour que l'Équipe Logiciel soit informée de l'existence de la politique Open Source. Bien qu'aucune exigence ne définisse ici les aspects à inclure dans cette politique, d'autres sections peuvent définir des exigences sur son contenu.

1.2 Compétences

L'organisation doit :

■ **Déterminer les rôles et les responsabilités associés qui garantissent l'efficacité et la pertinence du Programme ;**

■ **Déterminer les compétences nécessaire des personnes remplissant les différents rôles**

■ **S'assurer que ces personnes sont compétentes au regard de leur parcours académique, de formations suivies ou de leur expérience professionnelle ;**

■ **Le cas échéant, prendre des mesures pour acquérir les compétences nécessaires ; et**

■ **Conserver les documents nécessaires pour fournir la preuve de ces compétences.**

Élément(s) de vérification :

□ 1.2.1 Une liste détaillée des rôles et des responsabilités assoicées pour chaque participant au Programme.

□ 1.2.2 Un document qui détermine les compétences requises pour chaque rôle.

□ 1.2.3 Des documents attestant que les compétences de chaque participant au Programme ont été évaluées.

Raison :
S'assurer que les personnes choisies pour tenir les différents rôles du Programme disposent des compétences nécessaires pour assumer responsabilités qui en découlent.

1.3 Sensibilisation

L'organisation doit s'assurer que les participants au programme sont tenus informés de :

a) De sa politique Open Source ;

b) Des enjeux de l'Open Source ;

c) De leur contribution à la réussite du Programme, et

d) Des conséquences du non-respect des exigences du Programme.

Élément(s) de vérification :

□ 1.3.1 Preuves documentées que chaque membre du Programme a bien intégré, les objectifs du Programme, sa contribution au sein du Programme et les répercussions des manquements aux exigences du Programme.

Raison :
S'assurer que le personnel associé au Programme a obtenu un niveau de sensibilisation suffisant concernant ses rôles et responsabilités au sein du Programme.

1.4 Périmètre du Programme.

Différents programmes peuvent porter sur des périmètres différents. Par exemple, un Programme peut concerner une seule gamme de produits, un département entier ou l'ensemble de l'organisation. Chaque Programme doit explicitement énoncer le périmètre auquel il s'applique.

Élément(s) de vérification :

□ 1.4.1 Une déclaration écrite qui définit clairement la portée et les limites du Programme.

Raison :
Offrir à l'organisation la flexibilité nécessaire pour qu'elle élabore le Programme qui corresponde le mieux à ses besoins. Certaines organisations peuvent choisir de poursuivre un Programme pour une gamme de produits donnée, tandis que d'autres peuvent implémenter un Programme qui régit l'ensemble des Logiciels Fournis par l'organisation.

1.5 Obligations liées aux licences

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

Élément(s) de vérification :

□ 1.5.1 Une procédure documentée pour vérifier et documenter les obligations, restrictions et droits accordés par chaque Licence Identifiée.

Raison :
S'assurer qu'il existe un processus pour contrôler et identifier les obligations des licences pour chaque Licence Identifiée, et ce, pour chaque cas d'usage qu'une organisation est susceptible de rencontrer (comme défini à l'exigence 3.2)

2.0 Définition des tâches nécessaires et des ressources associées

2.1 Visibilité externe

Il existe un processus maintenu pour répondre efficacement aux demandes externes concernant la conformité Open Source. Un acteur externe doit pouvoir facilement identifier un moyen pour adresser une demande liée aux questions de conformité Open Source.

Élément(s) de vérification :

□ 2.1.1 Une méthode publiquement accessible qui permette à toute tierce partie de faire une demande liée aux questions de conformité(par exemple via une adresse email de contact publique ou l'annuaire Open Compliance Directory de la Linux Foundation).

□ 2.1.2 Une procédure interne documentée pour répondre à toute demande tierce ayant trait à la conformité Open Source.

Raison :
S'assurer qu'un tiers puisse raisonnablement contacter l'organisation pour lui adresser ses demandes relatives à la conformité Open Source, et que l'organisation est en mesure d'y répondre de manière efficace.

2.2 Ressources adaptées

Identifiez et attribuez des ressources aux tâches du programme :

■ Des responsables sont désignés pour assurer la bonne exécution des différentes tâches du Programme.

■ Les tâches du Programme disposent des ressources nécessaires :

- □ Un temps suffisant a été alloué pour la réalisation des tâches du Programme ;
- □ un budget adapté leur a été alloué.

■ Il existe un processus d'examen et de mise à jour de la politique et des tâches qui en découlent ;

■ L'expertise juridique sur la conformité des licences Open Source est accessible à ceux qui peuvent en avoir besoin; et

■ Un processus est mis en place pour résoudre les problèmes de conformité Open Source.

Élément(s) de vérification :

□ 2.2.1 Un document listant les noms des personnes, leur groupe ou leur fonction pour chaque rôle identifié au sein du Programme.

□ 2.2.2 Les rôles définis pour le Programme ont été suffisamment pourvus en personnel et un financement adéquat est prévu.

□ 2.2.3 Identification de l'expertise juridique disponible pour traiter les questions de conformité Open Source. L'expertise peut être interne ou externe.

□ 2.2.4 Une procédure documentée qui attribue les responsabilités internes correspondant à la gestion de la conformité Open Source.

□ 2.2.5 Une procédure documentée pour la vérification de la conformité et le traitement des cas de non-conformité.

Raison :

Assurer : i) que les responsabilités attribuées dans le cadre du Programme sont dotées de ressources et d'accompagnement suffisants. ii) que les processus et les politiques pour la mettre en œuvre sont régulièrement mis à jour pour tenir compte de l'évolution des bonnes pratiques en matière de conformité Open Source.

3.0 Contrôle et validation des composants Open Source

3.1 Liste exhaustive des composants

Il existe une procédure pour créer et gérer une liste exhaustive des composants Open Source et de leurs licences associées (« bill of materials ») pour chaque version du Logiciel Fourni.

Élément(s) de vérification :

□ 3.1.1 Une procédure documentée pour identifier, tracer, contrôler, approuver et archiver les informations sur l'ensemble des composants Open Source inclus dans le Logiciel fourni.

□ 3.1.2 Des documents relatifs aux composants Open Source pour le 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 exhaustive des composants Open Source 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 Conformité aux licences

Le Programme doit être en mesure de gérer les cas d'usage courants de licences Open Source auxquels peut être confrontée l'Équipe Logiciel pour le Logiciel fourni. Ces cas peuvent notamment être 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 Open Source qui peuvent déclencher des obligations liées aux clauses de réciprocité (copyleft) ;
- inclusion de logiciels Open Source modifiés;
- inclusion de logiciels Open Source ou propriétaires diffusés sous des licences incompatibles dans le cadre de leur interaction au sein du Logiciel Fourni; et/ou
- inclusion de composants Open Source portant des obligations de mentions de paternité.

Élément(s) de vérification :

□ 3.2.1 Une procédure documentée pour traiter les cas d'usages courants des licences Open Source des composants Open Source des Logiciels Fournis.

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

4.0 Création et fourniture des Livrables de Conformité

4.1 Livrables de conformité

Il existe une procédure pour créer l'ensemble des Livrables de conformité pour le Logiciels Fourni.

Élément(s) de vérification :

□ 4.1.1 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 Une procédure documentée pour archiver des copies des Livrables de Conformité de la version du Logiciel Fourni et qui précise une durée de conservation adaptée1 à compter de la date de la dernière offre pour le Logiciel fourni, ou conforme aux exigences des Licences Identifiées (selon la durée la plus longue). Des documents prouvent que la procédure a été correctement suivie.

Raison :

S'assurer que des efforts commerciaux raisonnables ont été déployés pour l'élaboration des Livrables de conformité correspondant au Logiciel Fourni, comme l'exigent les licences identifiées.

5.0 Maîtrise de la participation aux communautés Open Source

5.1 Contributions

Si une organisation autorise les contributions à des projets Open Source, alors

- Il existe une politique formelle pour cadrer les contributions aux projets Open Source ;
- Cette politique doit être communiquée en interne; et
- Il existe une procédure d'implémentation de la politique

Élément(s) de vérification :
Si une organisation autorise les contributions à des projets Open Source, alors les documents suivants doivent exister :

☐ 5.1.1 une politique de contribution Open Source documentée ;

☐ 5.1.2 une procédure documentée qui encadre les contributions Open source; et

☐ 5.1.3 une procédure documentée informant l'Équipe Logiciel de l'existence d'une politique de contribution Open Source (par exemple, via des formations, un wiki interne ou tout autre moyen de communication).

Raison :
Lorsqu'une organisation autorise des contributions Open Source, nous voulons nous assurer qu'elle a accordé une attention raisonnable à l'élaboration et à l'implémentation d'une politique de contribution. Cette politique de contribution Open Source peut figurer dans la politique générale Open Source ou dans un document distinct.

6.0 Conformité aux exigences des Spécifications

6.1 Respect des exigences

Pour qu'un programme soit certifié OpenChain, l'organisation doit attester qu'il répond aux exigences énoncées dans la présente Spécification.

Élément(s) de vérification :

□ 6.1.1 Un document confirmant que le Programme tel que décrit à l'exigence 1.4 satisfait à toutes les exigences de la présente spécification.

Raison :
S'assurer, que, si une organisation déclare disposer d'un programme conforme à OpenChain, ce programme réponde effectivement à l'ensemble des exigences de la présente spécification. Le simple respect d'un sous-ensemble de ces exigences est insuffisant

6.2 Durée

La conformité d'un programme avec cette version de la spécification OpenChain dure 18 mois à partir de la date de la validation de cette conformité. La procédure d'enregistrement de la validation de la conformité sont disponibles sur le site Web du projet OpenChain.

Élément(s) de vérification :

□ 6.2.1 Un document stipulant que le Programme répond à toutes les exigences de la présente spécification (version 2.0), au cours des 18 derniers mois suivant l'obtention de la validation de la conformité.

Raison :
Il est important que l'entité reste en phase avec la spécification si elle souhaite continuer à pouvoir afficher sa conformité dans la durée. 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.

Parce qu'OpenChain fonctionne comme un projet Open Source, ceux qui sont prêts à consacrer leur temps et leur expertise pour effectuer des traductions respectent la politique de traduction du projet, et soumettent ces dernières à la licence CC-BY-4.0. Les traductions et les détails de la politique sont disponibles sur le wiki du projet OpenChain.