Spécification OpenChain Version 2.1

Cette spécification est fonctionnellement identique à :

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

Pour en savoir plus : www.openchainproject.org

Table des matières

Introduction

Ce document définit les exigences fondamentales d'un programme de conformité aux licences open source de qualité. Son objectif est de fournir un point de référence qui instaure la confiance entre organisations qui échangent des solutions logicielles composées de logiciels open source. Le respect de cette spécification assure qu'un programme a été mis en œuvre pour produire les livrables de conformité (c.-à-d. notices juridiques, code source, etc.) pour chaque solution logicielle. Ce document se concentre sur le « quoi » et le « pourquoi » d'un programme de conformité plus que sur le « comment » et le « quand ». Ceci offre à des organisations de tailles différentes, opérant dans des marchés différents, la flexibilité nécessaire pour choisir des politiques et des processus spécifiques qui soient adaptés à leur taille, leurs objectifs ainsi qu'à leurs champs d'application. Un programme conforme à OpenChain peut par exemple porter sur une seule gamme de produits ou bien sur l'ensemble de l'organisation.

Cette introduction présente le contexte pour l'ensemble des utilisateurs potentiels. La clause 2 définit les termes clés utilisés dans le cadre du présent document. La clause 3 définit les exigences requises pour qu'un programme soit considéré comme conforme. Chaque exigence est constituée d'un ou plusieurs éléments de vérification (c.-à-d. archives) qui doivent être produits pour que l'exigence soit considérée comme satisfaite. Il n'est pas exigé que les éléments de vérification soient rendus publics mais une organisation peut choisir de les communiquer à des tiers, éventuellement sous entente de non-divulgation (END).23

Le présent document a été élaboré de manière ouverte et collaborative, grâce à la participation de plus de 200 contributeurs. L'historique de son développement peut être perçu à travers la lecture de la liste de diffusion et de la FAQ de la spécification.

Technologies de l'information - Spécification OpenChain

1 Champ d'application

Ce document spécifie les principales exigences d'un programme de conformité aux licences de logiciels open source de qualité afin de fournir un point de repère à même de renforcer la confiance entre organisations échangeant des logiciels contenant des composants open source.

2 Termes et définitions

Les termes et définitions suivants s'appliquent aux fins du présent document.

2.11
livrables de conformité
un ensemble de livrables qui constituent la matérialisation du programme de conformité et qui accompagnent pour le logiciel fourni

Remarque : cet ensemble peut notamment comprendre : des notices d'attribution, du code source, des scripts de construction et d'installation, des copies des licences, des notices de droits d'auteur, des notifications de modifications, des offres écrites de mise à disposition, une liste des composants open source (BOM) et des documents SPDX.

2.22
licences identifiées
un ensemble de licences open source identifiées grâce à une méthode pertinente pour identifier les composants open source intégrés au logiciel fourni

2.33
conforme à OpenChain
un programme qui satisfait toutes les exigences de cette spécification

2.44
open source
qualifie un logiciel soumis à une ou plusieurs licences qui respectent l'Open Source Definition publiée par l'Open Source Initiative (opensource.org/osd) ou la Free Software Definition publiée par la Free Software Foundation (gnu.org/philosophy/free-sw.html) ou une licence similaire

2.55
programme
l'ensemble de politiques, de processus et d'acteurs qui constituent les activités de conformité aux licences open source au sein d'une organisation

2.66
participants au programme
tout employé ou consultant qui définit, contribue à, ou est responsable de préparer, le logiciel fourni

Remarque : en fonction des organisations, ceci peut notamment inclure les développeurs de logiciels, les gestionnaires de version, les ingénieurs qualité, les responsables marketing et les chefs de produit.

2.77
SPDX
le format standard créé par le groupe de travail SPDX (Software Package Data Exchange) de la Linux Foundation pour l'échange de listes de composants pour un paquet logiciel donné, y compris les informations relatives aux licences et aux droits d'auteur

2.88
logiciel fourni
logiciel qu'une organisation fournit à une tierce partie (personne morale ou physique)

2.99
éléments de vérification
éléments qui démontrent qu'une exigence de la spécification est satisfaite

L'ISO et la CEI tiennent à jour des bases de données terminologiques destinées à la normalisation aux adresses suivantes :

— Plate-forme de navigation en ligne de l'ISO : https://www.iso.org/obp

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

3 Exigences

3.1 Fondamentaux du programme

3.1.1 Politique open source

Il doit exister une politique formelle qui régit la conformité aux licences open source contenues dans les logiciels fournis. Cette politique doit être communiquée en interne.

Élément(s) de vérification :

- 3.1.1.1 Une politique open source documentée.
- 3.1.1.2 Une procédure documentée qui informe les participants au programme de l'existence de la politique open source (par des formations, un wiki interne ou tout autre moyen de communication).

Raison :

S'assurer que des mesures ont été prises pour que les participants au programme soient informés de l'existence d'une 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.

3.1.2 Compétences

L'organisation doit

- Déterminer les rôles et les responsabilités associées qui garantissent la performance et l'efficacité du programme ;
- Déterminer les compétences nécessaires des participants au programme qui remplissent les différents rôles
- S'assurer que les participants au programme sont compétents au regard de leur parcours académique, des 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 :

- 3.1.2.1 Une liste détaillée des rôles et des responsabilités associées pour chaque participant au programme.
- 3.1.2.2 Un document qui détermine les compétences requises pour chaque rôle.
- 3.1.2.3 Des documents attestant que les compétences de chaque participant au programme ont été évaluées.

Raison :

S'assurer que les participants au programme ont atteint un niveau de compétence suffisant pour assumer leurs rôles et les responsabilités qui en découlent.

3.1.3 Sensibilisation

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

- sa politique open source ;
- des enjeux de l'open source ;
- de leur contribution à la réussite du programme, et
- des conséquences du non-respect des exigences du programme.

Élément(s) de vérification :

- 3.1.3.1 Preuves documentées que les participants au programme ont bien intégré les objectifs du programme, leur contribution au sein du programme et les répercussions des manquements aux exigences du programme.

Raison :

S'assurer que les participants au programme ont obtenu un niveau de sensibilisation suffisant pour assumer leurs rôles et les responsabilités qui en découlent au sein du programme.

3.1.4 Périmètre du programme

Différents programmes peuvent être régis par différents niveaux de périmètre. Par exemple, un programme peut ne concerner qu'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 :

- 3.1.4.1 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 correspond 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.

3.1.5 Obligations liées aux licences

Il doit exister un processus pour examiner les licences identifiées afin de déterminer les obligations, restrictions et droits accordés par chacune d'elles.

Élément(s) de vérification :

- 3.1.5.1 Une procédure documentée pour examiner et documenter les obligations, restrictions et droits accordés par chaque licence identifiée.

Raison :

S'assurer qu'il existe un processus pour examiner 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 en 3.3.2).3.3.2

3.2 Définition des tâches nécessaires et des ressources associées

3.2.1 Visibilité externe

Maintenir un processus afin de répondre efficacement aux demandes externes relatives au code open source. Identifier publiquement une méthode par laquelle une tierce partie peut effectuer une demande relative à la conformité des licences open source.

Élément(s) de vérification :

- 3.2.1.1 Une méthode publiquement accessible qui permet à toute tierce partie d'effectuer une demande relative à la conformité aux licences open source (au moyen d'une adresse courriel de contact rendue publique, de l'annuaire Open Compliance Directory de la Linux Foundation, etc.).
- 3.2.1.2 Une procédure interne documentée pour répondre aux demandes de tierces parties relatives à la conformité aux licences open source.

Raison :

S'assurer qu'il existe une méthode raisonnable pour une tierce partie de contacter l'organisation pour lui adresser ses demandes relatives à la conformité open source, et s'assurer que l'organisation est en mesure d'y répondre de manière efficace.

3.2.2 Ressources adaptées

Identifier et attribuer 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 de ressources suffisantes :
  - un temps suffisant a été alloué pour la réalisation des tâches du programme ; et
  - 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 relative à la conformité aux licences open source est accessible à ceux qui peuvent en avoir besoin ; et
- Un processus est en place pour la résolution des problèmes de conformité aux licences open source.

Élément(s) de vérification :

- 3.2.2.1 Un document comportant le nom des personnes, leur groupe ou leur fonction pour chaque rôle identifié au sein du programme.
- 3.2.2.2 Les rôles définis pour le programme ont été suffisamment pourvus en personnel et un financement adéquat a été fourni.
- 3.2.2.3 Identification de l'expertise juridique disponible pour traiter les questions de conformité aux licences open source. Cette expertise peut être interne ou externe.

- 3.2.2.4 Une procédure documentée qui attribue les responsabilités internes pour la conformité open source.
- 3.2.2.5 Une procédure documentée pour traiter l'examen et la correction des cas de non-conformité.

Raison :

S'assurer : i) que les responsabilités dans le cadre du programme sont efficacement soutenues et dotées de ressources et ii) que les politiques et les processus de soutien sont régulièrement mis à jour pour tenir compte des changements dans les meilleures pratiques de conformité à l'open source.

3.3 Examen et validation des contenus open source

3.3.1 Liste des composants

Il doit exister une procédure pour créer et gérer une liste de composants qui inclut chacun des composants (et leurs licences associées) qui constituent le logiciel fourni.

Élément(s) de vérification :

- 3.3.1.1 Une procédure documentée pour identifier, suivre, examiner, approuver et archiver les informations au sujet de l'ensemble des composants open source dont est composé le logiciel fourni.
- 3.3.1.2 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. Une liste des composants est nécessaire à l'examen et l'approbation systématique des termes des licences de chacun des composants afin de comprendre les obligations et restrictions qui en découlent dans le cadre de la distribution du logiciel fourni.

3.3.2 Conformité aux licences

Le programme doit être en mesure de gérer les cas d'usage de licences open source communes rencontrées par les participants au programme pour le logiciel fourni qui peuvent inclure les cas d'utilisation suivants (cette liste n'est pas exhaustive et tous les cas d'utilisations ne sont pas nécessairement applicables) :

- distribué sous forme de binaire ;
- distribué sous forme de code source ;
- intégré à d'autres logiciels open source de sorte qu'il entraîne des obligations supplémentaires en matière de licence ;
- contient du code open source modifié ;
- contient du code open source ou du code diffusé sous une licence incompatible qui interagit avec d'autres composants du logiciel fourni ; ou
- contient du code open source avec des exigences d'attribution.

Élément(s) de vérification :

- 3.3.2.1 Une procédure documentée pour traiter les cas de licence open source commune des composants open source des logiciels fournis.

Raison :

S'assurer que le programme est suffisamment robuste pour traiter les cas d'utilisation de licences open source communes par l'organisation, qu'une procédure existe pour soutenir cette activité, et que cette procédure est suivie.

3.4 Création et fourniture de livrables de conformité

3.4.1 Livrables de conformité

Il doit exister un processus pour créer l'ensemble des livrables de conformité pour le logiciel fourni.

Élément(s) de vérification :

- ☐ 3.4.1.1 Une procédure documentée qui décrit le processus selon lequel les livrables de conformité sont préparés et distribués avec le logiciel fourni comme requis par les licences identifiées.
- ☐ 3.4.1.2 Une procédure documentée pour archiver les copies des livrables de conformité du logiciel fourni qui prévoit une durée d'archivage raisonnable[1] depuis la précédente version du logiciel fourni ; ou une durée 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.

3.5 Comprendre les engagements de la communauté open source

3.5.1 Contributions

Si une organisation envisage de contribuer à des projets open source, alors

- il doit exister une politique écrite qui régit les contributions aux projets open source ;
- cette politique doit être communiquée en interne ; et
- il doit exister un processus qui met en œuvre la politique

Élément(s) de vérification :

Si une organisation autorise les contributions à des projets open source, alors les documents suivants doivent exister :

- ☐ 3.5.1.1 une politique de contribution open source documentée ;
- ☐ 3.5.1.2 Une procédure documentée qui encadre les contributions open source ; et
- ☐ 3.5.1.3 Une procédure documentée qui informe tous les participants au programme de l'existence de la politique de contribution open source (par des formations, un wiki interne ou tout autre moyen de communication).

Raison :

Lorsqu'une organisation autorise les contributions open source, l'intention est que l'organisation ait accordé une attention raisonnable à l'élaboration et la mise en œuvre d'une politique de contribution. Cette politique de contribution open source peut être intégrée à la politique générale open source ou constituer une politique distincte.

[1] Déterminée par le domaine, la juridiction légale ou les contrats clients

3.6 Conformité aux exigences de la spécification

3.6.1 Conformité

Pour qu'un programme soit jugé conforme à OpenChain, l'organisation doit attester que le programme satisfait aux exigences présentées dans ce document.

Élément(s) de vérification :

- 3.6.1.1 Un document affirmant que le programme spécifié au §3.1.4 satisfait à toutes les exigences de ce document.3.1.4

Raison :

S'assurer que, si une organisation déclare disposer d'un programme conforme à OpenChain, ce programme répond effectivement à l'ensemble des exigences de la présente spécification. Le simple respect d'un sous-ensemble de ces exigences n'est pas considéré comme suffisant.

3.6.2 Durée

Un programme conforme à cette version de la spécification OpenChain doit durer 18 mois à compter de la date de validation de la conformité. La procédure d'enregistrement de la validation de la conformité est disponible sur le site web du projet OpenChain.

Élément(s) de vérification :

- 3.6.2.1 Un document attestant que le programme répond à toutes les exigences de ce document, dans les 18 derniers mois suivant l'obtention de la validation de conformité.

Raison :

Il est important qu'un programme reste conforme aux spécifications si une organisation veut affirmer sa conformité dans la durée. Cette exigence garantit que les processus et contrôles de soutien du programme ne se dégradent pas pour qu'une organisation continue à affirmer la conformité du programme dans la durée.

Annex A
(informatif)

Traductions de cette spécification

Afin de faciliter son adoption mondiale, les efforts de traduction de la spécification dans différentes langues sont encouragés. OpenChain fonctionne comme un projet open source. Les traductions sont assurées par ceux qui souhaitent fournir du temps et de l'expertise à leur élaboration. Les traductions sont i) proposées selon les termes de la licence CC-BY-4.0 et ii) en accord avec la politique de traduction du projet. Les détails de cette politique ainsi que les traductions disponibles peuvent être trouvés sur le wiki du projet OpenChain.