Specifiche OpenChain
Versione 2.1

Questa specifica è funzionalmente identica a:

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

Per ulteriori informazioni: www.openchainproject.org

Indice

Introduzione

Questo documento definisce i requisiti chiave di un programma di conformità open source di qualità. L'obiettivo è fornire un benchmark che costruisca fiducia tra le organizzazioni che scambiano soluzioni software che includono software open source. La conformità alla specifica garantisce che è stato progettato un programma di creazione degli elaborati di conformità necessari (ossia avvertenze legali, codice sorgente e così via) per ciascuna soluzione software. Questo documento si focalizza sul "cosa" e il "perché" del programma, piuttosto che sul "come" e "quando". Questo assicura a diverse organizzazioni, di diversa grandezza e che operano in differenti mercati, la flessibilità di scegliere specifici contenuti di politiche e procedimenti affinché si adattino alla loro grandezza, ai loro obiettivi e al loro ambito di applicazione. Ad esempio, un programma conforme a OpenChain può essere indirizzato a una singola linea di prodotto o all'intera organizzazione.

Questa introduzione fornisce il contesto per tutti i potenziali utenti. La Clausola 2 definisce i termini chiave utilizzati in questo documento. La Clausola 3 definisce i requisiti che un Programma deve soddisfare per ottenere la conformità. Un requisito consiste in uno o più materiali di verifica (ossia, registrazioni) che devono essere prodotti per soddisfare i requisiti. I materiali di verifica non devono essere resi pubblici, anche se un'organizzazione può scegliere di fornirli a terzi, eventualmente nell'ambito di un accordo di non divulgazione (NDA).

Questo documento è stato sviluppato come un'iniziativa aperta con feedback ricevuti da oltre 200 collaboratori. Per avere una panoramica della sua evoluzione storica, è possibile consultare la mailing list della Specifica e le domande più frequenti (FAQ).

Tecnologia dell'informazione - Specifica OpenChain

1 Ambito di applicazione

Questo documento specifica i requisiti chiave di un programma di conformità alle licenze open source di qualità, al fine di fornire un benchmark che costruisca fiducia tra le organizzazioni che si scambiano soluzioni software che includono software open source.

2 Termini e definizioni

Ai fini del presente documento, si applicano i seguenti termini e definizioni.

2.1elaborati di conformità
– una raccolta di elaborati che rappresentano il risultato di un programma di conformità e accompagnano il software fornito

Nota: La raccolta può includere, ma non è limitata a, uno o più dei seguenti: note di attribuzione, codice sorgente, script di compilazione e installazione, copia di licenze, note sul diritto d'autore, notifiche di modifica, offerte scritte, distinta dei materiali dei componenti open source e documenti SPDX.

2.2
licenze identificate – un insieme di licenze software open source identificate seguendo un metodo appropriato di identificazione dei componenti open source di cui è composto il software fornito

2.3
conforme a OpenChain
un programma che soddisfa tutti i requisiti di questo documento

2.4
open source
software sottoposto a una o più licenze che rispettano la Open Source Definition pubblicata dalla Open Source Initiative (vedi opensource.org/osd) o la Free Software Definition pubblicata da Free Software Foundation (vedi gnu.org/philosophy/free-sw.html) o licenze simili

2.5
programma
l'insieme delle politiche, dei processi e del personale che costituiscono le attività di conformità alle licenze open source di un'organizzazione

2.6
partecipanti al programma
qualsiasi dipendente o collaboratore esterno dell'organizzazione che definisce, contribuisce o ha responsabilità circa la preparazione di software fornito

Nota: A seconda dell'organizzazione, ciò può includere (ma non è limitato a) sviluppatori software, specialisti del rilascio, responsabili della qualità, responsabili del marketing di prodotto e responsabili di prodotto.

2.7
SPDX
lo standard di formato creato dal gruppo di lavoro SPDX (Software Package Data Exchange) della Linux Foundation per lo scambio di distinte di materiali per un determinato pacchetto software, comprese le informazioni sulle licenze e i copyright associati (vedi spdx.org)

2.8
software fornito
software che un'organizzazione distribuisce a terze parti (ad esempio, altre organizzazioni o persone)

2.9
materiali di verifica
materiali che dimostrano che un determinato requisito della specifica è soddisfatto

ISO e IEC mantengono database terminologici da utilizzare nella standardizzazione ai seguenti indirizzi:

- Piattaforma di navigazione online ISO: disponibile su https://www.iso.org/obp

- IEC Electropedia: disponibile su http://www.electropedia.org/

3 Requisiti

3.1 Fondazione del Programma

3.1.1 Politica

Deve esistere una politica open source scritta che regola il rispetto delle licenze open source del software fornito. La politica deve essere comunicata internamente.

Materiale(i) di Verifica:

- 3.1.1.1 Una politica open source documentata.
- 3.1.1.2 Una procedura documentata che rende i partecipanti al programma consapevoli dell'esistenza di una politica open source (ad esempio, tramite formazione, wiki interno o altro metodo pratico di comunicazione).

Razionale:

Assicurare che siano intrapresi passi per creare, registrare e rendere i partecipanti al programma consapevoli dell'esistenza di una politica open source. Sebbene qui non sono forniti requisiti su cosa debba essere incluso in tale politica, altre sezioni potrebbero imporre requisiti sulla politica.

3.1.2 Competenza

L'organizzazione deve

- Identificare i ruoli e le responsabilità corrispondenti a quei ruoli che influenzano l'esecuzione e l'efficacia del programma;
- Determinare le competenze necessarie dei partecipanti al programma che ricoprono ciascun ruolo
- Garantire che i partecipanti al programma siano competenti in base a un'adeguata istruzione, formazione e/o esperienza;
- Se del caso, adottare misure per acquisire le competenze necessarie; e
- Conservare appropriate informazioni documentate come prova della competenza.

Materiale(i) di Verifica:

- 3.1.2.1 Un elenco documentato dei ruoli con le responsabilità corrispondenti per i diversi partecipanti al programma.
- 3.1.2.2 Un documento che identifica le competenze per ciascun ruolo.
- 3.1.2.3 Prove documentate delle competenze valutate per ciascun partecipante al programma.

Razionale:

Assicurare che i partecipanti al programma abbiano ottenuto un livello di competenza sufficiente per i rispettivi ruoli e responsabilità.

3.1.3 Consapevolezza

L'organizzazione deve garantire che i partecipanti al programma siano a conoscenza di:

- La politica open source;
- Obiettivi pertinenti dell'open source;
- Il loro contributo all'efficacia del programma; e
- Le implicazioni del mancato rispetto dei requisiti del Programma.

Materiale(i) di Verifica:

- 3.1.3.1 Prove documentate della valutata consapevolezza dei membri del personale del programma, anche riguardo gli obiettivi del programma, il contributo di ciascuno nel quadro del programma e le implicazioni della non conformità del programma.

Razionale:

Assicurare che il personale del programma abbia ottenuto un livello sufficiente di consapevolezza dei rispettivi ruoli e responsabilità all'interno del programma.

3.1.4 Ambito del programma

Programmi diversi possono essere regolati da diversi livelli di ambito. Ad esempio, un programma può governare una singola linea di prodotti, un intero reparto o un'intera organizzazione. La designazione dell'ambito di applicazione deve essere dichiarata per ogni programma.

Materiale(i) di Verifica:

- 3.1.4.1 Una dichiarazione scritta che definisce chiaramente l'ambito di applicazione e i limiti del programma.

Razionale:

Consentire flessibilità per creare un programma che meglio si adatta alle differenti esigenze di un'organizzazione. Alcune organizzazioni possono scegliere di adottare il programma per una specifica linea di prodotti, mentre altre possono adottare il programma per controllare il software fornito dell'intera organizzazione.

3.1.5 Obblighi di licenza

Deve esistere un processo di revisione delle licenze identificate per determinare gli obblighi, le condizioni e i diritti stabiliti da ciascuna licenza.

Materiale(i) di Verifica:

- 3.1.5.1 Una procedura documentata per controllare e documentare gli obblighi, le condizioni e i diritti stabiliti da ogni licenza identificata.

Razionale:

Assicurare l'esistenza di un processo di revisione e identificazione degli obblighi di licenza per ciascuna licenza identificata per i vari casi d'uso che un'organizzazione può incontrare (come definito in §3.3.2).

3.2 Compiti definiti e supportati

3.2.1 Accesso

Mantenere un processo per rispondere efficacemente alle richieste di informazioni esterne riguardo all'open source. Identificare pubblicamente un mezzo attraverso il quale un terzo può effettuare una richiesta di conformità open source.

Materiale(i) di Verifica:

- 3.2.1.1 Un metodo pubblicamente visibile che consente a terzi di richiedere informazioni riguardo alla conformità alle licenze open source (ad esempio, tramite un indirizzo e-mail di contatto pubblicato o l'Open Compliance Directory della Linux Foundation).
- 3.2.1.2 Una procedura interna documentata per rispondere alle richieste di informazioni riguardo alla conformità alle licenze open source effettuate da terzi.

Razionale:

Garantire che ci sia un metodo ragionevole attraverso il quale i terzi possano contattare l'organizzazione per quanto riguarda le richieste di conformità open source e che l'organizzazione sia pronta a rispondere efficacemente.

3.2.2 Risorse efficaci

Identificare e attribuire risorse alle attività del Programma:

- Assegnare responsabilità per assicurare la corretta esecuzione delle attività del programma.
- Le attività del Programma sono dotate di risorse sufficienti:
  - Tempo per svolgere le attività è stato assegnato; e
  - Fondi sufficienti sono stati assegnati.
- Esiste un processo di revisione e aggiornamento della politica e delle attività di supporto;
- Competenze legali circa la conformità alle licenze open source sono accessibili a coloro che potrebbero aver bisogno di tale guida; e
- Esiste un processo per la risoluzione di questioni di conformità delle licenze open source.

Materiale(i) di Verifica:

- 3.2.2.1 Documento che identifica i nomi delle persone, del gruppo o della funzione nel/nei ruolo/i all'interno del programma.
- 3.2.2.2 I ruoli identificati all'interno del programma sono stati adeguatamente dotati di personale e adeguatamente finanziati.
- 3.2.2.3 Identificazione di competenze legali disponibili per affrontare questioni di conformità alle licenze open source, che potrebbero essere interne o esterne.
- 3.2.2.4 Una procedura documentata per assegnare le responsabilità interne per la conformità open source.

- 3.2.2.5 Una procedura documentata per gestire la revisione e la risoluzione dei casi di mancata conformità.

Razionale:

Assicurare che: i) le responsabilità del programma siano efficacemente sostenute e finanziate e ii) le politiche e i processi di supporto siano regolarmente aggiornati per tenere conto dei cambiamenti nelle migliori pratiche di conformità open source.

3.3 Verifica e approvazione dei componenti open source

3.3.1 Distinta dei materiali

Deve esistere un processo per creare e gestire una distinta dei materiali che include ciascun componente open source (e le sue licenze identificate) del quale è composto il software fornito.

Materiale(i) di Verifica:

- 3.3.1.1 Una procedura documentata per identificare, tracciare, rivedere, approvare e archiviare le informazioni sulle raccolte di componenti open source dei quali è composta il software fornito.
- 3.3.1.2 Registrazioni dei componenti open source per il software fornito che dimostrino che la procedura documentata è stata seguita correttamente.

Razionale:

Assicurare l'esistenza di un processo per creare e gestire una distinta dei materiali del componente open source utilizzata per la costruzione del software fornito. Una distinta dei materiali è necessaria per supportare la revisione sistematica e l'approvazione dei termini di licenza di ogni componente al fine di comprendere gli obblighi e le restrizioni applicabili alla distribuzione del software fornito.

3.3.2 Conformità alla licenza

Il programma deve essere in grado di gestire i casi comuni d'uso della licenza open source incontrati dai partecipanti al programma per il software fornito, che possono includere i seguenti casi d'uso (si noti che l'elenco non è esaustivo e potrebbero non applicarsi tutti i casi d'uso):

- Distribuito in formato binario;
- Distribuito in formato sorgente;
- Integrato con altro open source, tale da attivare degli obblighi di licenza aggiuntivi;
- Contiene open source modificato;
- Contiene open source o altro software con una licenza incompatibile che interagisce con altri componenti del Software Fornito; e/o
- Contiene open source con requisiti di attribuzione.

Materiale(i) di Verifica:

- 3.3.2.1 Una procedura documentata per la gestione dei casi comuni d'uso di licenza open source per i componenti open source del software fornito.

Razionale:

Assicurare che il Programma sia sufficientemente robusto per gestire i casi comuni d'uso di licenza open source per un'organizzazione. Assicurare che esiste una procedura per supportare quest'attività e che la procedura è seguita.

3.4 Creazione e consegna degli elaborati di conformità

3.4.1 Elaborati di conformità

Deve esistere un processo per creare l'insieme degli elaborati di conformità per il software fornito.

Materiale(i) di Verifica:

- 3.4.1.1 Una procedura documentata che documenta il processo secondo il quale gli elaborati di conformità vengono preparati e distribuiti con il software fornito come richiesto dalle licenze identificate.
- 3.4.1.2 Una procedura documentata per archiviare copie dei materiali di conformità del software fornito – dove è pianificato che l'archivio esista per un periodo di tempo[1] ragionevole dall'ultima offerta del software fornito; o per il periodo richiesto dalle licenze identificate (a seconda di quale sia il più lungo). Esistono registrazioni che dimostrano che la procedura è stata seguita correttamente.

Razionale:

Assicurare che siano stati stabiliti ragionevoli sforzi commerciali per la preparazione degli elaborati di conformità che accompagnano il software fornito, come richiesto dalle licenze identificate.

3.5 Comprendere il coinvolgimento della comunità open source

3.5.1 Contributi

Se un'organizzazione permette di contribuire a progetti open source, allora

- deve esistere una politica scritta che regola le contribuzioni ai progetti open source;
- la politica deve essere comunicata internamente; e
- deve esistere un processo che attua la politica

Materiale(i) di Verifica:

Se un'organizzazione consente di contribuire a progetti open source, devono esistere:

- 3.5.1.1 Una politica di contributo open source documentata;
- 3.5.1.2 una procedura documentata che regola i contributi open source; e
- 3.5.1.3 Una procedura documentata che rende tutti i partecipanti al programma consapevoli dell'esistenza di una politica di contributo open source (ad esempio, tramite formazione, wiki interno o altro metodo pratico di comunicazione).

Razionale:

Quando un'organizzazione permette contribuzioni open source, si presume che l'organizzazione abbia ragionevolmente preso in considerazione lo sviluppo e l'implementazione di una politica di contribuzione. La politica di contribuzione open source può far parte della politica open source globale o può essere una politica specifica.

[1] Determinato in base al dominio, alla giurisdizione legale e/o ai contratti coi clienti

3.6 Adesione ai Requisiti della Specifica

3.6.1 Conformità

Affinché un programma sia conforme a OpenChain, l'organizzazione deve dichiarare che il programma soddisfa i requisiti descritti in questo documento.

Materiale(i) di Verifica:

- 3.6.1.1 Un documento che dichiara che il programma specificato in §3.1.4 soddisfa tutti i requisiti del presente documento.

Razionale:

Assicurare che se un'organizzazione dichiara di avere un programma che è conforme a OpenChain, tale programma ha soddisfatto tutti i requisiti del presente documento. La semplice conformità a un sottoinsieme di tali requisiti non è considerata sufficiente.

3.6.2 Durata

Un programma che è conforme a Openchain con questa versione della specifica durerà 18 mesi dalla data di ottenimento della convalida della conformità. La procedura di registrazione della convalida di conformità è disponibile sul sito web del progetto OpenChain.

Materiale(i) di Verifica:

- 3.6.2.1 Un documento che dichiara che il programma soddisfa tutti i requisiti di questo documento, entro 18 mesi dall'ottenimento della convalida di conformità.

Razionale:

È importante che il programma rimanga aggiornato con la specifica, se un'organizzazione vuole dichiarare la conformità nel tempo. Questo requisito assicura che i processi e i controlli di supporto del programma non si erodono se un'organizzazione continua a dichiarare la conformità del programma nel tempo.

Annex A
(informativa)

Traduzioni in lingua di questa specifica

Per facilitare l'adozione globale, gli sforzi per tradurre le specifiche in più lingue sono benvenuti. Poiché OpenChain funziona come un progetto open source, le traduzioni vengono preparate da coloro che desiderano contribuire con il proprio tempo ed esperienza per eseguire alle traduzioni. Le traduzioni sono i) offerte secondo i termini della licenza CC-BY-4.0 e ii) coerenti con la politica di traduzione del progetto. I dettagli della politica e le traduzioni disponibili si trovano sulla pagina web della specifica del progetto OpenChain.