

DETERMINA A CONTRARRE ART. 17 D.LGS. N. 36/2023

OGGETTO DELL'ACQUISIZIONE	Fornitura subscription prodotti Sonatype Nexus
CODICE IDENTIFICATIVO	RdA 51972
BENEFICIARIO	SOGEI
AVVISO DI PREINFORMAZIONE	No
TIPOLOGIA DI PROCEDURA PRESCELTA	affidamento diretto sul MEPA ex art. 50 D.Lgs. 36/2023, comma 1, lettera b
IMPORTO MASSIMO STIMATO	Euro: 139.920,00
DURATA DEL CONTRATTO	Mesi: 12
REQUISITI DI PARTECIPAZIONE	Rispetto degli artt. 94 e 95 D.Lgs. 36/2023
REQUISITI GENERALI E DI IDONEITÀ	Abilitazione al bando Mepa Beni - Licenze software
CRITERIO DI AGGIUDICAZIONE	N.A.
SUDDIVISIONE IN LOTTI	NO - Ai sensi e per gli effetti dell'art. 58, del D.lgs. n. 36/2023, si precisa che la presente procedura non viene suddivisa in lotti in quanto le varie prestazioni oggetto del contratto fanno parte di un'unica tipologia e sono funzionalmente connesse da un punto di vista tecnico. Di conseguenza un'eventuale suddivisione in lotti potrebbe compromettere l'economicità e l'efficienza del servizio oggetto del contratto.
MOTIVAZIONI	<p>La Sogei nell'ambito della sua attività di Continuous Integration e Continuous Deployment, utilizza il Repository Manager Sonatype Nexus, una piattaforma di repository per artifact che offre un sistema centralizzato per archiviare, gestire e distribuire componenti software, garantendo agli sviluppatori automatismi in grado di aumentare la produttività e la qualità del software. Il suddetto prodotto permette di automatizzare il processo di build del codice sorgente e centralizzare il controllo delle librerie.</p> <p>Nell'ambito della sua missione di erogazione dei servizi per l'Amministrazione Finanziaria, Sogei è impegnata nella costante realizzazione di nuove funzionalità ottenute attraverso lo sviluppo di applicazioni e moduli ai diversi livelli dell'architettura software. Le moderne tecniche di sviluppo del software fanno sempre più leva su automatismi in grado di aumentare la produttività e la qualità del software prodotto. Tali automatismi, replicabili indefinite volte, vanno ad eliminare la possibilità di errori umani durante l'attuazione di processi fondamentali nel ciclo di vita del software. Inoltre vanno ad esonerare le persone</p>

dall'esecuzione di continui task di verifica, controllo e gestione sul software prodotto.

L'insieme delle suddette tecniche di sviluppo del software è un fondamento imprescindibile nell'attuazione della disciplina del DevOps, che è un set di pratiche e di cambiamenti culturali supportati da strumenti automatici e processi di Lean Management, il quale consente di automatizzare il rilascio del software rispetto alla sua catena di produzione, permettendo alle organizzazioni di poter contare su un software e applicazioni di qualità superiore e sicura in modo estremamente più rapido, per accontentare i clienti nel modo migliore e più rapidamente. Tra gli strumenti di automazione per migliorare la qualità/produzione del software, quello di maggior interesse riguarda le build automatiche ovvero delle procedure codificate che utilizzano un'ampia gamma di prodotti disponibili per tutti i linguaggi di programmazione di maggiore successo. La maggior parte dei suddetti prodotti utilizzati dalle build automatiche offre delle funzionalità che permettono di reperire dipendenze in rete piuttosto che doverle scaricare e salvare nel controllo di versione insieme al software. Tali dipendenze vengono reperite dai suddetti tool su dei repository pubblici, ma hanno tutti la possibilità di riferirsi in alternativa ad un repository privato aziendale.

I vantaggi nell'utilizzo di un repository aziendale con questo tipo workflow di lavoro sono molteplici, tra cui:

- la possibilità di visionare degli artefatti estremamente più leggeri in quanto liberi dalle librerie;
- la possibilità di centralizzare il controllo sulle librerie in termini di versione;
- la possibilità di applicare policy sull'utilizzo delle librerie in azienda;
- la possibilità di verificare la sicurezza e le licenze delle librerie utilizzate;
- la possibilità di effettuare i rilasci del software prodotto su tale repository piuttosto che all'interno del controllo di versione.

Alla luce di quanto sopra, Sogei ha l'esigenza di acquisire la soluzione Repository Manager Sonatype Nexus per la gestione, archiviazione e condivisione di artefatti e delle dipendenze di componenti software, integrabile con Azure DevOps, garantendo sicurezza e qualità. Nello specifico, le motivazioni che inducono Sogei a richiedere la deroga al principio di rotazione ai sensi dell'art. 49, comma 4, del D.Lgs. n. 36/2023, affidando il contratto avente ad oggetto la fornitura del Repository Manager Sonatype Nexus al contraente uscente indicato nella scheda di sintesi sono le seguenti:

1) Struttura del mercato:

Sogei ha effettuato un'analisi di mercato esaminando diversi prodotti open source e tra questi sono stati individuati soltanto due prodotti Nexus e JFrog che, in prima analisi, sembrano soddisfare le esigenze di gestione del repository. In particolare, Sogei ha necessità di un prodotto con determinate caratteristiche tecniche che, sul mercato di riferimento analizzato, solo la soluzione Sonatype Nexus è in grado di soddisfare e che di seguito si riportano:

- gestione centralizzata dei repository e delle dipendenze;

- controllo degli accessi e sicurezza;
- integrazione analisi della sicurezza per identificare e affrontare potenziali vulnerabilità nei componenti software;
- compatibilità con diversi linguaggi e tecnologie;
- monitoraggio delle attività legate ai repository, consentendo di tracciare le modifiche, le distribuzioni e le altre operazioni correlate allo sviluppo del software;
- integrazione con strumenti di build e CI/CD;
- archiviazione e gestione di snapshot e release;
- funzionalità di “proxy repository” quale interfaccia verso i repository public domain disponibili su internet per tutte le tecnologie supportate indicate in precedenza;
- verifica automatica della tipologia di licenza (open source o proprietaria) delle librerie referenziate dai progetti che accedono ai repository;
- possibilità di definire delle policies di sicurezza rispetto all’utilizzo di librerie di terze parti contenenti vulnerabilità note e di corretto utilizzo delle licenze nei termini descritti all’interno delle stesse licenze o dalle loro tipologie.
- interfaccia di accesso web sia alle funzioni di amministrazione che alle funzioni di consultazione per tutti gli utenti registrati.

2) Effettiva assenza di alternative:

A seguito della suddetta analisi di mercato, è stato considerato l’utilizzo di Nexus in versione open source. Questo prodotto soddisfa tutte le feature richieste tranne la possibilità di verificare la sicurezza e le licenze delle librerie Open Source utilizzate e la possibilità di definirne delle policy di utilizzo. Queste funzionalità sono per Sogei imprescindibili nell’ottica di una maggiore apertura verso il mondo Open Source in quanto l’utilizzo di librerie non adeguatamente controllate, da un punto di vista della sicurezza e dei termini di licenza, esporrebbe l’azienda ed i suoi clienti ad un elevato rischio in termini di danno di immagine, se non, in alcuni casi, anche economico. Nel caso di Nexus, tuttavia, risulta disponibile sul mercato la versione “Enterprise”, denominata Sonatype Nexus, che fornisce le funzionalità di verifica della sicurezza e delle licenze delle librerie open source, oltre la possibilità di definirne le policy di utilizzo, mancanti nella versione open source, nonché avente tutti gli altri requisiti tecnici richiesti da Sogei e sopra indicati. La versione Enterprise Sonatype Nexus, essendo in utilizzo presso Sogei, è stata oggetto di importanti progetti di integrazione nei processi DevOps aziendali e pertanto l’eventuale adozione di prodotti alternativi comporterebbe la necessità di un’attività dispendiosa per la revisione di tali processi e modalità di integrazione. Sogei si impegna ad effettuare un monitoraggio costante di quanto disponibile sul mercato ed è pronta a valutare tempestivamente tutte le soluzioni alternative che si dovessero rendere disponibili.

Il produttore Sonatype Inc. ha dichiarato che Profesia srl è operatore economico avente diritti esclusivi per la

	commercializzazione del prodotto e la prestazione di servizi di manutenzione e assistenza. 3) Accurata esecuzione del precedente contratto: L'esecuzione della precedente prestazione è stata eseguita a regola d'arte e non è stato necessario applicare penali.	
NOMINATIVO DELL'OPERATORE ECONOMICO	Profesia S.r.l.	
ELEMENTI ESSENZIALI DEL CONTRATTO	Condizioni contratto standard Sogei	
DEROGA AL BANDO TIPO	N.A.	
RESPONSABILE PROCEDIMENTO	Il Responsabile unico del progetto è Gianandrea Greco, ferma restando l'applicazione dell'art. 15, comma 2 D.Lgs. 36/2023 Il Responsabile del procedimento per la fase di affidamento è Lucia Magliocco ferma restando l'applicazione dell'art. 15, comma 2, secondo periodo D.Lgs. 36/2023	
FIRMA DEL RESPONSABILE APPROVAZIONE DETERMINA E DATA	Gianandrea Greco	Vale la data della firma digitale del documento

Per gli acquisti effettuati per altre Amministrazioni/Società nella determina di cui sopra sono recepite le esigenze dalle stesse manifestate