Consip S.p.A.

"Acquisto licenze software Checkmarx"

CAPITOLATO TECNICO

ACQUISTO LICENZE SOFTWARE CHECKMARX

INDICE

1. PREMESSA

1.1 DEFINIZIONI

Nel corpo del documento, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:

- CONSIP: la società che, in qualità di stazione appaltante, affida la fornitura oggetto del presente Capitolato;
- SOGEI: la Società Generale di Informatica S.p.A. beneficiaria della Fornitura;
- Amministrazione: si intende il Ministero dell'Economia e delle Finanze, che è proprietario dell'intero capitale di Sogei, con riferimento alle proprie strutture organizzative destinatarie dei servizi erogati dalla Sogei sia attraverso infrastrutture proprietarie che attraverso infrastrutture proprietarie delle singole strutture organizzative; rientrano nella presente definizione le altre Amministrazioni, ivi compresi gli Enti e le Società pubbliche per cui Sogei svolge e/o svolgerà, per disposizione legislativa o amministrativa, (decreto ministeriale, decreto di natura normativa o decreto presidenza consiglio dei ministri), ogni altra attività di natura informatica;
- Capitolato tecnico: il presente documento che enuncia le specifiche tecniche alle quali dovrà conformarsi la fornitura;
- Contratto: il contratto che verrà stipulato tra la SOGEI e l'impresa che enuncia le regole giuridiche alle quali si dovrà conformare la fornitura;
- Fornitura: il complesso delle attività oggetto del presente Capitolato;
- Società: la società aggiudicataria della fornitura;
- Checkmarx: Produttore;
- Malfunzionamento: qualsiasi anomalia funzionale dei prodotti software e, in ogni caso, ogni difformità del prodotto in esecuzione rispetto alla relativa documentazione tecnica e manualistica d'uso;
- Responsabile delle attività contrattuali: la persona individuata dalla Società come interlocutore di Sogei e responsabile di tutte le attività contrattuali;
- Sistema Informativo: il sistema informativo gestito da Sogei con sede in Via Mario Carucci 99.

1.2 CONTESTO TECNICO ORGANIZZATIVO

Il moderno processo di sviluppo del software di sistemi complessi presente in Sogei prevede, attualmente, un elevato numero di piccoli rilasci in tempi sempre più brevi. Sia in caso di nuovi sviluppi che di manutenzioni correttive e/o evolutive, il software prodotto deve rispettare elevati standard di qualità e sicurezza in linea con il flusso DevSecOps previsto in Sogei. Per la realizzazione

di questo scenario non è, quindi, possibile ricorrere esclusivamente a controlli manuali di sicurezza sul codice prodotto svolti da personale qualificato, in quanto tali controlli rallenterebbero in modo inaccettabile i tempi di ogni rilascio, ma è necessario introdurre dei controlli automatici che, in tempi brevi, possano verificare e segnalare eventuali problemi di sicurezza. Inoltre i controlli, se eseguiti per ogni modifica e fin dalle prime fasi dello sviluppo del codice, permettono di intervenire sulle versioni del software non definitive abbattendo tempi e costi di ogni intervento. Tra i controlli automatici è di fondamentale importanza l'analisi SAST – Static Application Security Testing che verifica la sicurezza delle applicazioni analizzando direttamente il codice sorgente alla ricerca di problemi che possano comportare la presenza di vulnerabilità sul prodotto finale.

A partire dal 2021 Sogei ha iniziato ad utilizzare lo strumento di analisi statica di sicurezza Checkmarx. L'introduzione dell'analisi statica di sicurezza si inquadra in un obiettivo più ampio che è quello di investire in un modello decentralizzato in cui i team di sviluppo abbiamo l'autonomia richiesta dal paradigma DevOps. Al fine di effettuare lo shift left dei controlli, in ottica DevSecOps, è stato necessario mettere a disposizione dei gruppi di sviluppo gli strumenti necessari a spostare questi controlli nelle prime fasi dello sviluppo, riducendo il tempo e costo degli interventi ed evitando il replicarsi di vulnerabilità note nei moduli sviluppati successivamente.

Nell'ambito del progetto si è definito il flusso relativo all'analisi SAST e si è introdotto il ruolo del Security Champion, con lo scopo di creare una figura che facesse da riferimento all'interno dei gruppi applicativi.

Attualmente in Sogei le scansioni SAST vengono effettuate tramite Checkmarx – CxSAST. A partire da gennaio 2022 è iniziato il processo di onboarding delle applicazioni presenti nei repository GIT.

Nella seconda parte del 2022 si procederà con l'introduzione di blocchi nelle build delle pipeline per tutti i progetti che non passeranno i controlli di sicurezza. Al momento si hanno a disposizione un numero limitato di licenze utente (40) ma il flusso SAST richiede che all'interno di ciascuna U.O che sviluppa si abbiano a disposizione due tipologie di utenze (Security Champion e Developer), è quindi necessario effettuare un upgrade in termini di numero di licenze. Inoltre, per far fronte al carico dovuto all'aumentare dei progetti analizzati dalla piattaforma, è anche necessario aumentare il numero delle scansioni concorrenti del prodotto.

2. OGGETTO

Il presente Capitolato disciplina la sottoscrizione di licenze software Checkmarx, da erogarsi in favore della Sogei, ivi comprese tutte le attività connesse allo svolgimento delle prestazioni medesime così come regolamentate, oltre che dal presente Capitolato, anche dallo Schema di contratto e dalle Condizioni particolari.

2.1 DETTAGLIO DELLA FORNITURA

La Società dovrà fornire le sottoscrizioni software riportate in Tabella 1 un periodo di 6 (sei) mesi decorrenti dal 01/01/2023.

Code	Product Name	Descrizione	Quantità	Metrica	Durata in mesi	Periodo di riferimento
CxSAST_150_6M	CxSAST	Subscription 6 Months of CxSAST on premise. 150 users	150	n° sottoscrizioni mensili	6	01/01/2023 – 30/06/2023
CxCodebashing_50_6M	Codebashing (CB)	Subscription 6 Months of CB. 50 users	50	n° sottoscrizioni mensili	6	01/01/2023 – 30/06/2023

Tabella 1: sottoscrizioni software

Di seguito si riportano le principali caratteristiche che meglio definiscono la Fornitura:

- SAST (6 Months):
  - 150 users as reviewer (1 user with CxAudit permissions);
  - 30.000 projects;
  - 5 Concurrent scans;
- Code Bashing (6 Months):
  - 50 users.

Si segnala che il numero di progetti è un parametro indicativo, la componente determinante il costo totale è il numero di utenti.

2.1.1 ARCHITETTURA DI RIFERIMENTO

Si riportano di seguito le informazioni circa l'architettura attuale e la nuova architettura.

Architettura attuale (con licenza in EOL)

CXMNG-01 (32 GB RAM, 8 core, 500 GB space): è il server su cui è installata la componente core che gestisce il carico sui vari engine e rende disponibile il portale da cui è possibile gestire il prodotto e far visualizzare la reportistica agli utenti.

CXENG-01, CXENG-02 (48 GB RAM, 8 core, 100 GB space): Engine per effettuare le scansioni per progetti di medie/grandi dimensioni

Nuova Architettura (con licenza a canone):

CXMNG-01 (32 GB RAM, 8 core, 500 GB space): è il server su cui è installata la componente core che gestisce il carico sui vari engine e rende disponibile il portale da cui è possibile gestire il prodotto e far visualizzare la reportistica agli utenti.

CXENG-01, CXENG-02 (48 GB RAM, 8 core, 100 GB space): saranno gli engine per effettuare le scansioni per progetti di medie/grandi dimensioni.

CXENG-03, CXENG-04 (48 GB RAM, 8 core, 100 GB space): saranno gli engine per scansioni di piccole dimensioni.

2.2 SERVIZIO DI MANUTENZIONE E LIVELLI DI SERVIZIO

Nell'ambito della fornitura, di cui al precedente paragrafo 2.1 del presente Capitolato Tecnico, è inclusa l'erogazione del servizio di manutenzione che dovrà comprendere:

- l'eliminazione di malfunzionamenti riscontrati sui prodotti software forniti;
- la fornitura degli aggiornamenti dei prodotti offerti quali patch, nuove release (major e minor release), completi di tutta la documentazione e manualistica (entro 30gg dalla data di rilascio);
- il deploy degli aggiornamenti dei prodotti offerti sull'architettura della Sogei (dopo richiesta specifica della Sogei a seguito della valutazione di applicabilità degli stessi);
- il servizio di supporto telefonico per:
  - le richieste di supporto informativo su quegli errori che eventualmente si riscontrino nei prodotti offerti o nella soluzione in generale;
  - le richieste di supporto e correzioni sulla documentazione connessa ai prodotti software.

Per malfunzionamento si intende qualsiasi anomalia funzionale che, direttamente o indirettamente, provochi l'interruzione o la non completa disponibilità del servizio all'utenza basato sull'utilizzo del software oggetto di manutenzione e, in ogni caso, ogni difformità dei prodotti in esecuzione dalla relativa documentazione tecnica e manualistica d'uso.

Il servizio di manutenzione ordinaria dovrà essere svolto dal lunedì al venerdì dalle ore 08:00 alle ore 20:00 (ad eccezione delle festività nazionali) e con i seguenti livelli di servizio:

- la **presa in carico** del malfunzionamento dovrà avvenire entro e non oltre **1 giorno lavorativo** dalla segnalazione;

- la **risoluzione** del problema/malfunzionamento e ripristino della completa funzionalità del prodotto software dovrà avvenire entro e non oltre **3 giorni lavorativi** dalla presa in carico del malfunzionamento.

Le comunicazioni e le richieste della Sogei al Fornitore potranno essere effettuate tramite mail, numero verde o tramite un sito Web messo a disposizione dal Fornitore stesso. L'indirizzo di mail, numero verde o indirizzo del sito Web dovranno essere comunicati alla Sogei **entro 5 giorni** dalla stipula del contratto.

A fronte di una segnalazione il Fornitore sarà tenuto a coordinare ed eventualmente ad effettuare un intervento di assistenza tecnica nel rispetto dei livelli di servizio indicati precedentemente.

Tutti gli elementi necessari allo svolgimento del servizio saranno comunque a cura ed a carico del Fornitore, ivi inclusi i componenti che eventualmente si rendessero necessari per la diagnosi e per la risoluzione dei malfunzionamenti, ovvero i costi di trasferimento, riparazione e/o sostituzione dei prodotti software.

A fronte degli interventi di manutenzione, tutti i prodotti aggiornati e l'eventuale nuova documentazione a corredo dovranno essere consegnati presso la medesima sede di utilizzo dei prodotti riparati e/o sostituiti.

La struttura di assistenza tecnica del Fornitore dovrà essere costituita da personale dedicato allo svolgimento di tutte le attività tipiche di gestione di malfunzionamenti e quindi dovrà:

- accogliere ed analizzare la segnalazione ricevuta o la problematica rilevata;
- notificare alla Sogei l'apertura del guasto riportando data e orario di accettazione;
- avviare una preliminare fase di analisi del malfunzionamento al termine della quale potrà essere eventualmente fornita una soluzione temporanea (workaround);
- comunicare l'esito della prima diagnosi alla Sogei indicando i tempi di ripristino ipotizzati;
- coordinare gli interventi delle strutture di assistenza tecniche della Società coinvolte;
- concordare con la Sogei le modalità ed i tempi di intervento, curarne il monitoraggio;
- sollecitare l'esecuzione degli interventi nel rispetto dei livelli di servizio;
- verificare con il personale della Sogei l'effettiva risoluzione del problema;
- chiudere la segnalazione comunicando le cause del disservizio;
- notificare alla Sogei la chiusura del guasto riportando data e orario di risoluzione.

La registrazione delle segnalazioni dovrà avvenire attraverso un sistema di Trouble Ticketing del Fornitore in grado di tracciare le informazioni seguenti:

- identificativo del ticket;
- data e orario di apertura ticket;
- nominativo della persona che effettua la chiamata e richiede l'apertura del ticket;
- problematica riscontrata;
- tipologia del guasto segnalato degrado, disservizio ecc;
- diagnosi del problema;
- data e orario di comunicazione della prima diagnosi riscontrata;
- descrizione della soluzione;
- data e orario di chiusura ticket.

3. SERVIZI CONNESSI ALLA FORNITURA

I servizi di seguito descritti sono connessi alla Fornitura prevista nel presente Capitolato Tecnico e quindi andranno prestati dalla Società unitamente alla medesima Fornitura e senza alcun onere aggiuntivo per la Sogei.

La Società provvederà ad erogare, nei tempi e nei modi che verranno successivamente illustrati, i servizi connessi di:

- consegna dei prodotti software di cui al precedente paragrafo 2.1;
- consegna della documenta a corredo della Fornitura;
- supporto alla verifica di conformità dei prodotti software forniti e di manutenzione ordinaria.

3.1 CONSEGNA

Per effettuare la consegna delle sottoscrizioni di cui al paragrafo 2.1, il Fornitore dovrà attivare la procedura per consentire alla Sogei di effettuare il download del software dei prodotti richiesti e delle relative chiavi, e consegnare via email, entro 10 (dieci) giorni lavorativi decorrenti dalla data stipula all'indirizzo asset_sw@sogei.it: i) la ragione sociale del Fornitore; ii) il numero di repertorio del Contratto; iii) la descrizione dettagliata dei prodotti, con i relativi quantitativi e il tipo, modello e numero seriale delle versione dei prodotti software, nonché la dichiarazione di rispondenza dei prodotti software forniti alle specifiche, le informazioni utili per accedere al sito del download (indirizzo web del sito, utenza e password).

Il Fornitore dovrà inviare ogni informazione necessaria per l'identificazione delle sottoscrizioni software e la conseguente possibilità di utilizzarle e dare informativa circa la disponibilità delle nuove versioni del prodotto.

Di seguito si riporta il tracciato record a cui l'impresa dovrà attenersi per la consegna e l'invio dei dati alla casella asset_sw@sogei.it:

Repertorio Contratto	Produttore	Nome licenza	Quantità	Unità di misura	Versione	Sistema operativo	Part number

Tabella 2: Tracciato record per la consegna dei prodotti software

Nel caso in cui il Fornitore non rispetti i termini indicati per la consegna delle sottoscrizioni a seguito della richiesta della Committente, la Sogei applicherà le penali previste contrattualmente.

Si precisa che la consegna della Fornitura si intende comprensiva di ogni relativo onere e spesa.

Il Fornitore si impegna ad informare la Committente delle eventuali variazioni dei prodotti che dovessero intervenire nel corso della validità contrattuale.

La ricezione della mail da parte della Committente vale esclusivamente come avviso di ricezione dell'oggetto di fornitura, essendo la sua accettazione definitiva subordinata all'esito positivo della verifica di conformità. Qualora, a seguito di successive verifiche, la Committente rilevasse che il Fornitore abbia erogato delle sottoscrizioni software non conformi ai quantitativi e/o alle caratteristiche tecniche previste nel Contratto, essa si riserva la facoltà di respingere l'erogazione di tali prodotti.

3.2 CONSEGNA DELLA DOCUMENTAZIONE A CORREDO

Per tutta la durata contrattuale, la Società sarà tenuta a predisporre e fornire alla Sogei, tutta la documentazione a corredo della Fornitura quali ad esempio i manuali di gestione della soluzione, la documentazione tecnica dei prodotti installati, ecc.

La tipologia di documentazione da predisporre sarà concordata di volta in volta dalla Sogei con la Società. In ogni caso, tutta la documentazione prodotta dal Fornitore dovrà essere preferibilmente in lingua italiana.

La consegna sarà ritenuta valida se il documento consegnato rispetterà quanto concordato con la Committente e se sarà completo di tutti gli allegati.

La consegna della documentazione a corredo sarà a totale carico della Società e senza alcun onere economico aggiuntivo oltre quanto previsto dall'art. "Corrispettivo" del Contratto e le modalità di consegna saranno concordate tra Sogei e il Responsabile della fornitura, successivamente alla data di stipula.

3.3 VERIFICA DI CONFORMITÀ

La verifica di conformità verrà eseguita entro 10 (dieci) giorni decorrenti dalla data di consegna delle licenze software di cui al precedente par. 2.1 ed entro il mese successivo al trimestre di riferimento, per quanto riguarda i servizi di manutenzione e sarà effettuata dal Direttore dell'Esecuzione Sogei con il supporto del Responsabile della Fornitura della Società.

La verifica di conformità si intende positivamente superata solo se tutte le prestazioni contrattuali siano state eseguite a perfetta regola d'arte e secondo la documentazione tecnica e d'uso fornita dalla società.

A seguito della positiva verifica di conformità verrà emesso il relativo Verbale di "Verifica di conformità" che dovrà essere sottoscritto dal Responsabile della Fornitura della società e dal Direttore dell'Esecuzione Sogei.

La Società è tenuta a prestare alla Sogei, a propria cura e spese, l'assistenza tecnica necessaria e a mettere a disposizione della Sogei quanto necessario alle operazioni di verifica di conformità.

La Società potrà intervenire alla verifica di conformità, anche attraverso propri rappresentanti. In tal caso detti rappresentanti sono tenuti a sottoscrivere i documenti di verifica di conformità che verranno redatti da Sogei (verbali, certificato, ecc.)

In caso di esito negativo della verifica di conformità, ferma restando l'applicazione delle penali, di cui al successivo paragrafo 5, la Società dovrà provvedere, a propria cura e spese, entro il termine che le verrà comunicato dalla Sogei, alla eliminazione dei difetti e/o delle carenze riscontrati entro il termine massimo di 5 giorni lavorativi, oppure di 3 giorni lavorativi se il malfunzionamento segnalato riguarda problemi di sicurezza del prodotto, ovvero una vulnerabilità tecnica che metta in pericolo l'integrità della piattaforma e dei contenuti esposti.

Dopo la comunicazione, da parte della Società, dell'avvenuta eliminazione dei difetti e/o delle carenze, la Sogei procederà a nuova verifica di conformità nei termini e con le modalità di cui ai commi precedenti.

In caso di ulteriore esito negativo della verifica di conformità, la Sogei avrà facoltà di risolvere il contratto e di fare eseguire tutta o in parte la fornitura a terzi in danno della Società e fatto salvo in ogni caso il diritto al risarcimento di tutti i danni comunque subiti.

4. GESTIONE DEL CONTRATTO

Il contratto avrà efficacia dalla data della sua stipula e avrà una durata di 6 (sei) mesi, in coerenza con le tempistiche indicate all'interno della Tabella 1, e comunque, sino al completo adempimento di tutte le obbligazioni contrattuali.

4.1 RESPONSABILE DELLA FORNITURA/DELLE ATTIVITÀ CONTRATTUALI

La Società dovrà comunicare, trasmettendolo con la documentazione per la stipula, il nominativo del Responsabile della fornitura, nonché un numero di telefono e un indirizzo e-mail al quale indirizzare eventuali comunicazioni. La Società deve provvedere in piena autonomia al coordinamento e all'organizzazione delle attività nel rispetto delle specifiche e dei tempi forniti da Sogei.

Sarà compito del Responsabile curare la gestione amministrativa del contratto e delle attività legate alla fatturazione e verificare il rispetto di tutti gli adempimenti contrattuali.

4.2 MODALITÀ DI COMUNICAZIONE

La Società si impegna a comunicare, contestualmente alla presentazione della documentazione per la stipula, un numero di fax, un indirizzo e-mail, un indirizzo pec e un numero di telefono al quale rivolgersi, senza alcun limite sul numero di chiamate, per ogni comunicazione relativa alla fornitura.

Resta inteso che, per tutta la durata contrattuale, la Società dovrà garantire la piena funzionalità dei suddetti mezzi di comunicazione comunicando tempestivamente a Sogei eventuali modifiche.

4.3 ADEMPIMENTI PER LA SICUREZZA

La Società s'impegna a porre in essere quanto necessario a garantire l'esecuzione delle attività in piena aderenza con le disposizioni del D. Lgs. 81/2008 "Testo Unico sulla sicurezza durante il lavoro", cooperando e coordinandosi, in particolare, con i referenti della Committente e degli uffici dell'Amministrazione Finanziaria presso cui dovranno essere svolte le attività contrattuali, ai fini degli adempimenti di cui al comma 2 dell'art. 26 del citato decreto.

Si evidenzia che le attività di cui al presente capitolato rientrano nelle fattispecie di cui al comma 3-bis del suddetto articolo, per le quali non sussiste l'obbligo di redigere il DUVRI (Documento Unico di Valutazione dei Rischi da Interferenze).

4.4 LINGUA

Tutte le attività e la documentazione sarà in lingua italiana e/o lingua inglese.

4.5 RISERVATEZZA

Tutte le informazioni trattate e tutti i documenti, anche parziali, scambiati tra la Società e Sogei sono riservati, pertanto è richiesta la massima attenzione per il loro utilizzo, in particolare se questo avviene al di fuori delle sedi Sogei.

La Società non potrà utilizzare o condividere con terzi, a nessun titolo e in nessun modo, la documentazione, i dati o qualsiasi altra informazione fornita da Sogei, al di fuori delle attività oggetto del contratto.

5. PENALI

Sogei applicherà le penali, secondo le modalità previste in contratto, nei seguenti casi:

- per ogni giorno lavorativo di ritardo nella consegna dei prodotti software, di cui al precedente par. 2.1, si applicherà una penale pari all'1 (uno) per mille dell'importo massimo del contratto. Resta inteso che l'Impresa s'intende in ritardo anche nel caso in cui fornisca prodotti software non conformi alle prescrizioni contenute nella documentazione tecnica e d'uso;
- in caso di esito negativo della verifica di conformità di cui al paragrafo 3.3, si applicherà una penale pari all'1‰ (uno per mille) dell'importo massimo contrattuale, per ogni giorno intercorrente tra la data del verbale negativo e quello positivo;
- per ogni giorno di ritardo rispetto ai termini previsti per la presa in carico della segnalazione di malfunzionamento, di cui al precedente paragrafo 2.2, si applicherà una penale pari all'1 (uno) per mille dell'importo massimo del contratto;
- per ogni giorno di ritardo rispetto ai termini previsti per la risoluzione del malfunzionamento, di cui al precedente paragrafo 2.2, si applicherà una penale pari all'1 (uno) per mille dell'importo massimo del contratto;

Nell'ipotesi in cui l'importo delle penali applicabili superi l'ammontare del 10% (diecipercento) dell'importo contrattuale complessivo, la Sogei avrà il diritto di risolvere, totalmente o parzialmente, il contratto in danno della Società, salvo il diritto dell'eventuale maggior danno.

6. MODALITÀ DI FATTURAZIONE

In relazione alla fornitura di cui al precedente paragrafo 2, la Società potrà emettere fattura successivamente alla sottoscrizione della nota di verifica di conformità positiva.

La fattura dovrà riportare il numero di repertorio del contratto ed il codice CIG.

Si precisa che la mancanza di uno di questi elementi consente al committente di rifiutare la fattura entro il termine previsto.