MINISTERO DELL'INTERNO

MINISTERO DELL'INTERNO

LOTTO 1

CAPITOLATO TECNICO

Sistema Software per il *Web Single Sign-On*

per il CEN di Napoli

INDICE

1 OGGETTO DELLA FORNITURA

Presso il Centro Elaborazione Dati della Polizia di Stato (di seguito CEN di Napoli) dovrà essere fornita in opera una infrastruttura software per l'implementazione di meccanismi di *Identity Management* e di *Web Single Sign-On* per i sistemi informativi ivi ospitati.

Pertanto saranno oggetto della presente fornitura i prodotti software e servizi professionali specialistici di CA Technologies di seguito elencati:

- Fornitura di Licenze CA Single Sign-On for Business Users (Web SSO);
- Servizio di Progettazione, Installazione e Configurazione della Soluzione Sw di *Single Sign On for Business Users (attività da erogarsi a corpo) [Rif. Cod.* CASRVCEN003*];*
- Fornitura di Licenze CA Identity Suite for Business Users (IDM);
- Fornitura di Licenze CA Privileged Access Manager (PAM);
- Fornitura di Licenze CA Privileged Access Manager Virtual Appliance;
- Servizio di Progettazione Installazione e Configurazione delle Soluzioni Sw di *Identity Management* (IDM) e di *Privileged Access Management* (PAM) *[Rif. Cod.* CASRVCEN004*]* per complessive **244** gg/uomo da erogarsi nell'arco di **36 mesi** dall'esecutività del contratto a decorrere dall'avvenuta verifica inventariale delle licenze oggetto di fornitura;
- Servizio Assistenza Tecnica e manutenzione per 36 mesi sui prodotti software CA Technologies oggetto di fornitura, decorrenti dal collaudo inventariale dei prodotti Sw oggetto di fornitura;

Oltre alla fornitura della soluzione Sw, dovranno quindi essere erogati servizi di installazione configurazione e messa in esercizio dei prodotti in maniera integrata con le tecnologie CA già presenti presso detto Centro.

1.1 Luogo e condizioni di erogazione

Le Soluzione Sw oggetto del presente fornitura dovrà essere installata presso il Centro Elettronico Nazionale della Polizia di Stato (Napoli – Capodimonte) ed il relativo sito di Disaster Recovery presso il Centro Polifunzionale della Polizia di Stato di Bari. I servizi professionali dovranno essere erogati presso tali sedi.

L'infrastruttura Hw ed i software di base necessari per l'implementazione della soluzione saranno messi a disposizione dall'Amministrazione, secondo le specifiche ed il dimensionamento elaborato nell'ambito della fase di Progettazione.

1.2 Orario di lavoro

Per i Servizi di Progettazione Installazione Configurazione delle Soluzioni Sw di Web SSO, Identity Management e Privileged Access Management, orario standard 9-18, per ciascuna settimana lavorativa.

Per l' Assistenza Tecnica e Manutenzione di 36 mesi, il servizio viene erogato in modalità h24 per 365 giorni l'anno.

1.3 Durata

Il periodo di durata contrattuale per l'infrastruttura è fissato in 36 (trentasei) mesi dal collaudo inventariale dei prodotti software oggetto di fornitura.

2 DESCRIZIONE DELLA FORNITURA E DEI SERVIZI CONNESSI

2.1 Licenze CA

Di seguito vengono riportati i codici e le quantità delle licenze e dei Servizi Specialistici oggetto della presente fornitura

DESCRIZIONE	CODICE	QUANTITÀ
CA Single Sign-On for Business Users	CASITMBS990	25.000
Servizio di Progettazione, Installazione e Configurazione della Soluzione Sw di Single Sign On for Business Users	CASRVCEN003	1
CA Identity Suite for Business Users	CAIDSBUX990	25.000
CA Privileged Access Manager e CA Privileged Access Manager Virtual Appliance	CAPAMXSU995	10
Servizio di Progettazione Installazione e Configurazione delle Soluzioni Sw di Identity Management (IDM) e di Privileged Access Management (PAM)	CAPAMVAP995	1
Servizio di Progettazione Installazione e Configurazione delle Soluzioni Sw di Identity Management (IDM) e di Privileged Access Management (PAM)	CASRVCEN004	1

Di seguito viene fornita una descrizione di massima delle attività oggetto della presente acquisizione.

2.2 CA Single Sign-On for Business Users (Rif. CASITMBS990)

Attraverso l'utilizzo della soluzione CA Single Sign-On for Business Users l' Amministrazione intende fornire ai propri utenti accesso in modalità Single Sign-On (SSO) sicuro di classe Enterprise alle proprie risorse applicative, e centralizzare, in modalità sicura e flessibile, le funzioni di gestione dell'accesso alle identità per monitorare l'accesso ad applicazioni web e portali.

2.3 Servizio di Progettazione, Installazione e Configurazione della Soluzione Sw di Single Sign On for Business Users [Rif. Cod. CASRVCEN003]

Questa fase prevede la l'implementazione della soluzione completa per l'accesso in Single Sign On. Lo scopo di questa componente progettuale è quello di predisporre tutti gli ambienti (Sviluppo, Test, Produzione) per integrazione verso VDI Citrix tramite Federazione (SAML) con Netscaler, verso il portale ed ulteriore integrazione di altre tipologie di Web Application sulle 2 sedi di Napoli e Bari.

Il fornitore ha l'onere di redigere il progetto esecutivo relativo alle attività di installazione, configurazione, e rilascio delle soluzioni software. Deve altresì fornire la documentazione relativa alle configurazioni di dettaglio di tutti i sottosistemi coinvolti nonché alle specifiche tecniche.

L'architettura e le configurazioni definite e documentate nel progetto esecutivo saranno oggetto di approvazione da parte dell'Amministrazione. Il fornitore si impegnerà ad apportare eventuali modifiche e integrazioni su indicazione dell'Amministrazione al fine di condividere il progetto esecutivo.

Il progetto esecutivo deve includere un piano dettagliato delle attività comprensivo delle fasi di installazione, configurazione, test, collaudo.

Per ciascuna delle fasi deve essere presentata una scheda dettagliata comprensiva delle seguenti informazioni:

- obiettivo;
- responsabilità;
- prerequisiti e dipendenze;
- tempi di esecuzione;
- risorse impiegate;
- potenziali disservizi e criticità.

Inoltre il fornitore si impegna a nominare un responsabile tecnico incaricato di curare il coordinamento tecnico delle attività in fase di realizzazione e di migrazione dei primi ambienti, nonché di svolgere la funzione di unico referente nei confronti dell'Amministrazione.

Il progetto deve essere redatto entro 20 giorni dalla data di esecutività contrattuale.

A valle dell'approvazione, avranno luogo le attività di installazione e configurazione, che dovranno essere ultimate ed approntate al collaudo entro 150 gg solari dalla data di approvazione del progetto esecutivo.

2.4 CA Identity Suite for Business Users (Rif. CAIDSBUX990)

Attraverso l'adozione della soluzione CA Identity Suite l' Amministrazione intende dotarsi di funzioni di Provisioning e Deprovisioning per la gestione delle identità nel processo di accesso alle risorse/applicazioni.

CA Identity Suite permette di accrescere l'usabilità delle componenti di sicurezza da parte degli utenti finali (con funzionalità di Self Service), consentendo ai responsabili dell'autenticazione di concentrarsi sui processi di approvazione.

2.5 CA Privileged Access Manager e CA Privileged Access Manager Virtual Appliance (Rif. CAPAMXSU995 e CAPAMVAP995)

CA Privileged Access Manager incrementa la sicurezza proteggendo le credenziali amministrative sensibili come le password Root e amministrative, controllando l'accesso degli utenti con privilegi, applicando proattivamente i criteri di sicurezza, monitorando e registrando le attività degli utenti con privilegi su tutte le risorse IT.

2.6 Servizio di Progettazione Installazione e Configurazione delle Soluzioni Sw di Identity Management (IDM) e di Privileged Access Management (PAM) [Rif. Cod. CASRVCEN004]

Questa fase prevede le seguenti attività, suddivise per le due soluzioni tecnologiche:

CA Identity Management

- Setup dell'infrastruttura in tutti gli ambienti (3 ambienti: Test, Sviluppo e Produzione);
- Analisi, progettazione ed implementazione della soluzione di alimentazione dati da fonti DBMS (Rimozione FIM);

- Implementazione provisioning utenze su AD (ADN) e configurazione della funzionalità di Self service (reset password, unlock account, etc..);
- Configurazione di Workflow approvativi: Nel caso in cui fosse necessario sarà possibile analizzare in dettaglio l'implementazione di eventuali flussi autorizzativi (workflow) per gestire le approvazioni delle attività inoltrate direttamente da Identity Minder;
- Configurazione notifiche via email;

CA Privileged Access Manager

- Analisi, progettazione ed implementazione di una soluzione centralizzata per la gestione degli accessi privilegiati.

Tali attività dovranno essere elaborate con personale specializzato sulle tecnologie oggetto della fornitura, per complessivi **244** gg/uomo, da erogarsi nell'arco di **36 mesi** a decorrere dall'avvenuta approvazione del certificato di verifica inventariale.

2.7 Consegna della fornitura

La consegna delle licenze avverrà presso le sedi indicate dall'Amministrazione.

2.8 Assistenza e manutenzione soluzioni Software

Per tutte le licenze in fornitura deve essere fornito un servizio di assistenza e garanzia per un periodo di trentasei mesi (36) decorrendo dalla data di verifica di conformità inventariale.

Il fornitore deve garantire la fornitura di patch e aggiornamenti durante il periodo di copertura del contratto, inoltre deve permettere l'accesso gratuito al sito del supporto CA, dal quale sia possibile ricevere informazioni su nuove versioni e aggiornamenti dei prodotti software installati.

Il servizio di manutenzione deve garantire una copertura di 7 giorni la settimana con orario h24.

2.8.1 Modalità di esecuzione del servizio di manutenzione Software

Il servizio di manutenzione dovrà prevedere l'attivazione da parte del fornitore di un sistema per la gestione delle richieste di assistenza tecnica, che dovrà comprendere il supporto sia "online", mediante posta elettronica, sia telefonico (numero verde gratuito per il chiamante), attivo h24, sette giorni su sette, per 365 giorni l'anno. Entro la data di inizio dei servizi l'Amministrazione comunicherà alla società aggiudicataria dell'appalto i nominativi e i gruppi di lavoro abilitati all'apertura delle chiamate da parte dell'Amministrazione.

Si precisa che, ai fini della misurazione dei livelli di servizio, l'orario di inoltro della chiamata via telefono o dell'email da parte dell'Amministrazione è considerato il riferimento temporale di apertura del ticket.

Il fornitore prenderà in carico tale richiesta, evidenziandone il livello di servizio ed assegnando ad essa un identificativo che dovrà comunicare all'Amministrazione all'apertura del guasto. Il sistema di gestione dovrà garantire il tracciamento della richiesta (stato dell'intervento) in tutte le sue fasi, fino alla chiusura dell'intervento stesso.

3 LIVELLI DI SERVIZIO

L'Amministrazione richiede che il fornitore adotti ogni misura ragionevole atta a soddisfare gli obiettivi del livello di servizio indicati nella tabella qui di seguito, in relazione al supporto correttivo software, e che si impegni in modo continuativo per risolvere gli incidenti di supporto con livello di priorità 1.

Tutte le chiamate dovranno poter essere inviate al fornitore 24 ore al giorno, 7 giorni la settimana, 365 giorni l'anno. A motivo delle complessità degli ambienti tecnici, la tabella indica unicamente una stima dei tempi di risposta; i tempi di risposta effettivi possono variare.

Descrizione dei livelli di priorità

"Priorità 1" indica una condizione di indisponibilità del sistema o di inoperatività del prodotto con impatto su un ambiente di produzione, in relazione alla quale non sia immediatamente disponibile alcun Workaround, come nei casi seguenti: (i) inoperatività di server di produzione o altro sistema mission critical; (ii) rischio significativo di perdita o danneggiamento di una parte sostanziale di dati mission-critical; (iii) verificarsi di una perdita sostanziale di servizio; (iv) interruzione importante delle operazioni di business; o (v) incidente nel quale il software causa problemi catastrofici di rete o di sistema o che compromette l'integrità globale del sistema o dei dati, quando il software viene installato o quando è operativo (ovvero blocco del sistema, perdita o danneggiamento di dati o compromissione della sicurezza del sistema), con notevole impatto sulle normali operazioni in un ambiente di produzione.

"Priorità 2" indica una condizione di business di impatto elevato, che potrebbe mettere a rischio un ambiente di produzione. È possibile che il software funzioni, ma con limitazioni importanti.

"Priorità 3" indica una condizione di business di impatto limitato, con la maggioranza delle funzioni software comunque utilizzabili; potrebbe tuttavia essere necessario applicare un qualche tipo di misura per fornire il servizio.

"Priorità 4" indica (i) un problema o evento di natura problematica minore, senza impatto sul funzionamento del software, (ii) un errore nella documentazione del prodotto software, senza effetto significativo sulle operazioni; o (iii) un suggerimento relativo a nuove funzionalità o miglioramenti del prodotto software.

Service Level Objectives (SLO)	
Priorità delle richieste	**Tempi di risposta iniziali**
1	1 ora
2	2 ore lavorative**
3	4 ore lavorative**
4	1 giornata lavorativa**

**Durante il normale orario lavorativo, in base all'inserimento in CA Support Online e all'orario in cui l'incidente viene inizialmente segnalato, online o telefonicamente.

4 VERIFICA DI CONFORMITÀ

Le operazioni di verifica di conformità saranno eseguite da una specifica commissione, a tal fine designata formalmente dall'Amministrazione, che dovrà verificare la rispondenza dei prodotti e dei servizi offerti.

E' prevista una verifica di conformità inventariale relativamente alle licenze Software.

Relativamente al servizio **CASRVCEN003**, per dare avvio alle operazioni di collaudo, l'Amministrazione dovrà ricevere da parte del fornitore una formale comunicazione di approntamento al collaudo.

All'atto dell'accettazione della fornitura, in caso di esito positivo del collaudo, verrà redatto e sottoscritto dall'Amministrazione il verbale di collaudo ed accettazione, cui sarà allegato il documento rapporto di collaudo in cui sono tracciate le attività svolte durante il collaudo stesso.

Relativamente al servizio **CASRVCEN004**, si procederà alla verifica circa il suo regolare svolgimento nel rispetto delle specifiche fornite dal Direttore dell'Esecuzione Contrattuale nell'arco del periodo previsto.