**CSI PIEMONTE**

**Soluzione SOFTWARE di enterprise key management**

**(APIM23\_002)**

**REQUISITI TECNICO - FUNZIONALI**

**E MODALITÀ DI FORNITURA**

**[***Indicare qui il nome dell’operatore 4economico partecipante***]**

# INTRODUZIONE

Il CSI-Piemonte intende acquisire una soluzione di Enterprise Key Management (altrimenti KMS – Key Management System) per soddisfare gli obblighi richiesti dalla qualificazione ACN (Agenzia per la Cybersicurezza Nazionale) con riferimento alla protezione dei dati memorizzati ed in transito.

L’ACN richiede che il servizio cloud Nivola CSI, oggetto di qualificazione, garantisca autonomia al consumer (Amministrazione) nella gestione delle proprie chiavi crittografiche, inoltre devono essere definiti e implementati processi, procedure e misure tecniche per la gestione delle medesime chiavi.

Se questo è considerato sufficiente per i dati servizi ordinari, per i dati e servizi critici è richiesto in aggiunta di rivisitare il processo in modo che il consumer possa adottare un meccanismo di cifratura di tipo BYOK (Bring Your Own Key) e contestualmente di generare autonomamente, almeno la chiave principale di cifratura (root key), attraverso un HSM (Hardware Security Module).

Il sistema di Enterprise Key Management oggetto di indagine deve pertanto essere stato progettato in modo da ritenersi root of trust e, quando necessario, integrato con un HSM.

Fra i dati memorizzati rientrano anche le copie di backup di informazioni, software e immagini di sistema del servizio cloud da proteggere con crittografia forte. Mentre fra i dati in transito rientrano la trasmissione protetta con crittografia forte di backup e la gestione, importazione ed esportazione di dati operazionali.

Per i dati in transito debbono essere implementati protocolli di rete cifrati e standardizzati.

La soluzione di Enterprise Key Management viene pertanto acquisita per essere adottata nei servizi IaaS e PaaS erogati da Nivola CSI per offrire cloud infrastructure security (responsabilità del cloud provider) e cloud data security (responsabilità del cloud user), come previsto dal Cloud Shared Responsibility Model. Gli user di Nivola CSI possono interagire con il key management per gestire il proprio key material per mezzo di API o Web Interface.

Nel seguito con il termine ‘***sistema di Enterprise Key Management’*** si intende la soluzione di Enterprise Key Management integrata con un HSM, mentre con il termine ‘***soluzione di Enterprise Key Management***’ si intende il solo key management.

Il presente documento – che costituisce l’allegato 1 all’*Avviso di indagine di mercato nell’ambito dell’analisi comparativa finalizzata all’individuazione di una soluzione di Enterprise Key Management ai sensi dell’art. 68 del D. Lgs. 82/2005 e s.m.i. – Codice dell’Amministrazione Digitale (CAD)”* – ha l’obiettivo di verificare la presenza sul mercato di soluzioni dotate – in tutto o in parte – di caratteristiche funzionali e tecniche atte a soddisfare le esigenze del CSI-Piemonte, conoscendone anche le relative modalità di fornitura/distribuzione oltre che le stime di massima su costi e tempi di messa a disposizione.

# Nota bene: in considerazione della natura dell’Indagine in corso e dei relativi fini di analisi comparativa ai sensi dell’art. 68 CAD – è richiesto di omettere ovvero di non inserire tra le informazioni, elementi protetti da segreto industriale, know-how, proprietà intellettuale e/o industriale o analoga normativa (si veda anche quanto al riguardo precisato nell’avviso cui il presente documento costituisce allegato).

# RIFERIMENTI

Art. 68 CAD –.

# DESCRIZIONE IN SINTESI DELLA SOLUZIONE PROPOSTA

*Inserire qui una breve descrizione (max 2 pagine) della soluzione proposta e delle tecnologie di riferimento adottate dalla soluzione.*

# SODDISFACIMENTO DEI REQUISITI

Nel seguito sono elencati i requisiti individuati per la soluzione sulla base delle esigenze espresse anche dagli Enti fruitori del servizio.

Si distinguono in tabelle separate:

* i requisiti funzionali (RF),
* i requisiti non funzionali (RNF),
* la modalità di fornitura del sistema (software e/o hardware) (MF)

Nel seguito si descrive il significato delle colonne:

* **Gruppo di requisiti**: per i requisiti non funzionali e le modalità di fornitura descrive il raggruppamento logico del requisito. (NON MODIFICARE)
* **ID**: descrive il codice univoco del requisito (NON MODIFICARE)
* **Requisito**: descrive il singolo requisito individuato (NON MODIFICARE)
* **Obbligatorio (O) Informativo (I):** i requisiti contrassegnati con la
  + **O** sono considerati essenziali/imprescindibili. La loro assenza non permette di prendere in considerazione la soluzione proposta;
  + **I** sono utili a comprendere elementi alternativi o utili ma non bloccanti ai fini della valutazione in termini quantitativi della soluzione valutata
* **Requisito soddisfatto:** indica la disponibilità del requisito da parte della soluzione proposta nella versione attualmente disponibile (COMPILARE). La disponibilità/non disponibilità deve essere indicata con “SI/NO”.
* **Note** (DA COMPILARE OPZIONALMENTE E/O OVE RICHIESTO): spazio da utilizzare per fornire precisazioni esplicative rispetto al soddisfacimento del requisito.

**Requisiti funzionali**

| **ID** | **Requisito funzionale (RF)** | **Obbligatorio (O)** **Informativo (I)** | **Requisito soddisfatto (SI/NO)** | **Note** |
| --- | --- | --- | --- | --- |
| **RF1** | **Funzionalità utente della soluzione di enterprise key management** | **-** |  |  |
| **RF1.1** | La soluzione deve consentire la gestione unificata del key material da un’unica console centralizzata che permette di operare su tutti gli oggetti coinvolti. | **O** |  |  |
| **RF1.2** | La soluzione deve implementare meccanismi affidabili di controllo delle policy di accesso dei client al key material. | **O** |  |  |
| **RF1.3** | La console centralizzata della soluzione deve mettere a disposizione degli amministratori di sistema almeno le seguenti funzionalità:   * amministrazione centralizzata * monitoring * audit trails * audit logs * rotazione dei log * backups automatici e programmati * funzionalità di recovery e restore * report di tutte le operazioni di gestione ed encryption eseguite sul key material | **O** |  | In caso positivo fornire in allegato dettaglio delle funzionalità |
| **RF1.4** | La soluzione deve consentire l’accesso alla gestione di keys e policies per mezzo di ruoli assegnati agli utenti (role-based access). | **O** |  |  |
| **RF1.5** | La soluzione deve mettere a disposizione la funzionalità di Quorum Authorization (Dual Control) a favore di amministratori di sistema per richiedere l’approvazione multipla per operazioni sensibili. | **O** |  |  |
| **RF1.6** | La soluzione deve implementare il principio della separazione del controllo (separation of duties) nella definizione delle funzioni critiche assegnate agli amministratori di sistema. Deve essere assicurato che nessun individuo abbia sufficienti informazioni o privilegi di accesso per perpetrare frodi o danneggiamenti. | **O** |  |  |
| **RF1.7** | La soluzione deve consentire di delegare la gestione utenti ad amministratori di sistema diversi all’interno di domini multi-tenant. | **O** |  |  |
| **RF1.8** | La soluzione deve implementare meccanismi per la gestione di domini multi-tenant nel sistema. | **O** |  |  |
| **RF1.9** | La soluzione deve consentire agli utenti di creare e gestire secrets (passphrases, passwords, non key ma sensibili) ed opaque objects (passwords, non-cryptographic secrets, sia sensibili che non) in modo che i client possano utilizzarli dal sistema. | **O** |  |  |
| **RF1.10** | La soluzione deve mettere a disposizione degli utenti la funzionalità di Bring Your Own Key (BYOK) in modo da poter importare key material generato in propri sistemi. | **O** |  |  |
| **RF1.11** | La console centralizzata della soluzione deve mettere a disposizione degli utenti almeno le seguenti funzionalità di gestione del ciclo di vita delle keys:   * generazione * rotazione * distruzione * import & export | **O** |  | In caso positivo fornire in allegato dettaglio delle funzionalità |
| **RF2** | **Requisiti per la custodia sicura del key material** | **-** |  |  |
| **RF2.1** | La soluzione deve poter essere configurata come root of trust integrata da un HSM (Hardware Security Module). | **O** |  |  |
| **RF2.2** | Sono disponibili meccanismi per configurare la soluzione come root of trust singolo o centralizzato. | **I** |  | In caso positivo fornire in allegato dettaglio delle funzionalità |
| **RF2.3** | Tutte le operazioni crittografiche devono dipendere dalle key memorizzate nell’HSM. | **O** |  |  |
| **RF2.4** | La soluzione costituita da hardware e software abilita un sistema intrinsecamente affidabile. | **I** |  | In caso positivo fornire in allegato dettaglio delle funzionalità |

**Requisiti non funzionali**

I requisiti “non funzionali” includono requisiti tecnici o di servizio.

| **Classe del Requisito** | **ID** | **Requisito tecnico, architetturale, infrastrutturale e non funzionale (RNF)** | **Obbligatorio (O)**  **Informativo(I)** | **Requisito soddisfatto**  **(SI/NO)** | **Note** |
| --- | --- | --- | --- | --- | --- |
| **Standardisation** | **RNF1** | **Integrazione della soluzione con client ed applicazioni di terze parti** | **-** |  |  |
| **Standardisation** | **RNF1.1** | La soluzione deve mettere a disposizione una RESTful API semplificata per operazioni crittografiche e di gestione del key material (Create, Read, Update, Delete). | **O** |  |  |
| **Standardisation** | **RNF1.2** | L’interoperabilità con i sistemi esterni è basata su protocolli di comunicazione a Web Services. | **I** |  | In caso positivo indicare i sistemi ed i protocolli adottati |
| **Standardisation** | **RNF2** | **Integrazione della soluzione con client KMIP (Key Management Interoperability Protocol)** | **-** |  |  |
| **Standardisation** | **RNF2.1** | La soluzione deve essere compatibile con la specifica del protocollo KMIP version 1.4 o successive. | **O** |  |  |
| **Standardisation** | **RNF2.2** | La soluzione è compatibile con le librerie client open quali KMIP, OpenKMIP e PyKMIP. | **I** |  | In caso positivo indicare le librerie |
| **Standardisation** | **RNF3** | **Integrazione della soluzione con soluzioni di security dei dati e di storage** | **-** |  |  |
| **Standardisation** | **RNF3.1** | La soluzione deve mettere a disposizione un connettore per consentire la data encryption di campi sensibili dei databases in modo nativo. Il connettore deve essere compatibile con uno o più dei seguenti database engine:   * Oracle * MariaDB * MySQL * PostgreSQL * Microsoft SQL Server | **I** |  | In caso positivo indicare i database engines |
| **Standardisation** | **RNF3.2** | La soluzione deve mettere a disposizione un connettore per consentire la Transparent Data Encryption (TDE) di databases. Il connettore deve essere compatibile con uno o più dei seguenti database engine:   * Oracle * MariaDB * MySQL * PostgreSQL * Microsoft SQL Server | **O** |  | In caso positivo indicare i database engines |
| **Standardisation** | **RNF3.3** | La soluzione deve mettere a disposizione un connettore per consentire la encryption di dati mantenuti in file systems (a livello di blocchi, files, directories) o dispositivi di storage, altrimenti detti dati a riposo (data-at-rest). | **O** |  |  |
| **Standardisation** | **RNF3.4** | La soluzione deve mettere a disposizione un connettore per consentire la encryption di dati trasportati (data-in-transit) esercitando il controllo sui protocolli di rete. | **O** |  |  |
| **Standardisation** | **RNF4** | **Integrazione della soluzione con containers e ambienti Kubernetes** | **-** |  |  |
| **Standardisation** | **RNF4.1** | La soluzione mette a disposizione un connettore per eseguire processi di data security all’interno dei containers così da eseguire encryption, controllo accessi e log dell’accesso ai dati container per container. | **I** |  | In caso positivo, fornire descrizione del connettore |
| **Standardisation** | **RNF4.2** | La soluzione mette a disposizione un connettore per eseguire processi di encryption sui dati generati e memorizzati localmente all’interno dei container, ed ai dati acceduti dai container nei file systems di rete. | **I** |  | In caso positivo, fornire descrizione del connettore |
| **Standardisation** | **RNF4.3** | La soluzione mette a disposizione un connettore per applicare singole policy a tutti i containers all’interno di un Kubernetes cluster oppure policies distinte ad ogni container del cluster. | **I** |  | In caso positivo, fornire descrizione del connettore |
| **Standardisation** | **RNF4.4** | La soluzione mette a disposizione un connettore per applicare policy di accesso con granularità a livello di utenti specifici, processi e resource sets all’interno dei containers. | **I** |  | In caso positivo, fornire descrizione del connettore |
| **Standardisation** | **RNF4.5** | La soluzione implementa meccanismi di isolamento fra containers così che solo containers autorizzati possano accedere ad informazioni sensibili. | **I** |  | In caso positivo, fornire descrizione del meccanismo |
| **Security** | **RNF5** | **Requisiti di sicurezza della soluzione** | **-** |  |  |
| **Security** | **RNF5.1** | La soluzione di enterprise key management deve fornire agli amministratori di sistema un canale sicuro SSL/TLS e SSH per l’accesso remoto. | **O** |  |  |
| **Security** | **RNF5.2** | La comunicazione tra i sistemi (sia con i sistemi esterni, sia le componenti interne alla soluzione) avviene in modalità sicura, adottando politiche di cifratura del canale e securizzando le comunicazioni proteggendo i servizi con meccanismi idonei (HTTPS/SSH). | **O** |  |  |
| **Security** | **RNF5.3** | La soluzione permette l'aggiornamento delle patch di sicurezza dei System Software garantendo completa compatibilità applicativa e senza necessità di sospensione del servizio applicativo nel pieno rispetto dei livelli di servizio. | **O** |  |  |
| **Security** | **RNF5.4** | Sono disponibili i risultati dei test di vulnerabilità della soluzione, effettuati periodicamente, per le istanze già installate. | **I** |  |  |
| **Security** | **RNF5.5** | È garantito il monitoraggio e controllo della sicurezza applicativa del sistema (vulnerable assessment e patching di sicurezza). | **I** |  |  |
| **Security** | **RNF5.6** | Sono prontamente evidenziate le situazioni legate ad anomalie di sicurezza (accessi anomali, brute force attack, ecc.). | **I** |  |  |
| **Performance & Availability** | **RNF6** | **Requisiti prestazionali e di disponibilità** | **-** |  |  |
| **Performance & Availability** | **RNF6.1** | Sono disponibili i risultati dei test di carico (Stress Test) della soluzione. | **I** |  |  |
| **Performance & Availability** | **RNF6.2** | La soluzione continua ad essere disponibile indipendentemente dalla quantità di accessi, senza soluzione di continuità né decadimento significativo delle prestazioni. | **I** |  |  |
| **Backup** | **RNF7** | **Requisiti di backup della soluzione** | **-** |  |  |
| **Backup** | **RNF7.1** | Sono previste delle procedure di backup delle configurazioni dei sistemi hardware e software utilizzati dal sistema. | **I** |  | In caso positivo, fornire descrizione delle procedure |
| **Disaster Recovery & Business Continuity** | **RNF8** | **Requisiti di affidabilità, scalabilità e disponibilità** | **-** |  |  |
| **Disaster Recovery & Business Continuity** | **RNF8.1** | La soluzione di enterprise key management deve implementare meccanismi automatici di replica del key material, delle configurazioni, di bilanciamento del carico dei client e failover. | **O** |  |  |
| **Disaster Recovery & Business Continuity** | **RNF8.2** | La soluzione deve implementare meccanismi di cluster active-active. | **O** |  |  |
| **Disaster Recovery & Business Continuity** | **RNF8.3** | La soluzione deve prevedere almeno 3 cluster geograficamente separati per i data center del servizio cloud Nivola CSI. | **O** |  | In caso positivo fornire in allegato la rappresentazione dell'infrastruttura di rete comprensiva di diagramma |
| **Disaster Recovery & Business Continuity** | **RNF8.4** | La soluzione di enterprise key management configurata come root of trust integrata da un HSM, deve prevedere hardware ridondante e failover per essere altamente disponibile. | **O** |  |  |
| **Usability** | **RNF9** | **Requisiti di usabilità della soluzione** | **-** |  |  |
| **Usability** | **RNF9.1** | La console centralizzata della soluzione deve essere fruibile da web browser e/o da command line interface. | **O** |  |  |
| **Monitoring** | **RNF10** | **Requisiti di monitoraggio della soluzione** | **-** |  |  |
| **Monitoring** | **RNF10.1** | La soluzione mette a disposizione avvisi Simple Network Management Protocol (SNMP) e funzionalità di analisi dei logs per integrazione con il Security Information and Event Management (SIEM) di Nivola CSI. | **I** |  |  |
| **Monitoring** | **RNF10.2** | La soluzione deve mettere a disposizione logs in uno o più dei seguenti formati per integrazione con il SIEM di Nivola CSI:   * RFC-5424 - The Syslog Protocol * CEF - Common Event Format * LEEF - Log Event Extended Format | **O** |  | In caso positivo indicare i formati |
| **Monitoring** | **RNF10.3** | La soluzione integra o si interfaccia nativamente con strumenti per il monitoraggio infrastrutturale, ovvero si integra o si interfaccia coi log o servizi/informazioni esposte dai System Software e/o dalle componenti applicative utilizzate della soluzione. | **I** |  | In caso positivo indicare gli strumenti di monitoraggio |
| **Monitoring** | **RNF10.4** | La soluzione integra o si interfaccia nativamente con strumenti per il monitoraggio applicativo, ovvero sono indicati tutti gli eventi applicativi critici che possono occorrere durante l’esecuzione della soluzione in modo da permettere un intervento tempestivo. | **I** |  | In caso positivo indicare gli strumenti di monitoraggio |
| **Compliance** | **RNF11** | **Requisiti di conformità della soluzione** | **-** |  |  |
| **Compliance** | **RNF11.1** | L’HSM integrabile con la soluzione di enterprise key management deve possedere una o più delle seguenti certificazioni:   * eIDAS - EU regulation on electronic identification and trust services N°910/2014 * eIDAS - Common Criteria (CC) - Protection Profile EN 419221-5 * Common Criteria (CC) - Evaluation Assurance Level (EAL 2+) * NIST FIPS 140-2 certified * EU General Data Protection Regulation (GDPR) 2018 | **O** |  | In caso positivo indicare le certificazioni |
| **Compliance** | **RNF11.2** | La soluzione è stata progettata e realizzata in conformità ai requisiti previsti dal Regolamento UE 2016/79 (GDPR - General Data Protection Regulation).  In particolare, sono presi in considerazione i seguenti articoli del regolamento:   * art 25 - privacy by design. La Soluzione garantisce che gli aspetti legati all'implementazione della privacy sono tenuti in considerazione sin dalla fase di progettazione. * art 25 - privacy by default. La Soluzione garantisce che per impostazione predefinita siano trattati solo i dati personali necessari per garantire le funzionalità offerte dal servizio applicativo. * art 32 - la Soluzione garantisce l'implementazione di misure di sicurezza adeguate al rischio per i diritti e le libertà delle persone fisiche.   A titolo esemplificativo e non esaustivo:   * gestione dell'autenticazione degli utenti * gestione della profilazione utenti * gestione degli audit log * tracciamento degli accessi * storicizzazione dei dati * cifratura di canale * gestione delle sessioni e dei cookies | **I** |  |  |
| **Compliance** | **RNF11.3** | I metadati necessari per erogare i servizi del sistema di enterprise key management debbono essere trattati mediante l'impiego di infrastrutture fisiche e tecnologiche localizzate nel territorio dell'Unione europea. Ovvero i servizi del fornitore erogati da remoto(servizi cloud) debbono essere ospitati in infrastrutture localizzate nel territorio dell'Unione europea. | **O** |  | In caso positivo indicare la collocazione geografica delle infrastrutture |
| **Testability** | **RNF12** | **Requisiti di test della soluzione** | **-** |  |  |
| **Testability** | **RNF12.1** | La soluzione prevede l'esecuzione di test automatici per valutazioni di non regressione in caso di upgrade della soluzione. | **I** |  |  |
| **Testability** | **RNF12.2** | La soluzione dispone della documentazione riferita all'esecuzione dei casi di test funzionali (unit and integration test). | **I** |  |  |
| **Deployment** | **RNF13** | **Requisiti di installazione della soluzione** | **-** |  |  |
| **Deployment** | **RNF13.1** | La soluzione prevede l'utilizzo di script di installazione automatici per l'upgrade del software da una versione alla successiva. | **I** |  | In caso positivo indicare le modalità |
| **Deployment** | **RNF13.2** | Le nuove release e patch del software garantiscono la "backward compatibility". | **O** |  |  |
| **Identity, Authentication, Authorization & Access Management** | **RNF14** | **Requisiti di autenticazione, autorizzazione ed accesso** | **-** |  |  |
| **Identity, Authentication, Authorization & Access Management** | **RNF14.1** | La soluzione deve disporre di un sistema di autenticazione e autorizzazione modulare compatibile con sistemi di autenticazione federata basata sul protocollo SAML2 per gli accessi via web. | **O** |  |  |
| **Identity, Authentication, Authorization & Access Management** | **RNF14.2** | La soluzione deve prevedere la possibilità di accesso applicativo mediante l’utilizzo di credenziali centralizzate gestite tramite protocollo LDAP. | **O** |  |  |
| **Identity, Authentication, Authorization & Access Management** | **RNF14.3** | La soluzione prevede l'integrazione con Microsoft Active Directory. | **I** |  |  |
| **Identity, Authentication, Authorization & Access Management** | **RNF14.4** | È prevista la scadenza automatica della sessione di lavoro in caso di inattività configurabile a sistema. | **I** |  |  |
| **Identity, Authentication, Authorization & Access Management** | **RNF14.5** | La soluzione ha un sistema di autenticazione e autorizzazione ulteriore dedicato all’esposizione delle API (OpenID Connect, Oauth 2.0, ecc…) | **I** |  |  |
| **Documentation** | **RNF15** | **Requisiti di documentazione della soluzione** | **-** |  |  |
| **Documentation** | **RNF15.1** | Internamente alla documentazione sono chiaramente individuabili le caratteristiche infrastrutturali di dettaglio di ogni componente architetturale, ovvero esiste un datasheet con il dimensionamento Server (virtuale o fisico, CPU, RAM, dimensione disco), spazio archiviazione dati richiesto (MIN-MAX) in funzione dei vari parametri che concorrono a definire tali valori (ad es. numero di utenti di front-office concorrenti/potenziali), S.O. richiesti e System Software utilizzati e relative versioni, ecc..  Inoltre, è presente la rappresentazione dell'infrastruttura di rete comprensiva di diagramma di dettaglio, con la capacità della banda richiesta, la latenza, ecc.. | **O** |  |  |
| **Documentation** | **RNF15.2** | Internamente alla documentazione sono presenti le istruzioni di configurazione, di avvio iniziale e il manuale di installazione della soluzione con la descrizione delle strutture dati e del loro popolamento iniziale. | **I** |  |  |
| **Documentation** | **RNF15.3** | Internamente alla documentazione o al sito on-line è presente la roadmap di evoluzione della soluzione con indicazione chiara delle features realizzate o previste e delle date di rilascio e ritiro di ogni singola versione. | **I** |  |  |

**Modalità di fornitura del sistema**

| **Classe del Requisito** | **ID** | **Modalità di fornitura (MF)** | **Obbligatorio (O)**  **Informativo(I)** | **Requisito soddisfatto**  **(SI/NO)** | **Note** |
| --- | --- | --- | --- | --- | --- |
| **Hardware** | **L1** | L’hardware deve essere provvisto di storage interno in configurazione mirror, doppie porte di rete, doppia alimentazione e raffreddamento ridondato. | **O** |  |  |
| **Hardware** | **L2** | L’hardware deve essere provvisto di una interfaccia terminale con linea seriale RS-232C e porta VGA per installazione e configurazione iniziale. | **I** |  |  |
| **Technological** | **L3** | La soluzione di enterprise key management può essere ospitata nella rete dei data center di Nivola CSI in una o più delle seguenti modalità:   * LAN Appliance * Virtual Appliance | **I** |  | In caso positivo indicare le modalità |
| **Measures** | **L4** | La licenza (hardware e software) non prevede limitazioni a metrica associata. Ad es.: numero di utenti e/o processori e/o accessi contemporanei o loro assenza; eventuale numero massimo di processori o core su cui il software può essere eseguito; numero di elaborazioni da effettuare nell'arco di validità della licenza superato il quale occorre corrispondere un controvalore maggiore. | **I** |  | In caso di uso di metrica specificare quale |
| **Licensing** | **L5** | Le condizioni di licenza con cui viene offerta la soluzione e/o il sistema permettono di offrire servizi a terzi basati su quest'ultima. | **O** |  | Se detti terzi sono in qualche modo categorizzati e/o limitati (es. controllate / controllanti) specificare quali |
| **Licensing** | **L6** | La licenza con cui viene messa a disposizione la soluzione è di tipo Software Libero o di tipo Open Source. | **I** |  |  |
| **Licensing** | **L7** | La licenza con cui viene messa a disposizione la soluzione è di tipo proprietario. | **I** |  |  |
| **Licensing** | **L8** | I diritti concessi in licenza si estendono ad ogni patch, aggiornamento e/o release eventualmente rilasciate sul prodotto in corso di contratto, senza costi aggiuntivi. | **O** |  |  |
| **Licensing** | **L9** | La licenza è concessa a tempo indeterminato/"perpetual". | **I** |  |  |
| **Licensing** | **L10** | La licenza è concessa a tempo determinato o in "subscription" o "canone di servizio". | **I** |  |  |
| **Dependencies** | **L11** | La licenza e/o il prodotto prevede dipendenze da elementi di terze parti eventualmente integrati nel prodotto in oggetto e/o da cui lo stesso dipenda per il relativo funzionamento. | **I** |  | In caso positivo, fornire qui o in allegato ad hoc l'elenco dettagliato corredato dagli annessi vincoli d'uso di qualsivoglia natura, indicando quali di detti elementi sono da acquisirsi nel caso autonomamente da parte del CSI-Piemonte |
| **Dependencies** | **L12** | L’HSM integrato nel sistema è fornito dal titolare della soluzione di enterprise key management secondo matrice di compatibilità del prodotto. | **I** |  |  |
| **Software Distribution** | **L13** | La soluzione di enterprise key management deve essere messa a disposizione "on-premises". | **O** |  |  |
| **Licensing** | **L14** | L’HSM integrato nel sistema può essere messo a disposizione dei data center di Nivola CSI anche attraverso modalità as a service (servizio erogato da remoto sui sistemi del fornitore o di terzi accreditati). | **I** |  |  |
| **Application Support** | **L15** | Il produttore della soluzione adotta un processo di gestione delle problematiche di sicurezza che prevede:   * la pubblicazione e la comunicazione puntuale di un bollettino delle security issues rilevate nelle varie versioni di strumento * la messa a disposizione di patch per la correzione delle security issues e/o di workaround da adottare in attesa della predisposizione delle patch | **O** |  |  |
| **Business Support** | **L16** | Il produttore della soluzione (hardware e software) opera tramite una rete di reseller, non in regime di esclusività, sul territorio italiano. | **I** |  |  |
| **Business Support** | **L17** | Il produttore della soluzione (hardware e software) opera in regime di esclusività sul territorio italiano, senza l'intermediazione di reseller. | **I** |  |  |
| **Business Support** | **L18** | Il fornitore dispone di personale tecnico certificato dal produttore, nel caso in cui il fornitore della soluzione non sia anche il produttore del software e/o hardware. | **O** |  |  |
| **Business Support** | **L19** | Il fornitore può erogare giornate di formazione e training on the job al personale del CSI-Piemonte. | **O** |  |  |

**DIMENSIONAMENTO DEL SISTEMA**

Per consentire al fornitore una stima dei costi si riportano di seguito alcuni dati di dimensionamento i cui volumi devono essere garantiti dalle condizioni contrattuali e dal piano tariffario applicato:

| **ID** | **Descrizione** | **Q.tà** |
| --- | --- | --- |
| **1** | Numero di clients e/o applicazioni di terze parti | **100** |
| **2** | Numero di data center del servizio cloud Nivola CSI | **3** |
| **3** | Numero di HSM keys | **2000** |
| **4** | Numero di transazioni al secondo (tps) per HSM | **450** |
| **5** | Numero di risorse CSI da formare. | **10** |

**COSTI E TEMPI INDICATIVI DELLA MESSA A DISPOSIZIONE DELLA SISTEMA**

Si richiede di compilare le seguenti tabelle relative a costi e tempi per la messa a disposizione del sistema desiderato. Si ricorda che si tratta di stime di massima, non impegnative (non costituiscono offerta), ma utili a definire la base d'asta e il capitolato per una eventuale gara finalizzata all’acquisizione del sistema dal mercato.

I valori economici stimati verranno considerati oneri fiscali esclusi.

**Requisiti funzionali e non funzionali**

In base alle modalità di fornitura del sistema come da requisiti:

* **L14**: HSM messo a disposizione in modalità as a service
* **L13**: KMS messo a disposizione "on-premises"
* **L12**: HSM fornito dal titolare del KMS
* **L10**: licenza concessa in "subscription" o "canone di servizio"
* **L9**: licenza "perpetual"
* **L3**: KMS in modalità LAN Appliance o Virtual Appliance

Possono individuarsi le seguenti tipologie di fornitura ovvero aggregati di oggetti con relativa tabella dei costi:

* **HSM fornito dal titolare del KMS**
* KMS LAN Appliance e HSM fisico con licenze perpetual o subscription (tabella **TB1**)
* KMS Virtual Appliance e HSM fisico con licenze perpetual o subscription (tabella **TB3**)
* KMS LAN Appliance e HSM as a service con licenze perpetual o subscription (tabella **TB2**)
* KMS Virtual Appliance e HSM as a service con licenze perpetual o subscription (tabella **TB4**)
* **HSM fornito da terze parti**
* KMS LAN Appliance con licenze perpetual o subscription (tabella **TB6**)
* KMS Virtual Appliance con licenze perpetual o subscription (tabella **TB5**)

In base ai dati di dimensionamento indicati, ogni tipologia di fornitura deve soddisfare il requisito RNF8.3 per continuità di servizio rispetto ai data center del servizio cloud Nivola CSI.

Ovviamente la classificazione non è da considerarsi esaustiva e sono possibili altri aggregati di oggetti a discrezione del fornitore, per questo è stata predisposta la tabella **TB7** per le tipologie diverse dalle precedenti.

| **TB1** | **HSM fornito dal titolare del KMS** | | |
| --- | --- | --- | --- |
| **ID** | **Voci di costo** | **Stima costo licenze perpetual**  **(Euro)** | **Stima costo** **licenze subscription**  **(Euro)** |
| 1 | KMS LAN Appliance on-premises |  |  |
| 2 | HSM fisico |  |  |
|  | **TOTALE** |  |  |

| **TB2** | **HSM fornito dal titolare del KMS** | | |
| --- | --- | --- | --- |
| **ID** | **Voci di costo** | **Stima costo licenze perpetual**  **(Euro)** | **Stima costo** **licenze subscription**  **(Euro)** |
| 1 | KMS LAN Appliance on-premises |  |  |
| 2 | HSM as a service |  |  |
|  | **TOTALE** |  |  |

| **TB3** | **HSM fornito dal titolare del KMS** | | |
| --- | --- | --- | --- |
| **ID** | **Voci di costo** | **Stima costo licenze perpetual**  **(Euro)** | **Stima costo** **licenze subscription**  **(Euro)** |
| 1 | KMS Virtual Appliance on-premises |  |  |
| 2 | HSM fisico |  |  |
|  | **TOTALE** |  |  |

| **TB4** | **HSM fornito dal titolare del KMS** | | |
| --- | --- | --- | --- |
| **ID** | **Voci di costo** | **Stima costo licenze perpetual**  **(Euro)** | **Stima costo** **licenze subscription**  **(Euro)** |
| 1 | KMS Virtual Appliance on-premises |  |  |
| 2 | HSM as a service |  |  |
|  | **TOTALE** |  |  |

| **TB5** | **HSM fornito da terze parti** | | |
| --- | --- | --- | --- |
| **ID** | **Voci di costo** | **Stima costo licenze perpetual**  **(Euro)** | **Stima costo** **licenze subscription**  **(Euro)** |
| 1 | KMS Virtual Appliance on-premises |  |  |
|  | **TOTALE** |  |  |

| **TB6** | **HSM fornito da terze parti** | | |
| --- | --- | --- | --- |
| **ID** | **Voci di costo** | **Stima costo licenze perpetual**  **(Euro)** | **Stima costo** **licenze subscription**  **(Euro)** |
| 1 | KMS LAN Appliance on-premises |  |  |
|  | **TOTALE** |  |  |

| **TB7** | **Fornitura custom** | | |
| --- | --- | --- | --- |
| **ID** | **Voci di costo** | **Stima costo licenze perpetual**  **(Euro)** | **Stima costo** **licenze subscription**  **(Euro)** |
| 1 | KMS on-premises (specificare la modalità di fornitura come da requisiti, es. virtual o LAN appliance, software distribution, ecc.) |  |  |
| 2 | HSM (se fornito dal titolare del KMS specificare la modalità di fornitura come da requisiti, es. LAN appliance, hardware, as-a-service, ecc.) |  |  |
|  | **TOTALE** |  |  |

Infine, per tutte le tipologie di fornitura come da tabelle TB1, TB2, TB3, TB4, TB5, TB6 e TB7, il fornitore può indicare i costi di oggetti accessori che rappresentano costi aggiuntivi necessari all’eventuale soddisfacimento dei requisiti Informativi (I), per questo è stata predisposta la tabella **TB8**.

| **TB8** | **Forniture aggiuntive** | |
| --- | --- | --- |
| **ID** | **Voci di costo** | **Stima costo**  **(Euro)** |
| 1 | Oggetto di fornitura (specificare il tipo di licenza, eventuale metrica, riferimento al requisito RF o RNF, fornitore se diverso dal titolare, ecc.) |  |
| 2 | … |  |
|  | **TOTALE** |  |

**Supporto per la formazione**

| **ID** | **Voci di costo** | **Stima costo (Euro)** | **Stima tempi (GG)** |
| --- | --- | --- | --- |
| 1 | Formazione alle risorse CSI che si occuperanno dell’amministrazione del sistema |  |  |
|  | **TOTALE** |  |  |