

Leistungsbeschreibung

Leistungsbeschreibung Secrets- und Privileged Access Management-System

Autor/in: kubus IT eGbR

Letzte Speicherung: 13.05.2026

Leistungsbeschreibung**Inhalt**

1	Teil A - Leistungsbeschreibung	4
1.1	Ziel der Ausschreibung	4
1.2	Begriffsklärung Secrets- und Privileged Access Management-System	4
1.3	Ausschreibungsgegenstand	4
1.3.1	Nicht-funktionale Anforderungen	4
1.3.1.1	Betriebssicherheit und Verfügbarkeit	4
1.3.1.2	Performance und Skalierbarkeit.....	4
1.3.1.3	Sicherheit und Compliance	5
1.3.1.4	Benutzerfreundlichkeit und Bedienbarkeit	5
1.3.1.5	Integration und Interoperabilität	5
1.3.1.6	Wartbarkeit und Updates	5
1.3.1.7	Reporting und Transparenz	5
1.3.2	Funktionale Anforderungen	5
1.3.2.1	Allgemeine Anforderungen an die Plattform	6
1.3.3	Einführungsprojekt	6
1.3.3.1	Allgemein	6
1.3.3.2	Mandantentrennung	7
1.3.3.3	Test und Dokumentation	7
1.3.3.4	Anbindung von Infrastruktur-Systemen.....	7
1.3.3.5	Anbindung von Datenbanken.....	7
1.3.3.6	Sicherheits- und Compliance-Anforderungen	8
1.3.4	Schulung	8
1.3.5	Lizenzen.....	8
1.3.5.1	Lizenzen für das Einführungsprojekt.....	9
1.3.5.2	Lizenzen für Nachkauf (optional)	9
1.3.5.3	Einzelabruf vor Ablauf der Rahmenvereinbarung	9
1.3.6	Consulting-/Supportdienstleistungen (optional).....	9
1.3.7	Support/Störungsbeseitigung.....	10
1.4	Leistungsumfang	10
1.4.1	Bereitstellung der Softwarekomponenten	11
1.4.2	Beauftragte Module	11
1.4.3	Rahmenvertrag und Erweiterungsoptionen	11
1.4.4	Wartung, Subskription und Herstellersupport	11
1.5	Abnahme.....	11
1.5.1	Allgemein.....	11
1.5.2	Frist zur Funktionsprüfung.....	12
1.5.3	Umgebung zur Funktionsprüfung	12
1.5.4	Abbruchbedingungen wegen betriebsverhindernden und/oder betriebsbehindernden Mängeln	12

Leistungsbeschreibung

1.5.5	Mangelklassifizierung	12
1.5.5.1	betriebsverhindernder Mangel	12
1.5.5.2	betriebsbehindernder Mangel	12
1.5.5.3	leichter Mangel.....	12
1.5.6	Abnahmewiederholung nach Abbruch wegen betriebsverhindernden und/oder betriebsbehindernden Mängeln	12
1.5.7	Abnahmewiederholung nach Abbruch wegen betriebsverhindernden und/oder betriebsbehindernden Mängeln trotz vollständiger Durchführung .	13
1.5.8	leichte Mängel	13
1.5.9	Teilabnahmen.....	13
1.5.10	förmliche Abnahme	13
2	Teil B – Leistungsbeschreibung	13
2.1	Vertragsgrundlage	13
2.2	Höchstvolumen	14
2.3	Laufzeit	14
2.4	Zertifikate	14
2.5	Einsatz von KI	14
2.6	No-spy-Erklärung.....	15
2.7	Außerordentliche Kündigung aus wichtigem Grund	15
2.8	Einsatz Unterauftragnehmer	16
2.9	Vertraulichkeit	16
2.10	Sublicensing-Vereinbarung	16

Leistungsbeschreibung

1 Teil A - Leistungsbeschreibung

1.1 Ziel der Ausschreibung

Ziel der Ausschreibung ist die Einführung eines Secrets Management Systems (SAM) mit angehängtem und schrittweise auszubauendem Privileged Access Management System (PAM).

Nach Wiedereinführung der regelmäßigen Secrets- und Passwortwechsel ist in vielen Teilen der kubus IT die Notwendigkeit für ein Secrets Management System deutlich geworden. Insbesondere durch die Zunahme von Infrastructure as Code und den vermehrten Einsatz containerbasierter Infrastruktur werden wesentlich mehr Secrets benötigt als noch in der Vergangenheit. Um dieser Herausforderung entgegenzutreten, ist die Umsetzung des Secrets und Access Management Systems On Prem geplant.

Das Produkt wird inklusive Implementierung ausgeschrieben, da insbesondere beim Erstanchluss der Systeme im Zuge einer Implementierung des Produktes i.d.R. komplexere Einstellungen nötig sind.

1.2 Begriffsklärung Secrets- und Privileged Access Management-System

Unter einem Secrets- und Privileged Access Management-System versteht die Auftraggeberin ein System zur Verwaltung und Sicherung privilegierter Zugriffe und zum automatischen Passwortwechsel (Privileged Access Management System (PAM) bzw. Secrets und Access Management System (SAM)).

1.3 Ausschreibungsgegenstand

1.3.1 Nicht-funktionale Anforderungen

Die eingesetzte Softwarelösung muss neben den funktionalen Anforderungen auch bestimmte nicht-funktionale Kriterien erfüllen. Diese Anforderungen betreffen die Betriebssicherheit, Performance, Skalierbarkeit, Zuverlässigkeit, Sicherheit, Benutzerfreundlichkeit und Integrationsfähigkeit.

1.3.1.1 Betriebssicherheit und Verfügbarkeit

- Die Lösung muss eine Hochverfügbarkeit der zentralen, die Kernfunktionen des Secrets- und Privileged Access Management-System realisierenden, Komponenten sicher stellen.
- Wartungs- und Supportmaßnahmen dürfen den produktiven Betrieb nicht unzulässig beeinträchtigen.
- Systemkomponenten müssen fehlerresistent und stabil betrieben werden können.
- Bei Ausfällen müssen Monitoring- und Alarmierungsmechanismen vorhanden sein, um rechtzeitig reagieren zu können.

1.3.1.2 Performance und Skalierbarkeit

- Die Software muss leistungsfähig sein und auch bei einer steigenden Anzahl von Endgeräten stabil arbeiten.
- Sie muss eine skalierbare Architektur besitzen, die auch über die oben angegebenen Dimensionierungskennzahlen hinaus performant funktionsfähig ist.
- Performanceindikatoren wie Antwortzeiten müssen auch unter Last zuverlässig eingehalten werden.

Hinweise zur Dimensionierung:

Leistungsbeschreibung

Die Anzahl privilegierter Nutzer ist 500 im Vollausbau.

Die Anzahl an Cloudumgebungen ist 3 im Vollausbau.

Die Anzahl der Passwortsafe Nutzer ist 17000 im Vollausbau.

Die Anzahl an technischen Accounts zum Anschluss an das Secrets Management System ist prognostiziert mit 60000.

1.3.1.3 Sicherheit und Compliance

- Die Lösung muss Rollen- und Berechtigungskonzepte unterstützen, die den Zugriff auf Module, Funktionen und Daten streng steuern.
- Alle Kommunikations- und Datenübertragungen zwischen Servern, Clients und anderen Bestandteilen müssen verschlüsselt erfolgen und sollten soweit möglich authentifiziert erfolgen.
- Es müssen umfassende Audit- und Protokollierungsfunktionen vorhanden sein, die alle administrativen und operativen Aktionen nachvollziehbar dokumentieren.
- Die Lösung muss den aktuellen Stand der Technik insbesondere in Bezug auf IT-Sicherheit erfüllen und kontinuierlich aktualisierbar sein.
- Die Nutzung der Software muss DSGVO-konform erfolgen, insbesondere im Hinblick auf personenbezogene Daten von Endanwendern.
- Alle Funktionen der Lösung müssen datenschutzfreundlich konzipiert sein (Privacy by Design / Privacy by Default) und eine sichere Verarbeitung sensibler Daten sicher stellen.
- Die Lösung muss die Anforderungen gängiger Sicherheits- und Compliance-Standards erfüllen, insbesondere für die eingesetzte OS-Umgebung, On-Premise, Cloud- und hybride Betriebsmodelle.

1.3.1.4 Benutzerfreundlichkeit und Bedienbarkeit

- Die Plattform muss eine intuitive, konsistente Benutzeroberfläche bieten, die eine effiziente Nutzung aller Module ermöglicht.
- Administrations- und Reporting-Funktionen sollen klar strukturiert und nachvollziehbar sein.
- Remote- und Automatisierungsfunktionen müssen auch für Standard-Administratoren ohne umfangreiche Spezialkenntnisse bedienbar sein.

1.3.1.5 Integration und Interoperabilität

- Die Lösung muss nahtlos in bestehende Infrastrukturen integriert werden können. Insbesondere Anbindung an Active Directory zur Authentifizierung von Nutzern.
- Schnittstellen zu anderen IT-Systemen müssen verfügbar und dokumentiert sein, um eine einfache Anbindung an Monitoring- und Reporting-Lösungen zu ermöglichen.
- Die Lösung muss On-Premise, Cloud- und hybride Szenarien unterstützen

1.3.1.6 Wartbarkeit und Updates

- Alle Module müssen herstellerseitig regelmäßig aktualisiert und gewartet werden.
- Updates und Patches dürfen den produktiven Betrieb nicht gefährden.
- Die Software muss eine Versionierung und Nachvollziehbarkeit aller Änderungen und Updates sicherstellen.

1.3.1.7 Reporting und Transparenz

- Die Lösung muss eine zentrale Reporting-Funktion bereitstellen
- Reports müssen exportierbar, planbar und automatisierbar sein.

1.3.2 Funktionale Anforderungen

Die eingesetzte Softwarelösung muss die nachfolgend beschriebenen funktionalen Anforderungen erfüllen.

Leistungsbeschreibung

1.3.2.1 Allgemeine Anforderungen an die Plattform

Das System muss:

- grafische Verwaltungsoberflächen für alle eingesetzten Module bieten
- Umsetzbarkeit eines Rollen- und Berechtigungskonzepts über alle Funktionsbereiche hinweg mit Anbindung zum Microsoft Active Directory realisieren können
- Mandanten- und gruppenbasierte Verwaltung von Secrets unterstützen
- Vollständig virtualisiert lauffähig als Appliance oder auf Windows/Linux Systemen sein
- Das Management von Secrets (z.B. SSH Keys) und technischen Accounts ermöglichen
- einen automatisierten Passwortwechsel für technische Accounts ermöglichen
- eine Anbindung an ein Identity- und Access-Management ermöglichen
- spezialisierte Sicherheitslösungen für DevOps-Umgebungen (DevSecOps), um Secrets, Passwörter und kryptografische Schlüssel in CI/CD-Pipelines, Containern und Cloud-nativen Anwendungen automatisiert verwalten
- ein Endpointmanagement unterstützen, dass die lokalen Administratorrechte auf Windows- und Linux-Endgeräten entfernt
- eine Aufzeichnung von Sitzungen zu Windows und Linux Systemen ermöglichen
- eine Supervision von Sitzungen zu Windows und Linux Systemen ermöglichen und dieses durch den Supervisor unterbrechen lassen. (4-Augen-Prinzip)
- Aufzeichnung und Supervision gruppenbasiert berechtigen und durchführen können

1.3.3 Einführungsprojekt

Position	Beschreibung/Bezeichnung	Einheit	Anzahl	Anzahl Monate
EI-1	Einführung des Secrets- und Privileged Access Management-Systems inkl. Installation Herstellung der Funktionsbereitschaft und Funktionstest (Eine Test- und eine Produktionsumgebung auf Ressourcen die durch die der kubus IT oder ihren RZ-Dienstleister zur Verfügung gestellt werden)	Pauschal	1	Nicht zutreffend

Hinweis: Notwendige Lizenzen für die Herstellung der Abnahmebereitschaft sind in die Pauschale einzukalkulieren. Im Falle einer Nutzung von Testlizenzen ist die Auftraggeberin auf eventuelle Abweichung zum Funktionsumfang bei der Nutzung der Produktivlizenzen vor der Anzeige der Abnahmebereitschaft mindestens in Textform per E-Mail hinzuweisen.

Hinweis: Für die Einführung des Systems (Produktions- und Testumgebung) für einen weiteren Mandanten wird die Auftraggeberin die Aufwandsschätzung über die Consulting Position beim Auftragnehmer anfordern und diese dann über nachgewiesene Aufwände über diese Position abrechnen.

1.3.3.1 Allgemein

Der Auftragnehmer soll für die kubus IT die Einführung des Secrets- und Privileged Access Management-Systems übernehmen.

Der Auftragnehmer installiert und richtet alle notwendigen Komponenten nach vorheriger Absprache mit der Auftraggeberin ein, um die Funktionalität sicherzustellen.

Es ist eine Test- und eine Produktionsumgebung auf Ressourcen, die durch die der kubus IT oder ihren RZ-Dienstleister zur Verfügung gestellt werden, herzustellen.

Hochverfügbarkeit, Disaster Recovery Fähigkeit und Skalierbarkeit sind hierbei sicherzustellen.

Die notwendigen Ressourcen für Storage und Compute sowie die Betriebssysteme und Lizenzen, sofern benötigt, werden durch die der kubus IT oder ihren RZ-Dienstleister bereitgestellt.

Leistungsbeschreibung

Der Auftragnehmer stellt der Auftraggeberin eine Checkliste der benötigten Komponenten (Server mit CPU, RAM und Storageanforderungen, IPs/Netzgrößen, Kommunikationsbeziehungen mit Protokoll und Port) bereit anhand derer, die für die Umgebung notwendigen Systeme innerhalb der Systemlandschaft der kubus IT bereitgestellt werden können.

Die sonstigen notwendigen Lizenzen für das Secrets- und Privileged Access Management-System selbst werden in separaten Positionen aufgelistet und von der kubus IT über diese Positionen abgerufen und vergütet.

1.3.3.2 Mandantentrennung

Die Einführung erfolgt zunächst nur für den Mandanten kubus IT. Da die kubus IT-Dienstleister für die AOK PLUS und AOK Bayern ist, sieht der Vertrag ebenfalls eine optionale weitere Einführung bei diesen Gesellschaftern als weitere Mandaten vor. Wie die Einführung bei den anderen Mandanten realisiert werden könnte und, sofern relevant, welche Risiken bei unterschiedlichen Varianten der Mandantentrennung bestehen, ist vom Auftragnehmer, sofern es unterschiedliche Möglichkeiten gibt, der Auftraggeberin schriftlich darzulegen.

1.3.3.3 Test und Dokumentation

Der Auftragnehmer führt innerhalb des Einführungsprojektes alle notwendigen Funktionstests und Sicherheitsprüfungen zusammen mit einem Mitarbeiter der Auftraggeberin durch.

Die Konfiguration der Systeme sowie die notwendigen Prozesse zum Betrieb und zur Wartung der Systembestandteile werden vom Auftragnehmer dokumentiert und an die Auftraggeberin in editierbarer Form übergeben.

1.3.3.4 Anbindung von Infrastruktur-Systemen

Darüber hinaus ist, innerhalb des Einführungsprojektes, exemplarisch die Integration von 3 Windows- und 3 Linux-Servern vorzunehmen, um automatisierte Passwortrotation für lokale und Domänenkonten an 3 Beispielen (Accounts sind Teil der Mindestabnahmemenge) zu demonstrieren.

Es soll jeweils ein System als Vollintegration durch den Auftragnehmer, ein System als begleitete Integration durch die Auftraggeberin und ein System als Integration durch die Auftraggeberin unter Beobachtung des Auftragnehmers im System hinzugefügt werden.

Die Integration des SAM ist mit 3 bestehenden Anwendungen, 3 Container-Plattformen und CI/CD-Tools zu demonstrieren.

Zur Anbindung weiterer zu verwaltender Systeme an das Secrets- und Privileged Access Management-System sind vom Auftragnehmer Anleitungen in deutscher Sprache und in editierbarer Form, gern unterstützt durch entsprechende Screenshots, anzufertigen.

1.3.3.5 Anbindung von Datenbanken

Die Unterstützung für gängige Datenbanktypen (z. B. Oracle, MSSQL, MySQL, PostgreSQL) ist sicherzustellen. Die Einrichtung von sicheren Zugriffen für Service-Accounts und privilegierte Datenbank-Benutzer ist, innerhalb des Einführungsprojektes, exemplarisch an 3 Accounts (Accounts sind Teil der Mindestabnahmemenge) zu demonstrieren ebenso wie die automatisierte Passwortrotation und Auditierung. Zur Anbindung weiterer Datenbanken sind vom Auftragnehmer Anleitungen in deutscher Sprache und in editierbarer Form, gern unterstützt durch entsprechende Screenshots, anzufertigen.

Leistungsbeschreibung

1.3.3.6 Sicherheits- und Compliance-Anforderungen

Die Umsetzung des Einführungsprojekts muss entlang der relevanten Standards (ISO 27001, BSI und DSGVO) erfolgen. Die Einführung bei der kubus IT hat insbesondere entlang der Organisationssicherheitsleit- und -richtlinien zu erfolgen. Der Auftragnehmer unterstützt dahingehend die Auftraggeberin bei der Erstellung der relevanten Dokumente (z.B. OSRL-Tabellen und Risikoanalysen) sowie bei der Erstellung und Umsetzung eines rollenbasierten Zugriffskontrollmodells (RBAC). Die Protokollierung und das Monitoring aller privilegierten Sitzungen im System sind einzurichten. Eine Anbindung an das SIEM der Auftraggeberin ist ebenfalls zu realisieren.

1.3.4 Schulung

Position	Beschreibung/Bezeichnung	Einheit	Anzahl	Anzahl Monate
SI-1	Produktschulung für die im Rahmen der Implementierung installierten Produkte für bis zu 5 Mitarbeiter	Schulung	1	Nicht zutreffend

Position	Beschreibung/Bezeichnung	Einheit	Anzahl	Anzahl Monate
SO-1	Produktschulung für die im Rahmen der Implementierung installierten Produkte für bis zu 5 Mitarbeiter	Schulung	1	Nicht zutreffend

Die Schulung soll remote abgehalten werden und wenigstens alle Bestandteile und Mechaniken/Prozesse enthalten, die für den Betrieb notwendig sind. Da die Installation im Einführungsprojekt durch den Auftragnehmer erfolgen soll, ist eine Installationsschulung nicht notwendig. Es sind die entsprechenden die Kosten für eine Inhouse-Schulung remote zu kalkulieren. Zu schulende Mitarbeiter andere Firmen sind zu dieser Schulung nicht zugelassen. Die Auftraggeberin kann hierfür die Plattform Microsoft Teams bereitstellen, um eine Webkonferenz zu ermöglichen.

Die Schulung muss in deutscher oder englischer Sprache erfolgen (Sprachniveau mindestens C1).

Der Auftragnehmer muss der Auftraggeberin ebenfalls ermöglichen über diesen Vertrag weitere Mitarbeitende nachschulen zu lassen (vgl. Position SO-1)

Die Schulung muss regelmäßig wenigstens alle 2 Jahre durchführbar sein.

1.3.5 Lizenzen

Die Lizenzkosten sind hier pro Monat abgefragt, da die Möglichkeit gegeben sein soll flexibel Lizenzen nachzufordern, um auf wechselnde Gegebenheiten zu reagieren.

Eine Mindestmietdauer für die Lizenzen aus dem Initialaufbau wird hierbei zugesichert (vgl. Tabelle).

Leistungsbeschreibung

1.3.5.1 Lizenzen für das Einführungsprojekt

Position	Beschreibung/Bezeichnung	Einheit	Anzahl Einheiten	Anzahl Monate
LI-1	PAM-Nutzer (Aufzeichnungssystem für privilegierte Zugriffe, incl. Passwortspeicher, Weboberfläche zur Passwortverwaltung)	USER	20	48
LI-2	Secrets Provider für Cloud- und Containerisierte Systeme	RZ/CLOUD	1	48
LI-3	Secrets Provider als zentralisierte Einheit für OnPrem-Umgebung (ein HA-Paar)	Stück	1	48

1.3.5.2 Lizenzen für Nachkauf (optional)

Die Lizenzkosten sind hier pro Monat abgefragt, da die Möglichkeit gegeben sein soll flexibel Lizenzen nachzufordern, um auf wechselnde Gegebenheiten zu reagieren. Die Auftraggeberin möchte hiermit ein „Co-terming“ realisieren (Alle Lizenzen laufen bis zum selben Zeitpunkt bzw. können dann einheitlich über den nächsten Zeitraum verlängert werden).

Position	Beschreibung/Bezeichnung	Einheit	Anzahl Einheiten	Anzahl Monate
LO-1	PAM-Nutzer (Aufzeichnungssystem für privilegierte Zugriffe, incl. Passwortspeicher, Weboberfläche zur Passwortverwaltung)	USER	1	1
LO-2	Secrets Provider für Cloud- und Containerisierte Systeme	RZ/CLOUD	1	1
LO-3	Secrets Provider als zentralisierte Einheit für OnPrem-Umgebung (ein HA-Paar)	Stück	1	1
LO-4	Secrets Provider als Agent auf einem Server	Stück	1	1
LO-5	Nutzer von Passwortspeicher, Weboberfläche zur Passwortverwaltung ohne Aufzeichnung	USER	1	1

Die Anzahl der angegebenen Einheiten im Preisblatt (Voraussichtliche Abnahmemenge) dient der Vergleichbarkeit und stellt keine Abnahmegarantie, Mindest- oder Maximalmenge dar.

1.3.5.3 Einzelabruf vor Ablauf der Rahmenvereinbarung

Die Auftraggeberin behält sich vor, vor Ablauf der Rahmenvereinbarung über einen weiteren Einzelabruf die Subscription zu beauftragen. Eine etwaige Nachbestellung wird der Höhe nach durch das Höchstvolumen der Rahmenvereinbarung gedeckelt und wird die Laufzeit von 12 Monaten nicht überschreiten.

1.3.6 Consulting-/Supportdienstleistungen (optional)

Zusätzliche Consultingleistungen in deutscher oder englischer Sprache (Sprachniveau mindestens C1), die über das Einführungsprojekt hinaus gehen, werden gesondert vergütet. Die Consultingleistungen sind remote, mit Hilfe eines von der Auftraggeberin zur Verfügung zu stellenden Webkonferenzsystems (aktuell MS Teams), zu erbringen.

Supportdienstleistungen sind Leistungen, die nicht über Consulting oder den bestehenden Support vom Hersteller abgedeckt sind. Diese haben in deutscher oder englischer Sprache (Sprachniveau mindestens C1) zu erfolgen und sind remote, mit Hilfe eines von der Auftraggeberin zur Verfügung zu stellenden Webkonferenzsystems (aktuell MS Teams), zu erbringen.

Leistungsbeschreibung

Die Anzahl der angegebenen Einheiten dient der Vergleichbarkeit und stellt keine Abnahmegarantie, Mindest- oder Maximalmenge dar.

Position	Beschreibung/Bezeichnung	Einheit	Anzahl Einheiten	Anzahl Monate
CO-1	Consultingleistung innerhalb der normalen Geschäftszeiten*	Stunde**	10	Nicht zutreffend
CO-2	Consultingleistung außerhalb der normalen Geschäftszeiten*	Stunde**	10	Nicht zutreffend
CO-3	Supportdienstleistung innerhalb der normalen Geschäftszeiten*	Stunde**	10	Nicht zutreffend
CO-4	Supportdienstleistung außerhalb der normalen Geschäftszeiten*	Stunde**	10	Nicht zutreffend

*normale Geschäftszeiten sind Mo-Fr 08:00 -17:00 MEZ (UTC+1) bzw. MESZ (UTC+2)

** Abrechnung erfolgt anteilig je angefangene 15 Minuten

1.3.7 Support/Störungsbeseitigung

Der Support bzw. die Störungsbeseitigung ist in deutscher oder englischer Sprache zu leisten. Der Support ist direkt durch den Hersteller zu erbringen. Hierfür koordiniert der Auftragnehmer die Einrichtung der notwendigen Accounts auf dem Störungsmeldeportal des Herstellers über welches die Auftragnehmerin den Status der Bearbeitung der Störungen einsehen und kommentieren kann.

Alternativ kann eine Störungsbearbeitung per E-Mail erfolgen.

Zusätzliche Kosten pro Störung sind nicht zu erheben.

Die Kosten für Wartung und Support durch den Hersteller sind in den Lizenzkosten einzukalkulieren.

Der Support muss folgende Anforderungen erfüllen:

- 24x7 Support (24 Stunden am Tag, 7 Tage die Woche)
- Einstufung der Priorität/ Auswirkung in Abstimmung oder nach Vorgaben der Auftraggeberin

Reaktions- und Entstörungsvorgaben

Betriebsverhindernder Mangel

Reaktionszeit: 2 Stunden

Entstörung: Kontinuierlich bis zur Behebung der Störung

Betriebsbehindernder Mangel

Reaktionszeit: 4 Stunden

Entstörung: Kontinuierlich während normaler Geschäftszeiten*

Leichter Mangel

Reaktionszeit: 12 Stunden während normaler Geschäftszeiten*

Entstörung: Während normaler Geschäftszeiten*

(*normale Geschäftszeiten sind Mo-Fr 08:00 -17:00 MEZ (UTC+1) bzw. MESZ (UTC+2))

1.4 Leistungsumfang

Gegenstand der Ausschreibung ist die Lieferung einer Software inkl. Installation zur Verwaltung und Sicherung privilegierter Zugriffe und zum automatischen Passwortwechsel für mindestens in Summe 500 privilegierter Nutzer, 3 Cloudumgebungen und 60.000 technischen Accounts.

Leistungsbeschreibung

1.4.1 Bereitstellung der Softwarekomponenten

Der Auftragnehmer stellt der Auftraggeberin die in 1.3 ff. beschriebenen Softwarekomponenten und Lizenzen in der jeweils aktuellen, vom Hersteller freigegebenen Version zur Verfügung.

1.4.2 Beauftragte Module

Der Leistungsumfang umfasst, nach gegenwärtigem Stand, die Bereitstellung der folgenden Module:

- Passwortspeicher (Vault),
- Weboberfläche zur Verwaltung,
- Secrets Provider als zentralisierte Einheit,
- Secrets Provider als Agent auf einem Server
- Secrets Provider für Cloud- und Containerisierte Systeme
- Aufzeichnungssystem für privilegierte Zugriffe

Die benötigten Mengen/Dimensionierungen ergeben sich aus den Angaben im Preisblatt und den Beschreibungen zum Maximalausbau.

1.4.3 Rahmenvertrag und Erweiterungsoptionen

Der Vertrag wird als Rahmenvertrag geschlossen. Die Auftraggeberin behält sich ausdrücklich vor, während der Vertragslaufzeit zusätzliche Lizenzen des Herstellers zu den bestehenden Modulen abzurufen. Diese Erweiterungen erfolgen zu den im Rahmenvertrag festgelegten Konditionen.

Ein Anspruch des Auftragnehmers auf eine Mindestabnahmemenge über die initial beauftragten Module hinaus besteht nicht.

Die finanzielle Obergrenze für die in diesem Vertrag bereitzustellenden Leistungen beträgt 2.100.000€ netto.

1.4.4 Wartung, Subskription und Herstellersupport

Der Leistungsumfang umfasst für alle gelieferten Module:

- Wartungs- und Subskriptionsleistungen gemäß Herstellervorgaben
- Bereitstellung von Software-Updates, Patches und neuen Versionen
- Herstellerseitigen technischen Support im Rahmen der jeweiligen Supportlevel
- Zugriff auf Herstellerdokumentationen und Supportportale

Die Wartungs- und Supportleistungen sind für die gesamte Vertragslaufzeit sicherzustellen und müssen alle beauftragten Module vollständig abdecken.

1.5 Abnahme

1.5.1 Allgemein

Der Auftragnehmer hat die Software zu installieren, siehe insbesondere Punkt „Einführungsprojekt“. Diese Installationsleistungen sind Werkleistungen und unterliegen der Abnahme des Auftraggebers.

Der Auftragnehmer hat die Systemumgebung, Produktions- und Testumgebung, im Folgenden „Werkleistung/en“ genannt, zur Abnahme bereitzustellen. Nach Fertigstellung der jeweiligen Leistung zeigt der Auftragnehmer der Auftraggeberin deren Abnahmefähigkeit (vollständig und ohne wesentliche Mängel) an. Die Ankündigung muss per E-Mail an das von der Auftraggeberin bekanntgegebene Postfach erfolgen. Ab Eingang der Ankündigung beginnen anhängige Fristen zur Abnahme.

Leistungsbeschreibung

1.5.2 Frist zur Funktionsprüfung

Der Auftraggeberin steht das Recht zu, die Werkleistung innerhalb von 30 Tagen nach der Bereitstellung zur Abnahme einer Funktionsprüfung zu unterziehen (Funktionsprüfungszeit).

Der Auftragnehmer erhält nach erfolgreicher Bereitstellung der Testumgebung eine Abschlagszahlung in Höhe von 50 % der Pauschalvergütung nach Eingang einer prüffähigen Rechnung. Die Zahlung der Abschlagszahlung erfolgt unter Vorbehalt der Endabnahme.

1.5.3 Umgebung zur Funktionsprüfung

Die Funktionsprüfung erfolgt in der jeweils zur Prüfung angemeldeten Systemumgebung. Der Auftragnehmer führt die notwendigen Funktionsprüfungen und Sicherheitsprüfungen auf Verlangen der Auftraggeberin zusammen mit einem Mitarbeitenden der Auftraggeberin durch. In der Funktionsprüfung werden die Werkleistungen oder die teilabzunehmenden Leistungen auf Mangelfreiheit überprüft. Der Auftragnehmer wird der Auftraggeberin bei der Vorbereitung und Durchführung der Funktionsprüfung in angemessenem Umfang unterstützen.

1.5.4 Abbruchbedingungen wegen betriebsverhindernden und/oder betriebsbehindernden Mängeln

Werden betriebsverhindernde und/oder betriebsbehindernde Mängel festgestellt, kann die Auftraggeberin die Funktionsprüfung abbrechen. Sofern lediglich betriebsbehindernde Mängel festgestellt werden, darf die Auftraggeberin die Funktionsprüfung jedoch nur abbrechen, wenn deren Fortsetzung aufgrund der Mängel nicht mehr sinnvoll erscheint. Die Auftraggeberin teilt dem Auftragnehmer nach Abschluss oder Abbruch der Funktionsprüfung bei der Funktionsprüfung festgestellte Mängel entsprechend der nachfolgenden Mängelklassifizierung mit.

1.5.5 Mangelklassifizierung

1.5.5.1 betriebsverhindernder Mangel

Ein betriebsverhindernder Mangel liegt vor, wenn die Nutzung einer vertraglichen Leistung unmöglich oder schwerwiegend eingeschränkt ist.

1.5.5.2 betriebsbehindernder Mangel

Ein betriebsbehindernder Mangel liegt vor, wenn die Nutzung einer vertraglichen Leistung erheblich eingeschränkt ist.

Ein betriebsbehindernder Mangel liegt auch vor, wenn die leichten Mängel insgesamt zu einer nicht unerheblichen Einschränkung der Nutzung einer vertraglichen Leistung führen.

1.5.5.3 leichter Mangel

Ein leichter Mangel liegt vor, wenn die Nutzung einer vertraglichen Leistung ohne oder mit unwesentlichen Einschränkungen möglich ist.

1.5.6 Abnahmewiederholung nach Abbruch wegen betriebsverhindernden und/oder betriebsbehindernden Mängeln

Hat die Auftraggeberin die Funktionsprüfung abgebrochen, setzt sie dem Auftragnehmer eine angemessene Frist, die Mängel zu beseitigen. Nach deren Beseitigung hat der Auftragnehmer die Leistungen erneut zur Teil- oder Gesamtabnahme bereitzustellen. Die Auftraggeberin hat das Recht zur erneuten Funktionsprüfung. Soweit nichts anderes vereinbart ist, beträgt der dafür vereinbarte Zeitrahmen 14 Tage.

Leistungsbeschreibung

1.5.7 Abnahmewiederholung nach Abbruch wegen betriebsverhindernden und/oder betriebsbehindernden Mängeln trotz vollständiger Durchführung

Das vorstehende gilt auch, wenn die Funktionsprüfung trotz betriebsverhindernder Mängel und betriebsbehindernder Mängel vollständig durchgeführt wird.

1.5.8 leichte Mängel

Die Auftraggeberin erklärt nach Ende der Funktionsprüfungszeit die Abnahme der Werkleistungen, wenn diese lediglich leichte Mängel aufweisen und diese in ihrer Summe auch nicht gemäß der Mangelklassifizierung als betriebsbehindernde Mängel gelten. Diese werden in der Abnahmeerklärung als Mängel festgehalten und vom Auftragnehmer im Rahmen seiner Haftung für Sach- und Rechtsmängel unverzüglich beseitigt, soweit nicht eine Frist für die Beseitigung vereinbart ist.

1.5.9 Teilabnahmen

Teilabnahmen finden nur statt, wenn sie ausdrücklich vereinbart sind. Soweit nicht anders vereinbart, ist Gegenstand der Teilabnahme die Funktionsfähigkeit der Teilleistung isoliert betrachtet, das heißt sie umfasst grundsätzlich weder systemübergreifende Funktionalitäten noch die Interoperabilität der Teilleistung mit anderen Teilen der Werkleistungen. Systemübergreifende Funktionalitäten und die Interoperabilität der Teilleistungen sind dann Gegenstand der Teilabnahme, soweit die Nutzung dieser Teilleistungen vor der Gesamtabnahme vereinbart ist und diese Nutzung deren Interoperabilität vereinbarungsgemäß voraussetzt. Nach Erklärung der Abnahme der letzten Teilleistung erfolgt eine Gesamtabnahme (auch Endabnahme genannt). Gegenstand der Gesamtabnahme ist insbesondere die Prüfung der systemübergreifenden Funktionalitäten sowie der Interoperabilität aller Teile der Werkleistungen. Die Erklärung der Gesamtabnahme bleibt erforderlich. Die Erfüllung des Vertrags richtet sich ausschließlich danach, ob die Werkleistungen wie vertraglich vereinbart insgesamt abnahmefähig sind. Hierfür bleibt der Auftragnehmer nachweisspflichtig. Im Übrigen gelten die Regelungen zur Abnahme der Werkleistungen entsprechend.

1.5.10 förmliche Abnahme

Die Abnahme hat förmlich zu erfolgen, hierzu ist das Abnahmeprotokoll, Anlage Nr. 8 der Rahmenvereinbarung, zu verwenden.

2 Teil B – Leistungsbeschreibung

Nachfolgend werden zusätzliche Regelungen aufgeführt, welche die EVB-IT Rahmenvereinbarung ergänzen.

2.1 Vertragsgrundlage

Die Auftraggeberin beabsichtigt, Standardsoftware lizenztlich als Miete in dem Betriebsmodell On Prem zu beschaffen (inkl. herstellereitige Schulungs- und Supportleistungen sowie Leistungen zur Softwarepflege). Der Auftragnehmer soll zudem auf Abruf Consulting- oder Supportleistungen erbringen.

Vor diesem Hintergrund kommt als vertragliche Grundlage die EVB-IT-Rahmenvereinbarung mit den Modulen

- Überlassung von Standardsoftware auf Zeit (EVB-IT Überlassung Typ B),
- Erbringung von EVB-IT Dienstleistungen (EVB-IT Dienstleistung)

zum Einsatz.

Leistungsbeschreibung

Für die jeweiligen Einzelbestellungen, je nach Leistungsart, werden die folgenden EVB-IT AGB Vertragsbestandteil:

- EVB-IT Überlassung Typ B-AGB
- EVB-IT Dienstleistungs-AGB

2.2 Höchstvolumen

Das Höchstvolumen der Rahmenvereinbarung, d. h. der Höchstwert, beträgt 2.100.000 Euro (netto). Bis zu dieser Summe kann die Auftraggeberin Einzelbestellungen auslösen. Es besteht kein Anspruch auf Abnahmeverpflichtung und Ausschöpfung dieser Summe.

2.3 Laufzeit

Die Rahmenvereinbarung tritt mit Zuschlagserteilung in Kraft. Sie endet mit Ablauf von 4 Jahren nach Abnahme der Installationsleistungen (Einführungsprojekt), ohne dass es einer Kündigung bedarf, bzw. vorzeitig bei Erreichen der Höchstvolumina.

Sofern die Laufzeit der bestellten Lizenzen die Laufzeit der Rahmenvereinbarung überschreiten, gelten die Regelungen der Rahmenvereinbarung trotz ihrer Beendigung weiter fort.

2.4 Zertifikate

Der Bieter muss über eine Zertifizierung nach ISO/IEC 27001 oder vergleichbar verfügen. Die Einhaltung dieser Zertifizierung (ISO/IEC 27001 oder vergleichbar) in der Lieferkette muss gewährleistet sein. Daher darf der Bieter ausschließlich Unterauftragnehmer zur Erbringung seiner Leistung einsetzen, die über die entsprechende Zertifizierung verfügen. Sofern die Unterauftragnehmer weitere Unterauftragnehmer zur Erbringung der Leistung einsetzen, gilt dies entsprechend.

Die geforderten Zertifizierungen sind von allen Betroffenen über die gesamte Vertragslaufzeit aufrechtzuerhalten.

2.5 Einsatz von KI

Die Auftraggeberin ist als öffentliche Auftraggeberin der KI-VO (EU AI-Act) in der jeweils aktuell geltenden Fassung unterworfen. Sofern der Auftragnehmer künstliche Intelligenz (KI) (einschließlich Machine Learning, Deep Learning) zur Leistungserbringung einsetzen möchte oder Kundendaten wie z. B. personenbezogene Daten (auch in pseudonymisierter Form) für das Training von KI nutzen möchte, hat er die Auftraggeberin vor dem Tätigwerden frühzeitig, transparent und umfassend zu informieren. Dazu hat der Auftragnehmer Informationen über die Funktionsweise des KI-Systems der Auftraggeberin bereitzustellen und gegebenenfalls entsprechende Dokumentationen revisionssicher (in unveränderbarer Form, keine Verlinkung) zu übergeben. Dies umfasst unter anderem Informationen über

- den Verwendungszweck,
- die Algorithmen,
- die Art und Herkunft des Trainingsmaterials,
- die technischen Parameter und die Leistungsfähigkeit des Systems sowie
- über die potentiellen Risiken und Nebenwirkungen, die aus dem Einsatz des Systems resultieren könnten.

Die Aufzählung ist nicht abschließend.

Beim Einsatz von Hochrisiko-KI-Systemen zur Leistungserbringung, verpflichtet sich der Auftragnehmer,

- die technische Dokumentation fortlaufend zu aktualisieren und der Auftraggeberin zur Verfügung zu stellen,
- dieses System fortlaufend zu überwachen, zu aktualisieren und zu pflegen, um die Sicherheit des KI-Anwendung zu gewährleisten,

Leistungsbeschreibung

- wesentliche Änderungen des KI-Systems der Auftraggeberin schriftlich anzuzeigen
- bei wesentlichen Änderungen ein Konformitätsbewertungsverfahren gem. Art. 43 KI-VO durchzuführen,
- unverzüglich über sicherheitsrelevante Vorfälle zu informieren, die im Zusammenhang mit dem Betrieb des KI- Systems stehen
- bei sicherheitsrelevanten Vorfällen, die im Zusammenhang mit dem Betrieb des KI- Systems stehen, unverzüglich Sicherheitsmaßnahmen zu ergreifen.

Die bei sicherheitsrelevanten Vorfällen zu ergreifenden Sicherheitsmaßnahmen werden zwischen dem Auftragnehmer und der Auftraggeberin bereits vor dem Einsatz der Hochrisiko-KI-Systeme abgestimmt und fortlaufend unter Berücksichtigung sich ändernder Rahmenbedingungen bzw. Vorgaben der Aufsichtsinstanzen sowie aktueller, insbesondere technischer Entwicklungen und Neuerungen fortgeschrieben.

Die Auftraggeberin behält sich die Option vor, dass der Auftragnehmer der Auftraggeberin ein nachrangiges Kontrollrecht einräumt, welches diesem ermöglicht, den Einsatz des Hochrisiko-KI-Systems zu überwachen und bei Bedarf anzupassen oder zu unterbrechen bzw. zu beenden, falls dies zur Einhaltung gesetzlicher Vorschriften, sofern insbesondere Schadenersatzansprüche gegen die Auftraggeberin wegen des Einsatzes von KI geltend gemacht werden, und/oder Vorgaben der Aufsichtsinstanzen erforderlich wird. Entsprechende Kontrollinstrumente sind durch den Auftragnehmer der Auftraggeberin in diesem Fall einzuräumen, um eine angemessene Überwachung durch die Auftraggeberin zu ermöglichen.

Erfolgt die Leistungserbringung durch einen Unterauftragnehmer, verpflichtet sich der Auftragnehmer, den Unterauftragnehmer entsprechend vertraglich zu verpflichten, damit diese Leistungspflichten eingehalten werden.

Aufgrund dessen, dass die am 18.11.2024 veröffentlichte EU-Produkthaftungsrichtlinie 2024/2853 noch nicht in deutsches Recht umgewandelt worden ist und die Regelungen betreffend KI z.B. im Zusammenhang mit der KI-Verordnung in Art und Umfang weiter fortgeschrieben werden, ist es nicht auszuschließen, dass eine Auftragsänderung während der Vertragslaufzeit erforderlich werden kann. Sollten weitere Regelungen erforderlich oder bestehende Regelungen geändert werden müssen, die insbesondere im Zusammenhang mit dem zu verabschiedenden Produkthaftungsgesetz oder mit der KI-Verordnung stehen oder aufgrund entsprechender aufsichtsrechtlichen Weisungen/Hinweisen erforderlich werden, ist die Auftraggeberin berechtigt, die bisherigen Regelungen zu überprüfen und unter Wahrung des Charakters dieses Vertrages entsprechend anzupassen bzw. Regelungen neu aufzunehmen. Dabei darf sich der Gesamtcharakter dieser Rahmenvereinbarung nicht ändern. Eine Änderung des vertraglichen Höchstwertes ist nicht vorgesehen.

2.6 No-spy-Erklärung

Der Auftragnehmer ist rechtlich nicht zur Weitergabe von vertraulichen Daten an ausländische Geheimdienste oder Sicherheitsbehörden verpflichtet. Davon ausgenommen sind Offenlegungspflichten gegenüber anderen ausländischen Stellen (z.B. Börsenaufsicht oder die Finanzverwaltung).

2.7 Außerordentliche Kündigung aus wichtigem Grund

Die Auftraggeberin hat das Recht zur außerordentlichen Kündigung der gesamten Rahmenvereinbarung, von Einzelbestellungen oder jeweils Teilen davon aus wichtigem Grund fristlos oder mit einer Frist. Ein wichtiger Grund für die Auftraggeberin liegt insbesondere in folgenden Fällen vor:

- Die Grundlage der Vertragserfüllung aufgrund einer Änderung der Rechts- oder Gesetzeslage oder wegen aufsichtsrechtlicher Maßnahmen wesentlich verändert wird oder ganz entfällt.
- Der Auftragnehmer verletzt die gesetzlichen oder vertraglichen Datenschutz- und IT-Sicherheitsbestimmungen sowie die gesetzlichen oder vertraglichen Bestimmungen zum

Leistungsbeschreibung

Einsatz von KI nicht nur unwesentlich. Die Parteien sind sich einig, dass jede Verletzung, die Sozialdaten oder diesen gleichgestellten Betriebs- und Geschäftsgeheimnissen betrifft, eine wesentliche Verletzung ist.

- Die geforderte Zertifizierung, d.h. ISO/IEC 27001 oder vergleichbar nicht mehr bestehen. Im Falle einer vorzeitigen Beendigung des Vertrages ist die bis zu diesem Zeitpunkt bereits geleistete Vorauszahlungen anteilig für die verbleibenden Restmonate, um den Teil zurückzuerstatten, um welchen die Auftraggeberin die Leistung des Auftragnehmers aufgrund der vorzeitigen Vertragsbeendigung nicht mehr nutzen konnte. Die Einrede der Entreicherung ist ausgeschlossen.

2.8 Einsatz Unterauftragnehmer

Der Auftragnehmer hat jede im Rahmen der Auftragsausführung eintretende Änderung bei den Unterauftragnehmern der Auftraggeberin mitzuteilen. Dies schließt die Nennung der Namen, der Kontaktdaten und der gesetzlichen Vertreter seiner Unterauftragnehmer sowie den übernommenen Leistungsbereich nebst des Nachweises zum Vorliegen der geforderten Zertifikate mit ein.

2.9 Vertraulichkeit

Die Nennung der Auftraggeberin als Referenzauftraggeber ist nur mit ausdrücklicher der Auftraggeberin zulässig.

2.10 Sublicensing-Vereinbarung

Die Parteien sind sich darüber einig, dass die Nutzung der Software nicht auf mit der Auftraggeberin rechtlich „verbundene Unternehmen“ im Sinne gesellschaftsrechtlicher Kontrollbegriffe beschränkt sein, sondern eine weitere, organisationsbezogene Nutzung ermöglicht werden soll. Dies schließt eine Nutzungsänderung aufgrund möglicher organisationsbezogener Änderungen bei der Auftraggeberin mit ein. Eine entsprechende Sublicensing-Vereinbarung über die erweiterte Lizenznutzung und Unterlizenzierung wird unter Teil B Nummer 25.16.6 der Rahmenvereinbarung geschlossen.