

Leistungsbeschreibung

Passwort Management System

Inhaltsverzeichnis

Inhalt

1.1 Überblick über die Telematikinfrastruktur	3
1.2 Ausgangssituation	3
2.1 Leistungsportfolio	4
2.2 Anforderungen an das Passwort-Management System	4
2.3 Mengengerüst.....	5
2.4 Zeitplanung und Vertragslaufzeit	5

1 Rahmenbedingungen und Überblick

1.1 Überblick über die Telematikinfrastuktur

Die Digitalisierung wird das Gesundheitswesen künftig weiter und nachhaltig verändern. Die Erfassung, Verarbeitung und Nutzung medizinischer Daten beflügelt die Forschung, revolutioniert Therapien und sorgt dafür, dass wir immer gesünder, länger und besser leben. Diesen Prozess in Deutschland entschlossen voranzutreiben und konstruktiv mitzugestalten, ist Ziel, Aufgabe und Mission der gematik.

Die gematik trägt die Gesamtverantwortung für die *Telematikinfrastuktur* (TI), die zentrale Plattform für digitale Anwendungen im deutschen Gesundheitswesen. Mit der Definition und Durchsetzung verbindlicher Standards für Dienste, Komponenten und Anwendungen in der TI gewährleistet die gematik, dass diese zentrale Infrastruktur sicher, leistungsfähig und nutzerfreundlich ist und bleibt.

Die Arbeit der gematik als Nationale Agentur für Digitale Medizin reicht weit über Landesgrenzen hinaus – für die beste medizinische Versorgung der Menschen kooperiert sie international mit „National Digital Health Agencies“ anderer Länder. Sie ist Kompetenzzentrum und Koordinierungsstelle für Interoperabilität und versteht sich dabei nicht nur als Prüferin und Standardgeberin, sondern auch als Vermittlerin, Moderatorin und Beraterin.

Die gematik ist zwar kein KRITIS-Unternehmen, muss jedoch aufgrund ihrer zentralen Rolle im Gesundheitswesen vergleichbare Anforderungen an Informationssicherheit, Resilienz und Risikomanagement bewältigen.

1.2 Ausgangssituation

Vor allem – aber nicht nur - in den technischen Bereichen der gematik müssen zahlreiche Passwörter oder Schlüsseldateien sicher und von mehreren berechtigten Mitarbeitern gehandhabt werden. In den letzten Jahren wurde dazu der Passwort-Manager KeePass verwendet.

Zum gemeinsamen Arbeiten mit den Passwörtern muss die entsprechende Datei auf einem gemeinsamen Dateisystem verfügbar gemacht werden, was zu folgenden Schwächen/Risiken führt:

- Damit ist der Inhalt bei einem Ausfall der IT-Infrastruktur nicht mehr verfügbar.
- Zudem führt die Notwendigkeit, nur wenige KeePass-Dateien zu verwalten, dazu, dass umfangreiche Passwortspeicher entstehen, auf die viele Benutzer Zugriff haben.
- Die Dateien sind nicht zwangsläufig aktuell, was zu kritischen Fehlern führen kann.
- Für den Zugriff auf die Passwörter genügt der Zugang zur Passwort-Datei sowie das Passwort – es gibt keine Möglichkeit, den Zugang zu entziehen

2 Leistungsumfang

2.1 Leistungsportfolio

Um die Sicherheit im Umgang mit Passwörtern im Unternehmen signifikant zu erhöhen, will die gematik ein geeignetes Passwort-Management-System *bzw. -Lösung* beschaffen. Der Auftragnehmer muss eine Lösung für die gematik als Software-as-a-Service (SaaS)-Lösung bereitstellen und betreiben, die die daran aufgestellten MUSS-Anforderungen und die vom Auftragnehmer mit seinem Angebot zugesicherten SOLL-Anforderungen erfüllt.

2.2 Anforderungen an das Passwort-Management System

Die Anforderungen an das Passwort Management System sind in dem Anforderungskatalog (Anlage 02_A) und in dem Kriterienkatalog zu dem EVB-IT Cloudvertrag (Anlage 09_A) aufgelistet.

Die im EVB-IT-Kriterienkatalog ausgewählten Kriterien sind zwingend einzuhalten.

Die Anforderungen im Anforderungskatalog sind unterteilt in:

- **MUSS-Anforderungen (Mindestanforderungen):** Die im Anforderungskatalog aufgeführten **MUSS**-Anforderungen sind Mindestanforderungen, die bereits zum Zeitpunkt der Angebotsabgabe erfüllt sein müssen. Wird eine oder werden mehrere dieser Mindestanforderungen nicht erfüllt, wird der Bieter zwingend vom Vergabeverfahren ausgeschlossen. Der Auftraggeber wird das Vorliegen der MUSS-Anforderungen im Vergabeverfahren mittels Teststellung verifizieren (vgl. die Ausführungen im Verfahrensbrief, Anlage 01).
- **SOLL-Anforderungen (in die Wertung einfließende Kriterien):** Die im Anforderungskatalog aufgeführten **SOLL**-Anforderungen sollten erfüllt werden, dabei handelt es sich demnach nicht um Mindestanforderungen. Die vom Bieter zugesicherten SOLL-Anforderungen müssen bereits zum Zeitpunkt der Angebotsabgabe erfüllt sein und gehen entsprechend der angegebenen Parameter in die fachliche Bewertung ein. Der Auftraggeber wird das Vorliegen der jeweils zugesicherten SOLL-Anforderungen im Vergabeverfahren mittels Teststellung verifizieren (vgl. die Ausführungen im Verfahrensbrief, Anlage 01). Diese Anforderungen führen bei Nichterfüllung NICHT zum Ausschluss des Bieters. Er erhält in diesem Fall für das betroffene Kriterium 0 Punkte.

Die vorgegebenen MUSS- und die zugesicherten SOLL-Anforderungen müssen zwingend spätestens zum Zeitpunkt der Angebotsabgabe im Vergabeverfahren (und damit auch zum Zeitpunkt der späteren Bereitstellung der Passwort Management System) erfüllt sein.

Der Auftragnehmer ist zudem verpflichtet, das Hosting der Passwort Management System zu übernehmen. Der Auftraggeber wird die Lösung nicht selbst hosten.

2.3 Mengengerüst

Das Passwort-Management-System ist für eine Mindestabnahme von 300 Benutzern in den ersten sechs Monaten anzubieten. Anschließend ist eine Erweiterung auf 500 Benutzer vorgesehen. Darüber hinaus besteht die Möglichkeit, die Nutzerzahl während der Erstlaufzeit bedarfsabhängig um bis zu weitere 100 Benutzer auf insgesamt maximal 600 Benutzer zu erhöhen.

Geschätzte Benutzerzahlen über die initiale Vertragsjahre:

Jahr	1-6 Monate	7-12 Monate	Zweites Jahr	Drittes Jahr	Viertes Jahr
Benutzeranzahl	300	500	550	600	600

Während der Gesamtlaufzeit des Vertrages (nach der Erstlaufzeit) wird geschätzt, dass die Anzahl der Nutzer Lizenzen die Größenordnung von 700 Nutzer nicht übersteigen wird.

Für das vorstehend geschätzten Mengengerüst besteht keine Abnahmeverpflichtung seitens des Auftraggebers.

2.4 Zeitplanung und Vertragslaufzeit

- Geplanter Vertragsbeginn: 30.11.2026
- Ordnungsgemäße und vollumfängliche Bereitstellung der Passwort Management Lösung durch den Auftragnehmer: innerhalb von zwei Wochen nach Zuschlag
- Laufzeit des Vertrages: 4 Jahre ab Bereitstellung der Passwort Management Lösung durch den Auftragnehmer (Erstlaufzeit). Nach dem Ablauf der Erstlaufzeit von 4 Jahren verlängert sich der Vertrag automatisch um jeweils ein (1) weiteres Jahr, sofern er nicht zuvor vom Auftraggeber gekündigt wird.