Leistungsverzeichnis

zum

Offenes Verfahren Nr. 0424/I/01

Lieferung und Einführung eines

Identity & Access Managementsystems

für den Konzern Klinikum Chemnitz gGmbH

Inhalt

1 Allgemein

Die Klinikum Chemnitz gGmbH ist ein Krankenhaus der Maximalversorgung und befindet sich zu 100 Prozent im Eigentum der Stadt Chemnitz. Das Klinikum ging 1994 aus den Städtischen Kliniken hervor, deren historische Wurzeln im mittelalterlichen Hospital St. Georg liegen, das im 14. Jahrhundert gegründet wurde. Das gemeinnützige Unternehmen verfügt über 1.785 Planbetten an drei Standorten in Chemnitz. Es ist damit das drittgrößte Krankenhaus Deutschlands in kommunaler Trägerschaft.
Im Jahr 2022 wurden rund 56.200 Patienten voll- und teilstationär sowie etwa 75.000 Patienten ambulant im Klinikum Chemnitz behandelt. Derzeit sind im Klinikum Chemnitz sowie in den Tochter- und Beteiligungsunternehmen rund 7.000 Mitarbeiter beschäftigt. Der Konzern Klinikum Chemnitz realisierte im Jahr 2021 einen Jahresumsatz von etwa 560 Mio. €.
Das Klinikum Chemnitz ist akademisches Lehrkrankenhaus der Universitäten in Dresden und Leipzig. Die TU Dresden und das Klinikum Chemnitz bieten gemeinsam den medizinischen Modellstudiengang MEDiC an.
Als kritischer Dienstleister im Bereich Gesundheitswesen nach §8a Bundesamt für Sicherheit in der Informationstechnik ist der Konzernverbund der Klinikum Chemnitz gGmbH, im weiteren als Klinikum Chemnitz (KC) bezeichnet, wichtiger Bestandteil der Gesundheitsversorgung in der Region Süd- und Südwestsachsen,
Das Klinikum Chemnitz (KC) hat sich zum Ziel gesetzt das Thema „Identity and Access Management/Identitäts- und Zugriffsmanagement“ (IAM) den gesetzlichen und internen Anforderungen entsprechend umzusetzen.
In diesem Zuge wurde ein eigenes Projekt etabliert. Im Ergebnis wurden hausinterne IAM-Standards und –Prozesse nach Best Practice definiert und der Entschluss gefasst, ein professionelles IAM-System zu beschaffen.
Inhalt dieser Leistungsbeschreibung, zur Ausschreibung eines IAM-Systems, ist im ersten Teil die kurze Darstellung, wie das Thema IAM im Unternehmen in Zukunft verstanden und umgesetzt werden soll.
Im zweiten Teil werden Anforderungen (inkl. Leistungsverzeichnis) an das zu beschaffende IAM-System detailliert beschrieben.

1.1 Grundinformationen zum Unternehmen Klinikum Chemnitz gGmbH

Der Aufbau des Unternehmens stellt sich wie folgt dar: *(siehe auch: https://www.klinikumchemnitz.de/das-klinikum/ueber-uns/organisation)*
Das Unternehmen besteht aus der Klinikum Chemnitz gGmbH und mehreren Tochterunternehmen in einem gemeinsamen IT-Netz und einer gemeinsamen Windowsdomäne.
Mitarbeiter können einem Unternehmensteil oder auch mehreren gleichzeitig angehören. Die Personalstammdaten werden in einem gemeinsamen Personalwirtschaftssystem gepflegt. Ein Mitarbeiter kann mehrere Verträge innerhalb eines Unternehmensteils oder über beide hinweg besitzen. Seine Beschäftigung endet erst mit dem Ende aller Verträge.
Das KC ist ein Krankenhaus der Maximalversorgung und somit ein wichtiger Baustein in der ambulanten und stationären Versorgung in der Region.
Gemeinsam mit der Medizinischen Fakultät der Technischen Universität (TU) Dresden bietet die Klinikum Chemnitz gGmbH einen Modellstudiengangs MEDiC an, der es Studierenden bereits mit Beginn des ersten Semesters ermöglicht, in das ärztliche Berufsfeld einzutauchen und praktische Erfahrungen aus dem klinischen und ambulanten Sektor zu erwerben.
Weiterführende Informationen können Sie unserer Homepage unter www.klinikumchemnitz.de – „Das Klinikum“ entnehmen.

2 Geplantes Nutzungskonzept IAM am KC

2.1 Herleitung und Motivation

Am KC gibt es eine Vielzahl von Datenspeichern und IT-Anwendungen, die fachbereichsbezogen, aber auch fachbereichsübergreifend besonders schützenswerte Daten halten oder verarbeiten. Damit haben die Prozesse zur Vergabe, zur Anpassung bis zum Entzug von Berechtigungen auf Speicherbereiche, Anwendungen oder Gebäudebereiche, nicht zuletzt aus gesetzlichen Vorgaben, eine große Bedeutung. Kontrolle und Sicherheit bei der Arbeit mit personenbezogenen und anderen Unternehmensdaten müssen im geschützten Netzwerk und über dessen Grenzen hinaus, etwa bei einem Zugriff von extern, sichergestellt werden.
Die handelnden Personen, also Mitarbeiter, sowie externe Fachkräfte und Partner, die auf die oben genannten Daten Zugriff haben und diese bearbeiten können, müssen in diesen Kontexten identifizierbar sein und es muss sichergestellt werden, dass jede Identität zum richtigen Zeitpunkt mit den richtigen Zugangs- und Zugriffsrechten ausgestattet ist.

Aus folgendem Grund wird bei dem hier zu beschaffenden **Identity & Access Managementsystem** konkret das Produkt **OGiTiX unimate**, nachfolgend als **IAM** bezeichnet, des Herstellers Imprivata Ogitix GmbH ausgeschrieben:

- Nur das Produkt OGiTiX unimate hat eine direkte standardmäßige Verbindung/Schnittstelle zum bereits beim Auftraggeber vorhandenen und im Einsatz befindlichen Single-Sign-on (SSO)-Produkt „Imprivata OneSign. Damit ist aus technischen Gründen kein Produktwettbewerb möglich.
  Die Integration in unsere bestehende SSO-Landschaft, Imprivata OneSign, muss unkompliziert möglich sein

Darüber hinaus muss das IAM-System zum Zeitpunkt der Angebotsabgabe insbesondere:

- eine Schnittstelle in unser HR-System SAP HCM besitzen
- eine Schnittstelle in unser KIS-System Cerner/Oracle i.s.h.med besitzen
- eine grafische Erstellung & Bearbeitung von Workflows ermöglichen.
- die Skriptbasierte Erstellung von Schnittstellen und mit dem integrierten „Schnittstellen Designer“ eine Unabhängigkeit von den Herstellern der Zielsysteme (IT-Systeme, Fachanwendungen) bzw. den entsprechenden Anbindungsdienstleistern ermöglichen.
- die Erstellung kundenspezifischer IAM-Services ermöglichen.
- die Erweiterung um Funktionen ohne Herstellerleistungen ermöglichen.
- als On-Premise Software bereitgestellt werden.
- ein mindestens 2-Stufiges Staging bieten.
- eine Mandantenfähigkeit auch über mehrere Domänen bieten.
- die parallele Verarbeitung mehrerer Quellsysteme ermöglichen.

Weiterhin:

- Es muss ein Password Reset Management für AD und SAP angeboten werden.

Aus der **Verbindung von SSO und IAM**-Lösung versprechen wir uns einen **Synergieeffekt**, einen **Mehrwert und Kostensenkungen**.

Bei allen im Folgenden an das zu beschaffende IAM-System gestellten Anforderungen handelt es sich um Mindestanforderungen, die das vom Bieter angebotene Produkt zwingend erfüllen muss.
Auch wenn nur eine Mindestanforderung vom angebotenen Produkt nicht oder nur teilweise erfüllt wird, wird das Angebot von der weiteren Bewertung ausgeschlossen.
Insofern das Produkt eine Mindestanforderung nicht oder nur teilweise erfüllt, ist der Bieter verpflichtet dies unter Bezugnahme auf die geforderte Mindestanforderung oder Funktionalität anzugeben.

Werden seitens der Vergabestelle im Leistungsverzeichnis vom Bieter Erläuterungen gefordert so sind diese vom Bieter unter Bezugnahme auf den entsprechenden Punkt des Leistungsverzeichnisses in einer gesonderten Anlage zu tätigen.
Generell sollten alle Zusatzangaben, die der Anbieter für eine vergleichbare Bewertung seines Angebotes für erforderlich erachtet, als den Kriterien einzeln und eindeutig zugeordnete Anlagen (ggfs. in Tabellenform) übergeben werden. Fehlende Angaben können zu Nachteilen für den Anbieter in der Bewertung des Angebotes führen.
Der Auftraggeber fühlt sich im Rahmen der Bewertung nicht verpflichtet, fehlende oder unvollständige Angaben zu hinterfragen.
Stellt sich nach Zuschlagserteilung heraus, dass der Bieter im Rahmen der Ausschreibungsbearbeitung / Angebotserstellung zum anzubietenden Produkt bzw. zu den anzubietenden Leistungen (siehe hierzu insbesondere die an die Qualifikation der Mitarbeiter des Bieters gestellten Anforderungen (Eignungsnachweise)) bewusst oder unbewusst Falschangaben gemacht hat, behält sich die Vergabestelle den Rücktritt vom Vertrag sowie die Geltendmachung von Ansprüchen aus entstandenen Schäden vor.
Hierzu zählen auch solche Schäden, die durch notwendige Deckungskäufe entstanden sind, wie z. B. administrative Mehraufwendungen, höhere Einkaufspreise sowie Bezugskosten.

Insofern im Leistungsverzeichnis von AN die Rede ist handelt sich hierbei um die Abkürzung für Auftragnehmer bzw. den Bieter (AG = Auftraggeber).

2.2 Geltungsbereich des IAM

Das IAM soll Identitäten und Zugriffsrechte aller Mitarbeiter von KC verwalten. Als Mitarbeiter (MA) im Sinne des IAM gelten sowohl festangestellte Mitarbeiter als auch Mitarbeiter mit befristetem Arbeitsverhältnis, des Weiteren alle Praktikanten, Studenten, Aushilfskräfte, Mitarbeiter externer Partnerunternehmen oder Lieferanten, Dienstleister oder Hersteller, sofern sie eine wie auch immer geartete Zugangs- oder Zugriffserlaubnis zu Räumlichkeiten oder Systemen des KC benötigen. Alle anderen Personen werden nicht erfasst, dies beinhaltet insbesondere Gäste und Patienten.

Dies sind ca. 7.500 Identitäten. Details dazu unter Pkt. *3.1.1 Mengengerüst.*

2.3 Definitionen

2.3.1 Typen von Identitäten

Über den Typ der Identität wird die Datenhoheit definiert. So wird bestimmt, an welcher Stelle bzw. in welchem System die Daten zu Identitäten gepflegt werden.

2.3.1.1 Interne Identitäten

Interne Identitäten sind Mitarbeiter oder Studenten. Die Verwaltung der Personeninformationen findet im System SAP HCM statt. Diese Informationen werden jedoch nur als Arbeitsverträge betrachtet, von denen mehrere gleichzeitig aktiv sein können.

2.3.1.2 Externe Identitäten

Externe Identitäten sind diejenigen, die nicht Mitarbeiter des Unternehmens sind, mit denen aber vertragliche Vereinbarungen getroffen wurden. Sie greifen, im Rahmen der vertraglich fixierten Tätigkeiten, ebenfalls auf Ressourcen (Daten, Systeme, Räume) des Unternehmens zu.

2.3.2 Verfahren

Unter Verfahren wird ein geregelter, in Schritte zerlegbarer, nachvollziehbarer und wiederholbarer Ablauf verstanden. Verfahren und Prozess wird synonym verwendet.

2.3.3 Attribute

Attribute definieren die Eigenschaften eines Datenobjekts. Das Attribut ist eine Eigenschaft oder ein Merkmal, das eine Person, eine Gruppe oder ein Datenobjekt definiert. Es sind eigentlich die Eigenschaften, die den Typ der Entität definieren. Ein Attribut kann einen einzelnen oder mehrere Werte oder einen Wertebereich haben. Spezielle Attribute sind Referenzen auf andere Objekte, so genannte Kontexte: Ein Kontext beschreibt einen inhaltlichen Zusammenhang und eine Beziehung zwischen Entitäten. Diese Zusammenhänge können organisatorischer oder funktionaler Natur sein.

2.3.4 Klassifizierung von Benutzerkonten oder Accounts

Grundsätzlich werden die Konten zum Anmelden an oder Verwalten von IT-Systemen in zwei Kategorien unterteilt, in personalisierte und nicht personalisierte Konten.

2.3.4.1 Personalisierte Konten

Benutzerkonten dieser Kategorie sind einer Identität eineindeutig zugeordnet. Systemseitig ist das über eine feste Verknüpfung des Kontos mit der für die Person im IAM gepflegten Identität abgebildet.
Bsp.: Persönliche, Administrative und Testkonten
Alle Aktivitäten, die in einer Anwendung oder einem System von diesen Konten ausgeführt werden, sind zweifelsfrei zu der Identität zurückzuverfolgen und liegen damit in der Verantwortung der mit dieser Identität verbundenen Person.

2.3.4.2 Nicht personalisierte Konten

Anders als bei personalisierten Konten besteht hier keine direkte Zuordnung des Kontos zu einer Identität. Nicht personalisierte Konten werden dazu verwendet, den Betrieb und die Funktion von Anwendungen und Systemen bereitzustellen. In dieser Kategorie wird zwischen Funktions- und technischem Konto unterschieden.
Bsp.: Konfigurationskonto, Dienstkonto (Service-Account), Sammelkonto (PC bezogen), Autologin-Konto.
Um auch die nicht personalisierte Konten automatisiert rezertifizieren zu können, muss ein Besitzer bzw. Verantwortlicher hinterlegt/zugewiesen werden.

2.4 Allgemeine Ziele und Designvorgaben für ein IAM-Konzept

Eine Kernfunktion eines IAM-Systems ist es, wie in der nachfolgenden Abbildung gezeigt, dass der korrekte Personenkreis mit den notwendigen Zugriffen auf die notwendigen Systeme und Applikationen ausgestattet wird um seine ihm zugewiesenen Tätigkeiten/Aufgaben auszuüben. Optional können die Zugriffe über Definition von möglichen Zugriffzeiten weiter beschränkt werden.

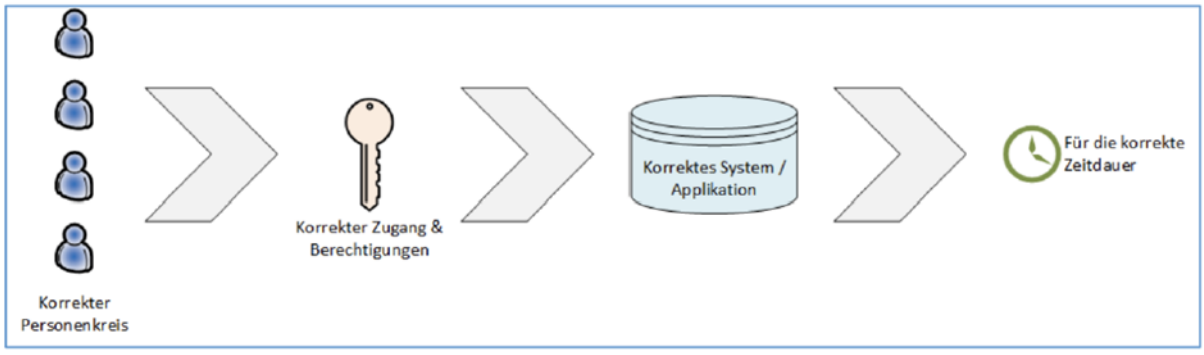

Abbildung 1: Kernfunktion eines IAM

Mit der Etablierung eines IAM werden folgende Ziele und Nutzeffekte am KC angestrebt:

- Automatisierung des Identity LifeCycle, siehe Anwendungsfälle 3.2.1, 3.2.2, 3.2.3
- Überführung manueller, papierbasierter Beantragungs-Prozesse in eine toolgestützte, digitale Implementierung
- Damit Schaffung eines einheitlichen und transparenten Prozesses für die Beantragung und Änderung von Zugriffsrechten.
- Unkomplizierte Anbindung der im KC **bereits vorhanden Single Sign-on – Lösung Imprivata OneSign**.
- Etablierung einer eigenen Einrichtung mit entsprechender Zuständigkeit und Verantwortlichkeit zur Umsetzung der IAM-Prozesse, sowie für den Betrieb und die Pflege der IAM-Software

- Umstellen aller bekannten und im Servicekatalog des Unternehmens geführten Systeme/IT-Systeme auf Verwendung des zentralen IAM, soweit sinnvoll und möglich
- Minimierung der Durchlauf- und Antwortzeiten durch effektiven und stabilen Betrieb der IAM-Software
- steigende Benutzerzufriedenheit, Verringerung des administrativen Aufwandes und Verringerung der Fehleranfälligkeit durch Senkung der Durchlaufzeit des Identity LifeCycle und des Berechtigungsmanagements
- Schaffung der Grundlage weiterer Prozessoptimierungen, insbesondere Automatisierungen in der Rechtevergabe und Provisionierung
- Datenschutzkonforme und revisionssichere Dokumentation der Rechtevergabe
- Erstellen von Ad-hoc Reports für Audits (Report-Inhalte orientieren sich mind. an den gesetzlichen Vorgaben s. a. Pkt. 2.5.). Reports dürfen vom AG zusätzlich erstellt und können selbst angepasst werden.
- Unterstützung beim Anbinden weiterer Anwendungen durch einen tool-gestützten Applikations-Onboarding-Prozess und Unterstützung beim Rückbau von Anwendungen durch das IAM-Tool
- Automatisierte Provisionierung von Benutzer-Konten an Zielsysteme zur Erhöhung der Datenqualität und Zuverlässigkeit über standardisierte Schnittstellen/ Konnektoren
- Grundlegende Verbesserung der Informationssicherheit
- Reduzierung der mit dem On- und Offboarding von Mitarbeitern verbundenen Risiken
- Vermeidung fehlerhafter Rechte-Vergabe durch bessere Erkennbarkeit von zum Beispiel Verletzungen des Funktionstrennungs-Prinzips
- Sicherstellen organisatorischer Ziele durch auditkonforme Abläufe und Vermeiden von Gefahren fehleranfälliger manueller IAM-Prozesse
- Vermeiden von Doppelarbeit und Insellösungen durch Vereinheitlichung von Prozessen und die Fokussierung auf ein zentrales führendes IAM-System

2.5 Vorschriften, Vorgaben und Ziele für das IAM

Die Vorgaben aus Gesetzen, Standards und Normen:
Vorschriften aus Gesetzen:
Europäische Datenschutz-Grundverordnung (EU DS-GVO)
IT-Sicherheitsgesetz (IT-SiG)
BSI-Gesetz (BSIG)
Sächsisches Krankenhausgesetz (SächsKHG)

Vorgaben aus Standards und Normen:
Branchenspezifische Sicherheitsstandards (B3S)
BSI IT-Grundschutz
ISO27001

AN unterstützt den AG bei der Erstellung bzw. Anpassung der entsprechenden Nutzungsrichtlinie und des Sicherheitskonzeptes „Identitäts- und Zugriffsmanagement“, welche ggf. als Ergebnis der unter Pkt. 4.2.x genannten Tätigkeiten entstehen kann.

2.6 Einbindung des IAM-Systems in die Systemlandschaft

Um die Vorteile von IAM bestmöglich zu nutzen, soll ein zentrales IAM-System etabliert werden. Dieses für das Identitätsmanagement und die Verwaltung der Berechtigungen zuständige System wird in die bestehende IT-Landschaft (siehe Abbildung 2) eingebunden. Das bestehende **SAP HCM – System (HR) ist das führende System und liefert** über einen Connector die entsprechenden Daten.

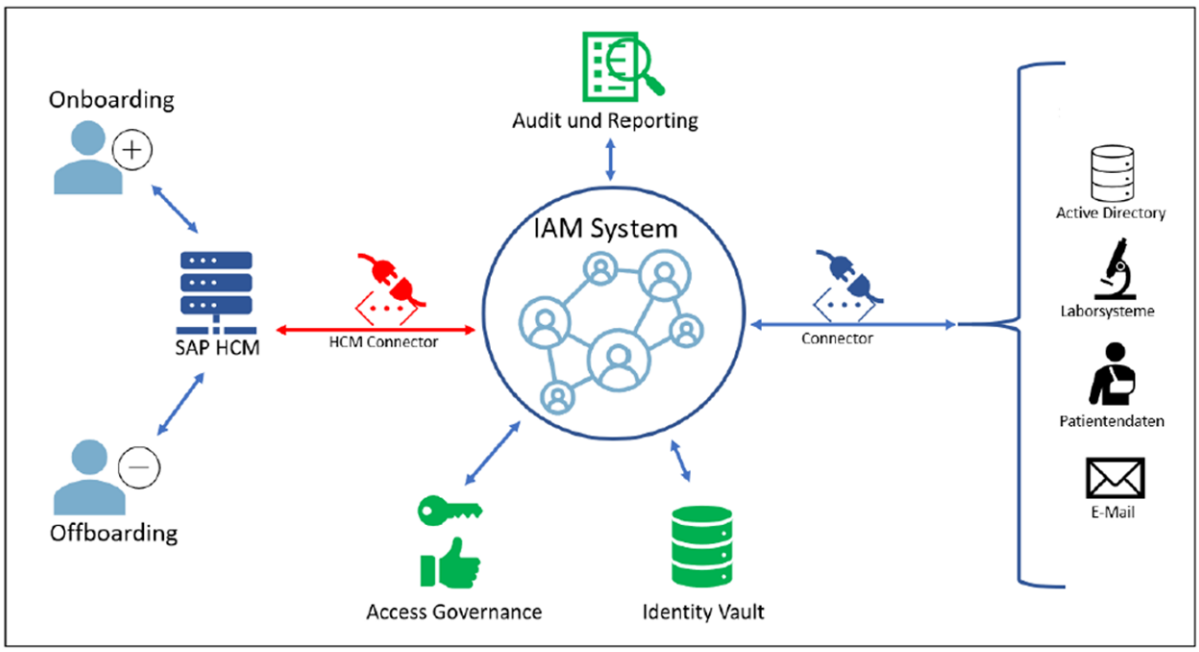

Abbildung 2: Einbindung IAM-System in vorhandene Landschaft

Über die SAP HCM-Schnittstelle werden Daten in das IAM übertragen, aufbereitet und strukturiert.

Neben dem SAP HCM sollen so viel wie möglich Systeme an das zentrale IAM-System angebunden werden, um die Vorteile der zentralen Identitäts- und Rechteverwaltung in die gesamte Anwendungslandschaft auszurollen. Die Priorität der anzubindenden Systeme sind der anbei gefügten Übersicht, Anlage „Liste-der-IT-Systeme-IAM“ zu entnehmen. Die Anbindung erfolgt schrittweise in Abstimmung AG - AN. Die Möglichkeit, zukünftige Systeme vom AG selbst anzubinden, sollte bestehen und Möglichkeiten hier bzw. in einer Anlage erläutert werden.
Es sind damit alle Systeme oder Anwendungen gemeint, an denen sich Benutzer anmelden, um Zugriff auf Ressourcen zu erhalten (s. Anlage: Liste-der-IT-Systeme-IAM).

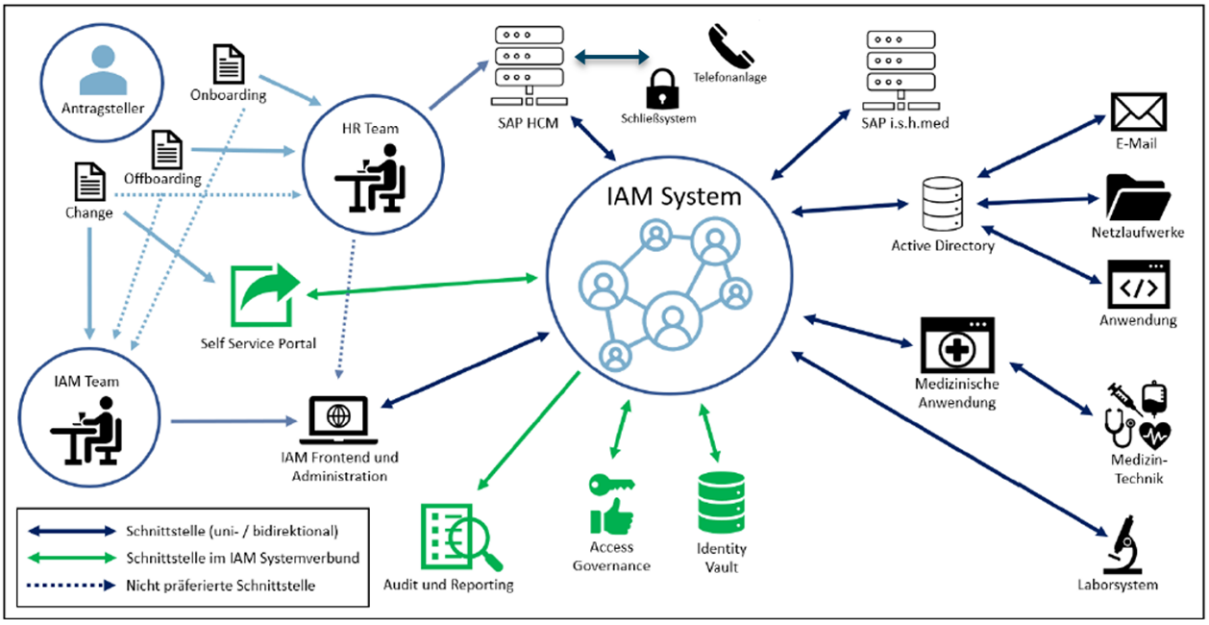

Abbildung 3: Das zentrale IAM-System im Verbund mit der gesamten Landschaft in KC

2.7 Berechtigungsmodell

Das KC verfolgt bei der Vergabe von Berechtigungen das Prinzip des Berechtigungsobjekt-Modells. Ein Management von Berechtigungen allein an Hand von Unternehmensrollen ist in der Umsetzung zu komplex und aufwändig.
Die Steuerung von Berechtigungen in IT-Systemen hängt von den in IT-Systemen verwendeten Ressourcen ab. Eine Ressource kann eine Datei, eine Datenbank, eine Information, ein Raum, ein Drucker usw. sein.
Wer im Unternehmen auf diese Ressourcen, im Rahmen seiner Tätigkeiten, wie zugreifen darf, wird in Form von Berechtigungsobjekten definiert und in einem Berechtigungskonzept dokumentiert.
Der Aufbau der Berechtigungsobjekte ist standardisiert und identisch für alle Verfahren. Ein zukünftiges IAM-System muss in der Lage sein dieses Modell technisch abzubilden.

Ein Berechtigungsobjekt besitzt folgende zu definierenden Attribute:

Attribute-Kategorie	**Attribut**	**Beschreibung**
Ressourcen	Sprechende Bezeichnung	für Anwender lesbare Beschreibung, welche in einem Berechtigungsantrag verwendet wird
Ressourcen	Ressourcenname	beschreibt auf welche Ressource berechtigt wird
Personenkreis	Organisationseinheit	definiert für welche Identitäten dieses Berechtigungsobjekt anzuwenden ist
Personenkreis	Dienstart	definiert für welche Identitäten dieses Berechtigungsobjekt anzuwenden ist
Personenkreis	betriebliche Funktion	definiert für welche Identitäten dieses Berechtigungsobjekt anzuwenden ist
Berechtigung	Verfahren/System	definiert in welchem System dieses Berechtigungsobjekt angewendet wird
Berechtigung	Art der Zuweisung	definiert ob eine Berechtigung standardisiert/automatisch zugewiesen wird oder beantragt werden muss
Berechtigung	Art der Berechtigung	definiert die Art der Berechtigung (z.B. lesend, ändernd, drucken, …) die auf die Ressource angewendet wird
Freigabe	Risikoeinstufung	definiert das Risikopotential der Ressource
Freigabe	Gültigkeit	definiert die Gültigkeitsdauer der Berechtigung auf das Objekt, von – bis
Freigabe	Fachliche Freigabe	definiert wer Zugriff auf das Berechtigungsobjekt gewährt

Tabelle 1: zu definierende Attribute eines Berechtigungsobjektes

Das IAM-System bündelt die Berechtigungen aus dem System zu logischen Verfahrens- oder Applikationsrollen.

2.7.1 Automatische Vergabe von Berechtigungen

Ziel ist es, Berechtigungen im Zuge des Identitätslebenszyklus automatisch zu vergeben und wieder zu entziehen und dabei das Prinzip der geringsten Privilegien (Principle of Least Privilege, PoLP, Least Privilege-Prinzip oder „Need to know“-Prinzip) zu wahren.

Die automatische Vergabe von Berechtigungen erfolgt auf Grundlage definierter Richtlinien bzw. Zuweisungsregeln. Diese Regeln können eine Vielzahl von Attributen berücksichtigen. Wichtige Attribute sind dabei die Organisationseinheit, die Dienstart und die betriebliche Funktion.

2.7.2 Beantragen von Berechtigungen

Beim Beantragen und Genehmigen müssen weitere Attribute, auch Attribute der beantragten Ressourcen, in den Prozess einbezogen werden.
Diese Attribute können sein:

- Typ der Identität und Gültigkeit – Externe Identitäten dürfen z.B. beantragte Rechte maximal 1 Jahr behalten.
- Kritikalität des Verfahrens/des Systems/der Ressource: risikoreiche Zugriffe müssen durch mehrere Ebenen bzw. Instanzen genehmigt werden (fachliche und disziplinarische Freigabe)

2.7.3 Berechtigungsportfolio

Das individuelle Berechtigungsportfolio einer Identität ergibt sich aus der Kombination aller automatisierten und den speziell beantragen Berechtigungsobjekten, basierend auf den importierten Daten aus SAP HCM.

2.8 Identifikation von Personen bzw. Identitäten

Das führende Personalsystem SAP HCM, wird von der Personalabteilung des KC (PW) genutzt und Datenbestände nur von dieser gepflegt.
Eine Person kann aber gleichzeitig im Hauptunternehmen, aber auch in einem oder mehreren Tochterunternehmen angestellt sein. Das führende Personalsystem liefert Identitäts- und Organisationsdaten zu einer Person.
Es ist somit Aufgabe des IAM-Systems, diese Organisationsdaten zu Identitäten zusammenzuführen.

2.8.1 Personendaten zur Identifikation einer Person/Identität

Es wird auf Personendaten zurückgegriffen, die bei der Einstellung dem Personalbereich übermittelt und im SAP HCM gespeichert werden. Diese Daten werden an das IAM-System übertragen und dort verarbeitet.
Ziel ist es, eine Dubletten Prüfung einzuführen, die Ergebnisse mit einer definierten Unschärfe liefern kann.
Persönliche Merkmale (z.B. Fingerabdruck, Iris), die ihr zugeordnet werden könnten und anhand derer sie identifiziert werden könnten, werden aber nicht im elektronischen System beachtet/gespeichert und können somit nicht zur internen Identifikation zw. Systemen verwendet werden.
Personen, welche nicht im SAP HCM geführt werden, können nach Prüfung zusätzlich per Hand oder automatisiert im IAM erfasst werden.

Frage an/Ergänzung vom Bieter? *Erhalten diese einen eigenen Nummernkreis? Bitte erläutern!*

……

……

2.8.2 Unternehmens-Identifikatoren zur eindeutigen Identifikation einer Person

Bei der Anlage von Verträgen im Personalsystem werden Identifikatoren (Personenkennzeichen) für jeden Vertrag generiert bzw. angegeben die zur eindeutigen Identifikation verwendet werden können.

Folgende Tabelle führt einen Teil dieser Identifikatoren auf und erklärt, ob sich diese zur eindeutigen Identifikation einer Person eignen.

Identifikator	Veränderbarkeit	Hinweis
einfache Personalnummer (PNr.)	Veränderbar	Ändert sich der Vertrag erhält der Mitarbeiter eine neue PNr.
eindeutige Personalnummer (ePNr.)	i.d.R. unveränderbar	Bei Aus- und späterem Wiedereintritt wird die PNr. ggf. neu vergeben. Die Daten müssen dann zusammengeführt werden. Dabei wird die eindeutige PNr. wieder zugeordnet. Die Feststellung ob Identitäten zusammengehören erweist sich derzeit als schwierig.

Tabelle 2: Übersicht der Identifikatoren einer Person

Erläuterung: Wer erneut im Unternehmen anfängt (onboarding), erhält die gleiche Personalnummer. Nur wer bei einem Tochterunternehmen anfängt, bekommt eine neue Nummer bzw. bei Wiedereintritt die gleiche Personalnummer der Tochter.

Frage an Bieter: *Wie geht das IAM mit einem doppeltem/mehrfach Arbeitsverhältnis um? Was passiert, wenn bei 2 Verträgen, einer wegfällt?*

……

……

……

2.8.3 Eindeutige Personalnummer

Die eindeutige Personalnummer dient zur Identifizierung einer Person im KC und wird in den Personalstammdaten neben der einfachen Personalnummer hinterlegt.
Der Grund für die Anwendung einer ePNr. liegt in der Nachweispflicht in medizinischen Systemen. Es muss immer nachweisbar sein, welche Identität was in diesen Systemen wann getan hat. Dazu muss die Zuordnung des Zugangs zur Identität zweifelsfrei nachvollziehbar sein.

- Besitzt ein Mitarbeiter mehrere Verträge ist er über die eindeutige Personalnummer identifizierbar
- Besitzt der Mitarbeiter nur einen Vertrag, dann ist die vertragliche (einfache) PNr. identisch mit der ePNr
- Ändert sich die einfache PNr., z.B. durch einen Vertragswechsel, dann bleibt die ePNr. unverändert
- Die ePNr. wird nach einem Austritt nicht für andere Identitäten verwendet.
- Kommt ein Mitarbeiter nach einem Austritt wieder zurück, erhält er die alte ePNr. wieder.
- Bei Aus- und späterem Wiedereintritt wird die ePNr. ggf. neu vergeben, wenn eine Zuordnung zu einem älteren Datensatz nicht sofort auffällt – z.B. bei Änderung des Namens durch Heirat. Hier müssen die Datensätze dann wieder miteinander verknüpft werden. Die Feststellung erweist sich aktuell als schwierig, da eine technische Unterstützung zum Aufspüren von Dubletten fehlt.

2.9 IAM Zuständigkeiten

Für das IAM wird eine organisatorisch selbstständige Zuständigkeit definiert. Diese ist für den bestimmungsgemäßen Ablauf der IAM-Prozesse verantwortlich.

Dies beinhaltet:

1. Steuerung und Management der Rezertifizierungen von Berechtigungen in IT-Systemen entsprechend der Governance- und der IAM-Richtlinien

2. Steuerung von Prozessen im Identitäts- und Berechtigungsmanagement
   – Anpassung von Abweichungen in laufenden Prozessen und Weiterentwicklung der Prozessmodelle

3. Koordination der LifeCycle-Management-Prozesse

4. Beratung bei IAM-Themen im Unternehmen und in Projekten:
   – Ansprechpartner für ISB, DSB, Governance und Revision

5. Entwicklung und Qualitätssicherung von Berechtigungskonzepten & IAM-Richtlinien:
   – Sicherstellung der Einhaltung von IAM-Richtlinien
   – Erarbeitung und Etablierung aller technischen und organisatorischen Maßnahmen für ein unternehmensweites Berechtigungskonzept
   – Begleitung der produktiven Umsetzung der Berechtigungskonzepte in Anwendungen/Systemen
   – kontinuierliche Weiterentwicklung und Monitoring des Berechtigungskonzeptes unter Zuhilfenahme einer IAM-Softwarelösung

6. Betreuung und Weiterentwicklung des internen Identitäts- und Berechtigungsmanagementsystems:
   - Entwicklung von Workflows für den Self-Service-Teil des IAM-Systems

Um die Funktionsbereitschaft des IAM-Systems, die Entwicklung von Schnittstellen zu IT-Systemen und die Unterstützung im allgemeinen Umgang mit dem IAM-System zu gewährleisten, ist die Bindung an einen externen Dienstleister notwendig.

3 Anforderung an das zu implementierende IAM System

Auf Grundlage der in Kapitel 2 beschriebenen Anforderungen und Inhalte wird ein IAM-System ausgeschrieben.

Im Folgenden sind die Anforderungen an Systemanbindungen, Prozesse, Funktionen, Inbetriebnahme, Produktpräsentation, Betriebskonzept und weiteres beschrieben.

3.1 Allgemeine Anforderungen

3.1.1 Mengengerüst

Das zukünftige IAM-System muss ca. 7.500 Identitäten verwalten.
Die Identitäten teilen sich wie folgt auf:

- ca. 7.500 MA werden im Personalsystem HR verwaltet,
- im ActiceDirectory sind das ca. 7300,
  - davon ca. 6800 MA (aus HR),
  - + ca. 200 Dienstleister (werden im HR System nicht erfasst, jedoch im AD geführt),
  - + ca. 250 MEDiC Studierende (werden im HR System nicht erfasst, jedoch im AD geführt) und
  - + ca. 50 Serviceaccounts für Dienste/Systeme u.a. (nicht personalisierte Konten).

3.1.2 Systemanbindungen

Die im Folgenden beschriebenen IT-Systeme sollen an das IAM-System angebunden werden. Dafür stellt das IAM-System standardisierte Schnittstellen bereit.
Die Reihenfolge und Priorität ist der beigefügten **Anlage „Liste-der-IT-Systeme-IAM“** zu entnehmen.
Beispielhaft werden nachfolgend die wichtigsten IT-Systeme aufgeführt.

3.1.2.1 SAP HCM (Personalwirtschaftssystem)

Durch das SAP HCM werden alle Verträge der Mitarbeiter des Unternehmens verwaltet. Das Personalwirtschaftssystem ist das führende System für die Stellenplanung. Die Prozesse Onboarding, Offboarding und Change (z.B. Anpassungen an Attributen zu Personen oder Zuordnungen von Einrichtungen und Dienstarten) werden primär hier gestartet. Das IAM-System muss über eine geeignete Schnittstelle zur automatisierten Verarbeitung der oben genannten Prozesse verfügen.

Modul	**Eingesetzte Version im KC**
SAP HCM	SAP ERP 6.0 EHP 7

Durch den Anbieter ist zu erläutern, wie die Schnittstelle des IAM-Systems an das SAP HCM technisch umgesetzt wird.
Eine Umstellung auf S4/HANA ist in unserem Haus in Planung und muss schnittstellenmäßig unterstützt werden.

3.1.2.2 SAP i.s.h.med

Das primäre klinische Informationssystem im KC ist SAP i.s.h.med. Die Anmeldung am SAP i.s.h.med erfolgt mit der SAP-internen Authentifizierungsmethode, dabei sind die SAP-Anmeldenamen identisch mit den Windows-Anmeldenamen. Das IAM-System muss über eine geeignete Schnittstelle verfügen um Konten und Berechtigungen zu provisionieren.

Modul	**Eingesetzte Version im KC**
SAP – i.s.h.med	IS-H, Release 617 SAP-BASIS, Release 740

Durch den Anbieter ist zu erläutern, wie die Anbindung des IAM-Systems an SAP i.s.h.med technisch realisiert wird.

3.1.2.3 Imprivata OneSign / System Single Sign-On (SSO)

Die unkomplizierte Weiternutzung der im Haus bereits vorhandenen und eingesetzten Single Sign-On – Lösung zur Anmeldung am PC (Windows), KIS und Fachanwendungen muss gewährleistet sein (weiterer Ausbau an div. Subsystemen geplant).

Modul	Eingesetzte Version im KC
Imprivata OneSign	23.2

3.1.2.4 Microsoft Active Directory Services und DFS

Zur Windows-Authentifizierung setzt das KC eine Active Directory Windows Domäne ein. Alle Windowszugänge des KC werden dort verwaltet. Berechtigungen für an das AD angeschlossene IT-Systeme werden über entsprechende Rollen- und Berechtigungsgruppen verwaltet. Das IAM-System muss über eine direkte Schnittstelle zur Verwaltung von AD-Konten und AD-Gruppen verfügen.

Dateiablagen werden im KC als sogenannte Netzlaufwerke für die Kliniken/Bereiche zur Verfügung gestellt. Dazu wird das Microsoft DFS genutzt. Rechteverwaltungen erfolgen bisher über Gruppen und Gruppenzugehörigkeiten der Benutzer/Identitäten im AD.

Modul	Eingesetzte Version im KC
Active Directory (AD)	Functional Level 2016 (Domain und Forest), demnächst Upgrade auf 2019 + offen für Entra ID

Durch den Anbieter ist zu erläutern, wie die Anbindung des IAM-Systems an das Active Directory technisch umgesetzt wird. Eine später Nutzung von Microsoft Entra ID muss unterstützt werden.

3.1.2.5 Microsoft Exchange

Persönliche E-Mail-Postfächer, E-Mail-Verteiler und geteilte Postfächern werden in Microsoft Exchange organisiert. Das IAM-System muss über eine direkte Schnittstelle zu Microsoft Exchange verfügen, um alle notwendigen Eigenschaften der E-Mail-Postfächer, -Verteiler und geteilten Postfächer zu verwalten.
Das IAM erlaubt die Verwaltung von Postfächern für mehrere Mail-Domains (Multi-Domainfähigkeit).

Weitere Informationen entnehmen sie bitte Kapitel 3.2.8. – Anbindung an Exchange online muss möglich sein!!

Modul	Eingesetzte Version im KC
Exchange	Aktuell Version 2016 CU23 + offen für Exchange online

3.1.2.6 Intranet Just Social

Just Social bildet die Plattform für das hausinterne Intranet. Hier werden u.a. Mitarbeiterdaten, wie Name, Vorname, Telefon, Arbeitsort und –bereich angezeigt.
Diese werden aus dem HR System importiert.

Modul	Eingesetzte Version im KC
Just Social	Version: 13.11.2-3645, Hosting bei externem DL, Schnittstelle ADFS

Durch den Anbieter ist zu erläutern, wie die Anbindung des IAM-Systems an Just Social technisch umgesetzt wird.

3.1.2.7 Assetsystem / Drucksystem

Als Assetsystem ist das System DeskCenter im Einsatz.
Damit können u. a. AD-Benutzer (Identitäten), IT-Systeme (PC, Server), IT-Komponenten (Drucker, Bildschirme u.a. Peripherie) verwaltet/inventarisiert werden. Zusätzlich beinhaltet es eine Softwareinventarisierung und Verteilung/Deployment.

Das Output-Managementsystem/Drucksystem MyQ erlaubt eine personalisierte Verwaltung und Ausgabe von Prints mit Hilfe von eindeutiger Indentifikation am Drucksystem. Dazu werden aktuell sog. Token genutzt. Durch den Anbieter ist zu erläutern, wie die Anbindung des IAM-Systems an Microsoft 365 umgesetzt werden könnte. Wie funktioniert das jetzt?

Modul	**Eingesetzte Version im KC**
Assetsystem DeskCenter	11.0.8904.1
Drucksystem MyQ	PrintServer 8.2

Durch den Anbieter ist zu erläutern, wie die Anbindung des IAM-Systems an das Asset- und Drucksystem umgesetzt werden kann.

3.1.2.8 Service Management / Ticketsystem

Als System des Service-Managements, sog. Ticketsystem, wird das System Jira von Atlassian in Verbindung mit Confluence genutzt.

Durch den Anbieter ist zu erläutern, wie die Anbindung des IAM-Systems an das Service-Management-System, erfolgen kann bzw. welches Spektrum der mitzuliefernde SelfService abedecken kann.

3.1.2.9 Radiologiesystem RIS / PACS

Nutzung von AD-Gruppen: prinzipiell:
RIS “Medavis“: System erfordert noch zusätzliche Anpassungen (Zuordnungen) zu Rollen und Zugriffsrechten.

PACS „Syngo“: Passwortabfrage über AD-Account, hier Mitgliedschaften in AD-Gruppen schon ausreichend. Das könnte über Rolle im SAP HCM, z. Bsp. „Arzt Radiologie“ schon geregelt werden.

Bildverteilung „JiveX“: Passwortabfrage über AD-Account, hier Mitgliedschaften in AD-Gruppen schon ausreichend. Das kann über Rolle im SAP HCM schon geregelt werden.

3.1.2.10.Laborinformationssystem LIS

aktuell eigene Nutzerverwaltung, Nutzung von FileShares per AD-Gruppen

3.1.3 Bereitstellung generischer Schnittstellen

Um weitere, auch proprietäre, Systeme eigenständig anbinden zu können soll das System ein entsprechendes Connectivity-Framework bereitstellen, welches aktuelle, plattformunabhängige, Schnittstellen nutzt. Diese Schnittstellen sind z.B.: SOAP, REST, OData, SCIM, LDAP, SQL, XML, CSV (ggf. aufzählen).

Fragen an Bieter: *Können selbständig eigene Schnittstellen Module erstellt werden? Welche Scriptsprachen können genutzt werden? (ggf. kurz nennen/aufzählen)*
Gibt es einen sog. „Schnittstellen Designer“? Bitte dieses Tool kurz beschreiben bzw. alternative Möglichleiten benennen.

……

……

……

3.1.4 Sicherheitsanforderungen

Der Auftraggeber wurde vom Gesetzgeber als kritische Infrastruktur eingestuft und ist demzufolge verpflichtet die daraus resultierenden gesetzlichen Anforderungen in Bezug auf Informationssicherheit und Datenschutz einzuhalten. Nachfolgende Anforderungen bilden eine Zusammenfassung der wichtigsten Sicherheitsanforderungen für Standard-Software.

Der Auftraggeber nutzt zur Gewährleistung der Informationssicherheit und des Datenschutzes sowie der daraus resultierenden gesetzlichen Anforderungen, die Vorgehensweise nach BSI Grundschutz oder nach einer gleichwertigen Methodik.

Der Bieter garantiert mit der Abgabe seines Angebotes, dass die Basis- und Standard-Anforderungen der relevanten Bausteine des Grundschutz-Kompendiums vollständig erfüllt werden bzw. nach der Übergabe durch den Auftraggeber erfüllt werden können.

Der Bieter garantiert mit der Abgabe seines Angebotes, dass mit dem Angebot die Betroffenenrechte nach Art. 15-21 DSGVO gewährleistet werden können.

Der Bieter muss beschreiben, wie die Forderungen nach Art. 25 DSGVO für „Privacy by Design“ sowie „Privacy by Default“ mit dem von ihm angebotenen Produkt umgesetzt werden.

3.1.4.1 Anforderungen an die Benutzerauthentifizierung und Zugriffskontrolle

Es gibt eine hinreichende Benutzerverwaltung mit unterschiedlichen Berechtigungen, z.B. nach dem Prinzip von Role Based Access Control (RBAC).

Alle kritischen Aktionen können ohne das Vorhandensein der dazu erforderlichen Rechte nicht ausgeführt werden. Berechtigungen werden nach dem Prinzip der minimal erforderlichen Rechte (least privilege) vergeben.

3.1.4.2 Anforderungen an die Wahrung der Vertraulichkeit von Daten (Verschlüsselung)

Es werden etablierte Algorithmen zur Wahrung der Vertraulichkeit von Daten verwendet, die dem aktuellen Stand der Technik entsprechen und von denen keine Sicherheitslücken bekannt sind.

Es wird auf anerkannte Verschlüsselungsbibliotheken zurückgegriffen, um Implementierungsfehler zu vermeiden.

Beim Einsatz kryptographischer Verfahren wird eine empfohlene Schlüssellänge nach aktuellem Stand der Technik eingesetzt.

Es wird eine Transportverschlüsselung (z.B. TLS) nach aktuellem Stand der Technik für alle Verbindungen (sowohl externe als auch Verbindungen zum Backend) verwendet, die vertrauliche Daten oder Funktionen beinhalten.

3.1.4.3 Anforderung an die Datenvalidierung

Es werden sämtliche Schnittstellen zur Software mit einer hinreichenden, serverseitigen Datenvalidierung nach aktuellem Stand der Technik abgesichert, um Manipulationen durch Buffer-Overflows, Command-Injection, SQL-Injection oder Cross-Site-Scripting (XSS) zu verhindern.

3.1.4.4 Anforderungen an die Fehlerbehandlung und das Logging

Es werden über alle sicherheitsrelevanten Vorgänge ausreichend Informationen aufgezeichnet, wobei über Logdaten oder Fehlermeldungen keine kritischen Informationen (z.B. Passwörter) preisgegeben werden.
Sämtliche Fehler (Exceptions) werden sicher behandelt, sodass sich die Software stets in einem sicheren Zustand befindet.

3.1.4.5 Anforderungen an die Konfiguration

Die Auslieferung des Produkts erfolgt in einer sicheren Basiskonfiguration, die dokumentiert ist und vor unbefugten Änderungen geschützt ist.
Komponenten und Dienste erhalten nur die minimal für den Systembetrieb notwendigen Rechte und Berechtigungen.
Die Passwörter, Zertifikate und Schlüssel sind für sämtliche Funktionen des Produkts austauschbar.

3.1.4.6 Anforderungen an den Datenschutz

Es werden so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder verwendet und alle technischen und organisatorischen Maßnahmen getroffen, die erforderlich sind, um ausreichenden Datenschutz zu gewährleisten.

3.1.4.7 2-Faktor-Authentifizierung (2FA) für administrative Konten an anderen IT-Systemen

(als Option zu verstehen)

Die sichere digitale Anmeldung ist eine Sicherheitsfunktion, bei der Nutzende (hier vorrangig Administrator:innen) zusätzlich zum Passwort ein zweites Sicherheitsmerkmal (zweiter Faktor) eingeben müssen. Diese wird daher auch als 2-Faktor-Authentifizierung bezeichnet (2FA).
Es können dabei wahlweise entweder eine Smartphone-App mit Einmal-Passwort, bevorzugt Authenticator, eine geheime Zeichenkette (ein sogenanntes Indexed Secret/PIN) oder ein USB-Token verwendet werden.

Fragen an Bieter: *Welche Verfahren können angeboten werden? Zusatzaufwände/Kosten?*

……

……

……

3.1.4.8 Privileged Access Management (PAM)

Ein Privileged Access Management (PAM), auch Privileged Account Management steht für eine portionierte und zeitlich begrenzte Zuteilung von Rechten und dem nötigen Zugriff nach gerechtfertigtem Bedarf. Dabei erfolgt das sogenannte Provisioning, also die Zuteilung von Rechten anhand der Aufgabe, die ein User/Identität bzw. seine Rolle stetig im System übernehmen, und anhand der Zusatzrechte, die für die Bearbeitung einer besonderen Aufgabe benötigt werden.
Eine spätere Nutzung von Microsoft Entra ID muss unterstützt werden.

3.2 Abzubildende Anwendungsfälle

3.2.1 Onboarding Mitarbeiter

Der Onboarding Prozess eines Mitarbeiters wird gestartet, wenn ein Mitarbeiter in das Unternehmen eintritt.

1. Die Personalabteilung erstellt bei Einstellung eines neuen Mitarbeiters einen Vertrag/Datensatz im SAP HCM.
2. Die für das IAM-System relevanten Informationen (Attribute) werden über eine geeignete Schnittstelle automatisch importiert.
3. Das IAM-System prüft anhand eines konfigurierbaren Algorithmus, ob die Identität schon vorhanden ist. Ist sie noch nicht vorhanden, wird sie erstellt. Wird ein Duplikat erkannt, muss ein Prozess ausgelöst werden, der den Bereich „Personal“ benachrichtigt und zum Zusammenführen der Vertragsdaten im Quellsystem auffordert.
4. Nach erfolgreichem Anlegen der Identität werden Basisrechte, auf Grund der Zugehörigkeit von Organisationseinheit, Dienstart und betrieblicher Funktion vergeben und in die angebundenen Zielsysteme provisioniert.
5. Es wird durch das IAM-System ein persönliches AD-Konto (nach Namenskonvention im KC) mit folgenden Grundfunktionen angelegt:
   - persönliches E-Mail-Postfach
   - Anmeldeskript (abhängig von der Zuordnung zur Organisationseinheit)
   - persönliches Laufwerk
   - Zuordnung von Basis-AD-Gruppen
   - Anpassungen der AD-Attribute (z.B. Anmeldename) nach Vorgabe des KC

3.2.2 Änderung Mitarbeiter

Als Ändern wird die Änderung der Organisationseinheit, der Dienstart, betrieblichen Funktion oder der Stammdaten eines Mitarbeiters verstanden.

3.2.2.1 Ändern von Dienstart oder Organisationseinheit

1. Die Personalabteilung nimmt Änderungen an den relevanten Attributen (z.B. Dienstart oder Organisationseinheit) einer Identität im SAP HCM vor.
2. Diese Änderungen werden über die Schnittstelle an das IAM-System transportiert.
3. Das IAM-System berechnet die sich aus den übermittelten Änderungen für Dienstart oder Organisationseinheit ergebenen Berechtigungen neu („vererbte Rechte“).
4. Das IAM-System startet einen Rezertifizierungsprozess für zuvor beantrage Berechtigungen.

3.2.2.2 Temporäre Abwesenheiten

1. Die Personalabteilung nimmt Änderungen an relevanten Attributen einer Identität im SAP HCM vor, die eine längere Abwesenheit, wie z.B. Elternzeit, anzeigen.
2. Das IAM-System deaktiviert oder entzieht Berechtigungen je nach Konfiguration des Abwesenheitsgrundes.

3.2.2.3 Wiedereintritt

Das Beenden einer temporären Abwesenheit veranlasst das IAM-System, deaktivierte Berechtigungen wieder zu aktivieren.

3.2.2.4 Änderung von Stammdaten

Jeder Benutzer im IAM-Systems kann persönliche Attribute seiner Identität anpassen (z.B. Namensänderung). Vorgesetzte, Account-Verantwortliche und Administratoren können zusätzlich auch weitere Attribute, wie z.B. Organisationseinheit oder Funktion, ändern. Diese Änderungen starten jeweils einen Genehmigungsprozess und nach Genehmigung werden die Änderungen zurück an das das führende System SAP HCM gesendet.

3.2.3 Offboarding Mitarbeiter

Der Offboarding Prozess eines Mitarbeiters beginnt, wenn ein Mitarbeiter das Unternehmen verlässt. Das Verlassen wird durch das Setzen und Erreichen des Gültig-Bis der Identität angezeigt. Dies erfolgt bei internen Mitarbeitern durch den Import aus dem HR-Import automatisch. Bei Externen greift das zuvor gesetzte Gültig-Bis.

1. Das „Gültig-Bis“ der Identität rückt in die Vergangenheit.
2. Die Identität wird beendet, alle Berechtigungen werden, unter Berücksichtigung von definierten Karenzzeiten deaktiviert. Nach Ablauf der Karenzzeiten werden die Berechtigungen entfernt. Das Deaktivieren bzw. Entfernen wirkt auch in den angebundenen Zielsystemen.
3. Das IAM-System prüft, ob der Identität noch Prozesse oder Aufgaben in solchen zugewiesen sind und weist diese ggf. neu zu.

3.2.4 Verwaltung von externen Identitäten

Externe Identitäten (s. Pkt. 2.3.1.2) unterliegen ebenfalls dem Identity LifeCycle. Jede externe Identität wird durch einen Verantwortlichen verwaltet.

<u>Onboarding:</u>
Neue externe Identitäten werden im IAM-System im Kontext der entsprechenden externen Firma über ein elektronisches Antragsformular beantragt. In diesem Antrag mit Genehmigungsworkflow können zeitgleich zusätzlich Berechtigungen mit angefordert werden.
Nach Durchlaufen des Genehmigungsprozesses muss die externe Identität ins System SAP HCM importiert werden, da alle Verträge mit internen und externen Mitarbeitern ursprünglich dort geführt werden. Die eigentliche externe Identität wird erst durch den Importprozess zw. SAP HCM und IAM-System erzeugt.

<u>Change:</u>
Änderungen werden durch einen Verantwortlichen direkt im IAM-System an der Identität vorgenommen. Diese Änderungen können, sofern erforderlich, einen Genehmigungsprozess starten und werden nach Abschluss des Prozesses an SAP HCM gemeldet.

<u>Offboarding:</u>
Siehe 3.2.3 Offboarding Mitarbeiter

3.2.5 Verwaltung von Mehrfach- und nicht personalisierten Konten

Neben dem persönlichen Konto müssen auch Administrations-, Test- und nicht personalisierte Konten (z.B. Autologin) verwaltet werden.
Über das IAM-System muss es möglich sein, diese Konten als Besitzer oder im Auftrag des Besitzers zu beantragen. Nach einem definierten mehrstufigen Genehmigungsworkflow werden diese Konten dann durch das IAM-System angelegt und die Zugangsinformationen übermittelt.
Jedes dieser Konten muss einem Besitzer oder einem organisatorischen Element zugeordnet werden.
In Zielsystemen nicht zugeordnete Konten werden entsprechend als „verwaist" gekennzeichnet und beispielsweise dem Informationseigentümer zur Zuordnung und Klassifizierung vorgelegt.

Frage an Bieter: *Empfehlung für Erstellung, Zuordnung und Verwaltung Mehrfach- und nicht personalisierter Konten geben.*

……

……

……

3.2.6 Berechtigungsmanagement

3.2.6.1 Self-Service Berechtigungsbeantragung mittels Genehmigungsworkflow

Zugriffe und Berechtigungen, die nicht auf Grund von Dienstarten bzw. Zugehörigkeiten zu Organisationseinheiten zugewiesen wurden, können durch den Anwender oder seinen Vorgesetzten oder Verantwortlichen im IAM-System, sofern erforderlich auch zeitlich beschränkt, beantragt werden.
Die im Antrag des Berechtigungsprozesses wählbaren Berechtigungen werden kontextbasiert, also zum Beispiel durch die Zugehörigkeit zu einer Organisationseinheit, angeboten bzw. eingeschränkt. Weiterhin soll eine einfach handhabbare Suchfunktion angeboten werden, sowie die Einschränkung der Suche auf Berechtigungen bestimmter Anwendungen möglich sein.
Die Freigabe bzw. Genehmigung der beantragten Berechtigung erfolgt, konfigurierbar und je nach Kritikalität der Systeme bzw. Anwendungen oder Berechtigungen, mehrstufig. Der Antragsteller kann jederzeit den aktuellen Stand der Bearbeitung nachvollziehen. Die Begründungen für Genehmigung oder Ablehnung werden im IAM-System gespeichert.

3.2.6.2 Self-Service Delegation

Unter Delegation wird ein permanentes oder zeitlich begrenztes Übertragen von Berechtigungen zur Genehmigung von Berechtigungen verstanden. Das bedeutet, dass ein Genehmiger (im Ursprung der Informationseigentümer oder personelle Vorgesetzte) das Recht zur Genehmigung des Workflows an eine andere Person übertragen kann.
Im IAM-System soll dazu eine entsprechende Funktion vorhanden sein, die es dem Genehmiger erlaubt eigenständig (z.B. über einen Self-Service) das Genehmigungsrecht an andere Personen im Unternehmen (wenn nötig zeitlich befristet) zu delegieren.
Bei der Delegation kann die Zuständigkeit in Abhängigkeit der Organisation definiert werden. (z.B. delegiert der Klinik-Leiter auf unterschiedliche Personen, je nachdem aus welchen Bereich der Workflow kommt.) Die Delegation kann festlegen ob sie direkt bei einem eintreffenden Workflow verwendet wird oder erst nach einer definierten Eskalationszeit.

3.2.6.3 Self-Service Vertretungen

Unter Vertretung wird ein zeitlich begrenztes Übertragen von Berechtigungen in Zielsystemen verstanden, die es dem Vertretenden erlaubt, die ihm übertragen Aufgaben auszuführen. Der zu Vertretende wählt im Self-Service seinen Vertreter und die zu vertretenden Berechtigungen für einen festgelegten Zeitraum aus. Der Vertreter erhält die Berechtigungen unmittelbar im festgelegten Zeitraum.

3.2.7 Self-Service Passwort zurücksetzen

Mit dieser Funktion soll der IT-Service-Desk entlastet werden, in dem der Endbenutzer sein Passwort eigenständig zurücksetzen kann.

3.2.7.1 Nicht-authentifizierter Passwort-Reset

Der Anwender der sein Passwort zu seinem persönlichen Windows-Zugangs vergessen hat, soll die Möglichkeit erhalten ein neues Initialkennwort über folgende Wege über das IAM-System zu beantragen:

- durch hinterlegtes Wissen (Passwort-Reset-Fragen)
- Zusendung des Initialkennworts an dessen Vorgesetzten oder eine andere definierte Person im Unternehmen.
- Zusendung einer Hälfte des Initialkennworts an dessen Vorgesetzten oder eine andere definierte Person im Unternehmen. Die andere Hälfte wird an den Anwender, der sein Passwort vergessen hat, übermittelt.

3.2.7.2 Authentifizierter Passwort-Reset

Der Endanwender möchte das Passwort eines Kontos in einem an das IAM-System angebunden System neu setzen. Er meldet sich mit seinem persönlichen Konto am IAM-System an, wählt den entsprechenden Self-Service und vergibt, unter Berücksichtigung der Kennwortrichtlinien, das neue Passwort für das Konto im Zielsystem.

3.2.8 Verwalten von E-Mail-Verteilern und Geteilten Postfächern in Exchange

Das IAM-System muss das Beantragen und Verwalten von E-Mail-Verteilern und Geteilten Postfächern als Self-Service ermöglichen.

Beim Beantragen kann eine andere Identität als die des Antragstellers als Verantwortlicher angegeben werden.

- Über ein im IAM-System erstelltes und bereitgestelltes Webformular können E-Mail-Verteiler und geteilte Postfächer beantragt werden
- Die Konfiguration des Webformulars muss durch die IAM-Abteilung anpassbar sein
- Bei der Anlage wird über die Schnittstelle zum Exchange Server entweder ein E-Mail-Verteiler oder ein geteiltes Postfach erstellt und konfiguriert
  - es muss möglich sein beim Antragstellen die Mitglieder anzugeben, die dann bei der Anlage automatisch dem E-Mail-Verteiler oder dem geteilten Postfach hinzugefügt werden
  - weitere technische Konfigurationen, wie z.B. Moderation müssen möglich sein
- die Pflege der Mitgliedschaften von E-Mail-Verteiler und Zugriff auf geteilte Postfächer muss durch den hinterlegten Besitzer möglich sein
- die Beantragung von Mitgliedschaften (E-Mail-Verteiler) bzw. Zugriffe (geteiltes Postfach), über einen Genehmigungsworkflow, von Nutzern muss möglich sein

Die Umsetzungsmöglichkeiten sind vom Anbieter darzulegen.
Im Folgenden sind die grundlegenden Unterschiede in Funktion und Handhabung von E-Mail-Verteiler und –geteiltem Postfach in der Umgebung des Auftraggebers beschrieben.

3.2.8.1 E-Mail-Verteiler

- Ein E-Mail-Verteiler ist gekennzeichnet durch die Weiterleitung von E-Mails an den im E-Mail-Verteiler enthaltenen Personenkreis.
- Die E-Mails werden lediglich an die Postfächer der Mitglieder verteilt.
- Organisatorisch verantwortlich für die Vollständigkeit der Mitgliedschaften ist der jeweilige Verantwortliche des E-Mail-Verteilers. Dieser wird bei der Anlage festgelegt. Es gibt keinen E-Mail-Verteiler ohne Verantwortlichen!
- Die Mitgliedschaften sind regelmäßig durch den entsprechenden Verantwortlichen zu kontrollieren und selbstständig zu korrigieren, wenn er die Berechtigung dazu besitzt.
- Eigenschaften und Festlegungen zu E-Mail-Verteilern sind entsprechend zu dokumentieren.
- Die Verantwortung für die Vollständigkeit der Dokumentation liegt beim Verantwortlichen des E-Mail-Verteilers.
- Die Notwendigkeit eines E-Mail-Verteilers ist regelmäßig durch den Verantwortlichen zu kontrollieren.
- Eine Löschung kann nur durch den Verantwortlichen beantragt oder eigenhändig durchgeführt werden.

3.2.8.2 geteiltes Postfach

- Ein geteiltes Postfach ist ein nicht personenbezogenes Postfach, vergleichbar mit einem Firmen-Briefkasten.
- E-Mails an dieses Postfach werden nur dem Postfach zugestellt.
- Berechtigte Nutzer haben Zugriff auf dieses Postfach und können sich dieses z. B. im Outlook einbinden.
- Bereitstellung eines übergreifenden Kalenders
- Organisatorisch verantwortlich für die Vollständigkeit der Mitgliedschaften ist der jeweilige Verantwortliche des geteilten Postfachs. Dieser wird bei der Anlage festgelegt. Es gibt kein geteiltes Postfach ohne Verantwortlichen.
- Die Zugriffe müssen regelmäßig durch den entsprechenden Verantwortlichen kontrolliert werden.
- Die Notwendigkeit eines geteilten Postfachs ist regelmäßig durch den Verantwortlichen zu kontrollieren.
- Eine Löschung kann nur durch den Verantwortlichen beantragt oder eigenhändig durchgeführt werden

3.2.9 Notfallsperre

Wenn eine Organisation den Verdacht hat, dass die Identität eines Benutzers kompromittiert wurde, ist es wichtig, schnell zu handeln, um den Schaden zu begrenzen.
Um dies zu erreichen, muss Verantwortlichen die Möglichkeit gegeben sein, alle Konten, die mit der Identität verbunden sind, auf einmal zu sperren und später auch wieder zu entsperren.

3.2.10 Verwaltung von Windows-Dateifreigaben

Der Austausch von Information zwischen IT-Systemen kann auch per File-Share erfolgen. Das IAM-System verwaltet (erstellt, löscht) die Freigaben und verwaltet die Berechtigungen darauf.

3.2.11 Versenden von E-Mail-Benachrichtigungen

Das IAM-System ermöglicht, je nach Prozess und Prozess-Konfiguration, das Versenden von E-Mail-Benachrichtigungen. Diese sind individuell einstellbar.
Beim Anlegen neuer Konten wird das initiale Kennwort, je nach Konfiguration, an den Kontoinhaber oder dessen Verantwortlichen oder Vorgesetzten übermittelt.

3.2.12 Anbinden von Applikationen

Das Anbinden von Onboarding beschreibt das Erstellen logischer Anwendungen, welche zum Teil aus mehreren Systemen bestehen können. Ziel ist, sprechende Berechtigungsobjekte zu erstellen, um die dahinterliegende Komplexität vor den Beantragenden und den Genehmigern zu verbergen. Das IAM-System unterstützt dieses Verfahren, indem es einen entsprechenden Prozess abbildet.

3.3 Technische Anforderungen

3.3.1 Systemaufbau

3.3.1.1 Anforderungen an System Infrastruktur

Das zukünftige IAM-System wird durch das KC in Eigenregie in einem Rechenzentrum in einer virtuellen Umgebung betrieben.
Der AG speichert die Daten seiner IT-Systeme standardmäßig in Microsoft SQL-Datenbankumgebungen (DBMS). Diese Umgebung ist gehärtet und entspricht dem Stand der Technik. Die Daten des zukünftigen IAM-Systems sollen ebenfalls in einem gehärteten DBMS gespeichert werden.

Frage an Bieter: *Empfehlung für Lösung bzgl. Verfügbarkeit und Backup geben.*
Welche DBMS werden eingesetzt? Entstehen dabei Zusatzkosten/Zusatzaufwände?

……

……

……

3.3.1.2 Authentifizierung am IAM-System

Die Authentifizierung eines Administrators gegenüber dem IAM-System sollte mit einer zusätzlichen Absicherung erfolgen, möglichst 2FA. Optional kann sich die Authentifizierung über einen Identity Provider erfolgen

3.3.1.3 Front-End / GUI

Das Front-End, also die sichtbare Benutzeroberfläche, muss Web-basiert sein. Sie soll nicht nur Endanwendern Berechtigungsanträge zugänglich machen, sondern auch Genehmigern, Auditoren, Betriebsverantwortlichen und Administratoren die notwendigen Operationen erlauben.
Werden zusätzliche Browser-Add-Ons benötigt, so sind diese durch den Bieter zu benennen.

3.3.1.4 Staging-Umgebungen

Test- und Produktivumgebung müssen voneinander logisch getrennt sein. Vor dem Einsatz im Produktivbetrieb sollen angemessene Integrations-, System- und Freigabetests durchgeführt werden, bei denen die Funktionalität und Sicherheit der Software geprüft und freigegeben wird.
Wir favorisieren eine 2-stufige Umgebung für das IAM. Für angeschlossene Quell-/Zielsysteme ist dies im Einzelfall zu prüfen und umzusetzen.

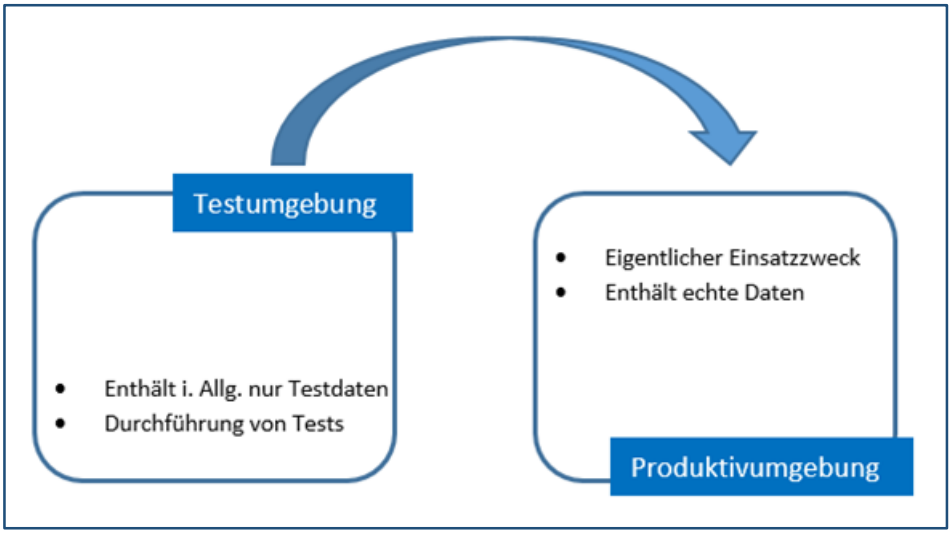

Abbildung 4: Überblick Staging-Umgebungen

Aufgabe an Bieter: *Bitte beschreiben Sie im Detail wie Systemänderungen produktiv gesetzt werden (Transportwesen). Welche Konequenzen (kurz- und mittelfristig) hat ein Ausfall des IAM für Quell- und Subsysteme?*

3.3.1.5 Flexibilität des Datenmodells

Datenobjekttypen, sowie deren Formulare und Listen sollen jederzeit erweiterbar und veränderbar sein. Das Hinzufügen eines Eigenschaftsfeldes zu einer Identität zum Beispiel, muss auf den entsprechenden Formularen veränderbar sein und das Hinzufügen zu Listenansichten möglich sein.
Entsteht beispielsweise die Notwendigkeit, die Telefonnummer zu hinterlegen, so muss es das Datenmodell erlauben dieses Attribut der Identität hinzuzufügen, ohne Anpassungen am Backend vornehmen zu müssen.

Virtualisierung

- Die Virtualisierung der Serversysteme mit VMware vSphere ESXi Version 7 oder neuer ist möglich

Serverbetriebssysteme

- Lauffähig in einer 64-Bit Umgebung
- Lauffähig unter Windows Server 2019, Windows Server 2022 oder neuer

SQL-Datenbanken

- Bei Nutzung von MS-SQL – Datenbanken ist die Version und Lizenzierung anzugeben (Beschaffung AG, AN, OEM…)

Aufgabe an Bieter: *Sollten andere DB-Systeme zu Grunde liegen, diese bitte analog beschreiben.*

Terminalserver

- Ein Terminalserverkonzept (XenApp/Citrix bzw. MS-Terminalserver) wird unterstützt
- Terminalserver RDP-Protokoll, Versionen 2019, 2022 wird unterstützt.

Datensicherung/Backup

- Backup
    - Backup-Strategie garantiert die Datensicherheit nach einem Systemabsturz.
    - Die Integration in das vorhandene Datensicherungssystem des AG ist möglich (Veeam Backup & Replication)
    - Es werden weitere Backup-Systeme unterstützt (bitte angeben).
    - Das Backup ist automatisiert und überwachungsfähig.
    - Es werden verschiedene Backup-Medien und Szenarien unterstützt. (bitte angeben)
    - Das Backup kann während der Laufzeit online durchgeführt werden.
    - Ein konsistentes Online-Backup ist möglich, d.h. alle Daten (auch offene Dateien) werden während des laufenden Betriebes gesichert
    - Während des Backups gibt es keine Performance-Einschränkungen des laufenden Betriebes

Frage an Bieter: *Wer richtet das DB-Backup ein? Welche Empfehlungen gibt es bzgl. Vollständigem, Differenziellem und Inkrementellen Backup der DB, des IAM-Systems? Wer richtet das DB-Backup ein? Wir sichern im Allg. die gesamte VM. Empfehlungen von Seite AN dazu!*

- Desaster und Recovery
    - Recovery-Strategie garantiert die Datensicherheit nach einem Systemabsturz.
    - Ein Havarie-Konzept für die angebotene Lösung liegt vor.
    - Nach einem Systemabsturz kann ein konsistenter Zustand sicher wiederhergestellt werden.

Hinweis an Bieter: *Beschreiben sie den empfohlenen Prozess der Wiederherstellung. Welche Zeiten und Ressourcen sind in dieser Umgebung einzuplanen?*

Systemüberwachung

- Es gibt Tools zur Überwachung der Systemprozesse (Monitoring von Platte voll, Table-Space voll etc.), um die eingesetzten Module auf Aktivität/Bereitschaft und auftretende Probleme hin zu überwachen.
- Die überwachten Daten zu Performance und Statistik können ausgewertet werden.
- Diese Tools sind Nagios checkmk-kompatibel.
- Diese Tools zur Überwachung der Systemprozesse (Monitoring) können auch vom AG genutzt werden.
- Es erfolgt eine Benachrichtigung der Systemadministration per Mail im Falle eines Prozessabsturzes bzw. dem Auftreten von Fehlersituationen.
- Diese Tools können - auch in einer verteilten Systemlandschaft – systemübergreifend eingesetzt werden.
- Die Nutzung und Integration eines eigenes Monitoring durch den AG ist möglich (SNMP, WMI, Agent auf Systemen usw.)

Drittanbietersoftware/Open Source

- Kommen Softwarelösungen von Drittanbietern (auch Java) bzw. Open Source Lösungen/-Module (auf Server bzw. Clients) zum Einsatz?

Aufgabe an Bieter: *Bitte ggf. inkl. Updateprozessen aufzählen und erläutern!*

Browser

- Der Browser MS Edge Chromium wird unterstützt.
- Der Browser Chrome Version min. 120.xxx wird unterstützt.
- Der Browser Safari bzw. ein aktueller Browser unter iOS/macOS wird unterstützt.

AntiViren-Security

- Es können Antiviren-Programme installiert werden, diese stören die Applikationen nicht. Bitte auflisten welche bereits erfolgreich getestet wurden. Geben Sie an welche Einstellungen benötigt werden.
- Insbesondere Trellix wir unterstützt. Geben Sie an, welche Einstellungen benötigt werden

3.3.1.6 Dokumentation

Neben einer Dokumentation der abgeschlossenen Prozesse über die Datenbank in Form von Log- bzw. Change-Dateien, müssen detaillierte, revisionssichere pdf-Dokumente erstellt, archiviert und bei Bedarf per E-Mail versendet werden können.
Diese Funktion wird u.a. benötigt, wenn Informationen in schriftlicher Form für ein Dokumentenmanagementsystem oder einen benötigten Ausdruck versendet werden.

3.3.1.7 Auswertung & Reporting

Alle Daten in dem Produkt müssen über definierte Schnittstellen für Auswertungen mit einer BI-Lösung genutzt werden können.
Das Produkt muss ein integriertes Reporting zur Verfügung stellen mit dem der AG eigene Auswertungen gestalten kann.

3.3.1.8 Compliance & Re-Zertifizierung

Basisleistung:
Die Anwendung muss über Compliance und Re-Zertifizierungsfunktionen verfügen, das betrifft die Vergabe von sicherheitskritischen Accounts. Änderungen an den Berechtigungen müssen in einer Historie dokumentiert sein.

Der Mitarbeiter muss in der Lage sein, für seine verwalteten Identitäten dargestellt zu bekommen, welche Berechtigungen er beantragt hat und welche bereits eingerichtet wurden.

Die IST-Daten aller angeschlossenen Systeme müssen regelmäßig mit dem SOLL Stand im IAM abgleichbar sein. Auf Differenzen muss entsprechend reagiert werden.

Erweiterter Funktionsumfang (optional):
Re-Zertifizierungen müssen in regelmäßigen Abständen automatisiert durchgeführt werden können. Verantwortliche Mitarbeiter sind in geeigneter Form zu informieren und müssen die zu überprüfenden Berechtigungen bestätigen oder ablehnen können. Der Mitarbeiter wird über diese Änderungen automatisch informiert.

3.3.1.9 Internet-Portal

Es muss möglich sein, von innerhalb des Netzwerkes des AG den Zugriff auf ein Webportal zu ermöglichen, über das externe und interne Mitarbeiter IAM-Prozesse initiieren können. Aktuell betrifft dies den Anwendungsfall 3.2.7.1 Nicht-authentifizierter Passwort-Reset.

3.3.2 Funktionalität

3.3.2.1 E-Mailversand

Das Produkt muss in der Lage sein, aus dem Prozess heraus E-Mails mit individuellen pdf-Dokumenten zu versenden. Eingehende E-Mails werden mit Anhang zu dem jeweiligen Prozess dokumentiert und gespeichert.

3.3.2.2 Antragsformulare

Die Antragsformulare sollen in Abhängigkeit von der Datenerfassung dynamische Änderungen (Ein- oder Ausblenden von zusätzlichen Eingabefeldern) ermöglichen. In vielen Fällen ist es sinnvoll, in Abhängigkeit von der Dateneingabe, weitere Eingabemöglichkeiten zur Verfügung zu stellen oder nachfolgende Eingabefelder auszublenden. Bei mehrstufigen Formularen soll auch die Verfügbarkeit ganzer Seiten darüber gesteuert werden können. Das erhöht die Akzeptanz, reduziert den Schulungsaufwand und Eingabefehler. Die damit verbundene dynamische Führung durch die Datenerfassung ist ein wichtiger Bestandteil für eine optimale Usability.

3.3.2.3 Massenverarbeitung von Prozessen / Anstoßen von Prozessen mit Massendaten

Es soll die Möglichkeit bestehen Prozesse in einer performanten Massenverarbeitung durchzuführen, ohne das für jeden Fall (z.B. Versetzung mehrere Mitarbeiter in eine neue Organisationseinheit) ein einzelner Verarbeitungsschritt durch den Administrator durchgeführt werden muss.
Dabei soll auch das initiieren neuer Prozessinstanzen für mehrere Datensätze desselben Typs im Bulk-Verfahren möglich sein.
Der Administrator muss die Möglichkeit haben, **vor** Einlesen der Datensätze, diese auf z. B. korrekte Formatierung zu prüfen.

Beispiel: Es wird ein Prozess für 15 neue externe Mitarbeiter gleichzeitig gestartet. Das IAM-System bietet dazu die Möglichkeit, beispielsweise eine CSV-Datei mit den notwendigen Informationen hochzuladen, vom Administrator prüfen zu lassen und zu verarbeiten.

3.3.2.4 Verwaltung nicht personalisierter Zugänge

Die Verwaltung von nicht personalisierten Zugängen von angeschlossenen Systemen (z.B. Active Directory) muss in gleicher Form gegeben sein, wie die Verwaltung von personalisierten Zugängen.

3.3.2.5 Berechtigungsobjektmodell

Das unter 2.7 beschriebene Berechtigungsmodell muss in der Software technisch umsetzbar sein.

3.3.2.6 Statusinformationen

Es muss möglich sein, Berichte bzw. Sichten so zu generieren, dass der aktuelle Status der in Bearbeitung befindlichen Prozesse anzeigt wird (wartend, in Arbeit, Status der Freigaben, erledigt, erfolgreich, Fehler, usw.). Die Berichte und Sichten müssen individualisierbar sein.
Der Nutzer muss nach Anmeldung am Web-Portal über den aktuellen Status seiner Anträge und ToDo´s informiert werden.

3.3.2.7 Dubletten Prüfung

In der Verarbeitung von Identitäten über die angeschlossenen Systeme (z.B. HCM, AD, Telefonbuch) müssen die Identitäten miteinander verglichen und auf Dubletten überprüft werden. In der Schreibweise kann es immer wieder zu Abweichungen kommen. Das System muss in der Lage sein mit diesen Abweichungen über einen vordefinierten Weg umzugehen, um Dubletten zu erkennen. Mögliche Wege zum Umgang mit Dubletten sind zu beschreiben.

3.3.2.8 Fehlermanagement

Beschreiben Sie detailliert das Fehlermanagement in Ihrem Produkt (Reaktion auf Fehler, Dokumentation, Teilumsetzung oder Roll-Back, Unterstützung für die Fehleranalyse und -behebung, Neustart bei Systemausfall, …).

3.3.2.9 Genehmigungsworkflow

In der Durchführung von Genehmigungsprozessen muss es Genehmigenden möglich sein die Freigaben über folgende Wege freizugeben:

- Web-Frontend
- Direkt über aus einer E-Mail über einen sogenannten Deeplink

Genehmigungsprozesse müssen mit multiplen Freigaben (mehrere Genehmiger) konfigurierbar sein.

3.3.2.10 Mandantenfähigkeit

Das Produkt muss in der Lage sein mehrere Mandanten zu verwalten.

3.3.2.11 Prozess-Designer

Das Produkt muss für den Administrator die Möglichkeit bieten, über eine grafische Oberfläche, intuitiv geführt und leicht verständlich, eigene Prozesse zu entwickeln, diese zu testen und in die produktive Umgebung zu überführen.

3.3.2.12 Umgang mit automatisierten Arbeitsaufträgen

Automatisierte Arbeitsaufträge müssen in der Form verwaltbar sein, dass Informationen über die Durchführung und den Status an definierbare Empfänger gemeldet werden. Als Kommunikationsweg müssen ein E-Mailversand und eine Information über das Web-Portal zur Verfügung stehen.

4 Anzubietende Leistungen

4.1 Softwarelizenzen

Der AN verkauft dem AG die notwendigen Softwarelizenzen für das IAM-System, inkl. für weitere benötigte Produkte, wie Schnittstellenlizenzen, mögl. Drittsoftware etc.. Im Preisblatt sind die damit verbundenen Kosten darzustellen. Zusätzlich sind eventl. anfallende Dienstleistungskosten bzw. Pauschalen für Wartungen etc. zu benennen (s. Pkt. 4.2.3.2). Sollte der AN. z. Bsp. der Hersteller, einen sog. Dritten, z. Bsp. Dienstleister, mit beauftragen, ist dies offenzulegen.
Die vom AG zu schaffenden Voraussetzungen, z. B. Spezielle Softwareprodukte, Betriebssysteme etc., sind zu benennen.

4.2 Inbetriebnahme des IAM-Systems

4.2.1 Anforderungen an den AN, Qualifikationen der Projektmitarbeiter

Siehe hierzu Dokument KCLW-V01EG „Aufforderung zur Abgabe eines Angebots“ Punkt 3.1.2. „sonstige, leistungsbezogene Nachweise / Unterlagen - Technische und berufliche Leistungsfähigkeit“

4.2.2 Projektdokumentation

Im Rahmen der Einführung des IAM-Systems ist durch den AN eine Projektdokumentation durchzuführen.

- Projektablaufplan
- Zeitplan
- Dokumentation der Systemkonfiguration und der abgebildeten Prozesse

4.2.3 Inbetriebnahme

In Zusammenarbeit mit dem Bereich 1 – Informationsmanagement und der IAM-Abteilung wird durch den AN die IAM-Software auf dafür bereitgestellten virtuellen Servern installiert und so konfiguriert, dass dann mit der Umsetzung der Anwendungsfälle begonnen werden kann.

4.2.3.1 Verantwortung AN

Der AN muss in der Lage sein, die folgenden grundsätzlichen im Rahmen dieses Projektes anzubietenden und zu realisierenden Leistungen zu erbringen:

- Anforderungsaufnahme und Aufbau einer IAM-Strategie
    - Prüfung der vorhandenen Unterlagen
    - IST-Zustand aufnehmen
    - Anforderungskatalog definieren
    - IAM-Strategie entwickeln mit kurz- und langfristigen Zielen
    - Empfehlung ausarbeiten
- Projektleitung und Unterstützung bei Erstellung Rollen & Rechte-Konzept
    - beinhaltet u. a.:
        - Durchführung von Rollenworkshops für einheitliches Verständnis
        - Analyse der Unternehmensstruktur, der bereits aufgenommenen Daten, der Berechtigungen und Anwendungen und
        - Aufbau eines Rollenkonzeptes im Rahmen des IAM-Kontextes
- Unterstützung bei Prozesseanalyse und Aufbereitung, z. Bsp. durch:
    - Durchführung eines Prozess-Workshops für einheitliches Verständnis
    - Analyse und Modellierung der aktuellen Prozesse (Onboarding, Change, Offboarding, "Notabmeldung/Notfallsperre")
    - Entwicklung und Modellierung der Soll-Prozesse (Onboarding, Change, Offboarding, Notfallsperre, Rezertifizierung)
- Installations-/Inbetriebnahmedienstleistungen und techn. Konfiguration aller notwendigen Komponenten der IAM Software. Diese beinhalten auch:
    - Bereitstellung der notwendigen Informationen für:
        - Konfiguration der Server-, Storage- und Betriebssystemkomponenten
        - Einbindung in Backup
        - Einbindung in das System Monitoring

- kundenindividuelle Konfiguration/Feintuning inkl. Workshop (“training on the job”)
- Unterstützung bei der Anbindung der aufgeführten Quell- und Zielsysteme (s. Anlage „Liste-der-IT-Systeme-IAM“)
- Tuning, Anlaufunterstützung, begleitete Testphase, Anpassungen, Troubleshooting
- Erstellung der Dokumentation
- Reaktion auf Fehlermeldungen / Anfragen innerhalb von 4 Stunden während der Bürozeiten des AG
- Der AN stellt eine telefonische Hotline und ein Ticketsystem bzw. Portal zur Fehlermeldung zur Verfügung
- Unabhängig vom Herstellersupport ist der AN verpflichtet, den AG bei auftretenden Problemen und Fragen zum gelieferten Softwaresystem bzw. den damit verbundenen Komponenten in gebotener Zeit fachlich qualifiziert zu unterstützen.

4.2.3.2 Dienstleistungsaufwand

Bitte geben Sie unter Pkt. 5.3 die Stunden- bzw. Tagessätze für die Dienstleistungen an, die sich mind. aus den in 4.2.3.1 geforderten Leistungen ergeben.

Die nachfolgend **abgefragten Preise beinhalten alle Neben- und Reisekosten sowie -zeiten**; sie gelten für normale Servicezeiten Mo-Fr. 8:00-17:00 mit Ausnahme gesetzlicher Feiertage in Sachsen. Werden Zuschläge für Arbeiten außerhalb dieser Zeiten fällig, so sind diese explizit anzugeben!

Die Dienstleistungsstunden sind monatlich nachträglich in Rechnung zu stellen.

Die kleinste Abrechnungseinheit ist eine viertel Stunde („0,25h“).

4.2.3.3 Verantwortung AG

- Bereitstellung und Konfiguration der Server-, Storage- und Betriebssystemkomponenten
- Bereitstellung Ansprechpartner
- Bereitstellung Systemzugänge
- Einbindung der IAM Software in:
    - Backupsystem
    - System Monitoring

4.2.4 Aufbau

Der Aufbau und Sizing der Umgebung ist durch den AN anzugeben.

4.2.5 Schulung

Das anzuschaffende IAM-System wird eigenständig durch das KC betrieben. Notwendige Schulungen für die IAM-Administratoren sind als Präsenzschulungen und in virtueller Form anzubieten.
Schulungsunterlagen sind in digitaler Form bereitzustellen.
Durch den Anbieter ist anzugeben, welchen initialen Schulungsaufwand er für sein IAM-System für notwendig erachtet. Sind jährliche Schulungen notwendig, so ist dies auszuweisen.

Es sind die Kosten pro Schulungstag á 8 h einschließlich Schulungsmaterial anzugeben.

Schulung/Einweisungen vor Ort (bis 10 Teilnehmer in den Räumen des AG)	……€/Tag
Schulungen virtuell (pro Teilnehmer)	……€/Tag

4.3 Unterstützung bei Umsetzung der Anwendungsfälle

Die unter 3.2 beschriebenen Anwendungsfälle werden in verschiedenen Phasen in Betrieb genommen. Die Inbetriebnahme der Anwendungsfälle erfolgt zusammen mit dem AN. Der AG liefert die Prozessinformationen, die Konfiguration des Systems für den konkreten Anwendungsfall erfolgt durch den AN.
Im Preisblatt sind nur die in den folgenden Phasen aufgeführten Prozesse bzw. Anwendungsfälle aufzunehmen. Nicht hier in den Phasen aufgeführte Prozesse, bzw. Anwendungsfälle werden zu einem späteren Zeitpunkt umgesetzt.

4.3.1 Phase I - Identity LifeCycle, automatische Provisionierung von Windows-Benutzerkonten, Passwort-Reset

Phase I umfasst, neben dem Anbinden der Systeme SAP HCM, MS Exchange und Active Directory, das Abbilden folgender Prozesse:

- Onboarding interne Mitarbeiter (siehe auch 3.2.1)
- Onboarding externe Mitarbeiter (sieh auch 3.2.4)
- Offboarding Mitarbeiter (siehe auch 3.2.3)
- Änderung Mitarbeiter (siehe 3.2.2)
- Notfallsperre (siehe 3.2.9)
- Self-Service Passwort zurücksetzen (siehe auch 3.2.7)

On- und Offboarding veranlassen das IAM-System, ein persönliches Konto im Active Directory zu erzeugen bzw. zu deaktivieren. Das beim Erzeugen gesetzte Kennwort muss dem Mitarbeiter in geeigneter Form zugänglich gemacht werden. E-Mail-Benachrichtigungen informieren die Beteiligten der Prozesse über den jeweiligen Status.
Vom Anbieter ist darzustellen wie er Phase I in Zusammenarbeit mit der IAM-Abteilung plant umzusetzen und welchen Kosten dabei entstehen. Die Kosten sind zu unterscheiden in:

Lizenzkosten für das IAM-System um die in Phase I notwendigen Funktionen in Betrieb zu nehmen.
Dienstleistungskosten zur Unterstützung für die Inbetriebnahme dieser Phase I (Bezug auf Pkt. 4.2.3.2).

4.3.2 Phase II - Verwaltung von Mehrfach- und nicht personalisierten AD-Konten

In dieser Phase wird der Self-Service Prozess (siehe auch 3.2.5) zur Beantragung von nicht personalisierten und administrativen AD-Konten und die dazugehörige Verknüpfung mit Identitäten etabliert.

Vom Anbieter ist darzustellen, wie er Phase II in Zusammenarbeit mit der IAM-Abteilung plant umzusetzen und welchen Kosten dabei entstehen. Die Kosten sind zu unterscheiden in:

Lizenzkosten für das IAM-System um die in Phase II notwendigen Funktionen in Betrieb zu nehmen.
Dienstleistungskosten zur Unterstützung für die Inbetriebnahme dieser Phase II (Bezug auf Pkt. 4.2.3.2).

4.3.3 Phase III - Berechtigungsmanagement

Phase III umfasst die Berechtigungsverwaltung von AD-Gruppen:

- Self-Service Berechtigungsbeantragung mittels Genehmigungsworkflow (siehe 3.2.6.1)
- Self-Service Delegation (siehe 3.2.6.2)
- Self-Service Vertretung (siehe 3.2.6.3)

Das Beantragen von Berechtigungen erfolgt nur durch Auswahl von Berechtigungsobjekten, die zuvor im Zuge des Prozesses bei der Anbindung von Applikationen (3.2.12) erstellt wurden.

Vom Anbieter ist darzustellen, wie er Phase III in Zusammenarbeit mit der IAM-Abteilung plant umzusetzen und welchen Kosten dabei entstehen. Die Kosten sind zu unterscheiden in:

Lizenzkosten für das IAM-System um die in Phase III notwendigen Funktionen in Betrieb zu nehmen.
Dienstleistungskosten zur Unterstützung für die Inbetriebnahme dieser Phase III (Bezug auf Pkt. 4.2.3.2).

4.3.4 Phase IV - Verwalten von E-Mail-Verteilern und geteilten Postfächern in Exchange

In Phase IV wird die Verwaltung von E-Mail-Verteilern und geteilten Postfächern mithilfe des IAM-Systems implementiert (siehe 3.2.8).

Vom Anbieter ist zu darzustellen, wie er Phase IV in Zusammenarbeit mit der IAM-Abteilung plant umzusetzen und welchen Kosten dabei entstehen. Die Kosten sind zu unterscheiden in:

Lizenzkosten für das IAM-System um die in Phase IV notwendigen Funktionen in Betrieb zu nehmen.
Dienstleistungskosten zur Unterstützung für die Inbetriebnahme dieser Phase III (Bezug auf Pkt. 4.2.3.2).

4.3.5 Phase V - Anbindung von SAP i.s.h.med

Das IAM-System ist in der Lage, neue Accounts zu provisionieren, vorhandene Accounts zu deaktivieren und zu löschen. Weiterhin stellt das IAM-System eine Funktion bzw. einen Service bereit, der das Passwort im Zielsystem über eine Schnittstelle setzen kann. Für diesen Service kann ein ggf. mehrstufiger Genehmigungsprozess aktiviert werden.

Die Verwaltung von Berechtigungen steht aktuell nicht im Fokus des IAM-Systems. Eine Schnittstelle muss dies aber vorsehen und sich diesbezüglich erweitern lassen.

Vom Anbieter ist darzustellen, wie er diese Phase in Zusammenarbeit mit der IAM-Abteilung plant umzusetzen und welchen Kosten dabei entstehen. Die Kosten sind zu unterscheiden in:

Lizenzkosten für das IAM-System um die in dieser Phase notwendigen Funktionen in Betrieb zu nehmen.
Dienstleistungskosten zur Unterstützung für die Inbetriebnahme dieser Phase (Bezug auf Pkt. 4.2.3.2).

4.4 Betrieb des IAM-Systems

4.4.1 Allgemein

Für die Inbetriebnahme und den späteren Betrieb der IAM-Lösung wird eine Unterstützung durch den AN in folgender Form benötigt:

Einführung des IAM-Systems:

- Inbetriebnahme
- Unterstützung bei Umsetzung der Anwendungsfälle
- Qualifikation IAM-Mitarbeiter

Betrieb des IAM-Systems

- temporärer Systembetrieb/Aufrechterhaltung Betrieb
- 2nd Level
- Betriebsunterstützung

4.4.2 temporärer Systembetrieb

Im Falle des Ausfalls des IAM-Teams beim AG ist durch den AN sicherzustellen, dass für diesen Zeitraum eine Unterstützung für den Zeitraum 5x9 (08:00-17:00) zur Verfügung steht.

Aufgaben sind dann u.a.:

- tägliche Überprüfung der Funktionalität des IAM-Systems, dazu gehört u.A.:
    - Monitoring der IAM-Systemumgebung (z.B. Überprüfung der Logdateien)
    - Eigenständiges Eingreifen bei Fehlern im System oder fehlerhaft ablaufenden Prozessen
- Weiterführung der unter 4.2.3.1 begonnen Dokumentation

Es sind im Rahmen des temporären Systembetriebs keine Anpassungen von größeren, planbaren Änderungen (Changes) am System durchzuführen.
Bei **geplanten** Abwesenheiten wird der AN spätestens 14 Tage vorab durch die IAM-Mitarbeiter per E-Mail informiert.

Bei **ungeplanten** Abwesenheiten (z.B. Krankheit) wird der AN kurzfristig durch das KC informiert und muss in der Lage sein, am nächsten Werktag den Systembetrieb zu übernehmen bzw. zu monitoren.

Der AG favorisiert folgendes Preismodell: jährlicher Basispreis + Stundenabrechnung bei Einsatz

Durch den Anbieter ist ein praktikables Konzept zur Unterstützung vorzustellen.
Durch den Anbieter sind die jährlichen Kosten für den Basispreis darzulegen.

4.4.3 Betriebsunterstützung

Im Rahmen eines Abrufkontingentes sind folgende Leistungen zu erbringen:

- Unterstützung bei Upgrades oder Versionswechseln innerhalb des IAM-Systems
- Unterstützung bei der Entwicklung von Workflows
- Unterstützung bei der Anbindung von IT-Systemen
- Entwicklung neuer Schnittstellen zu IT-Systemen

Der AG kalkuliert den jährlichen Aufwand mit 15 PT. Durch den Anbieter sind die dafür anfallenden Kosten anzugeben. Für Aufwände, die über die 15 PT hinausgehen ist der Tagessatzpreis anzugeben.

4.4.4 Softwarewartungsvertrag

Beschreiben Sie Ihr Servicekonzept bezüglich der Produktweiterentwicklung. (Zeitintervall für Updates, Auslieferung der Updates, Differenzierung Update versus Upgrade, …)

<u>Anforderungen an Support:</u>

- Deutsch sprechender Support
- erreichbar mind. zu den im KC üblichen Arbeitszeiten Mo – Fr., 08:00 – 17:00 Uhr

Der Bieter/Auftragnehmer verpflichtet sich, folgende Programmstände* für die aufgeführte IAM-Software zu überlassen, sobald sie am Markt verfügbar sind:

Überlassung aller verfügbaren Programmstände*			**Zeitpunkt der Leistung**	
Patches*, Updates*	Up-grades*	Releases/ Versionen*	Auf Anforderung des Auftraggebers	Unverzüglich sobald verfügbar
X	X	X		X

Tabelle 3: Softwarewartung

Zur Behebung von Fehlern im IAM-System ist durch den AN ein 2nd Level Support bereitzustellen, der durch die IAM-Abteilung kontaktiert werden kann, siehe Pkt. 4.2.3.1 Verantwortung AN.

Der AN bietet ein sinnvolles, notwendiges und mehrstufiges SLA-Konzept an, was den Anforderungen eines KRITIS-Betreibers und einer Einrichtung des Gesundheitswesens entspricht.
Aus diesem Konzept gehen mind. Reaktions-, Interventions- und Lösungszeiten sowie Anforderungen an den AG hervor.
Zusätzlich sind die jährlichen Kosten dafür in der Preisübersicht (Pkt. 5) anzugeben.

4.4.5 Fernwartung

Die Verpflichtung des AN zur Nutzung der im KC eingesetzten Fernwartungslösung „DameWare“ ist Voraussetzung für die Zusammenarbeit. Dabei kann die Remote Einwahl über unser Citrix-Portal mit Genehmigungsprozess (Standard) bzw. per 24x7 über selbigen Weg mit Zwei-Faktor-Authentifizierung genutzt werden. Zugriffe werden beim AN protokolliert, der AG protokolliert diese ebenfalls und darf Zugriffe zusätzlich monitoren.

4.5 Zeitplan

Nach aktuellem Stand ergibt sich für die Planung, Inbetriebnahme des IAM-Systems und die Realisierung der unterschiedlichen Phasen zur Umsetzung der Anwendungsfälle folgender Zeitplan.

Nr.	Phase	Start	Monat/Jahr	Dauer
1	Konzeptionelle-/Vorbereitungsphase(hier 4.2.3.1)			
2	Inbetriebnahme (4.2.3)			
3	Schulung IAM-Administratoren (4.2.5)			
4	Umsetzung Phase I			
5	Umsetzung Phase II			
6	Umsetzung Phase III			
7	Umsetzung Phase IV			
8	Umsetzung Phase V			
9	Betrieb des IAM-Systems			

Tabelle 4: Zeitplan für Inbetriebnahme und Umsetzung der Anwendungsfälle nach aktuellem Stand

Bei Vergabe wird mit dem AN ein konkreter Zeitplan, unter Berücksichtigung von Urlaub, Verfügbarkeiten der KC internen Projektbeteiligten erarbeitet.

5 Preiszusammenstellung

Ich/Wir biete(n) die Ausführung der beschriebenen Leistungen zu den von mir/uns eingesetzten Preisen und mit allen den Preis betreffenden Angaben wie folgt an:

Pos.	Bezeichnung der Leistung/Teilleistung	Hersteller-Ref.-Nr.	Menge / Anzahl	Mengen-einheit	Einzelpreise in € je Pos. netto	Gesamtbetrag in € (für Gesamtstückzahl ohne Optionen, netto)
5.1	**Anzubietende Softwarelizenzierung (siehe Punkt 4.1 des Leistungsverzeichnisses)**					
5.1.1	Lizenzierung aller zur Realisierung des gemäß Leistungsverzeichnisses beschriebenen Soll-Zustandes erforderlichen Softwareprodukte, Komponenten & Drittprodukte bis zu 7.500 Identitäten (siehe hierzu insbesondere Punkt 4 gemäß Leistungsverzeichnis)	.....	.....	.....	.....	.....
5.1.2	Schnittstellenlizenz für SAP HCM (s. 3.1.2.1)	.....	.....	.....	.....	.....
5.1.3	Schnittstellenlizenz für SAP i.s.h.med (s. 3.1.2.2)	.....	.....	.....	.....	.....
5.1.4	Schnittstellenlizenz für Imprivata OneSign (s. 3.1.2.3)	.....	.....	.....	.....	.....
5.1.5	Schnittstellenlizenz für Active Directory und DFS (s. 3.1.2.4)	.....	.....	.....	.....	.....
5.1.6	Schnittstellenlizenz für MS – Exchange (s. 3.1.2.5)	.....	.....	.....	.....	.....
5.1.7	Schnittstelle für JustSocial (s. 3.1.2.6)	.....	.....	.....	.....	.....
5.1.8	Schnittstelle für Assetsystem DeskCenter / Drucksystem MyQ (s. 3.1.2.7)	.....	.....	.....	.....	.....
5.1.9	Schnittstelle für Atlassian Jira/Confluence (s. 3.1.2.8)	.....	.....	.....	.....	.....

Pos.	Bezeichnung der Leistung/Teilleistung	Hersteller-Ref.-Nr.	Menge / Anzahl	Mengen-einheit	Einzelpreise in € je Pos. netto	Gesamtbetrag in € (für Gesamtstückzahl ohne Optionen, netto)
5.1.10	Schnittstelle für Radiologiesystem RIS / PACS (s. 3.1.2.9)	.....	.....	.....	.....	.....
5.1.11	Schnittstelle für Laborinformationssystem LIS (s. 3.1.2.10)	.....	.....	.....	.....	.....
Zwischensumme gemäß 5.1						.....
5.2	**Anzubietende Softwarewartung-/pflegegebühren (4.4.4 des Leistungsverzeichnisses)**					
5.2.1	Wartungs-/Pflegegebühren für alle gemäß 5.1 angebotenen Lizenzen	.....	12	Monate	.....	.....
Zwischensumme gemäß 5.2						.....
5.3	**Anzubietende Dienstleistungen (siehe Punkt 4 des Leistungsverzeichnisses)** - inkl. aller Neben-, Reise- und Übernachtungskosten sowie Reisezeiten für normale Servicezeiten Mo-Fr. / 8:00-17:00 mit Ausnahme gesetzlicher Feiertage in Sachsen - Folgekosten sind Teil des Wertungskriteriums Gesamtkosten (Preis)					
5.3.1	Dienstleistungen (siehe hierzu insbesondere Punkt 4.2.3.2 gemäß Leistungsverzeichnis)	.....	200	Stunden	.....	.....
5.3.2	Insofern der Bieter für eine An- & Abfahrt eine einmalige Pauschale berechnet, kann diese hier angegeben werden. Diese Pauschale beinhaltet dann sämtliche Reise- & Nebenkosten.	.....	.....	Stück	.....	.....
5.3.2	Aus Sicht des Bieters für dieses Projekt typischerweise erforderlicher Schulungsaufwand Die Schulungsdienstleistungs-pauschale beinhaltet sämtliche Reise- & Nebenkosten (siehe 4.2.5).	.....	.....	Stück	.....	.....
Zwischensumme gemäß 5.3						.....

Pos.	Bezeichnung der Leistung/Teilleistung	Hersteller-Ref.-Nr.	Menge / Anzahl	Mengen-einheit	Einzelpreise in € je Pos. netto	Gesamtbetrag in € (für Gesamtstückzahl ohne Optionen, netto)
5.4	**Anzubietende Dienstleistungen „temporärer Systembetrieb“** **(siehe Punkt 4.4.2 des Leistungsverzeichnisses)** - inkl. aller Neben-, Reise- und Übernachtungskosten sowie Reisezeiten für normale Servicezeiten Mo-Fr. / 8:00-17:00 mit Ausnahme gesetzlicher Feiertage in Sachsen - Folgekosten sind Teil des Wertungskriteriums Gesamtkosten (Preis)					
5.4.1	Dienstleistungen (siehe hierzu insbesondere Punkt 4.4.2 gemäß Leistungsverzeichnis)	.....	12	Monate	.....	.....
Zwischensumme gemäß 5.4						**.....**
5.5	**Sonstige aus Sicht des Bieters zwingend zur Erreichung des Sollzustandes erforderliche Komponenten und Leistungen**					
5.5.1	.....	.....	.....	.....	.....	.....
5.5.2	.....	.....	.....	.....	.....	.....
5.5.3	.....	.....	.....	.....	.....	.....
5.5.4	.....	.....	.....	.....	.....	.....
Zwischensumme gemäß 5.5						**.....**
Gesamtpreisangebot netto über alle Unterpositionen der Pos. 5.1, 5.2, 5.3, 5.4 & 5.5 **!! ohne Optionen !!**						***** **.....**

*** Der Gesamtpreis ist in die dafür vorgesehene Zelle im Punkt 6.1 des Angebotsschreibens (KCLW-V02) zu übertragen!**

Pos.	Bezeichnung der Leistung/Teilleistung	Hersteller-Ref.-Nr.	Menge / Anzahl	Mengen-einheit	Einzelpreise in € je Pos. netto	Gesamtbetrag in € (für Gesamtstückzahl ohne Optionen, netto)
5.6	**Sonstiges - OPTIONAL - nicht in Gesamtpreis netto (s. u.) einzurechnen** Optionale Komponenten, Erweiterungsmodule, etc., die aus Sicht des Bieters nicht zwingend zur Erreichung des Sollzustandes erforderlich sind					
5.6.1	2-Faktor-Authentifizierung (2FA) für administrative Konten an anderen IT-Systemen (s. Pkt. 3.1.4.7)	.....	.....	.....	.....	.....
5.6.2	.....	.....	.....	.....	.....	.....
5.6.3	.....	.....	.....	.....	.....	.....
5.6.4	.....	.....	.....	.....	.....	.....
5.6.5	.....	.....	.....	.....	.....	.....
5.7	**Dienstleistungen - OPTIONAL - nicht in Gesamtpreis netto (s. u.) einzurechnen** Optionale durch den AG abrufbare Betriebsunterstützungs- & Supportdienstleistungen des AN zur Unterstützung bei u. a. der weiteren Inbetriebnahme, Implementierung und Konfiguration nach Abschluss der Dienstleistungen des initialen Einführungsprojektes gemäß 5.3 **(siehe Punkt 4.4.3 des Leistungsverzeichnisses)** - inkl. aller Neben-, Reise- und Übernachtungskosten sowie Reisezeiten für normale Servicezeiten Mo-Fr. / 8:00-17:00 mit Ausnahme gesetzlicher Feiertage in Sachsen - Folgekosten sind Teil des Wertungskriteriums Gesamtkosten (Preis)					
5.7.1 **optional**	Stundensatz für Dienstleistungen auf Abruf	.....	1	Stunde	.....	.....
5.7.2 **optional**	Tagessatz für Dienstleistungen auf Abruf	.....	1	Tag	.....	.....
Bemerkungen: Insofern der Bieter für eine An- & Abfahrt eine einmalige Pauschale berechnet, kann diese hier angegeben werden.			1	An- & Abfahrt	.....	.....

Die o.g. Preise verstehen sich zuzüglich der gesetzlich geltenden Mehrwertsteuer.

Um einen reibungslosen Ablauf der Verhandlung zur Angebotseröffnung zu ermöglichen, wurden im Angebotsschreiben Eintragungsfelder für die unmittelbar nach dem Einreichungstermin zu dokumentierenden Endbeträge und andere den Preis betreffende Angaben sowie für weitere Angaben zum Angebot zusammengefasst.