|  |
| --- |
|  |
| Technisches KonzeptIAM – Identity Access Management |
|  |
|  |
|  |

Änderungsverzeichnis

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Autor | Beschreibung\* |
| 2.0 | 29.05.2024 | Ronald Rieth | Aktualisierung |
| 2.1 | 02.08.2024 | Carsten Steinke | Anpassung für die IAM-Ausschreibung |
|  |  |  |  |

\*Erstellung, Änderung, Aktualisierung, Überprüfung erfolgt

Inhaltsverzeichnis

[1 Einleitung 7](#_Toc173506311)

[2 Geltungsbereich des technischen Konzeptes 7](#_Toc173506312)

[2.1 Überblick 7](#_Toc173506313)

[2.2 Ziel des Projektes / der Umsetzung 7](#_Toc173506314)

[3 AMEOS IT-Architektur 8](#_Toc173506315)

[3.1 AMEOS Infrastruktur 8](#_Toc173506316)

[3.2 AMEOS Applikationsarchitektur 10](#_Toc173506317)

[3.3 Technische Anforderungen an die Lösung 11](#_Toc173506318)

[4 Beschreibung der angebotenen Lösung 12](#_Toc173506319)

[4.1 Architektur (Pflicht) 12](#_Toc173506320)

[4.1.1 Schematische Darstellung der Architektur (Pflicht) 12](#_Toc173506321)

[4.2 Technische Voraussetzungen (Pflicht) 12](#_Toc173506322)

[4.3 Lizenzierung (Pflicht) 12](#_Toc173506323)

[4.4 Technische Restriktionen (Pflicht) 13](#_Toc173506324)

[4.5 Datenmigration 13](#_Toc173506325)

[5 Beteiligte Ansprechpersonen (Pflicht) 13](#_Toc173506326)

[6 Ausführungsvarianten 14](#_Toc173506327)

[6.1 Software as a Service 14](#_Toc173506328)

[6.1.1 Systemanforderungen 14](#_Toc173506329)

[6.1.2 Ausfallkonzept 14](#_Toc173506330)

[6.1.3 Backup/Wiederherstellung 15](#_Toc173506331)

[6.2 On-Premise (Pflicht) 15](#_Toc173506332)

[6.2.1 Systemanforderungen – Hardware (Pflicht) 15](#_Toc173506333)

[6.2.2 Systemanforderungen – Software (Pflicht) 15](#_Toc173506334)

[6.2.3 Ausfallkonzept (Pflicht) 15](#_Toc173506335)

[6.2.4 Updates der Applikation (Pflicht) 16](#_Toc173506336)

[6.2.5 Betrieb, Backup, Wiederherstellung (Pflicht) 16](#_Toc173506337)

[7 Client Systeme 16](#_Toc173506338)

[7.1 Installationsanleitung der Herstellersoftware 16](#_Toc173506339)

[7.2 Systemvoraussetzungen Clientsysteme – Hardware 16](#_Toc173506340)

[7.3 Systemvoraussetzungen Clientsystem – Software 17](#_Toc173506341)

[8 Schnittstellen (Pflicht) 17](#_Toc173506342)

[9 Kommunikation 17](#_Toc173506343)

[9.1 Externe- und/oder Standortanbindung 17](#_Toc173506344)

[9.2 Kommunikationswege 18](#_Toc173506345)

[9.3 Externe Zugänge 18](#_Toc173506346)

[9.3.1 VPN Zugänge für externe Mitarbeiter 18](#_Toc173506347)

[9.3.2 Datenaustausch mit externen Dienstleistern 18](#_Toc173506348)

[10 Erforderliche Berechtigungen 19](#_Toc173506349)

[10.1 Rechte innerhalb des Active Directorys 19](#_Toc173506350)

[10.2 Rechte auf Betriebssystem Ebene 19](#_Toc173506351)

[10.3 Rechte auf Applikationsebene 19](#_Toc173506352)

Abbildungsverzeichnis

[Abbildung 1: Das ist ein Beispiel für Beschriftungen 6](#_Toc82781363)

Tabellenverzeichnis

[Tabelle 1: Das ist eine Tabelle 6](#_Toc82781364)

# Einleitung

Das technische Konzept dient als Grundlage für eine technische Implementierung einer Softwarelösung im Rahmen eines Projektes und muss immer ausgefüllt und gepflegt werden. Es beschreibt vollständig eine Umsetzung auf einer rein technischen Ebene. Es dient der technischen Darstellung, Dokumentation und Detaillierung der Softwarelösung in Bezug auf die durch die AMEOS IT-Architektur vorgegebenen Rahmenbedingungen.

In kursive dargestellte Textpassagen dienen als Hilfestellung zur Ausfüllung des Konzeptes.

In Tabellen voreingetragene und grau hinterlegte Einträge sind als Beispielwerte zu betrachten. Sofern für die Softwarelösung konkrete Angaben erforderlich sind, sind diese in den Tabellen zu ergänzen.

Alle Angaben sind in diesem Dokument zu machen. Beigefügte Dokumente können bei der Prüfung nicht berücksichtigt werden. Alle Punkte **ab** 3.2. Architekturbeschreibung sind entsprechend zu kommentieren.

Mit **(Pflicht)** markierte Punkte sind zwingend auszufüllen.

# Geltungsbereich des technischen Konzeptes

Dieses Konzept dient der technischen Beschreibung von *[Name des Projektes/der Lösung]* zur Bewertung einer Implementierung in die AMOES IT-Architektur. Es ist als technische Anlage Bestandteil der Unterlagen zu Auschreibungsverfahren.

## Überblick

*Bitte beschreiben Sie kurz und abstrakt die wichtigsten technischen Aufgaben und den Zweck des Projektes/der Lösung.*

## Ziel des Projektes / der Umsetzung

*Bitte beschreiben Sie hier kurz unter Angabe der wichtigsten Rahmenbedingungen das Ziel des Projektes. Rahmenbedingungen wären zum Beispiel*

* *Umfang des Projektes: Einführung als AMEOS Gruppenlösung oder nur als Standortlösung*
* *On Premise oder SaaS Lösung*
* *Allgemeine Informationen oder Anforderungen*
* *…*

Geplanter Starttermin:

Geplanter Fertigstellungstermin:

# AMEOS IT-Architektur

Dieser Abschnitt gibt Ihnen einen Überblick über die aktuelle IT-Architektur und beschreibt damit den technischen Rahmen, in dem die Softwarelösung zu implementieren ist.

## AMEOS Infrastruktur



Software wird für die jeweiligen Standorte im zentralen Rechenzentrum der CANCOM GmbH bereitgestellt. Die CANCOM stellt hierzu der AMEOS Gruppe einen aktuellen VMWare Cluster und entsprechenden Storage zur Verfügung. Zum Betrieb stehen unterschiedliche SLA auf Betriebssystem-, Storage- wie Applikationsebene zur Verfügung. Applikationen werden über Citrix veröffentlicht. Die Nutzer greifen via Thin- oder Fat Clients direkt oder über einen Zwischenschritt, Terminalserverpool im zugehörigen IT Standort, auf die Applikationen zu.

Zur zentralen Userverwaltung wird Active Directory sowie Imprivata als Single Sign-On Lösung eingesetzt.

Die Active Directory Struktur beinhaltet sowohl Subdomain als auch Active Directory die mittels bidirektionalem oder One-Way – Trust angebunden sind..

Anbindungen von remote bereitgestellten Diensten (z.B. SaaS etc.) ist möglich, allerding unter Berücksichtigung folgender Kriterien:

* Anbindung via IPSec VPN, die Credentials müssen aktuellen Kriterien entsprechen
* Anbindung über eine dezidierte leased Line
* Kein unverschlüsselter Datentransfer über öffentliche oder fremd mitgenutzte Netze

Als Mailsystem setzen wir domainübergreifend auf MS Exchange in den Versionen 2010 – 2016. Die AMEOS Gruppe stellt folgende Formen der verschlüsselten Kommunikation via Mail bereit:

* Verschlüsselung über SeppMail Domainverschlüsselung
* Benutzerbasierte Verschlüsselung auf Basis X.509 Zertifikat

Für alle Standorte liegt der zentrale Internetoutbrake im Rechenzentrum der CANCOM.

Bitte berücksichtigen Sie, dass wir keine administrativen Rechte auf Betriebssystem- sowie Active Directory - Ebene dauerhaft vergeben können (Ausnahme zur Installation). Dies betrifft sowohl Windows als auch Linuxsysteme. Näheres zu den benötigten Accounts für Mitarbeiter und für die einzurichtenden Services bitte in Kapitel 9 ausführen.

Alle unsere Rechenzentren sind Virtualisiert auf Basis VMWare ESXi.

Als Betriebssysteme stehen zur Verfügung:

* Windows 10 ENT
* Microsoft Windows 2019 und 2022
* Linux Red Hat
* Linux Debian
* IOS ab Version 12.0

Als Active Directory Domain Controller stehen zur Verfügung

* ab Windows 2012R2

Als Terminalserver stehen zur Verfügung:

* Terminalserver auf Basis ab Windows 2019

Als Datenbanksysteme stehen zur Verfügung:

* MSSQL (ab 2016)
* MARIA DB/MySQL
* Postgres SQL
* Oracle (bitte Anfragen)

Folgende Clientsysteme sind in Benutzung

* Thin Clients (Igel)
* Fat Clients und Notebooks auf Basis Windows 10 Pro bzw. Windows 10 ENT

Folgende Remote Access Systeme stehen zur Verfügung

* VPN und Zugriff via RDP
* Teamviewer (begleitet) in der jeweils aktuellen Version

Abweichung von den zur Verfügung gestellten Systemen/Softwaren sollten im Vorfeld abgestimmt werden.

## AMEOS Applikationsarchitektur

Führendes System in den klinischen Kernprozessen ist SAP IS-H / i.s.h.med. Der notwendige Datenaustausch zwischen dem KIS und untergeordneten Subsystemen, wie LABOR, RIS usw., ist über Schnittstellen, die sowohl File-basiert als auch als Server-Client-Architektur implementiert sein können, umgesetzt. Als Kommunikationsserver steht ein zentral im RZ CANCOM gehosteter Cloverleaf-Server zur Verfügung.

Eine Präsentation von Daten aus einem Subsystem im führenden KIS ist über einen Fremdsystemaufruf umgesetzt. Dies kann ein webbasierter Aufruf über eine parametrisierte URL sein oder ein parametrisierter Aufruf des Clients des Subsystems, der im klinischen Arbeitsplatz des KIS zu implementieren ist.

Für den Datenaustausch sind standardisierte Schnittstellen erforderlich. Um ein hohes Maß an Interoperabilität zu erreichen, muss die Lösung international anerkannte technische, syntaktische und semantische Standards unterstützen. Im Konkreten werden hierbei als Standard die über die KBV definierten Medizinischen Informationsobjekte (MIO) bzw. das Interoperabilitätsverzeichnis der Gematik erwartet. Für einen Datenaustausch zwischen Softwaresystemen, zum Beispiel mit einem KIS, muss die Lösung die Standards HL7 v2 und FHIR unterstützen.

Als zentrales Data Warehouse wird SAP BW verwendet. Daten, die aus SAP ausgeleitet, in Subsystemen verarbeitet werden, müssen für Analyse- und Reportinganfragen an SAP übermittelt werden.

Der Zugang zur Telematik Infrastruktur (TI) wird durch den externen Dienstleister Akquinet GmbH als TI as a Service bereitgestellt. Eine Integration der Fachanwendungen der TI in unser KIS i.s.h.med erfolgt über die Plattform OmniConnect der Firma x-tension.

Eine proprietäre Datenhaltung ist ausgeschlossen. Damit folgen wir strikt dem Prinzip einer Trennung von Applikation und Datenhaltung. Der Datenaustausch zwischen den Primärsystemen (KIS, RIS, PACS…) erfolgt nicht direkt, sondern über eine IHE-basierte Interoperabilitätsplattform. Anwendungen zu weiteren klinischen Prozessen (TI, MD-Kommunikation, Patientenportal, …) sind an Interoperabilitätsplattform angebunden.

Die Lösung muss kompatibel zu unserer IHE Plattform (DMI – Archivar 4.0) sein.



Abbildung 1 Schematische Darstellung der Applikationsarchitektur

## Technische Anforderungen an die Lösung

* Im Fall, dass Daten in irgendeiner Form klinikbasiert entstehen und oder verarbeitet, vorgehalten werden etc. setzen wir eine Mandantenfähigkeit der Lösung voraus. Bitte nehmen Sie hierzu in der Architekturbeschreibung unter 4.1 Stellung
* Zur Implementierung neuer Systeme mit userbasierter Authentifizierung setzen wir eine multidomainfähige und gruppenfähige (ActiveDirectory, LDAP) Anbindung voraus. Alternativ ist eine Gewährleistung der Anmeldevorgänge via Imprivata möglich. Bitte nehmen Sie hierzu in der Architekturbeschreibung unter 4.1 Stellung
* Sollte als Bestandteil der Lösung Drucken oder die Verarbeitung von Druckaufträge eine Rolle spielen, setzen wir eine eigene Druckeransteuerung der Lösung voraus. Bitte nehmen Sie hierzu in der Architekturbeschreibung unter 4.1 Stellung.
* Erläutern Sie sowohl für SaaS als auch für OnPrem Lösungen ein Business Continuity Konzept unter den entsprechenden Punkten im Kapitel 6
* Bei betriebskritischen Applikationen ein Konzept zur Hochverfügbarkeit mit Active / Passive oder Active / Active Funktion für Applikation und Datenbank
* Die Lösung muss von den Primärsystemen entkoppelt/unabhängig sein.
* Schnittstellenkommunikation muss über FHIR, HL7, REST implementiert sein.
* Die Lösung muss kompatibel zu unserer IHE-basierten Interoperabilitätsplattform sein.

# Beschreibung der angebotenen Lösung

## Architektur (Pflicht)

*Eine kurze strukturierte Beschreibung der Systeme & Komponenten sowie ihrer Beziehungen zueinander.*

* *Alle technischen Komponenten, welche beteiligt sind*
* *Kommunikationswege und –Richtungen*
* *Kommunikationsarten (WLAN, LAN, Seriell)*
* *Bandbreitenbedarf und Anforderungen an Kommunikationswege*
* *physikalische Standorte der Komponenten*
* *Schnittstellen: FHIR, HL7, REST, ..*
* *Nachweisbare IHE Kompatibilität, Connectathon Zertfikat*
* *Technisches Schaubild (Applikations-Logik) inklusive Datenfluss und Darstellung der eventuell benötigten Schnittstellen*
* *Darstellung der Archivierung von Daten, sofern archivierungswürdige Daten anfallen unter Berücksichtigung der Anbindung an die DMI-Plattform*

### Schematische Darstellung der Architektur (Pflicht)

*Eine grafische Gesamtdarstellung als Anwendungsdiagramm mit allen beteiligten Systemen. Aus der Darstellung muss erkennbar sein, welche Schnittstellen und Daten von und zu welchen Anwendungen / Servern / Instanzen / Abteilungen führen*. *Hier ist eine prinzipielle schematische Darstellung gemeint, nicht eine in Bezug auf die konkrete Implementierung. Diese ist Bestandteil eines Betriebshandbuches.*

*Mit Hilfe solcher Diagramme können z.B. noch unberücksichtigte Voraussetzungen oder Risiken von Seiteneffekten aufgedeckt werden. Dabei sollte der Fokus nicht nur auf das eigene Projekt sondern auch auf alle anderen beteiligten, existierenden oder möglicherweise noch in Entwicklungsphasen befindlichen Systeme liegen.*

## Technische Voraussetzungen (Pflicht)

*Folgende Voraussetzungen müssen für die Umsetzung erfüllt sein. Unter einer Voraussetzung ist eine vom Hersteller aufgeführte Voraussetzung gemeint, die bereits gegeben sein muss, wie z.B. das zur Verfügung stellen einer bestimmten Datenbankinstanz, eine bestimmte Bandbreite und Latenzzeit zwischen zwei Komponenten, WLAN oder sonstige Infrastrukturelle Gegebenheiten(Temperatur usw.)*

*Die detaillierten Hardware-- und Softwarevoraussetzungen zur Lösung werden ja nach Art der angebotenen Lösung (on Premise oder SaaS) unter Punkt 5 erfasst und müssen hier nicht angegeben werden.*

## Lizenzierung (Pflicht)

Lizenzierung:

Notwendige Zusatzlizenzen:

## Technische Restriktionen (Pflicht)

*Folgende Restriktionen sind bei der Umsetzung bekannt und müssen berücksichtigt werden. Unter einer Restriktion ist z.B. eine Einschränkung des Herstellers zu verstehen, wie z.B. dass nur bestimmte Betriebssysteme unterstützt werden, der Server nicht virtualisiert werden kann, etc.*

## Datenmigration

*Sofern Daten aus einem bereits vorhandenen System in das neue System übernommen werden sollen, beschreiben Sie bitte hier ein Migrationskonzept. Geben Sie bitte dazu eine Abschätzung der Zeitschiene an*

# Beteiligte Ansprechpersonen (Pflicht)

Folgende externe Personen sind bei der Umsetzung des technischen Konzeptes beteiligt:

**Ansprechpartner Softwarehersteller**

Name:

Firma:

E-Mail:

Telefon:

Aufgabe:

**Ansprechpartner Dienstleister**

Name:

Firma:

E-Mail:

Telefon:

Aufgabe:

**Technischer Ansprechpartner Dienstleister**

Name:

Firma:

E-Mail:

Telefon:

Aufgabe:

**Ansprechpartner Applikationsverantwortlicher der AMEOS**

Name:

Firma:

E-Mail:

Telefon:

Aufgabe:

# Ausführungsvarianten

Die AMEOS Gruppe ist in der Lage Systeme und Dienste auf vielfältige Weise einzubinden und Zur Verfügung zu stellen. Sollte Ihre Lösung zum Beispiel als SaaS und als On-premise Lösungen angeboten werden und in der Ausschreibung nicht zwingend eine Variante als Anforderung deklariert sein, füllen Sie bitte entsprechend alle Unterpunkte aus. Sollten Leistungs- und Feature – Unterschiede bestehen, z.B. schnellere Updates, existierende Schnittstellen usw. so zeigen Sie diese hier auf:

## Software as a Service

### Systemanforderungen

Folgende technischen Voraussetzungen müssen gewährleistet sein:

* *Latenzen und Bandbreitenbedarf*
* *Art der Anbindung (leased Line, IPSec VPN)*
* *Schnittstellen*
* *Art des Zugriffs auf die Anwendung*
* *etc.*

Folgende Systeme werden für die Umsetzung benötigt, welche noch nicht vorhanden sind:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Beschreibung | OS | CPU | RAM | HDD | Patchlevel |
| *HBSRZ-AS-01* | *Beispiel* | *W2K12* | *2 vCPU* | *8 GB* | *50 GB OS100 GB APP* | [*4022726*](https://support.microsoft.com/de-de/help/4022726) |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Folgende Systeme werden für die Umsetzung benötigt, welche bereits vorhanden sind und ggf. geändert werden müssen:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Beschreibung | OS | CPU | RAM | HDD | Patchlevel |
| *HBSRZ-FS-02* | *Ablage Daten, Keine Änderung* |  |  |  |  |  |
| *HBSRZ-AS-01* | *Anpassung HDD APP und RAM* |  |  | *12 GB* | *+ 50GB APP* |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### Ausfallkonzept

Bitte beschreiben Sie ein Business Continuity Konzept bei Nicht-Erreichbarkeit des SaaS - Plattform:

### Backup/Wiederherstellung

Bitte beschreiben Sie kurz das Backup- und Restoreverfahren, insbesondere geben Sie bitte an, welche Wiederherstellungszeiten zu erwarten sind.

## On-Premise (Pflicht)

### Systemanforderungen – Hardware (Pflicht)

Beschreiben Sie hier bitte vollständig und detailliert die Hardwareanforderungen Ihrer Lösung unter Berücksichtigung, dass der Betrieb in einer zentralen, virtualisierten Umgebung stattfindet.

Folgende Systeme werden für die Umsetzung benötigt, welche noch nicht vorhanden sind:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Beschreibung | OS | CPU | RAM | HDD | Patchlevel |
| *HBSRZ-AS-01* | *Beispiel* | *W2K12* | *2 vCPU* | *8 GB* | *50 GB OS100 GB APP* | [*4022726*](https://support.microsoft.com/de-de/help/4022726) |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Folgende Systeme werden für die Umsetzung benötigt, welche bereits vorhanden sind und ggf. geändert werden müssen:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Beschreibung | OS | CPU | RAM | HDD | Patchlevel |
| *HBSRZ-FS-02* | *Ablage Daten, Keine Änderung* |  |  |  |  |  |
| *HBSRZ-AS-01* | *Anpassung HDD APP und RAM* |  |  | *12 GB* | *+ 50GB APP* |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### Systemanforderungen – Software (Pflicht)

Beschreiben Sie hier bitte vollständig und detailliert die Softwareanforderungen Ihrer Lösung.

Geben Sie bitte, sofern Abhängigkeiten zu third party Software oder Betriebssystem Patches bestehen, diese hier an.

|  |  |  |  |
| --- | --- | --- | --- |
| Name System | Software  | Version | Patchlevel |
| *HBSRZ-FS-02* | *.NET Framework* | *3.5* | *Service Pack 1* |
|  |  |  |  |
|  |  |  |  |

### Ausfallkonzept (Pflicht)

Bitte beschreiben Sie ein Business Continuity Konzept bei Nicht-Erreichbarkeit der zentralen – Plattform.

### Updates der Applikation (Pflicht)

Beschreiben Sie hier bitte das prinzipielle Verfahren zu Updates der Applikation.

* *Installation der Updates*
* *Updatezyklus – in welchen Intervallen werden Updates zur*

### Betrieb, Backup, Wiederherstellung (Pflicht)

Sofern es von den üblichen Betriebsverfahren abweichende Besonderheiten zum Betrieb der Lösung gibt, beschreiben Sie sie bitte kurz.

Beschreiben Sie bitte kurz die zum Einsatz kommenden Backup- und Wiederherstellungsverfahren. Sofern es keine geben sollte, geben Sie bitte eine Empfehlung unter Berücksichtigung des Betriebes in einer virtuellen Umgebung ab.

# Client Systeme

## Installationsanleitung der Herstellersoftware

* *ggfs. Paketierung beschreiben*
* *ggfs. Roll-Out beschreiben*
* *ggfs. Manuelle Installation beschreiben*

Software die auf Clientsystemen (FAT Clients oder Terminalserver etc.) bereitgestellt wird, muss als MSI Paket oder in einem entsprechendem Paket, welches sich automatisiert installieren lässt zur Verfügung gestellt

## Systemvoraussetzungen Clientsysteme – Hardware

Terminalserver:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| OS | CPU | RAM | HDD | Patchlevel |
| *W2K12* | *2 vCPU* | *8 GB* | *50 GB OS100 GB APP* | [*4022726*](https://support.microsoft.com/de-de/help/4022726) |
|  |  |  |  |  |
|  |  |  |  |  |

FAT Client:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| OS | CPU | RAM | HDD | Patchlevel |
| WIN 10 | 1 CPU | 8 GB | 50 GB OS100 GB APP | **KB4478877** |
|  |  |  |  |  |
|  |  |  |  |  |

Citrix Veröffentlichung:

Unterstützte Citrixversionen:

## Systemvoraussetzungen Clientsystem – Software

|  |  |  |
| --- | --- | --- |
| Software  | Version | Patchlevel |
| .NET | 3.5 | ServicePack 1 |
|  |  |  |
|  |  |  |

# Schnittstellen (Pflicht)

*Bitte alle erforderlichen Schnittstellen auflisten.*

Folgende Schnittstellen werden etabliert oder angepasst:

|  |  |
| --- | --- |
| Name |  |
| Quell-System |  |
| Ziel-System |  |
| Art der Schnittstelle (z.B. BAPI, File, etc.) |  |
| Übertragene Daten |  |
| Direkt oder Kommunikationsserver |  |
| Beschreibung der Schnittstelle |  |

# Kommunikation

## Externe- und/oder Standortanbindung

Zur Umsetzung des Konzeptes werden die folgenden standortübergreifenden Kommunikationswege (IPSEC/dedizierte Anbindung) benötigt

|  |  |  |  |
| --- | --- | --- | --- |
| Quelle | Ziel | Übertragungsweg(IPSEC, MPLS) | Benötigte Bandbreite |
| Standort | System | Standort | System |
| *RZ Auftraggeber* | *AsA Cluster* | *Rechenzentrum**Hamburg* | *Fortinet* | *IPSEC* | *2Mbit/s* |
|  |  |  |  |  |  |

Bitte berücksichtigen, im Rahmen des Projektes, muss das Antragsformular pro IPSEC/dedizierte Anbindung Verbindung separat ausgefüllt werden.

## Kommunikationswege

Zur Umsetzung des Konzeptes werden die folgenden Firewall Regeln für den internen und den ggfs. den Zugriff auf externe Systeme benötigt

|  |  |  |
| --- | --- | --- |
| Quelle | Ziel | Bemerkung |
| Name | IP-Adress/Netz | Name | IP-Adress/Netz | Port/Protokolle |
| *Clients* | *192.168.0.1/24* | *Applikationsserver* | *10.133.10.10* | *80,443* |  |
|  |  |  |  |  |  |

## Externe Zugänge

### VPN Zugänge für externe Mitarbeiter

AMEOS bietet hier zwei mögliche Optionen an:

* Mobile VPN (bevorzugter Client: Forti)
* Side2side VPN

Folgende VPN Zugänge werden für die Implementierungsphase benötigt:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Firma | Zielsystem | Protokoll | VPN |
|  |  |  |  |  |
|  |  |  |  |  |

Folgende VPN Zugänge werden für die Betriebsphase benötigt:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Firma | Zielsystem | Protokoll | VPN |
|  |  |  |  |  |
|  |  |  |  |  |

Der jeweilige Freigabeprozess pro Zugang muss separat eingehalten werden! Für die entsprechenden VPN Anträge müssen auch entsprechende Anträge zur Firewallfreischaltung getätigt werden.

### Datenaustausch mit externen Dienstleistern

Folgende Daten werden mit dem externen Dienstleister ausgetauscht bzw. dem externen Dienstleister zur Verfügung gestellt (via VPN, FTP, SFTP, …)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Firma | Quellsystem | Art der Daten | Dateneigentümer | Begründung |
|  |  |  |  |  |
|  |  |  |  |  |

Der jeweilige Freigabeprozess pro Zugang muss separat eingehalten werden! Für die entsprechenden VPN Anträge müssen auch entsprechende Anträge zur Firewallfreischaltung getätigt werden.

# Erforderliche Berechtigungen

Bitte berücksichtigen Sie, dass keine administrativen Rechte dauerhaft vergeben werden. Bei der Beschreibung der Rechte berücksichtigen Sie bitte Rechte auf Dienste, den Taskplaner und NTFS wenn diese erforderlich sind.

## Rechte innerhalb des Active Directorys

Folgende Rechte werden innerhalb des Active Directorys global benötigt:

|  |  |
| --- | --- |
| Benutzer |  |
| Benötigte Rechte |  |

|  |  |
| --- | --- |
| Serviceaccount |  |
| Benötigte Rechte |  |

## Rechte auf Betriebssystem Ebene

Folgende Rechte werden für einzelne System & Service Accounts auf den jeweiligen Server benötigt (Bitte pro Server angeben).

|  |  |
| --- | --- |
| Benutzer |  |
| Benötigte Rechte |  |
| Auf folgendes System |  |

## Rechte auf Applikationsebene

Folgende Berechtigungen werden auf Applikationsebene benötigt:

|  |  |
| --- | --- |
| Benutzer |  |
| Benötigte Rechte |  |
| Auf folgendes System |  |