Lastverteilung und Performance beim Einsatz von KIM 1.0

In dem nachfolgenden Text werden Lösungen für den Einsatz von KIM 1.0 in Krankenhäusern unter den Aspekten der Lastverteilung und der Performance betrachtet.

Zunächst werden für das grundsätzliche Verständnis die Kommunikationswege von KIM 1.0 betrachtet: Beispielsweise wird hier die Möglichkeit aufgezeigt, das unterschiedliche Konnektoren für die VZD- und die Fachdienstzugriffe sowie für die Kryptographie verwendet werden können.

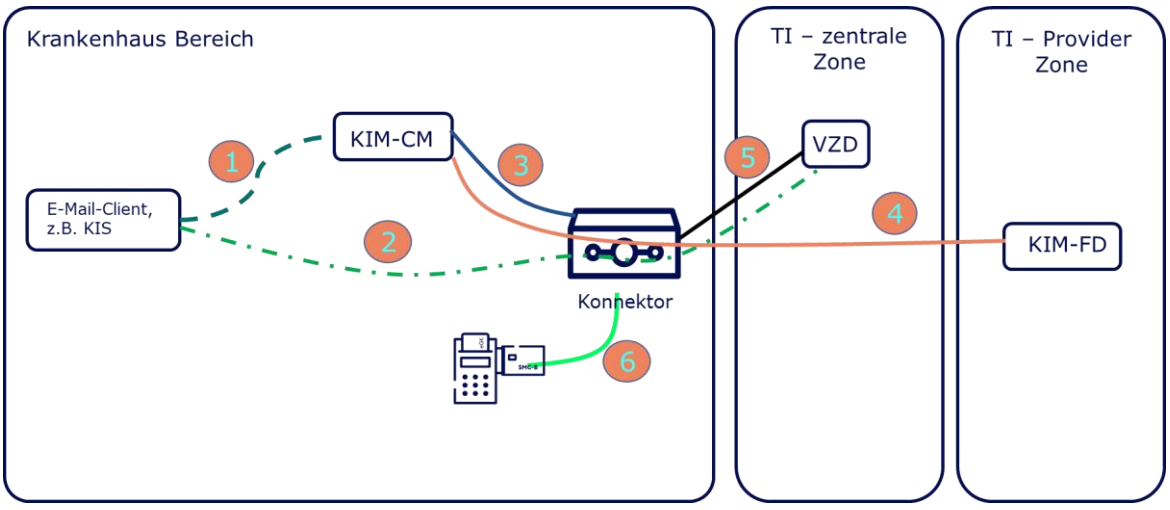
Im nächsten Kapitel wird der Zusammenhang zwischen einem EMail-Konto, den EMail-Adressen und den SMC-Ben dargestellt. Das Kapitel soll eine Hilfe für Krankenhäuser sein, eine Dimensionierung für die Anzahl der einzusetzenden SMC-Ben und Emailkonten zu ermitteln.

In den beiden nachfolgenden Kapiteln werden zum einen Performanceengpässe in Abhängigkeit der eingesetzten Komponenten erläutert. Zweitens werden Leitlinien zur Verminderung von Komplexität im Gesamtaufbau aufgezeigt.

Im letzten Kapitel sind die Deployments für Hot- und Cold-Standby dargestellt. Die Verfügbarkeit kann für KIM 1.0 durch Cold- oder Hot-Standby erhöht werden. Grundlage ist das Verständnis der im ersten Kapitel vorgestellten Kommunikationswege von KIM 1.0.

Kommunikationswege in KIM 1.0 anhand der verschiedenen Anwendungsfälle (Use Cases, UC)

Im nachfolgenden werden die in der Skizze dargestellten Kommunikationswege von KIM 1.0 anhand der Use Cases beschrieben.



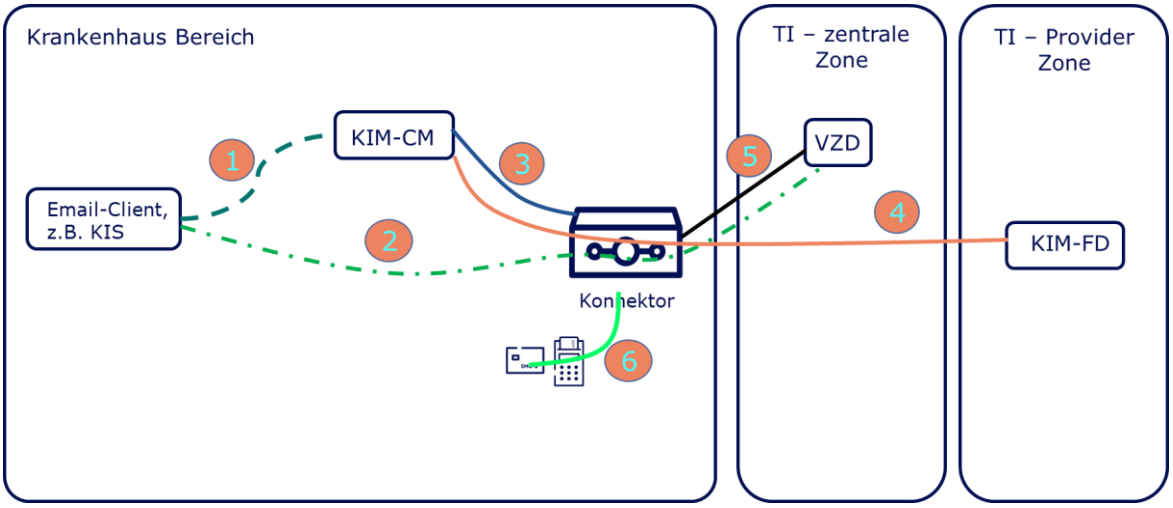


Abbildung 1: Verbindungen bei KIM 1.0

UC: KIM-FD auf neue Nachrichten prüfen (POP3)

Für die Abfrage neuer Nachrichten am KIM-Fachdienst (KIM-FD) KIM-FD initiiert das Krankenhaus-Informationssystem (KIS) die POP3-Verbindung zum KIM-Client-Modul (KIM-CM) KIM-CM (1). Hierbei wird der KIM-spezifische Aufrufkontext (siehe Kap. 3.3.2.2 Verbindungsaufbau mit MTA in gemSpec_CM_KOMLE) des Konnektors im Benutzernamen mitgesendet. Das KIM-CM baut über den Konnektor mittels Routing die POP3-Verbindung zum KIM-FD auf (4). Beim Verbindungsaufbau prüft das KIM-CM die Zertifikate des KIM-FD via Konnektor(3). Bei aufgebauter Verbindung geht die POP3-Antwort zurück an das KIS und die weitere POP3-Kommunikation zum Abfragen neuer Nachrichten kann erfolgen. Am Ende der E-Mail-Kommunikation wird die Verbindung abgebaut. Die Verbindung bleibt die komplette Dauer zwischen KIS, KIM-CM und KIM-FD geöffnet.

Beteiligte Komponenten:

- KIS
- KIM-CM (als POP3-Proxy)
- Konnektor (Signatur und Routing)
- KIM-FD

Abhängigkeiten in der Kommunikation

- KIS sendet im Benutzernamen den KIM-Aufrufkontext zum KIM-CM.
- Routing zwischen KIM-CM via Konnektor zum KIM-FD kann über beliebigen bzw. beliebige Konnektoren erfolgen.
- Das KIM-CM besitzt einen fest hinterlegten Konnektor (nur ein Konnektor kann pro KIM-CM in KIM 1.0 konfiguriert werden).

UC: KIM-Nachrichten am KIM-FD abrufen (POP3)

Das Abrufen einer auf dem KIM-FD befindlichen KIM-E-Mail erfolgt im Nachgang zum Anwendungsfall„KIM-FD auf neue Nachrichten prüfen (POP3)“. Hierbei initiiert das KIS über das Protokoll POP3 den Abruf der Nachricht am KIM-CM (1). Der Aufrufkontext für den Konnektor wird im Benutzernamen mitgesendet. Das KIM-CM ruft die Nachricht am KIM-FD ab (4) und speichert diese temporär zwischen, um sie zu entschlüsseln und anschliessend auf Integrität zu prüfen.

KIM-Nachricht entschlüsseln

Nach Laden der KIM-Nachricht in den KIM-CM wir sie vom KIM-CM zur Entschlüsselung an den Konnektor gesendet (3). Der Konnektor nutzt hierbei die zu dem KIM-Konto zugehörige SMC-B (6) indem er das entsprechende Kartenterminal anfragt, in welchem die SMC-B gesteckt ist. Die entschlüsselte Nachricht wird vom Konnektor an das KIM-CM zurückgesendet (3) und anschließend auf Integrität durch Signaturprüfung geprüft zu werden. Die POP3-Verbindung bleibt hierbei vollständig zwischen KIS und KIM-FD über das KIM-CM geöffnet.

Integrität der KIM-Nachricht prüfen

Das KIM-CM prüft die Integrität einer KIM-Nachrichtdurch Aufruf der Signaturprüfung am Konnektor (3). Der Konnektor prüft den Zertifikatsstatus des Signaturzertifikats durch Abfrage eines OCSP-Responders der TI. In diesem Schritt wird auch der Absender durch Abfrage des VZD vom KIM-CM verifiziert (3+5).

Beteiligte Komponenten:

- KIS
- KIM-CM (als POP3-Proxy)
- Konnektor (Signaturprüfung, Entschlüsselung und Routing für Kommunikation zum FD)
- KIM-FD
- VZD
- Kartenterminal
- SMC-B

Zusammenspiel der Komponenten untereinander

- Das KIS sendet im Benutzernamen den Aufrufkontext zum KIM-CM.
- Das KIM-CM nutzt den Aufrufkontext bei der Kommunikation mit dem Konnektor. In dem Aufrufkontext sind Informationen bzgl. des Users und Manadanten enthalten. Der aufgerufende Konnektor muss eine zum Aufkontext „passende“ Konfiguration haben.
- Das Routing zwischen dem KIM-CM und dem KIM-FD kann über einen beliebigen Konnektor erfolgen.
- Die LDAP-Kommunikation kann ebenfalls mit beliebigem Konnektor erfolgen.
- Das KIM-CM hat in KIM 1.0 nur einen Konnektor als Zugriff für die Kryptografischen Operationen konfiguriert (3).

UC: KIM-Empfänger-Adresse abfragen (LDAPv3)

Um eine Emfängeradresse zu ermitteln fragt das KIS den VZD via Konnektor mit Hilfe des LDAPv3-Protokolls ab. (2). Hierbei kommuniziert das KIS direkt mit dem Konnektor (nicht mit dem KIM-CM) und der Konnektor mit dem VZD. Der Konnektor prüft die Zertifikate des VZD auf Gültigkeit indem er den OCSP-Responder abfragt.

Beteiligte Komponenten:

- KIS
- Konnektor (als LDAP-Proxy)
- VZD

Abhängigkeiten in der Kommunikation

- Das KIS kann die Abfrage an einen beliebigen Konnektor senden
- Der Konnektor muss mit der TI verbunden sein

UC: KIM-Nachricht verschicken (SMTP)

Beim Versenden einer KIM-Nachricht öffnet das KIS die SMTP-Verbindung zum KIM-CM (1). Hierbei wird der Aufrufkontext des Konnektors im Benutzernamen mitgesendet. Das KIM-CM öffnet die Verbindung zum KIM-FD (4), authentisiert sich, prüft die Zertifikate mittels des Konnektors, und gibt den Verbindungsstatus an das KIS zurück. Danach sendet das KIS die KIM-Nachricht an das KIM-CM (1), welches die komplette Nachricht temporär zur Weiterverarbeitung zwischenspeichert.

KIM-Empfänger-Adressen prüfen und Zertifikate abrufen

Das KIM-CM entnimmt alle Empfänger der KIM-Nachricht und prüft über den Konnektor (LDAP-Proxy) mittels LDAPv3 (3)+(5) das Vorhandensein der EMail-Adressen. Danach ruft es zu allen EMail-Adressen sämtliche im VZD hinterlegten Zertifikate ab. Mit diesen wird die Nachricht, nachdem sie signiert wurde, verschlüsselt. (5).

KIM-Nachricht signieren

Zunächst wird die KIM-Nachricht signiert. Das KIM-CM sendet sie dazu zum Konnektor (3). Der Konnektor erstellt mit der eigenen SMC-B die Signatur (6) und gibt die signierte Nachricht an das KIM-CM zurück.

KIM-Nachricht verschlüsseln

Nach der Signatur sendet das KIM-CM die signierte Nachricht mit sämtlichen zuvor ermittelten Empfangerzertifikaten zur Verschlüsselung an den Konnektor. Der Konnektor erzeugt pro erhaltenes Zertifikat eine verschlüsselte Nachricht und gibt danach alle verschlüsselten Nachrichten an das KIM-CM zurück

Im Anschluss sendet das KIM-CM sämtliche verschlüsselten Nachrichten an den KIM-FD und schließt die Verbindungen zum KIM-FD und KIS.

Beteiligte Komponenten:

- KIS
- KIM-CM (als SMTP-Proxy)
- Konnektor (Signaturprüfung, Verschlüsselung und Routing für Kommunikation zum FD)
- KIM-FD
- VZD
- Kartenterminal
- SMC-B

Abhängigkeiten in der Kommunikation

- Das KIS sendet im Benutzernamen den Aufrufkontext zum KIM-CM.
- KIM-CM nutzt den erhaltenen Aufrufkontext für die Kommunikation mit Konnektor. Dadurch werden im Konnektor Mandant und Nutzer ausgewählt
- Für die kryptografischen Operationen müssen Kartenterminal und SMC-B-des Konnektors genutzt werden. Dazu kann nur der Konnektor genutzt werden, der im KIM-CM konfiguriert ist.
- Das Routing zwischen KIM-CM zum KIM-FD bzw. zum VZD (via LDAPv3) kann über einen beliebigen Konnektor erfolgen.

Übersicht der Abhängigkeiten zu einem EMail-Konto bei KIM 1.0

- Ein KIM-EMail-Konto ist mit genau einer Telematik-ID .verknüpft.
- Ein KIM-EMail-Konto kann bis zu 1000 EMail-Adressen enthalten.
- Eine SMC-B hat eine Telematik-ID, es kann aber mehrere SMC-Bs pro Telematik-ID geben. Damit stünden mehrere Zertifikate für ein KIM-EMail-Konto zur Verfügung und ein leistungssteigernder Parallelbetrieb wäre möglich.
- Ist eine SMC-B nicht freigeschaltet führt dies zu einem Problem beim Senden und Empfangen von KIM-Nachrichten im KIM-CM. Das KIM-CM meldet diesen Fehler dann an das KIS zurück.
- Ein KIM-CM kann nur einen Konnektor ansprechen
- Der Aufrufkontext, welcher vom KIS an das KIM-CM übermittelt wird, wird vom KIM-CM beim Aufruf des Konnektors verwendet um die „korrekte“ SMC-B des Konnektors auszuwählen.

Mögliche Performance-Engpässe und Lösungen

Nachfolgend sind mögliche leistungsbegrenzende Komponenten für KIM 1.0 benannt. Für jede dieser Komponenten ist ihr Einsatz und ihre leistungsbegrenzende Eigenschaft dargestellt:

1. SMC-B: wird zum Ver- und Entschlüsseln von Nachrichten verwendet und als Leistungsbegrenzend betrachtet werden. Der Paralleleinsatz von mehreren SMC-Ben mit gleicher Telematik-ID ist möglich.
2. Kartenterminal: Ob ein KT, in dem beispielweise 3 gleichzeitig genutzte SMC-Ben stecken, leistungsbegrenzend ist, kann hier nicht gesagt werden. Es hängt vom Produkt selbst ab. Abhilfe würde die Verteilung der SMC-Ben auf mehrere KT schaffen.

3. Konnektor (für Verschlüsselung und Entschlüsselung): Leistugsbegrenzend! Die Kryptographie ist die Performanceintensivste Operation auf dem Konnektor und hängt sehr stark von der Grösse der ausgetauschen Nachrichten ab.
4. Konnektor (für Routing in die TI und LDAP-Proxy): Unkritisch. Routing- und Proxy-Funktionalität benötigen wenig Leistung. Eine Paralleisierung von Konnektoren würde man wegen der Ausfallsicherheit, nicht aus Performancegründen, vornehmen
5. KIM-CM & KIS hängen in ihrer Leistungsfähigkeit von der eingesetzten Host-Hardware ab. Im Vergleich zum Konnektor benötigen sie eher wenig Performance. Um Ausfallsicherheit zu erreichen, könnten mehrere KIM-CMs eingesetzt werden (Zu den KIS macht die gematik keine Aussage).

Um Performanceengpässe möglichst zu vermeiden, sollte für bedacht werden,

- welche SMC-Bs (Telematik-IDs) werden für KIM 1.0 benötigt.
- Werden mehrere SMC-Ben mit gleicher Telematik-ID verwendet?
- Werden mehrere SMC-Ben in das gleiche KT gesteckt (bis zu 3)?
- Sind mehrere Konnektoren notwendig?
- Sindmehrere KIM-CM-Module notwendig?

Vermeidung von Komplexität und Performanceengpässen:

- So wenige unterschiedliche Telematik-IDs wie möglich und so viele wie nötig (bpsw. pro Krankenhaus nur die Krankenhaus-SMC-B nutzen und dort mehrere/alle notwendigen KIM-Adressen registrieren).
- So wenige KIM-Adressen wie möglich und so viele wie nötig (umso mehr KIM-Adressen registriert werden, umso aufwändiger werden mögliche Performance- und Verfügbarkeitslösungen).
- Eine eigene Infrastruktur (mind. eigene SMC-Bs und Kartenterminals, idealerwiese auch eigene Konnektoren) für die Fachanwendung KIM verwenden.
- Keine HBAs für KIM verwenden, da beim Senden und Empfangen immer der freigeschaltete HBA in einem für KIM konfigurierten Kartenterminal stecken muss.
- Das Routing zum KIM-Fachdienst der TI und die LDAP-Zugriffe zum VZDüber separate Konnektoren planen, da diese Kommunikationswege in der Leistungsbetrachtung sehr unterschiedlich zur Belastung durch die Kryptographie sind.
- Einfache Konnektor-Infomodelle planen und hierbei auch Redundanz-Konzept umsetzen.

Standby-Möglichkeiten: Hot oder Cold Standby

Um Verfügbarkeit und Performance für KIM 1.0 zu erreichen, könnten sowohl eine Cold-Standby- als auch eine Hot-Standby-Lösung eingesetzt werden. Beide Lösungen beeinflussen nicht die Nutzung des Aufrufkontexts der vom Arbeitsplatz bzw. KIS an das KIM-Clientmodul gesendet wird.

Anmerkung: *In den nachfolgendenAbbildungen sind jeweils auch Anti-Viren-Prüfungsmodule (AV) dargestellt. Sie zeigen lediglich die Position dieser AV-Prüfungseinrichtungen in Bezug auf das restliche KIM-Deployment an, spielen aber für die weitere Betracht keine Rolle.*

Cold Standby:

Die Arbeitsplätze (AP) werden auf die Konnektoren aufgeteilt, so dass jeder AP immer den gleichen Konnektor nutzt. Bei dieser Konfiguration wird die benötigte Performance statisch konfiguriert. Im Fall eines KIM-CM- bzw. Konnektor-Ausfalls muss das zweite KIM-CM/Konnektor-Paar aktiviert werden. Dies mussdurch eine schnell zu bewerkstelligende Umkonfiguration am KIS ermöglicht werden. Das KIS muss dies entsprechend zulassen.

Zu beachten: Fällt ein Konnektor KIM-CM aus, so weiß der AP-Nutzer sogleich, um welches KIM-CM-/Konnektor-Paar es sich handelt. Fällt dies an mehreren AP gleichzeitig auf, so bedarf es einer gewissen Abstimmung der Nutzer untereinander, sodass das Umschalten auf das Ersatz-KIM-CM-/Konnektorpaar abgestimmt erfolgt. Für die Cold-Standby-Lösung sind für jedes KIM-CM-/Konnektor-Paar ein Standby-Paar vorzusehen.

Hot Standby:

Hinweis: Der Hot-Standby schaltet zum nächsten KIM-CM-/Konnektor-Paar weiter. Im Fehlerfall auf Anwendungsebene weiß jedoch der AP-Nutzer nicht, welches KIM-CM-/Konnektor-Paar den Fehler verursacht hat. Dies könnte nur herausgefunden werden, wenn das KIS einen entsprechenden Aufruf unterstützt, der sich an ein konkretes KIM-CM-/Konnektorpaar richtet. im Falle einer gestörten SMC-B könnte dies beispielsweise „Geht-PIN-Status“ auf einen ausgewählten Konnektor sein.

Fazit:

Eine Entscheidung, eine Hot- oder Cold-Standby-Lösung einzusetzen, hängt von mehreren Faktoren ab:

- Kosten,
- Ausfallhäufigkeit von KIM-CM-/Konnektor-/SMC-B-Zusammenschaltungen,
- Fehlerprüfmöglichkeiten des KIS und der schnellen Umschaltmöglichkeit des KIS auf ein Ersatz-KIM-CM-/Konnektorpaar.

Deployment Hot Standby

Nachfolgend wird ein Vorschlag für die Anbindung der Anwendung KIM 1.0 skizziert, mit der Performance und Verfügbarkeit via Hot Standby erreicht werden können. Der Vorschlag beinhaltet neben der Beschreibung der allgemeingültigen Konfiguration eines entsprechenden Load Balancers auch die Beschreibung der notwendigen Konnektorkonfigurationen.

Lastverteilung und Ausfallsicherheit:

Die gematik empfiehlt eine kombinierte Lösung, um Performance und Ausfallsicherheit zu erreichen. Dazu wird ein Loadbalancer (LB) vor die KIM-CM geschaltet. Der LB nimmt über eine virtuelle Instanz alle Anfragen der AP an und verteilt diese auf die vorhandenen KIM-CM. Als Load-Balancing-Kriterium soll das Round-Robin-Verfahren zur Lastverteilung zum Einsatz kommen. Der Loadbalancer stellt über sein Monitoring auf Basis von ICMP- oder TCP-Requests sicher, dass die KIM-CM funktional sind. Dies kann beispielsweise durch einen PING auf die Anwendungs-„Ports“ (POP3 und SMTP) durchgeführt werden. Falls durch die Monitorfunktion im LB eine Fehlfunktion eines KIM-CM festgestellt wird, wird das

entsprechende KIM-CM aus dem Pool der möglichen Zielsysteme entfernt und erhält keine Anfragen mehr.

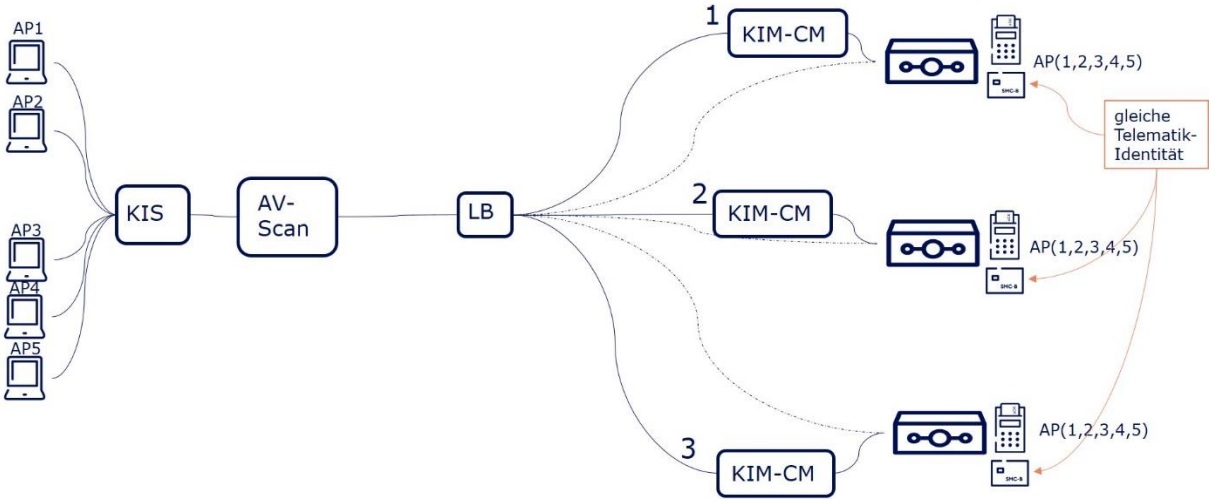


Abbildung 2: Einsatz eine Road Balancers (LB) zwischen KIS/E-Mail-Proxy und den KIM-CM

Erläuterung zur Abbildung:

Der LB befindet zwischen AV-Scan-Modul und den KIM-CM bzw. den Konnektoren (gestrichelt). Das Beispiel enthält 5 Arbeitsplätze (links), die jeweils auf jedem der Konnektoren eingerichtet sind. Auf den Konnektoren befinden sich diese Arbeitsplätze in jeweils einem Mandanten. Die Mandanten haben auf jedem Konnektor die gleiche ID. Außerdem befinden sich an jedem Mandanten angeschlossen eine SMC-B mit jeweils gleicher Telematik-Identität. Mit diesen Konnektorkonfiguration würden sich alle 3 Konnektoren hinsichtlich des Sendens/Empfangens identisch verhalten.

Performance/Verfügbarkeit für Senden/Empfangen von Nachrichten bei KIM 1.0

- Nach dem Round-Robin-Verfahren werden die KIM-CM abwechselnd verwendet. Das KIS stellt seine Anfrage zum Senden oder Empfangen via E-Mail-Proxy (der hier transparent ist und keine Rolle spielt) an die IP-Adresse des LB, der wiederum an eines der 3 KIM-CM weiterleitet. Ein KIM-CM wird dann ausgewählt, wenn es an der Reihe ist und aktiv. Als aktiv gilt es bei einem zuvor positiv durchgeführten PING.
- Sollte es der Funktionsumfang des LB zulassen, dass mehr als nur eine Komponente ge-PING-ed wird, könnte zusätzlich ein PING an den vom KIM-CM angesprochenen Konnektor durchgeführt werden. Dann wären beide Komponenten geprüft.

- Dadurch, dass alle Konnektoren gleich konfiguriert sind, sind sie auch alle in gleicher Art und Weise zum Senden und Empfangen bereit. Man hätte somit sowohl Performance (Round-Robin) als auch Verfügbarkeit (Active Health Check) hergestellt.

Performance/Verfügbarkeit für die LDAPv3-Abfrage des VZD durch den E-Mail-Client

Sollte ebenfalls nach dem Round-Robin-Verfahren abwechselnd über verschiedene Konnektoren durchgeführt werden. Allerdings steht hier eher die Verfügbarkeit im Vordergrund und nicht die Performance. Das KIS stellt seine Anfrage zum Senden oder Empfangen via E-Mail-Proxy, der hier transparent ist, an die IP-Adresse des LB, der wiederum an einen der 3 Konnektoren weiterleitet. Ein Konnektor wird dann ausgewählt, wenn er an der Reihe ist und aktiv. Als aktiv gilt er bei einem zuvor positiv durchgeführten PING.

Active Health Checks bei VZD und KIM-FD

Beide sind nicht direkt möglich.

- Der VZD ist nicht direkt erreichbar. Sein Ausfall würde beim Senden/Empfangen und LDAPv3-Anfragen über die jeweilige negative Quittung feststellbar sein. Falls der LB eine LDAP-Abfrage stellen kann, ist es möglich, den VZD über den Konnektor-LDAP-Proxy anzusprechen, da der Konnektor hier als echter Proxy fungiert und somit eine VZD-Antwort zurückkommen würde. Ein reiner Port-Check würde jedoch nicht funktionieren.

- Der KIM-FD kann via Konnektor nicht ge-PING-ed werden, da der Konnektor PINGs in Richtung offener Fachdienste blockt. Ein Port-Check über den Konnektor auf die FD-Ports würde aber funktionieren. Hierfür müsste der LB jedoch die Route über den oder die Konnektoren kennen.