Wesentliche Ergebnisse des Vorprojektes zur Entwicklung und Implementierung einer IT-Zielarchitektur für den ÖGD

1. Hintergrund

Im Verlauf der Pandemie hat sich deutlich gezeigt, dass eine Weiterentwicklung der durch den Bund bereitgestellten bzw. geförderten Bestandsysteme für den Infektionsschutz aufgrund technischer und infrastruktureller Herausforderungen nicht zielführend ist. Um die Digitalisierungspotenziale im ÖGD zu heben, bedarf es daher mittelfristig einer Reformierung des digitalen Infektionsschutzes. Diese Sichtweise wird vom RKI, den Ländern und kommunalen Spitzenverbänden, aber auch dem Beirat des Paktes für den ÖGD geteilt. Bereits in der Hochphase der Pandemie wurde hierzu durch das BMG und das RKI ein gemeinsames Konzept einer modularen IT-Zielarchitektur entwickelt, welches in der Folge weiterverfolgt und konkretisiert worden ist. Zur weiteren Konkretisierung dieser Überlegungen, wurde durch das Bundesministerium für Gesundheit ein Vorprojekt eingerichtet.

2. Zielstellung des Vorprojektes

Zielsetzung des Vorprojektes war es, Rahmenbedingungen für das eigentliche Entwicklungsprojekt zu schaffen und grundsätzliche Fragestellungen zu beantworten. Dazu zählt u. a., ein gemeinsames Verständnis über die funktionalen Erwartungen an die IT-Zielarchitektur zu gewinnen, die Anforderungen und Randbedingungen die sich für die Entwicklung der IT-Zielarchitektur ergeben frühzeitig zu erfassen und eine machbare, passgenaue technische Lösung (Architektur) der IT-Zielarchitektur zu skizzieren.

3. Wesentliche Ergebnisse des Vorprojektes

3.1. Primäre Ziele der IT-Zielarchitektur

Ausgehend vom IST-Zustand bzw. auf Basis der identifizierten Herausforderungen des aktuellen Meldewesens, wurden die **primären Ziele**, die mit der IT-Zielarchitektur adressiert werden sollen, abgeleitet.

Zu diesen zählen u. a., dass durch die neue IT-Zielarchitektur:

- ein medienbruchfreier Datenaustausch zwischen Gesundheitsämtern als auch externen Institutionen gewährleistet sein muss - ohne Informationsverluste zu riskieren,
- aufgrund der Standardisierung von Schnittstellen als auch der Daten(austausch)formate im Bedarfsfall auch bundesweit mit weiteren (neuen) Akteuren Daten ausgetauscht werden können,

- die Möglichkeit geschaffen werden soll, dass sich Drittanwendungen sicher an die IT-Zielarchitektur anbinden können, sodass weitere Synergien geschaffen werden können (z. B. durch die Nutzung von gemeinsamen Querschnittsdiensten; Prozessoptimierung etc.)[1]
- geänderte Anforderungen an das System, wie z. B. im Falle einer Pandemie, schnell umgesetzt und neue Funktionalitäten flexibel und unkompliziert bereitgestellt werden können,
- die Sachbearbeitung im Bereich des Infektionsschutzes in der Gesamtsicht prozessual vereinfacht und teilweise automatisiert wird und,
- den Gesundheitsämtern ein System mit moderner User Experience bereitgestellt wird, sodass komplizierte und unübersichtliche Bedienkonzepte und Programmoberflächen für den Bereich des Infektionsschutzes der Vergangenheit angehören.

3.2. Kernfunktionalitäten

Basierend auf zwischen RKI und dem BMG gemeinsam erarbeiteten SOLL-Geschäftsprozessen wurden die wesentlichsten Funktionalitäten der IT-Zielarchitektur abgeleitet und im weiteren weiter spezifiziert. Die wesentlichsten Funktionalitäten können Abbildung 1 entnommen werden.

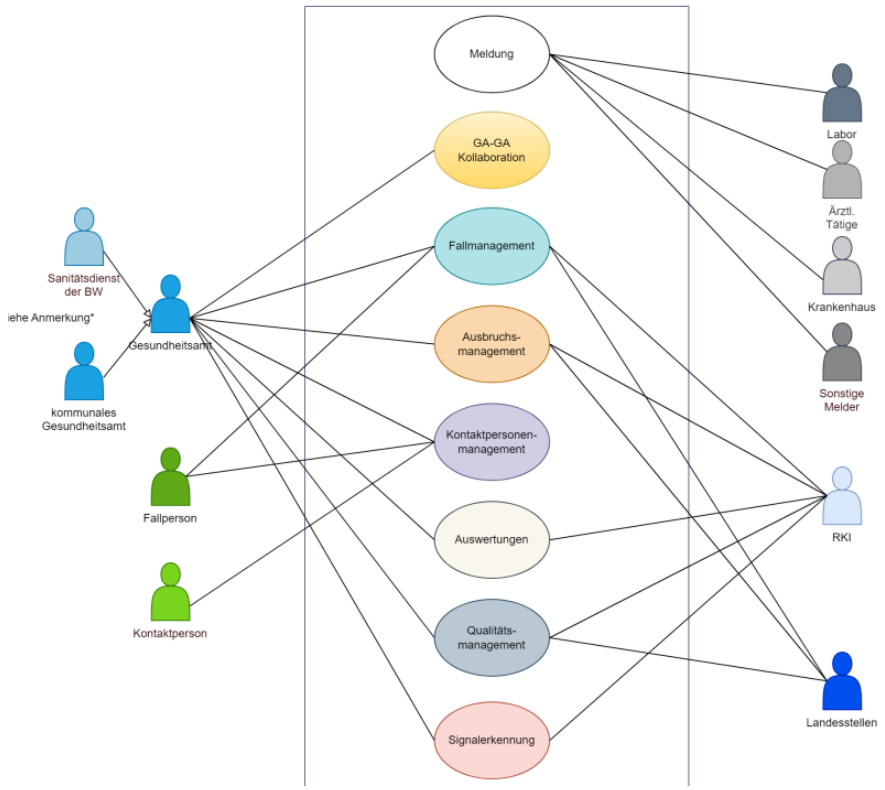
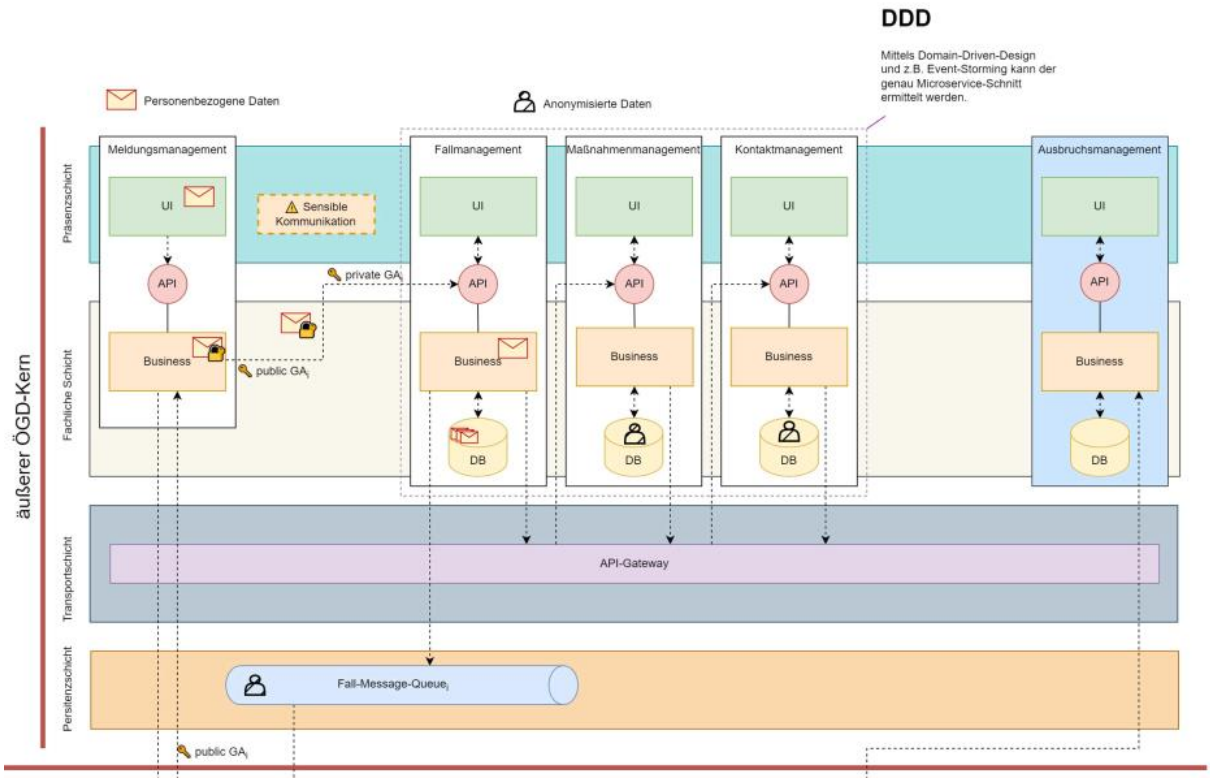


Abbildung 1: Kernfunktionalitäten

[1] Dies setzt voraus, dass die Drittanwendungen einerseits in der Lage sind, die beschriebenen Schnittstellen eigenständig einzubinden und andererseits, die zu definierenden Quality Gates für eine sichere Anbindung zu erfüllen.

3.3. Architekturansatz

Die IT-Zielarchitektur sollte den Empfehlungen des technischen Dienstleisters zu Folge als ein logischer, virtueller (d. h. verteilter) Kern aufgebaut werden, der aus zwei zu differenzierenden, inhaltlich jedoch zusammenhängenden Schichten besteht. Die Schichten unterscheiden sich insbesondere durch die in diesen gehaltenen Datensätze.
Als grundlegender **Architekturansatz** wird eine moderne **Microservice Architektur** empfohlen. Dieser Architekturansatz bedeutet im konkreten Falle der IT-Zielarchitektur, dass die einzelnen Funktionalitäten (z. B. das Kontaktpersonenmanagement oder das Ausbruchmanagement) als einzelne, voneinander unabhängige Dienste konzipiert werden. Das heißt, dass jeder einzelne Dienst (bzw. Microservice) für eine bestimmte fachliche Aufgabe oder Funktion verantwortlich ist. Dabei hält jeder Microservice eine eigene Datenbank, in der nur die Daten gespeichert werden, die für die Nutzung des konkreten Microservice benötigt werden (Konzept des „one-service-per-database“). Somit verfolgt dieser Ansatz eine Aufteilung einer großen (monolithischen) Anwendung in kleinere, voneinander unabhängige Dienste. Die Microservices kommunizieren miteinander mittels definierter Schnittstellen. So entsteht eine dezentrale, voneinander abgekoppelte Systemlandschaft, die eine granulare und flexible Skalierung als auch (Neu)Bereitstellung von Funktionalitäten ermöglicht.
Dem gegenüber steht der Aufbau einer zentralen ÖGD-Kerndatenbank, in der ausschließlich nicht-personenbezogene bzw. anonymisierte oder pseudonymisierte Daten gespeichert werden. Es ist somit durch den Aufbau der ÖGD-Kerndatenbank sichergestellt, dass auf die Gesamtheit der Daten in (anonymisierter oder pseudonymisierter Form) eine einheitliche Sicht besteht.



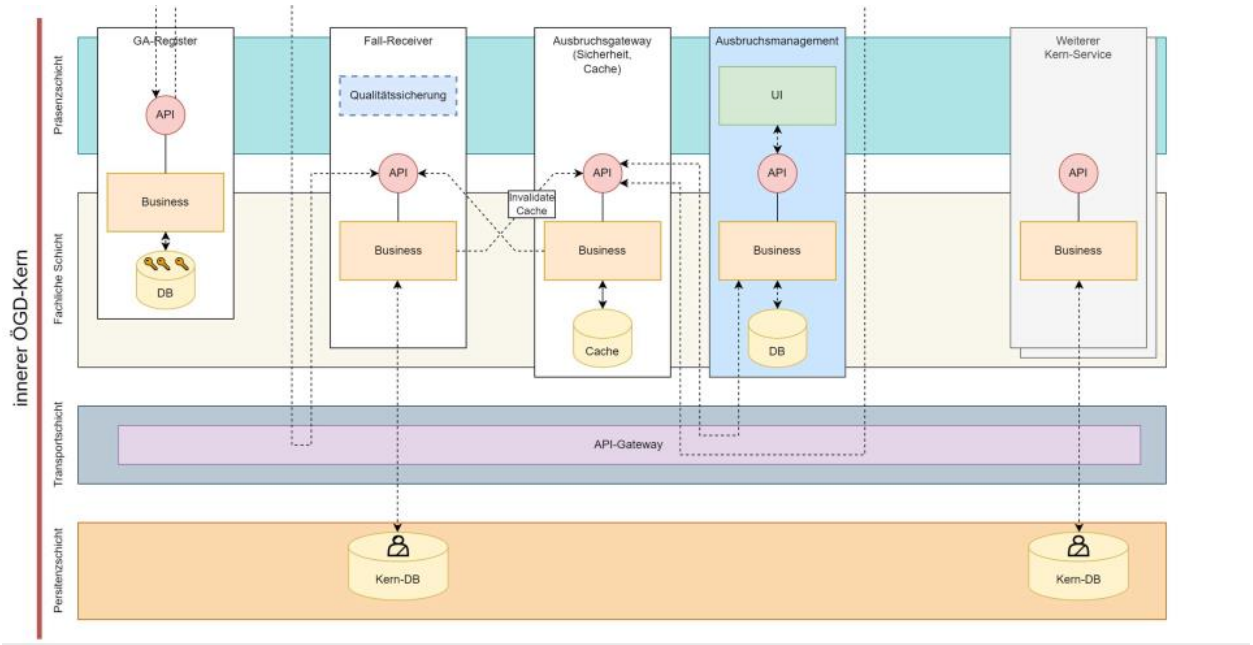


Abbildung 2: Architekturansatz

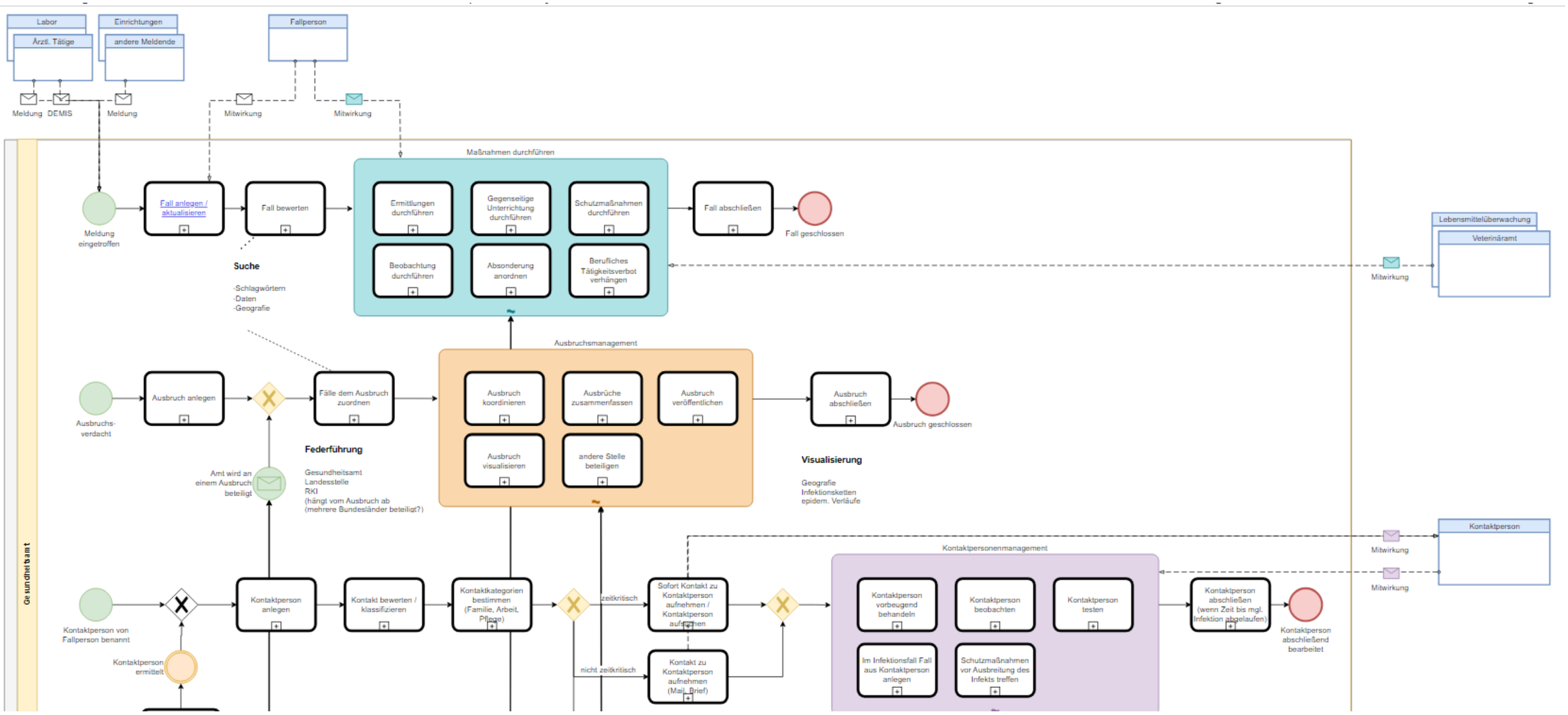
3.4. Mandantentrennung

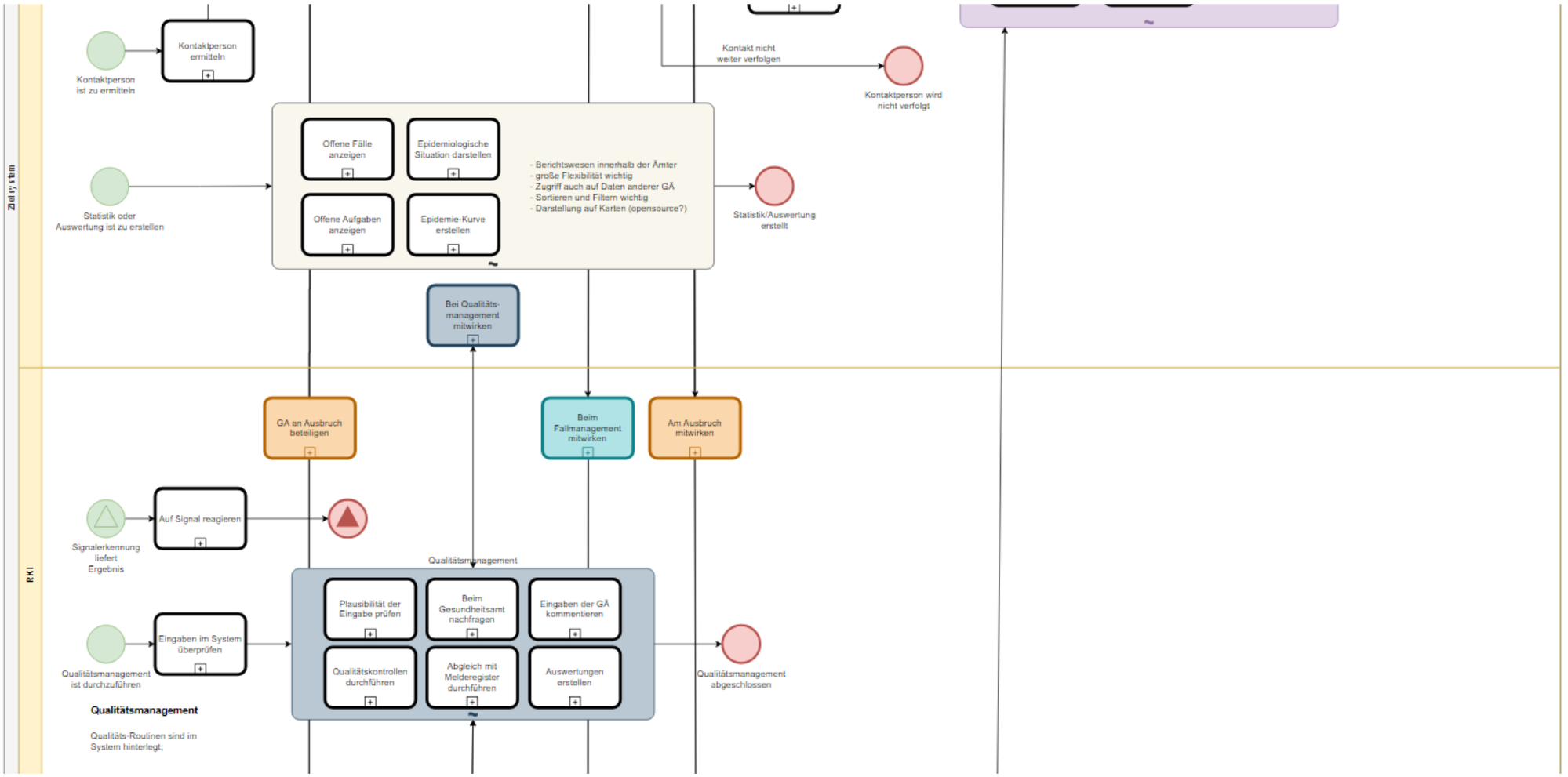
Die Ergebnisse sehen zudem eine Trennung auf Ebene der Umgebung vor. Dies bedeutet, dass jeder Mandant (hier das Gesundheitsamt bzw. RKI und Landesgesundheitsämter) seine eigene virtuelle Cloud-Instanz erhält; in dieser werden alle mandantenspezifischen Dienste betrieben, d. h. mit Blick auf die Gesundheitsämter ergeben sich insgesamt ca. 376 virtuelle Instanzen, in denen jeweils z. B. der Microservice zum Kontaktpersonenmanagement betrieben wird.

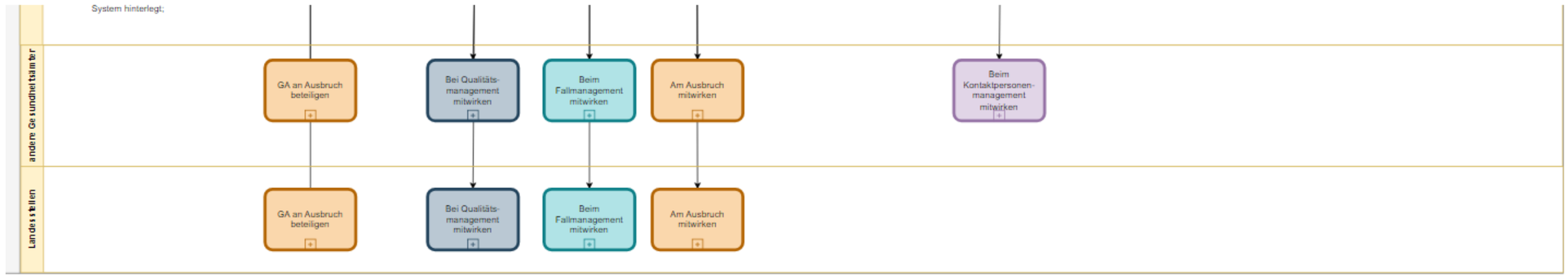
3.5. Zugriffsmöglichkeiten

Die IT-Zielarchitektur soll als Web-Anwendung für die Gesundheitsämter bereitstellt werden, wobei die eigentliche Datenhaltung bei einem IT-Dienstleister erfolgt, der prinzipiell in der Lage ist, Daten bis zur Stufe „Verschlusssache - Nur für den Dienstgebrauch“ zu verarbeiten. Eine Anbindung an die Netze des Bundes ist nicht erforderlich, da die Verschlüsselung der Daten bereits auf Anwendungsebene stattfindet und die Übermittlung der besonders schützenswerten Daten durch die Melde- und Benachrichtigungspflichtigen gemäß Infektionsschutzgesetz an die Gesundheitsämter auch in der IT-Zielarchitektur unverändert über das Deutsche Elektronische Melde- und Informationssystem für den Infektionsschutz (DEMIS) vorgesehen ist und DEMIS damit integraler Bestandteil der zukünftigen IT-Zielarchitektur sein wird.

3.6. Anhang: SOLL Geschäftsprozessmodellierung High-Level




Zielsystem
Kontaktperson ermitteln
Kontaktperson ist zu ermitteln
Kontakt nicht weiter verfolgen
Kontaktperson wird nicht verfolgt
Offene Fälle anzeigen
Epidemiologische Situation darstellen
Offene Aufgaben anzeigen
Epidemie-Kurve erstellen
- Berichtswesen innerhalb der Ämter
- große Flexibilität wichtig
- Zugriff auch auf Daten anderer GÄ
- Sortieren und Filtern wichtig
- Darstellung auf Karten (opensource?)
Statistik oder Auswertung ist zu erstellen
Statistik/Auswertung erstellt
Bei Qualitäts-management mitwirken
GA an Ausbruch beteiligen
Beim Fallmanagement mitwirken
Am Ausbruch mitwirken
RKI
Auf Signal reagieren
Signalerkennung liefert Ergebnis
Qualitätsmanagement
Plausibilität der Eingabe prüfen
Beim Gesundheitsamt nachfragen
Eingaben der GÄ kommentieren
Eingaben im System überprüfen
Qualitätsmanagement ist durchzuführen
Qualitätskontrollen durchführen
Abgleich mit Melderegister durchführen
Auswertungen erstellen
Qualitätsmanagement abgeschlossen
Qualitätsmanagement
Qualitäts-Routinen sind im System hinterlegt;


System hinterlegt;
anderen Gesundheitsämter
Landesstellen
GA an Ausbruch beteiligen
Bei Qualitäts-management mitwirken
Beim Fallmanagement mitwirken
Am Ausbruch mitwirken
Beim Kontaktpersonen-management mitwirken
GA an Ausbruch beteiligen
Bei Qualitäts-management mitwirken
Beim Fallmanagement mitwirken
Am Ausbruch mitwirken