Bericht der Arbeitsgruppe der Gesellschafterversammlung zur vorgezogenen Lösung für die Telematikinfrastruktur und einen stufenweisen Ausbau

Vorsitz:	Klaus Theo Schröder	
Mitglieder:	Dirk Schladweiler	BÄK
	Sven Tschoepe	BZÄK
	Gerd Bauer	DAV
	Jürgen Völlink	DKG
	Rainer Höfer	GKV-SV
	Christian Ummerle	GKV-SV
	Kerstin Tenbrock	KBV
	Irmgard Düster	KZBV

1. Auftrag

Die 36. Gesellschafterversammlung der gematik hat am 14.10.2011 den Auftrag erteilt, die Arbeit der Arbeitsgruppe (AG) fortzusetzen. Die AG wurde zur Prüfung einer vorgezogenen Lösung für die Telematikinfrastruktur und der Konkretisierung eines Stufenkonzeptes beauftragt und befasste sich in diesem Zusammenhang insbesondere mit den Fragen:

- effektive Governance,
- Fortentwicklung der laufenden Projekte,
- Teilnahmewettbewerb und Ausschreibebedingungen,
- Einführung einer qualifizierten elektronischen Signatur (QES).

Die AG wurde gebeten, bis Ende November einen Bericht vorzulegen der eine Entscheidungsgrundlage für einen gemeinsamen Beschluss aller Gesellschafter auf der 37. GSV, am 05.12.2011, darstellen sollte.

2. Vorgehensweise

Der Vorsitzende der AG hat ein Gutachten bei der EMDS AG, Stuttgart, in Auftrag gegeben das die Modalitäten und einen realistischen Zeitplan für die zeitnahe Implementierung der QES in das System möglichst in der 1. Stufe des Online-Rollouts“ geprüft hat.

Der Schwerpunkt des Gutachtens lag auf der Fragestellung, unter welchen technischen, zeitlichen und projektbezogenen Rahmenbedingungen eine QES in die Lösung sinnvoll implementiert werden kann, ohne die angestrebte Reduzierung der Komplexität zu gefährden.

Weiterhin wurde vom BMG, basierend auf dem Projektvorschlag „Alternative 2012“(Stand August 2011) gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und den Konnektorherstellern, ein Dokument verfasst, das sich mit der Erweiterung einer vorgezogenen Lösung um medizinische Anwendungen, die eine QES benötigen, befasst.

Die AG selbst hat in der Zeit vom 28. Oktober 2011 bis zum 22. November 2011 insgesamt fünf Sitzungen durchgeführt.

Die AG konstituierte sich am 06.09.2011 und führte gemäß des Auftrags aus der 36. GSV ihre Arbeit am 28. Oktober 2011 fort. Nach wie vor wurden dem GKV-Spitzenverband zwei Sitze in der AG zugestanden. Die übrigen Gesellschafter waren jeweils mit einem Teilnehmer vertreten.

Am 22. November 2011 hat die EMDS AG, Stuttgart, die wesentlichen Ergebnisse des von ihnen kurzfristig erstellten Gutachtens vorgestellt, das ausführlich besprochen wurde.

Außerdem wurde Herr Bonerz eingeladen, um das „Validierungsergebnis Szenario 3“ vorzustellen. Aus gesundheitlichen Gründen wurde Herr Bonerz von Herrn Bartkowiak vertreten.

Am 22.11.2011 hat die AG auch ihren Bericht abgestimmt und mit einem einvernehmlichen Ergebnis abgeschlossen.

3. Zusammenfassung der Ergebnisse

3.1 Voraussetzungen

Alle Gesellschafter unterstreichen noch einmal ihre Bereitschaft zur Beschleunigung der Arbeiten zur elektronischen Gesundheitskarte, der Telematikinfrastruktur und ihrer Anwendungen aktiv beizutragen.

3.2 Ergebnisse

Auf der Grundlage der „Beschreibung der vorgezogenen Lösung für die Telematikinfrastruktur als 1. Stufe des Online-Rollouts“ kann nach Auffassung der AG ein stufenweiser Ausbau der Anwendungen der elektronischen Gesundheitskarte und einer entsprechenden Infrastruktur erfolgen, wenn die entsprechenden Voraussetzungen geschaffen werden, wie sie in den Anlagen 1 bis 5 durch die AG erarbeitet worden sind.

Die 1. Stufe umfasst die beiden Teile VSDM mit korrespondierender Infrastruktur und QES. Die 1. Stufe wird in einem Verfahren ausgeschrieben und kann ggf. in 2 Phasen realisiert, getestet und für den Wirkbetrieb freigegeben werden. Dabei geht die AG davon aus, dass nach begründeten Aussagen z. B. der EMDS die 2. Phase QES ca. 10 Monate nach der 1. Phase realisiert werden kann.

Mit der Umsetzung des Konzeptes sollte umgehend begonnen werden.

Beschreibung der vorgezogenen Lösung für die Telematikinfrastruktur als 1. Stufe des Online-Rollouts

Vorliegende Fassung:
Stand November 2011

Inhaltsverzeichnis

Zusammenfassung

Das nachfolgende Dokument beschreibt die Kernpunkte des Konzeptpapiers zur vorgezogenen Lösung (Alternative 2012) des GKV-Spitzenverbandes. Um eine Beschlussfassung zu diesem Thema zu ermöglichen, wurde das Dokument wie folgt geändert:

- Entfernung der nachfolgenden Kapitel:
  - 1 Ausgangslage und Zielsetzung
  - 2 Unterstützung der „Alternative 2012“ durch das BMG
  - 6 Kosten der vorgezogenen Lösung
  - 7 Motivation der Leistungserbringer
  - 9 Umsetzungsorganisation
  - 10 Gesamtplanung
- Der Begriff „Alternative 2012“ wurde durchgängig durch „vorgezogene Lösung“ ersetzt
- Die Kapitelreferenzen wurden angepasst
- Aussagen (Ausblick) zum bundesweiten Ausschreibungsverfahren und Rollout sowie zum Zeitplan wurden gestrichen
- Der Begriff „Mini-Anwendungskonnektor“ wurde durch den Begriff Anwendungskonnektor „light“ ersetzt. Dies entspricht dem Funktionsumfang der Phase 1 der Stufe1 gemäß Ergebnis der Arbeitsgruppe

Mit diesem Anpassungen gibt das Dokument die Grundidee als Entscheidungsbasis wieder.

Das Dokument kann aber nur gemeinsam mit weiteren Dokumenten / Aussagen als Beschlussvorlage für die Umsetzung dienen. Hierfür sind die folgenden Themen zu behandeln:

- Umsetzungsorganisation / Governance
- Stufenkonzept für die Einführung der Anwendungen unter Berücksichtigung der heutigen gematik-Projekte
- Anforderungen an die Ausschreibung(en)
- Überarbeitung der Testteilnehmer / Anzahl der am Test teilnehmenden Primärsysteme
- Übergang vom Test- in den Wirkbetrieb
- Zeitplan gem. externer Gutachten (EMDS)

1 Leistungsumfang der vorgezogenen Lösung

1.1 Kurzbeschreibung der vorgezogenen Lösung

Die vorgezogene Lösung schafft eine sichere Vernetzung der beteiligten Akteure über eine einheitliche Infrastruktur. Diese Infrastruktur ermöglicht die komplette fachliche Umsetzung des Versichertenstammdatenmanagements analog der Ziellösung[1]. Darüber hinaus erlaubt die Infrastruktur die sichere Integration von Bestandsnetzen, wie z.B. KV-SafeNet mit sicherer Internetanbindung.

Die vorgezogene Lösung ist prinzipiell fachlich erweiterbar, soweit die sicherheitstechnischen Eigenschaften für neue Anwendungen ausreichend sind.

Grundlage für die Lösung ist der Basis-Rollout eGK und die dort ins Feld gebrachten Komponenten. Im Rahmen des Basis-Rollouts ersetzt die eGK die bisherige Krankenversichertenkarte und dient dem Nachweis der Berechtigung zur Inanspruchnahme von vertragsärztlichen oder -zahnärztlichen Leistungen (§ 15 SGB V). Sie enthält Angaben zum Mitgliedschaftsverhältnis des Versicherten und ergänzende Angaben, die der Leistungserbringer zur Abrechnung der medizinischen Leistungen benötigt.

Zum Auslesen der eGK werden im Basis-Rollout die Kartenterminals (eHealth-BCS) direkt an die Primärsysteme der Leistungserbringer angeschlossen. Es wird dabei keine Online-Funktionalität bereitgestellt. Die technischen Möglichkeiten der eGK können im Basis-Rollout noch nicht genutzt werden.

Die vorgezogene Lösung ermöglicht eine frühzeitige Nutzung des vollen sicherheitstechnischen Funktionsumfangs der eGK. Unter Verwendung der im Basis-Rollout bereitgestellten Komponenten erlaubt die vorgezogene Lösung die Verwendung der Online-Funktionen der Anwendung VSDM. Zur Verschlankung des Systems und zur schnellen und kompatiblen Einführung der vorgezogenen Lösung werden weitestgehend industrieerprobte Standards genutzt. Das Sicherheitsniveau der Lösung orientiert sich an den Erfordernissen der Anwendung VSDM. Aus diesem Grund können in der vorgezogenen Lösung anwendungsspezifische Anforderungen an die Verfügbarkeit der Prozesse und Technik und die Performance der Betriebsprozesse zu Grunde gelegt werden.

Eine klare Zielsetzung des Vorhabens ist die Migrationsfähigkeit in die spätere Ziellösung. Um dies zu gewährleisten, setzt die vorgezogene Lösung auf eine frühzeitige Installation und Bereitstellung einer TI-konformen Leistungserbringer-

[1] Unter „Ziellösung“ ist die Stufe 1 der Projekte zur Neuausrichtung der TI gemeint

Infrastruktur. Damit entsteht eine homogene und planbare Ausgangssituation bei den Leistungserbringern, die eine schnellere Migration in die Ziellösung ermöglicht.

Eine weitere Zielsetzung des Lösungsszenarios ist die Bereitstellung und Durchführung eines übergreifenden Supports mit größtmöglicher Ende-zu-Ende-Verantwortung.

1.1.1 Anwendungsüberblick VSDM

Die an der vertragsärztlichen Versorgung teilnehmenden Ärzte, Einrichtungen und Zahnärzte sind gesetzlich verpflichtet (§291 Abs. 2b SGB V), die vorgelegte eGK bei jeder erstmaligen Inanspruchnahme von Leistungen im Quartal auf Gültigkeit und Aktualität der Versichertendaten (online) zu prüfen. Die Onlineprüfung umfasst folgende drei Schritte:

1. Prüfung der Gültigkeit der eGK (Prüfung Authentifizierungs-Zertifikat)
2. Prüfung der Aktualität der Daten auf der eGK
3. Aktualisieren der Daten auf der eGK, sofern neuere Daten durch den Kostenträger bereitstehen

Sofern der Versuch zur Onlineprüfung fehlschlägt, muss dieser entsprechend der Zielsetzung des oben genannten Gesetzes wiederholt werden, sobald der Versicherte ein weiteres Mal in die Praxis des Leistungserbringers kommt.

Der Nachweis der durchgeführten Prüfung muss auf der eGK gespeichert werden (Prüfungsnachweis). Das gilt auch für den Fall, dass die Onlineprüfung nicht komplett und erfolgreich durchgeführt werden konnte. Das Praxisverwaltungssystem (PVS) muss neben den Daten des Versicherten auch den Prüfungsnachweis übernehmen und verarbeiten, um diesen später den Abrechnungsdaten nach §295 SGB V hinzufügen zu können. Dabei ist sicherzustellen, dass auch nur der Leistungserbringer, der den Prüfungsnachweis erstellt hat, diesen zur Weiterverarbeitung verwenden kann. Der Prüfungsnachweis kann zusätzlich zur Speicherung auf der eGK auch direkt dem PVS bereitgestellt werden.

Die vorgezogene Lösung ermöglicht die Überprüfung des Status des Authentifizierungszertifikats der eGK. Da die alleinige Sperrung des Authentifizierungs-Zertifikats keinen missbräuchlichen Einsatz der eGK in einem Offline-Szenario verhindern kann, kann zusätzlich eine Sperrung der Gesundheitsanwendung auf der eGK erfolgen. Die Sperrung und Entsperrung der Gesundheitsanwendung auf der eGK erfolgt über den Fachdienst CMS.

Krankenhäuser benötigen im stationären Bereich die Versichertenstammdaten für die elektronische Datenübertragung an die Krankenkassen nach §301 SGB V. Im Gegensatz zum vertragsärztlichen Versorgungsbereich besteht für den stationären Be-

reich keine gesetzliche Verpflichtung zur Onlineprüfung der Versichertenstammdaten auf der eGK. Die Krankenhäuser können aber ebenfalls die Dienste der Krankenkassen zur Onlineprüfung nutzen.

Der gesetzlichen Forderung, die Onlineprüfung durch Fachdienste der Kostenträger auch dann durchführen zu können, wenn das PVS nicht an das Netz der Telematikinfrastruktur angebunden ist, wird durch die Umsetzung eines sogenannten Standalone-Szenarios Rechnung getragen. Das Standalone-Szenario ist für die Umsetzung der gesetzlich geforderten Onlineprüfung und -aktualisierung der eGK im Rahmen der Anwendung VSDM konzipiert. Die Wahl des Standalone-Szenarios obliegt dem Leistungserbringer. Es besteht zwischen der genutzten IT-Infrastruktur des Standalone-Szenarios und dem PVS, welches am Praxisnetz angeschlossen ist, weder eine physische noch eine logische Verbindung. Die eGK muss daher nacheinander zunächst in das Kartenterminal des onlinefähigen Standalone-Szenarios gesteckt werden und anschließend in das Kartenterminal des Praxisnetzes. Die eGK dient bei Nutzung des Standalone-Szenarios als Transportmedium zur Übergabe des Prüfungsnachweises und der aktualisierten Versichertenstammdaten an das PVS.

Die vorgezogene Lösung stellt zur Abbildung des VSDM folgende Funktionen zur Verfügung:

- Onlineprüfung mit Lesen der VSD und ggf. Aktualisierung
- Onlineprüfung der VSD (Standalone-Szenario) und ggf. Aktualisierung
- Lesen der VSD
- Lesen der Versichertendaten von der KVK (sofern Versicherter noch nicht mit einer eGK ausgestattet ist)

Das Lesen der VSD von der KVK ist nur während der Übergangszeit, in der sowohl eGK als auch KVK parallel gültig sind, notwendig.

Die Initiierung der Anwendungsfälle erfolgt in der Regel durch einen Funktionsaufruf aus dem Primärsystem. Der Anwendungsfall „Onlineprüfung der VSD“ kann zudem automatisiert vom Fachmodul VSDM beim Stecken einer Karte in das Kartenterminal ausgeführt werden. Dies ist z.B. im Fall des Standalone-Szenarios notwendig.

1.1.2 Technische Infrastruktur

In der folgenden Abbildung wird das Lösungsszenario graphisch dargestellt und im Folgenden näher erläutert.

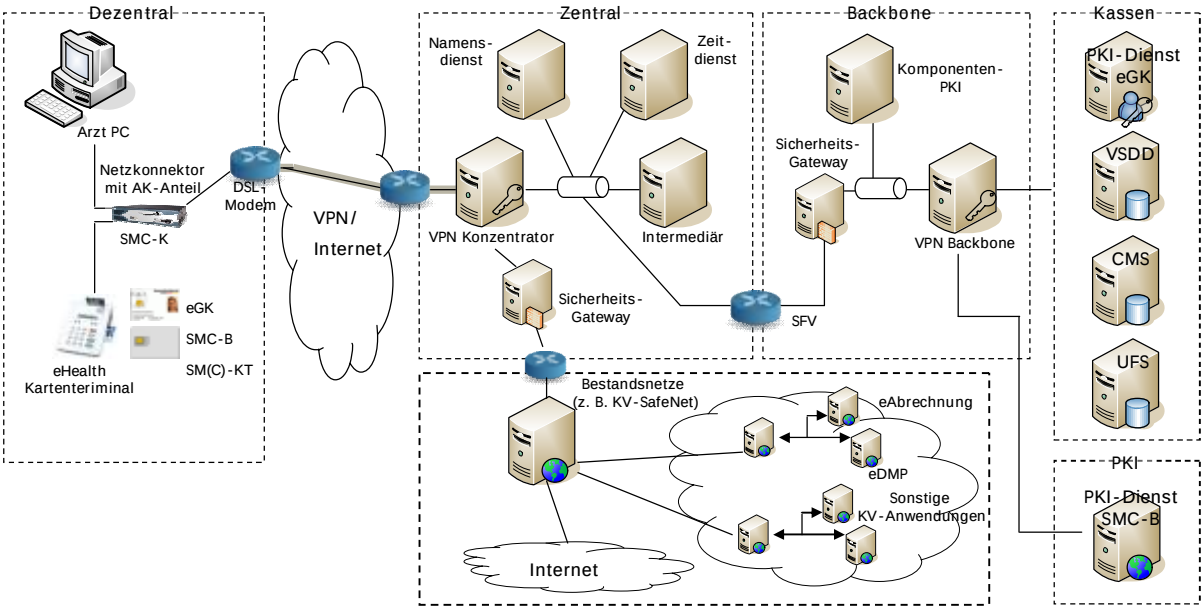


Abbildung 1: Technische Infrastruktur der vorgezogenen Lösung

Die Primärsysteme sind Anwendungsprogramme für Leistungserbringer. Sie umfassen im Umfeld der vorgezogenen Lösung die Praxisverwaltungssysteme (PVS) für Ärzte und Zahnärzte und die Krankenhausinformationssysteme (KIS) der Krankenhäuser. Sie werden für die Einführung der Lösung mit einer Schnittstelle zum Konnektor erweitert, die den Zugang zur Telematikinfrastruktur und die Nutzung der Chipkarten realisiert. Die Primärsystemhersteller müssen ihre Systeme so anpassen, dass die Geschäftsvorgänge in Praxen und ggf. Krankenhäusern optimal durch die vorgezogene Lösung unterstützt werden. Innerhalb der vorgezogenen Lösung findet die Installation und Konfiguration der dezentralen Komponenten statt. Das bedeutet, dass die Primärsysteme und eHealth-Kartenterminals (die per Update auf den SICCT-Standard gebracht wurden) per LAN an den zuvor installierten und konfigurierten Konnektor angebunden werden. Damit ist das Primärsystem mit der Telematikinfrastruktur vernetzt. Zur Onlineprüfung sowie für die Übernahme der Versichertendaten in das Primärsystem muss die eGK nur einmal gesteckt werden.

Die Primärsystemschnittstelle der vorgezogenen Lösung wird über Webservices umgesetzt, welche vom Fachmodul VSDM angeboten werden. Neben den Webservices des Fachmoduls VSDM benötigt das Primärsystem noch entsprechende Webservices zu Basisdiensten im Anwendungskonnektor.

Der Konnektor (Netzkonnektor mit Anwendungskonnektor „light“) als wichtige Sicherheitskomponente stellt den dezentralen Sicherheitsanker in der Telematik-

infrastruktur dar und gewährleistet, dass ein Lesen und Beschreiben einer eGK nur durch berechtigte Akteure in einer vertrauenswürdigen Umgebung durchgeführt werden kann. Sichergestellt wird dies durch eine rollenbasierte Berechtigungsprüfung, welche die gleichzeitige Anwesenheit einer eGK und einer Institutionskarte der Leistungsbringerinstitution (SMC-B) oder eines anderen berechtigten Akteurs (z.B. HBA) zwingend erfordert.

Wie in der folgenden Abbildung dargestellt ist, sind die Bestandteile des Konnektors ein Netzkonnektor und ein Anwendungskonnektor „light“.

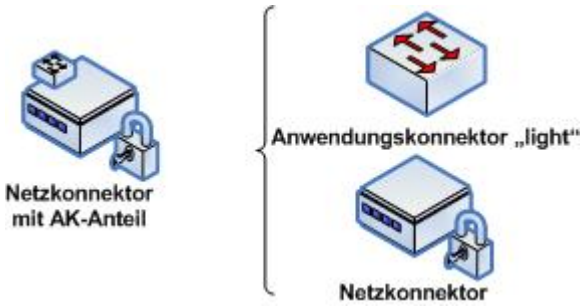


Abbildung 2: Funktionsaufteilung des Konnektors für die vorgezogene Lösung

Mittels des Konnektors wird der Zugriff der Primärsysteme zum Telematiknetzwerk gesteuert und die Zugriffe auf Kartenterminals durchgeführt. Der Konnektor besitzt Schnittstellen zu den Primärsystemen, zu den angebundenen Kartenterminals und über diese zu den Chipkarten sowie zum Telematiknetzwerk. Der Netzkonnektor stellt die Funktionen zur Einbindung des Konnektors in die Netzwerke der Leistungserbringer und der Telematikinfrastruktur zur Verfügung. Integriert ist eine funktionale Anwendungslogik (Anwendungskonnektor „light“) u.a. für die Gültigkeitsprüfung der Versichertenstammdaten (Fachmodul VSDM), die Verwaltung der Kartenterminals und eine Funktion, die ein sicheres Nachladen weiterer Anwendungslogiken ermöglicht.

„Vorgezogene Lösung“

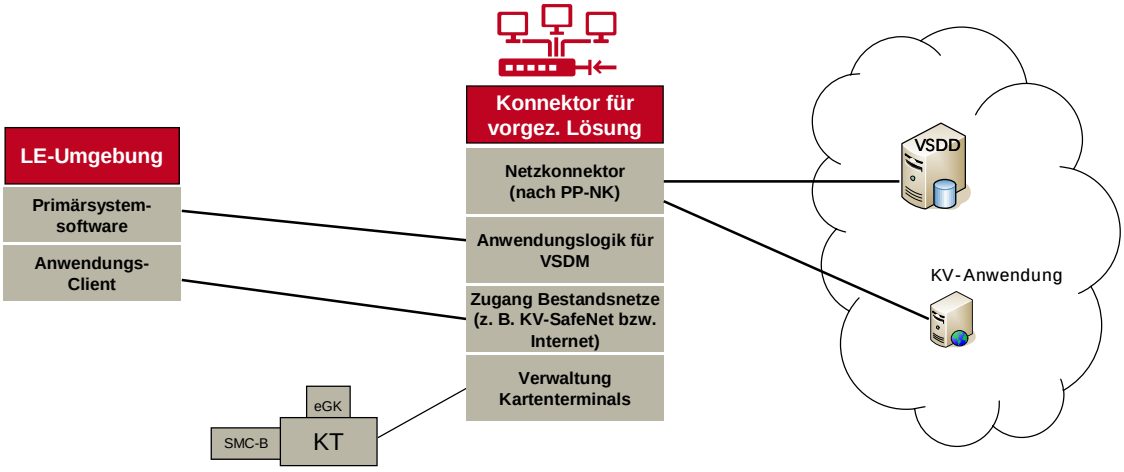


Abbildung 3: Schematische Darstellung der Konnektorschnittstellen

Die Schnittstelle des Konnektors zu den Primärsystemen bildet im Wesentlichen die fachlogischen Abläufe der Fachdienste ab. Sie kapselt die konkreten Abläufe zum Zugriff auf die karten- und serverbasierten Fachdienste und Datenobjekte gegenüber dem Primärsystem. Implementiert wird diese Schnittstelle über die Anbindung des Konnektors an das LAN der Leistungserbringer.

Über die Schnittstelle zu den Kartenterminals kann der Konnektor auf die Chipkarten im Gesundheitswesen zugreifen. Die Schnittstelle zum Telematiknetzwerk und zum Intermediär bietet dem Konnektor den Zugriff auf serverbasierte Fachdienste. Teil des Konnektors ist ein Virtual Private Network (VPN) –Client, der einen sicheren Kommunikationskanal über das letzte Stück des Transportnetzes zur Kommunikationsinfrastruktur aufbaut.

Für die vorgezogene Lösung werden verschiedene Chipkarten zur sicheren Authentifizierung der Akteure, zur Verschlüsselung von Daten (z.B. durch „Trusted Channel“) sowie zur elektronischen Signatur eingesetzt. Der Konnektor und das dezentrale Fachmodul der Anwendung VSDM kontrollieren den Datenfluss zwischen Kartenterminal, eGK und dem Primärsystem sowie die zur Aktualisierung der eGK notwendigen zentralen Dienste und die Fachdienste des Kostenträgers. Zu diesen kann, je nach Ausprägung der Fachdienste, auch der Zertifikats-Validierungsdienst gehören. Nach der Identifizierung und Authentifizierung des für die Aktualisierung der eGK zuständigen Fachdienstes erfolgt die Aktualisierung der eGK über einen gesicherten Transportweg („Trusted Channel“).

Einsatzfähigkeit im Krankenhaus

In der vorgezogenen Lösung muss bei der Architektur des Konnektors die Skalierbarkeit, wie es insbesondere für den Einsatz im Krankenhaus notwendig ist, gewährleistet sein. Für den Krankenhausbetrieb müssen zusätzliche Faktoren, wie

Load Balancing, 24x7-Verfügbarkeit, Failover-Betriebssicherheit und eine in der Regel sehr komplexe Netzwerk-Topologie berücksichtigt werden. Bei Einsatz im Krankenhaus kann die Funktionalität des Netzkonnektors und des Anwendungskonnektors „light“ als Konnektor – Cluster bzw. Mehrkomponentenkonnektor auf mehrere Instanzen verteilt werden. Die Mandantenfähigkeit des Konnektors muss gewährleistet sein. Eine skalierbare Lösung muss dementsprechend aus mindestens folgenden Komponenten bestehen:

- ein oder mehrere Anwendungskonnektoren “light“ und
- ein oder mehrere Netzkonnektoren.

Aus Gründen der Übersichtlichkeit sind in der folgenden Abbildung Komponenten für das Szenario Krankenhauskonnektor skizziert. Je nach Netzaufbau ist es denkbar, dass der Netzkonnektor beispielsweise in einer DMZ steht. Weitere mögliche Sicherheitszonen, wie z.B. eine DMZ der Anwendungskonnektoren, sind aus Gründen der Übersichtlichkeit ebenfalls nicht abgebildet. Bestehende Verbindungen des Krankenhauses aus der DMZ heraus sind von der Implementierung des Netzkonnektors nicht betroffen und bleiben bestehen.

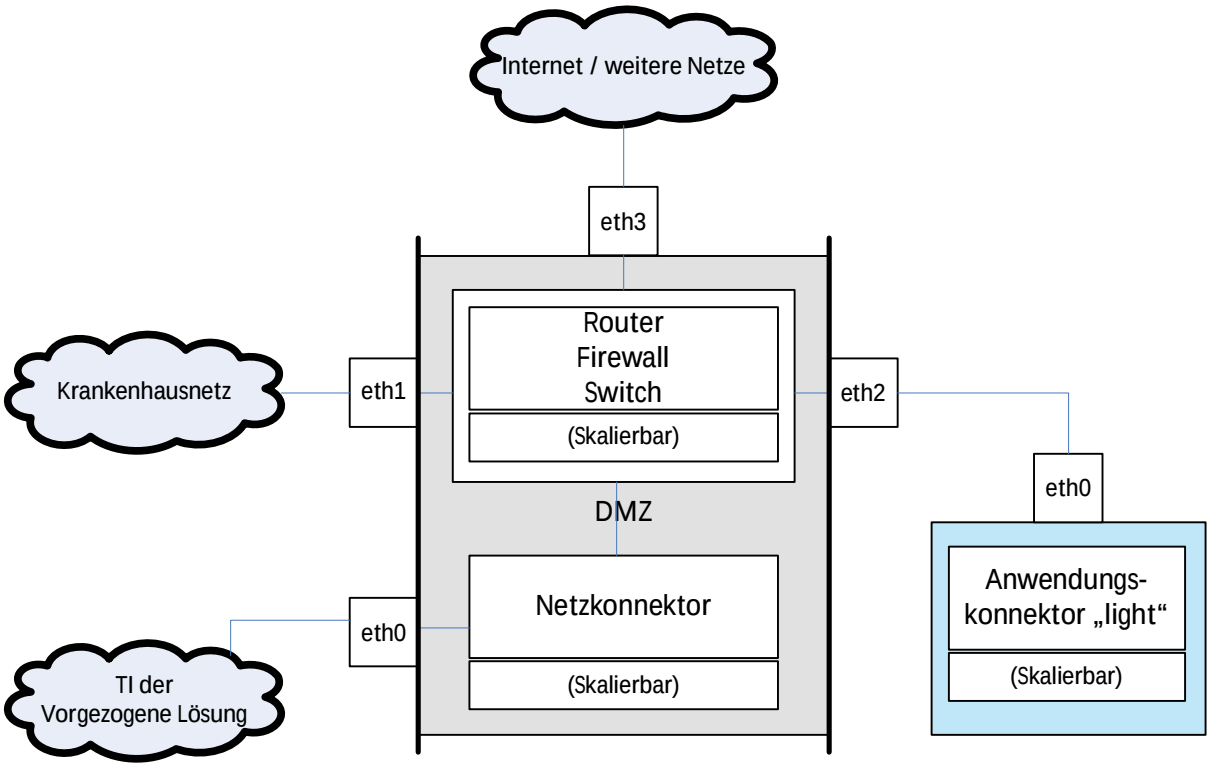


Abbildung 4: Darstellung der logischen Aufteilung eines Konnektors im Krankenhaus

Die Systeme des Krankenhauses kommunizieren über LAN mit den Anwendungskonnektoren. Jedes Primärsystem kann mehrere Anwendungskonnektoren nutzen. Die Kartenterminals sind den Anwendungskonnektoren zugeordnet.

Zentrale Systeme

Zentral wird eine einheitliche System- und Serverlandschaft aufgebaut, die die nachfolgend beschriebenen Funktionen erfüllt. Das zentrale Netz ist das Instrument, mit dem die Nutzung einzelner Dienste (Zeitdienst, Namensdienst etc.) angesteuert wird. Durch das Sicherheitsgateway wird die Sicherheit und demzufolge auch der Datenschutz gewährleistet. Dies bedeutet, dass insbesondere keine unbefugten Zugriffe und Durchleitungen erfolgen können. Dabei werden spezielle Firewalls eingesetzt. Bei diesen Komponenten handelt es sich um die marktübliche Standardnetzwerkleistung. Zu den zentralen Diensten der Lösung zählen alle zentralen Anteile, wie der Zeitdienst, der Namensdienst, die VPN-Konzentratoren inklusive Netzinfrastruktur (Gateways) sowie der Intermediär. Ebenso werden die zentralen Netze und das Transportnetz der Leistungserbringer zu den zentralen Diensten gezählt.

Zur Verbindung der zentralen und dezentralen Zugangskomponente können das Internet oder andere vom Transportnetzprovider angebotene Transportplattformen, wie Festverbindungen oder private Netze, genutzt werden. Da hier kein einheitliches Sicherheitsniveau zur Erreichung von Sicherheitszielen, wie Integrität und Vertraulichkeit, vorausgesetzt werden kann, muss die Übertragung der Daten über einen sicheren Kanal erfolgen. Hierfür wird ein VPN auf Basis von IPsec genutzt, dass zwischen den Zugangskomponenten etabliert wird. Unabhängig von der im Transportnetz genutzten Netztransportplattform erfolgt die Authentifizierung der Zugangskomponenten über X.509 Zertifikate, deren Zuordnung organisatorisch nachweisbar ist. Die gegenseitige Prüfung der in den Zertifikaten hinterlegten Identitäten erfolgt während des Verbindungsaufbaus des IPSec-VPN. Das Transportnetz verbindet die dezentralen Komponenten mit den zentralen Systemen über eine kontrollierte und sichere Anbindung. Die Vernetzung der dezentralen Komponenten erfolgt über die lokalen Netze der Leistungserbringer. Als Transportnetz zu den zentralen Systemen wird das Internet über DSL (alternativ, wenn kein DSL verfügbar: ISDN) gewählt. Über das Transportnetz erfolgt die kontrollierte und sichere Anbindung der dezentralen Systeme der Leistungserbringer und Kostenträger an das zentrale Netz. Es handelt sich um eine logische Bezeichnung für alle hierfür notwendigen Netzwerksegmente und Komponenten und stellt somit kein echtes physisch getrenntes und homogenes Netzwerk dar.

Der Intermediär, als zentrale Komponente, steuert und koordiniert die Verarbeitung der Nachrichten zwischen Konnektor und Fachdienst. Er lokalisiert abhängig vom Anwendungsfall den passenden Fachdienst und leitet die Nachricht an diesen weiter. Dabei reicht der Intermediär die Kommandos ohne Modifikation vom Konnektor weiter an den Fachdienst und wieder zurück. Eine Verarbeitung von Nachrichten im Intermediär findet nicht statt. Durch den Einsatz des Intermediärs kann bei mehreren Service-Instanzen die Anzahl der Verbindungen reduziert werden, wodurch die dezentralen Komponenten und die Fachdienste entlastet werden. Sie optimieren

somit die Betriebsführbarkeit, indem sie sowohl die Lokalisierung von Fachdiensten als auch Verbindungen zwischen Konnektoren und Fachdiensten auf eine beschränkte Anzahl von Gateways und Service-Busse, anstatt vieler Punkt-zu-Punkt-Verbindungen, zentralisieren.

Sicherheitsgateways

Ein Sicherheitsgateway ist ein System aus soft- und hardware-technischen Komponenten. Es gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden. Strukturell setzt sich ein Sicherheitsgateway aus einem Basisaufbau und modularen Erweiterungen dieser Basis zusammen. Die Basis wird dabei gebildet aus Paketfiltern und Application-Level-Gateways. Sicherheitsgateways werden am zentralen Übergang zwischen zwei unterschiedlich vertrauenswürdigen Netzen eingesetzt (siehe auch BSI-Dokument „Konzeption von Sicherheitsgateways“ – Version 1.0).

Die Sicherheitsgateways erbringen zusätzliche Sicherheitsleistungen für die Nutzung von Bestandsnetzen. Sie stellen Systeme für den Schutz vor Malware, Inhaltsfilter oder Angriffserkennung auf Netzwerkebene (IDS) transparent oder über Proxy-Technologien bereit. Sie kontrollieren somit inhaltlich den Datenfluss zwischen den zentralen Systemen und den Bestandsnetzen.

Die Anbindung von Bestandsnetzen erfolgt ausschließlich über die Sicherheitsgateways. Sie können hinsichtlich der Art der Anbindung und der zu transportierenden Daten konfiguriert werden.

Weiternutzung bestehender Netze

Der Zugang zu Bestandsnetzen (wie z.B. KV-SafeNet mit seinen Anwendungen) soll auch in der vorgezogenen Lösung möglich sein. Hierfür wird jedoch lediglich die Anbindung der Bestandsnetze an die vorgezogene Lösung realisiert. Damit wird auch das Ziel verfolgt, vorhandene bzw. sich schnell neu entwickelnde Insellösungen zu konsolidieren und in das Lösungsszenario zu integrieren. Maßgeblich für eine Integration ist jedoch, dass der Funktionsumfang des Lösungsszenarios nicht erweitert wird. Ein Bestandsnetz kann die vorgezogene Lösung als Transportnetz nutzen, sofern der zu Grunde liegende Funktionsumfang und das etablierte Sicherheitsniveau ausreichend sind. Der Zugang zu Fremdnetzen (Internet oder Bestandsnetze) beinhaltet die folgenden wesentlichen Aspekte:

- Auflösung unterschiedlicher Namensräume
- Sicherstellung der netzwerkseitigen Erreichbarkeit benötigter Adressräume

„Vorgezogene Lösung“

- Sichere Anbindung

Die Nutzung verschiedener Namensräume kann über einen DNS-Proxy-Nameserver, der die Anfragen an die jeweils zuständigen Nameserver weiterleitet, erfolgen.

Die Erreichbarkeit der Systeme in unterschiedlichen Adressräumen und eine möglicherweise notwendige Adressumsetzung werden über eine Routing/NAT-Komponente gewährleistet. Datenverkehr für den definierten Adressraum wird an die Transportnetzkomponenten weitergeleitet, alle anderen Datenpakete (Default Route) an die jeweilige Zugangskomponente des Fremdnetzes. Die Umsetzung ist in der nachfolgenden Abbildung dargestellt.

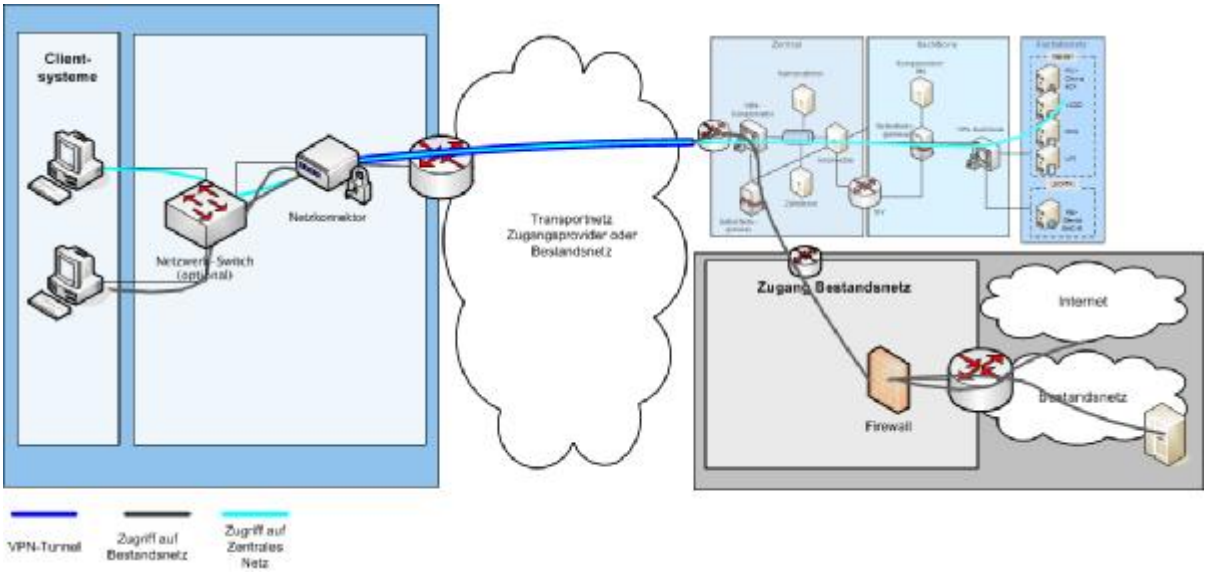


Abbildung 5: Weiternutzung bestehender Netze

Die Weiternutzung bestehender Netzwerke erfolgt über die Anbindung der Bestandsnetze an die Sicherheitsgateways der zentralen Systeme. Durch den Netzkonnektor bzw. den zentralen DNS-Server erfolgen die Netzwerkwegewahl und die Zuordnung der Namensräume.

Backbone

Der Backbone dient als sicherer Anschlusspunkt und Bindeglied für die zentralen Netze und Fachdienste. Er verbindet somit diese beiden Netzsegmente und stellt die Gesamtstrecke von Leistungserbringer zu Kostenträger her. Zudem beinhaltet er die PKI-Dienste der Komponenten.

VPN-Backbone / Zugangspunkte

Das zentrale Netz mit den zentralen Systemen wird über dedizierte Netzanschlüsse direkt an den Backbone angebunden. Beim Betrieb mehrerer Zentraler Systeme durch einen Betreiber können diese gemeinsam über einen Netzwerkanschluss an-

gebunden werden. Eine zusätzliche technische Authentifizierung wie bei der Anbindung der Leistungserbringer ist nicht notwendig, da über organisatorische Maßnahmen die Authentizität des angebundenen Dienstes nachgewiesen werden kann.

Die Anbindung von fachanwendungsspezifischen Diensten erfolgt im Standardfall identisch zu den Zentralen Netzen. Alternativ ist es möglich, diese über einen Transportnetzprovider an den Backbone anzuschließen. Hierfür ist allerdings wie bei der Anbindung von Leistungserbringern der Fachdienst über eine Zugangskomponente zu authentifizieren.

An den Anschlüssen zum Backbone wird nur der für deren Nutzung erforderliche Datenverkehr weitergeleitet. Die Freischaltung der IP-Adressen bzw. TCP/UDP-Ports erfolgt über eine Stateful-Inspection Firewall. Die hierüber erbrachte Sicherheitsleistung ist integraler Bestandteil des sicheren Zugangspunktes des Backbone der Lösung.

Betreiber von Zentralen Systemen und Fachdiensten können zusätzliche Sicherheitskomponenten in eigener Verantwortung an deren Zugangspunkten zum Backbone platzieren.

Komponenten-PKI

In der vorgezogenen Lösung ist die Kommunikation zwischen den Komponenten im Sinne von Geräten (Kartenterminal, Konnektor) und Diensten (Gateways, zentrale Infrastrukturdienste, Fachdienste) unter Einsatz von Zertifikaten und einer entsprechenden PKI abgesichert. Hierzu erhalten diese Komponenten und Dienste eine eindeutige Identität. Diese Identität wird durch ein Schlüsselpaar kryptographisch abgesichert. Der private Schlüssel dieses Schlüsselpaars hat einen sehr hohen Schutzbedarf und wird, je nach Komponente unterschiedlich, in einem besonders geschützten Schlüsselspeicher (bspw. Chipkarte oder HSM), aufbewahrt. Über den ihm zugehörigen öffentlichen Schlüssel wird ein X.509-Zertifikat ausgestellt. Diese Zertifikate werden durch die Komponenten-PKI verwaltet und herausgegeben. Als Vertrauensraum wird das durch die gematik spezifizierte Modell der Trust-service Status List (TSL) verwendet. Alle zum Einsatz kommenden Komponenten müssen diesen Vertrauensraum als Grundlage zur Verifikation von Zertifikaten verwenden. Für die Integration der Bestandsnetze wird ggf. eine eigene TSL etabliert.

Fachdienste

Die Fachdienste bilden den zentralen Anwendungsteil der Fachanwendungen. Bezogen auf die Anwendung „Versichertenstammdatenmanagement“ sind dies die Fachdienste

- Versichertenstammdatendienst (VSDD),
- Update Flag Server (UFS) und

- Card Management System (CMS).

Die Anbindung der fachanwendungsspezifischen Dienste an die zentralen Dienste erfolgt über den Backbone. Die Fachdienste der Kassen beinhalten verschiedene Elemente, wie einen PKI-Dienst für die Gesundheitskarte, den Versichertenstammdatendienst (VSDD), das Kartenmanagementsystem (CMS) und den Update Flag Service. Sie alle sind wichtig für die Funktion des VSDM. Diese Systeme sind bereits durch die Kassen umgesetzt und spielen im kommenden Beschaffungsverfahren für den Test der vorgezogenen Lösung nur bezüglich der Integration eine Rolle.

1.1.3 Erweiterbarkeit und Ausblick

Die Herausgabe der eGK der Kartengeneration 2 könnte in den geplanten Zeitraum zum Betrieb des Lösungsszenarios fallen. Aus diesem Grund sieht das Lösungsszenario eine Integration neuer Karten zur Nutzung der eGK G2 vor. Im Detail bedeutet dies, dass eine Interoperabilität zwischen Karten der Generation 1 und Generation 2 erzielt werden muss. Somit könnten beide Kartengenerationen parallel im Feld genutzt werden. Weitere Anpassungen der Infrastruktur werden nicht als notwendig angesehen, da zum Ende der geplanten Laufzeit des Lösungsszenarios eine vollständige Migration in die Ziellösung erfolgen soll.

In der folgenden Abbildung werden die Kern-Komponenten der vorgezogenen Lösung aufgelistet und hinsichtlich ihrer Migrationsfähigkeit bewertet. Dabei wurden die Kategorien von migrierbar (in der Abbildung mit der Farbe grün dargestellt) über migrierbar mit Anpassungen/Einschränkungen (gelb dargestellt) und voraussichtlich nicht migrierbar (rot dargestellt) gewählt. Da sich die Ziellösung noch größtenteils in der Entwicklung befindet, wurden die Komponenten schwerpunktmäßig hinsichtlich Standardkonformität, Nachladefähigkeit und Erweiterbarkeit betrachtet. Bei einigen Komponenten, wie Kartenterminals, den eingesetzten Karten und den Fachdiensten, kann aufgrund des Bestandsschutzes von einem unveränderten Einsatz in der Ziellösung ausgegangen werden.

Abhängig von der Ziellösung wird eine Anpassung bzw. ein Austausch von einzelnen Komponenten als notwendig angesehen und wurde entsprechend in der Kostenbetrachtung berücksichtigt.

„Vorgezogene Lösung“

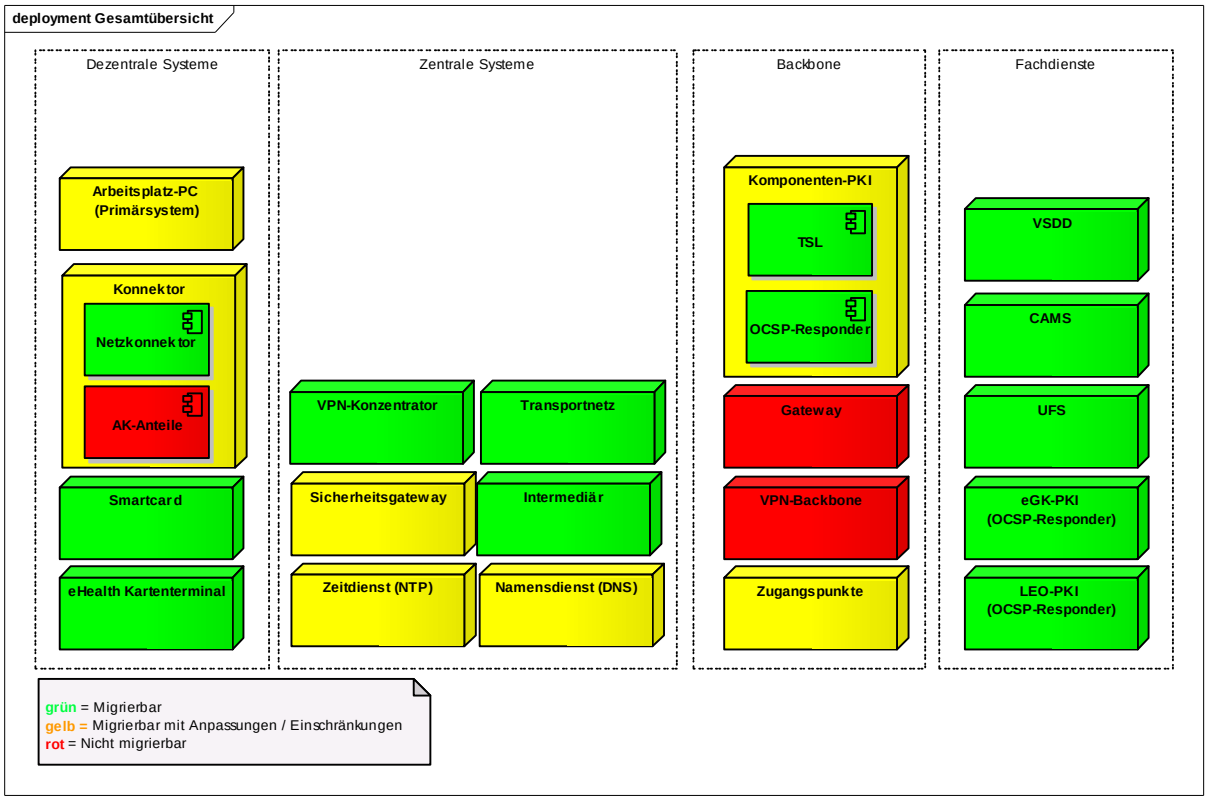


Abbildung 6: Bewertung der Migrationsfähigkeit einzelner Komponenten

Die elektronischen Gesundheitskarten der Generation 1 plus sind schon für die Verarbeitung in der Ziellösung vorbereitet und enthalten alle notwendigen Container und Zugriffregeln. Eine ggf. notwendige Schemaanpassung an ein aktuelleres VSD-Schema in der Ziellösung kann über die Aktualisierung online durchgeführt werden.

Aufgrund des definierten Bestandsschutzes wird sich die Schnittstelle der Fachdienste (UFS, VSDD, CMS) gegenüber der Ziellösung nicht verändern, so dass hier keine inhaltlichen Anpassungen durch die Kostenträger notwendig sind. Die Fachdienste müssen jedoch für die Migration in die Ziellösung an die zentrale Telematikinfrastruktur angebunden werden.

2 Leistungsumfang in den Testvorhaben

2.1 Allgemeine Rahmenbedingungen

Gemäß §2 der Rechtsverordnung (RVO) haben die Testmaßnahmen das Ziel der Überprüfung und Weiterentwicklung der Telematikinfrastruktur, die für die Einführung und Anwendung der elektronischen Gesundheitskarte erforderlich ist. Die Feldtests (im Folgenden auch als regionale Tests bezeichnet) sollen dabei insbesondere die Einsetzbarkeit des Gesamtsystems unter realen Einsatzbedingungen sowie den Einfluss auf die bestehenden Geschäftsprozesse prüfen. Dadurch soll sichergestellt werden, dass die elektronische Gesundheitskarte und die dafür notwendige Telematikinfrastruktur erfolgreich in die flächendeckende Versorgung überführt werden können.

Die Zielsetzung der Feldtests im Rahmen der vorgezogenen Lösung besteht in der Überprüfung der Kriterien Praxistauglichkeit, Akzeptanz, Betriebstauglichkeit und Datenschutz für Infrastrukturkomponenten und die Anwendung VSDM. Die Erkenntnisse aus den Feldtests bilden die Grundlage für die fachliche, technische und logistische Umsetzung des bundesweiten Rollouts.

Die Tests der vorgezogenen Lösung werden unter der aktuellen RVO durchgeführt.

Hieraus können die folgenden Rahmenbedingungen für die Durchführung der Tests abgeleitet werden:

- Definition von zwei Testregionen innerhalb eines Vergabeverfahrens und unter Berücksichtigung der aktuellen RVO sowie der Finanzierungsvereinbarung mit der gematik,
- Grundlage der Auswahl sind die existierenden sechs Testregionen unter Einbeziehung der Projektbüros,
- Änderungen werden im Benehmen mit den jeweils zuständigen obersten Landesbehörden vorgenommen (35 Abs. 6 RVO),
- Sicherstellung der Ausstattung einer möglichst hohen Anzahl an Leistungserbringern innerhalb einer Testregion (idealerweise Vollausstattung), damit genügend verwertbare Erkenntnisse nach Abschluss der Tests vorliegen,
- Möglichkeit der Einbindung aller an den Tests beteiligten Parteien. Die RVO beschreibt diesbezüglich das mögliche Einrichten von Beiräten, zusammengesetzt aus „Vertreterinnen und Vertretern der Leistungserbringer, der Pati-

entinnen und Patienten sowie der Kostenträger“[2] zur Sicherung der Praxistauglichkeit

Des Weiteren basiert die Konzeption der Tests für die vorgezogene Lösung auf den Erfahrungen aus den 10.000er Tests:

- Testung mit relevanter Grundgesamtheit: Die geringe Anzahl Testbeteiligter (Leistungserbringer und Versicherte) während der 10.000er Tests hat zu wenig aussagekräftigen Ergebnissen aufgrund geringer Fallzahlen geführt. Bei den Tests der vorgezogenen Lösung ist insbesondere auf eine deutlich höhere Anzahl beteiligter Leistungserbringer und Versicherter zu achten.
- Vermeidung kleinteiliger Vergabeverfahren: Aus Gründen der Interoperabilität der Komponenten werden die Lose im Vergleich zu den 10.000er Tests deutlich umfangreicher geschnitten. Die Erfahrungen aus den 10.000er Tests haben gezeigt, dass z.B. Interoperabilitätsprobleme zwischen den Komponenten der Telematikinfrastruktur und den Primärsystemen eine häufige Ursache für den fehlerhaften Betrieb der Lösung waren.
- Starke Angewiesenheit auf politische Lobby innerhalb der Testregion: Die 10.000er Tests haben gezeigt, dass die politische Unterstützung des Testvorhabens in einer Testregion erfolgskritisch ist, insbesondere in Bezug auf das Zusammenspiel der beteiligten Parteien von Kostenträgern und Leistungserbringerorganisationen.
- Beschaffung und Betrieb der Komponenten als einheitliches Los: Die Durchführung der 10.000er Tests haben die Problematik einer Trennung von Produktion und Betrieb einzelner Komponenten aufgezeigt. Die Beschaffung für die Durchführung der Tests der vorgezogenen Lösung sollte sich daher an einer Vergabe an gesamtverantwortliche Bieterkonstellationen orientieren.

In Anbetracht der oben genannten Rahmenbedingungen werden in den folgenden Abschnitten die Eckpunkte für die Testdurchführung im Hinblick auf die Auswahl der Testregionen, der Testziele, der Testdauer und der Evaluation der Tests definiert.

[2] Dritte Verordnung zur Änderung der Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte, § 5 Vorgaben zur Organisation der Testung durch die Gesellschaft für Telematik (10), Stand 11.01.2011

2.2 Eckpunkte der regionalen Tests

2.2.1 Auswahl der Testregionen

Es wird empfohlen, die Auswahl von zwei der sechs bestehenden Testregionen im Ausschreibungsverfahren den Bieterkonsortien zu überlassen, wobei Rahmenvorgaben, z.B. in Bezug auf die Anzahl einzubeziehender Leistungserbringer, gemacht werden können. Hierbei ist vorgesehen, dass sich alle Bieter für zwei Testregionen bewerben, in deren Rahmen sie die definierten Testziele erfüllen können. Eine Verbindung zweier Testregionen zu einer einzelnen, um die definierten Testziele zu erreichen, kann ebenfalls eingeräumt werden. Die finale Auswahl der Bieter für die beiden Testregionen bleibt dem Auftraggeber innerhalb des Verhandlungsverfahrens vorbehalten (siehe Kapitel 4).

2.2.2 Testziele

Ein primäres Ziel der Tests ist der Nachweis der Funktionsfähigkeit des Systems, der Betriebsprozesse in der konkreten Betriebsumgebung sowie der Prozesse und Organisation des Rollouts für die folgende bundesweite Einführung in der Fläche. Hierbei müssen die schnelle Herstellung des vollständigen Wirkbetriebs, die Erreichung der Qualitätsziele sowie der Nutzerakzeptanz sichergestellt sein. Ebenso müssen ein einheitliches Vorgehen und einheitliche Qualität bis in den Wirkbetrieb gewährleistet sein. Die Auftragnehmer müssen daher vordefinierten Anforderungen gerecht werden.

- Erstellung eines Testkonzepts: Der Betreiber muss in einem Testkonzept darlegen, wie die Betriebsfähigkeit des Systems nachgewiesen wird. Dieses Betriebstestkonzept ist im Angebot zu skizzieren und in der Einführungsphase soweit auszuarbeiten, dass die darin beschriebenen Tests und Testergebnisse als Grundlage für eine Abnahme des Systems genutzt werden können. Daneben sollte das Testkonzept auch regionale Unterschiede berücksichtigen, z.B. durch die Auswahl geeigneter Testregionen/Testteilnehmer.
- Durchführung der Tests: Zu den durchzuführenden Tests gehören unter anderem anwenderbezogene und funktionale Tests (Feldtests), Schnittstellen- und Kommunikationstests, Lasttests, Ausfall- und Failover-Tests. Ein weiteres zentrales Testziel besteht in der Planung und Durchführung des Rollouts (Planung, Logistik, Prozesse, Abwicklung, Support/Service, etc.) sowie im Zusammenspiel der Auftragnehmer-Parteien (Generalunternehmer, Service Provider, PS-Hersteller, etc.), insbesondere um Aussagen für den anschließenden bundesweiten Rollout ableiten zu können.

- Durchführung von Tests durch die gematik: Der Auftraggeber behält sich vor, die vom Betreiber durchgeführten Tests zu wiederholen und weitere eigene Tests durchzuführen. Der Betreiber muss ihm dies ermöglichen und ihn im angemessenen Rahmen dabei unterstützen.
- Durchführung von Zuslassungstests durch die gematik Die gematik wird im Zuge der Zulassung gewisser Komponenten Tests durchführen. Der Auftragnehmer verpflichtet sich, diese Tests in angemessenem Umfang zu unterstützen.

Sofern diese Anforderungen gegeben sind, haben die Auftragnehmer insbesondere Testziele zu erfüllen, die sich in drei Kategorien aufteilen lassen (weitere Testziele sind gegebenenfalls zu späterem Zeitpunkt innerhalb des Verhandlungsverfahrens zu definieren):

1. Mengengerüst

Für die Testung der vorgezogenen Lösung muss eine geeignete Anzahl Leistungserbringer ausgestattet werden. Unter den Krankenhäuser müssen unterschiedliche Versorgungsstufen (Größenordnungen) mit mindestens einer Universitätsklinik vertreten sein. Die Testmaßnahmen müssen die Nutzung eines erforderlichen Mehrkomponentenkonnektors ermöglichen. Hierbei wird vorausgesetzt, dass die Versicherten zum Großteil bereits mit eGKs ausgestattet sind und die Fachdienste der Kassen VSDM-funktionsfähig sind. Die vollständige Ausstattung der Leistungserbringer ist gleichzeitig eines der zu erfüllenden Testziele und setzt sich wie folgt zusammen: Siehe hierzu Dokument der Arbeitsgruppe.

Annahmen exemplarisch bezogen auf Arztpraxen:

- Anzahl einzubindender Leistungserbringer pro Testregion $M_{Ärzte} = 500$
- Anzahl Primärsystemhersteller $M_{PS} = 5$
- Daraus mindestens 3 PVS-Hersteller, die nicht gesellschaftlich verbunden sind
- Durchschnittliche Abrechnungsfälle pro Quartal = $M_{Abrechnungsfälle(Arzt)}$(Quartal)
- Durchschnittliche Patientenbesuche pro Quartal = $M_{Patientenbesuche(Arzt)}$(Quartal)
- Im ersten Quartal liegen für alle Versicherten Updates vor (Schemaänderung)

Aus diesen Annahmen ergeben sich die Ziele:

- Updates im Quartal = $M_{Ärzte}$ x $M_{Abrechnungsfälle(Arzt)}$(Quartal)
- Transaktionen im Quartal = $M_{Ärzte}$ x $M_{Abrechnungsfälle(Arzt)}$(Quartal) x $M_{Patientenbesuche(Arzt)}$(Quartal)

Anmerkung: Dies setzt voraus, dass in den regionalen Tests bei jedem Patientenbesuch die eGK gesteckt wird.

Das Mengengerüst ist für die endgültige Ausschreibung zu aktualisieren und um das Mengengerüst für Zahnarztpraxen und Krankenhäuser zu erweitern.

2. Messung und Reports

Ein weiteres Testziel ist die Bereitstellung von Testdaten für die begleitende Evaluation der Testmaßnahmen. Aus dem beschriebenen Mengengerüst lassen sich exemplarisch für Arztpraxen folgende Transaktionsraten herleiten:

Transaktionen	pro Arzt	Gesamt (pro Testregion)
pro Quartal	2.300,00	1.150.000,00
pro Tag (Arbeitstag)	38,33	19.166,67
pro Stunde (10 Std/Tag)	3,83	1.916,67
pro Minute		31,94
pro Sekunde		0,53

Updates	pro Arzt	Gesamt (pro Testregion)
pro Quartal	1.000,00	500.000,00
pro Tag (Arbeitstag)	16,67	8.333,33
pro Stunde (10 Std/Tag)	1,67	833,33
pro Minute		13,89
pro Sekunde		0,23

Abbildung 7: Beispielhafte Hochrechnung der Transaktionsraten während der regionalen Tests

Durch die notwendige Aktualisierung des VSD-Schemas im Online-Rollout, findet beim erstmaligen Stecken in jedem Fall ein Update der eGK statt.

3. Nicht-funktionale Anforderungen an die Komponenten

Schließlich müssen die Betreiber bei der Einführung des Systems die im Betriebstestkonzept definierten Tests durchführen und protokollieren. Die Protokollierung muss geeignet sein, den Erfüllungsgrad bezüglich funktionaler und nichtfunktionaler Anforderungen zu erkennen.

2.2.3 Dauer der Tests

Die Tests der vorgezogenen Lösung sollten über einen geeigneten Zeitraum stattfinden, der eine ausreichende Testung der durch die Anbieter betriebenen Telematikinfrastruktur sicherstellt. Gleichzeitig muss eine Verzögerung der vorgezogenen Lösung durch eine überflüssige, ausgedehnte Testung ohne zusätzliche Erkenntnisgewinnung vermieden werden. Die Dauer der Tests wurde daher auf Basis von folgenden Kriterien festgelegt:

- Die Tests finden über einen Zeitraum von mindestens drei Monaten und quartalsübergreifend statt. Hierdurch werden eine VSD-Aktualisierung durch das initiale Stecken der eGK sowie eine potenzielle, weitere Aktualisierung im anschließenden Quartal sichergestellt. Weitere Transaktionen über die Telematikinfrastruktur finden zusätzlich bei jedem weiteren Arztbesuch, auch ohne VSD-Aktualisierungsvorgang, statt. Diese Transaktionen liefern ebenfalls statistisch belastbare Daten über Traffic und Performance der Lösung.
- Gespräche mit Vertretern aus der Industrie haben die Dauer der Tests von drei bis sechs Monaten in Verbindung mit einer Ausstattung von ca. 500 Leistungserbringern pro Testregion als sinnvolle Parameter bestätigt, um statistisch signifikante Daten zur Verfügung stellen zu können.

2.2.4 Evaluation der Tests

Die Evaluation der Tests erfolgt primär zur auftraggeberseitigen Überprüfung der Einhaltung der Leistungsversprechen bzw. Testziele der beauftragten Bieterkonsortien. Die Methodik und das Vorgehen orientieren sich an den 10.000er Tests und wird unabhängig von den Industriekonsortien auf Auftraggeberseite durchgeführt. Aufgabe der Auftragnehmer besteht in der Bereitstellung entsprechender Daten zur Überprüfung der Testziele.

Des Weiteren ist die Befragung der am Test Beteiligten durch strukturierte Fragebögen in Betracht zu ziehen, z.B. in einer Akzeptanzanalyse durch Interviews sowohl bei Patienten, Leistungserbringern als auch bei Leistungserbringerorganisation und Vertretern der Kostenträger.

Eine wissenschaftliche Begleitung der Evaluation hat sich bereits während der 10.000er Tests bewährt, um objektive und belastbare Aussagen zur Zielerreichung zu erhalten. Hierzu kann auf den Erfahrungen innerhalb der gematik aufgesetzt werden.

2.3 Leistungsumfang und Losaufteilung in den Tests

Nachdem in den Punkten 2.1 und 2.2 die Rahmenbedingungen und der quantitative Umfang der Tests erläutert wurden, wird in diesem Abschnitt beschrieben, welche konkreten Aufgaben im Einzelnen erbracht werden müssen. Der Leistungsumfang der Tests ist entsprechend der zu beschaffenden Lose aufzuteilen. Es ist vorgesehen, zwei Lose für den eGK/TI Aufbau und Betrieb (Ende-zu-Ende-Verantwortung der Dienstleister) für jeweils eine Testregion sowie ein Los für den Aufbau und Betrieb des Backbone zu vergeben. Für die inhaltliche und vergaberechtliche Begründung der Losaufteilung wird an dieser Stelle auf Kapitel 4 verwiesen. Abschließend werden Aspekte bezüglich der Zusammenarbeit zwischen Auftragnehmer und Auftraggeber bei der Testung der vorgezogenen Lösung verdeutlicht.

In Anlehnung an das technische Konzept aus Kapitel 1 zeigt folgende Abbildung eine Übersicht über zentrale Komponenten des Backbone und der Fachdienste sowie über die zentralen und dezentralen Komponenten in den Regionen, die für die Durchführung des Tests in einer Region notwendig sind.

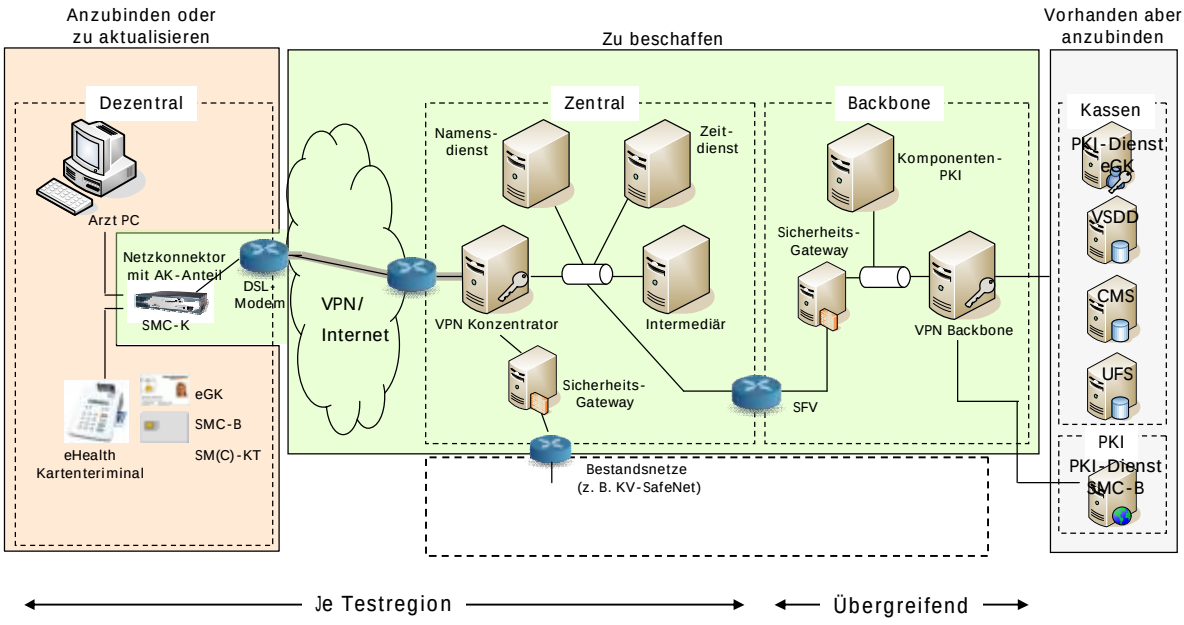


Abbildung 8: Übersicht über die zu beschaffenden Komponenten

Einige Komponenten sind dabei bereits in den Regionen vorhanden, andere müssen neu beschafft, angebunden oder aktualisiert werden. Die Auftragnehmer, die diese Testinfrastruktur umsetzen, müssen zwingend diese Komponenten einsetzen und dabei den Vorgaben (technischen Spezifikationen etc.) genügen.

Nur die Testung der Gesamtverfügbarkeit ist ein sinnvolles Vorgehen, was vom Auftragnehmer die Übernahme einer Ende-zu-Ende-Verantwortung erfordert. Die Bedeutung der Übernahme übergreifender Verantwortung wird aus nachstehender Ab-

bildung ersichtlich, in der das Versichertenstammdatenmanagement als übergreifende Anwendung mit den Prozessen Lesen der VSD, Onlineprüfung der VSD ohne Aktualisierung, Onlineprüfung der VSD mit Aktualisierung (siehe auch Kapitel 1) dargestellt ist.

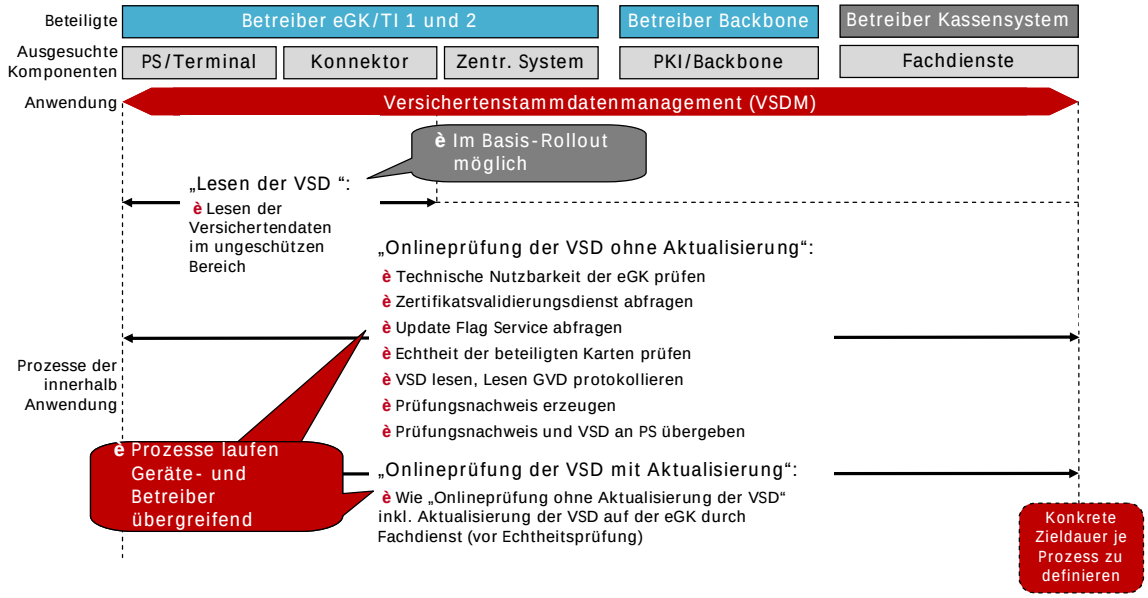


Abbildung 9: Übergreifende Anwendungen VSDM

Im Sinne der Ende-zu-Ende-Verantwortung sollen Auftragnehmer im Rahmen der Testung folgende Leistungen erbringen:

<u>Leistungsumfang des Auftragnehmers „eGK/TI Testbetrieb“ mit Ende-zu-Ende-Verantwortung:</u>

- Bereitstellung der Anwendung VSDM gemäß gematik-Vorgaben (Prozesse, technische Spezifikationen etc.) sowie der hierfür erforderlichen dezentralen Infrastruktur-Komponenten,
    - o Softwareanpassung des Primärsystems (Online-Schnittstelle)
    - o Bereitstellung des Konnektors mit Anwendungskonnektor „light“
    - o Installation des Transportnetzes
    - o Beschaffung der SMC-B (inklusive SM-KT), der SMC-K und Installation
    - o Konfiguration und Verkabelung der dezentralen Infrastruktur
- Bereitstellung des Transportnetzes
- Bereitstellung der zentralen Systeme
    - o VPN-Konzentrator
    - o Infrastrukturdienste
    - o Intermediär

  - Netzwerk (Transportnetz)
- Bereitstellung des Sicherheitsgateways und Anbindung von Bestandsnetzen (z.B. KV-SafeNet)
- Anbindung an den Backbone
- Erfüllung definierter Zielvorgaben (im Verhandlungsverfahren abschließend zu klären: operationalisierte Testziele wie Anzahl aktualisierter Versichertenkarten, Update-Dauer, Menge der angebundenen Leistungserbringer etc.),
- Projektmanagementfunktionen, einschließlich Reporting an den Auftraggeber zu Evaluationszwecken,
- Risiko-, und Changemanagement,
- Umsetzung übergreifender Support-Strukturen (User Help Desk, 1st-, 2nd-, 3rd-Level Support) für Leistungserbringer bei Fragestellungen und Störungen.
- QES gemäß Anlage 4 des Berichtes der Arbeitsgruppe

<u>Leistungsumfang des Auftragnehmers „Backbone-Testbetrieb“ als technische „Brücke“ zu den Kassensystemen:</u>

- Bereitstellung des Backbones
  - VPN-Backend
  - Sicherheitsgateway
- Aufbau und Betrieb der Komponenten-PKI
- Anbindungsmöglichkeit für Betreiber eGK/TI, Anbindung an die Provider der Kassen (für Fachdienste und PKI) und PKI der SMC-B Herausgeber
- Projektmanagementfunktionen (im Verhandlungsverfahren abschließend zu klären); v.a. Reporting an Auftraggeber
- Risiko-, Change- und Releasemanagement
- Integration des eigenen Supports in die übergreifenden Supportstrukturen der Betreiber eGK/TI

Im Vorhaben der vorgezogenen Lösung sollen Tests in zwei unterschiedlichen Testregionen durchgeführt werden, bevor der bundesweite Rollout beginnen kann. Dies hat folgende Gründe: Zuerst schreibt die Verordnung über Testmaßnahmen die Durchführung von mindestens zwei Feldtests vor. Sodann werden dadurch bewusst eine höhere Unabhängigkeit von einzelnen Anbietern sowie aussagekräftige Erkenntnisse für zukünftige Auftragsvergaben und einzelne Leistungen angestrebt. Eine Begrenzung auf zwei Testregionen erlaubt umgekehrt wiederum ein effizientes

und zielgerichtetes Vorgehen; sie vermeidet eine übergroße Komplexität bei der Testung.

Gemäß dem Prinzip der Ende-zu-Ende-Verantwortung werden die zwei Testregionen auf zwei Lose aufgeteilt und ausgeschrieben (siehe Abbildung 10). Die Auftragnehmer müssen hierfür der Übernahme von Ergebnisverantwortung und der Orientierung an konkreten Zielkennzahlen für die Testung (siehe Kapitel 2.2.2 und Kapitel 4) zustimmen.

Die Anbindung an die diversen Kassensysteme kann jedoch nur über einen Zugang geschehen. Infolgedessen ist ein Los vorgesehen, welches die Leistungen für die Backbone-Anbindung für den Testbetrieb umfasst.

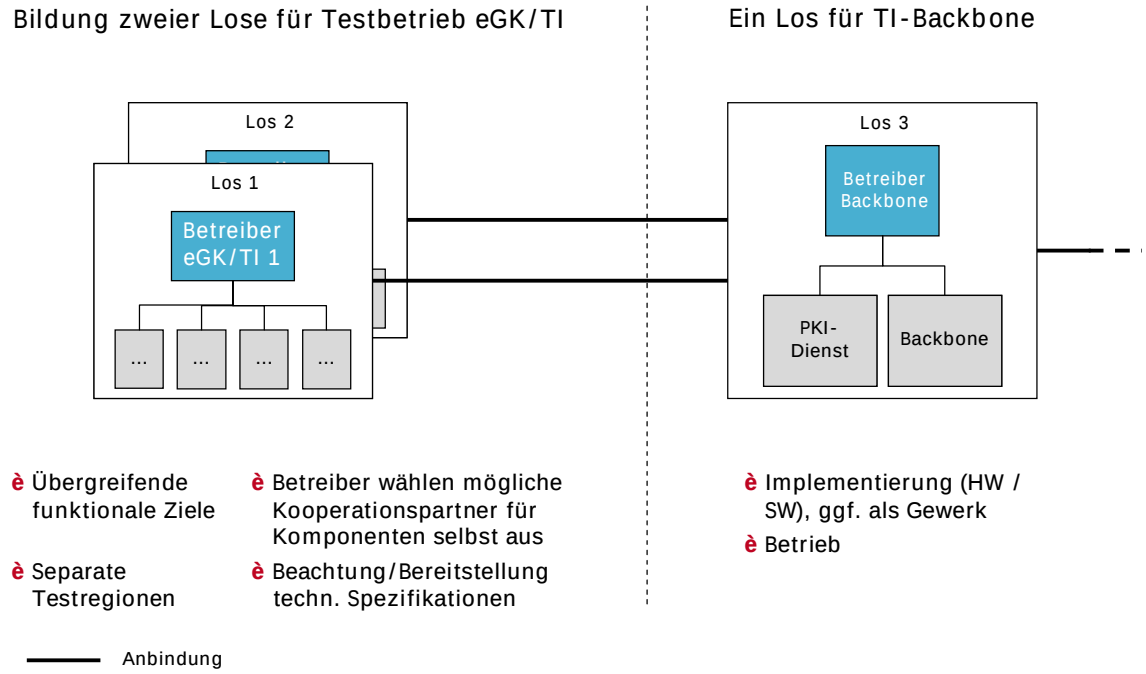


Abbildung 10: Grob-Beschreibung der Lose für die Testung

Die folgende Abbildung zeigt die an der Testorganisation Beteiligten. Die Verbindungslinien stehen dabei für direkte Kommunikationsstränge und somit für Schnittstellen.

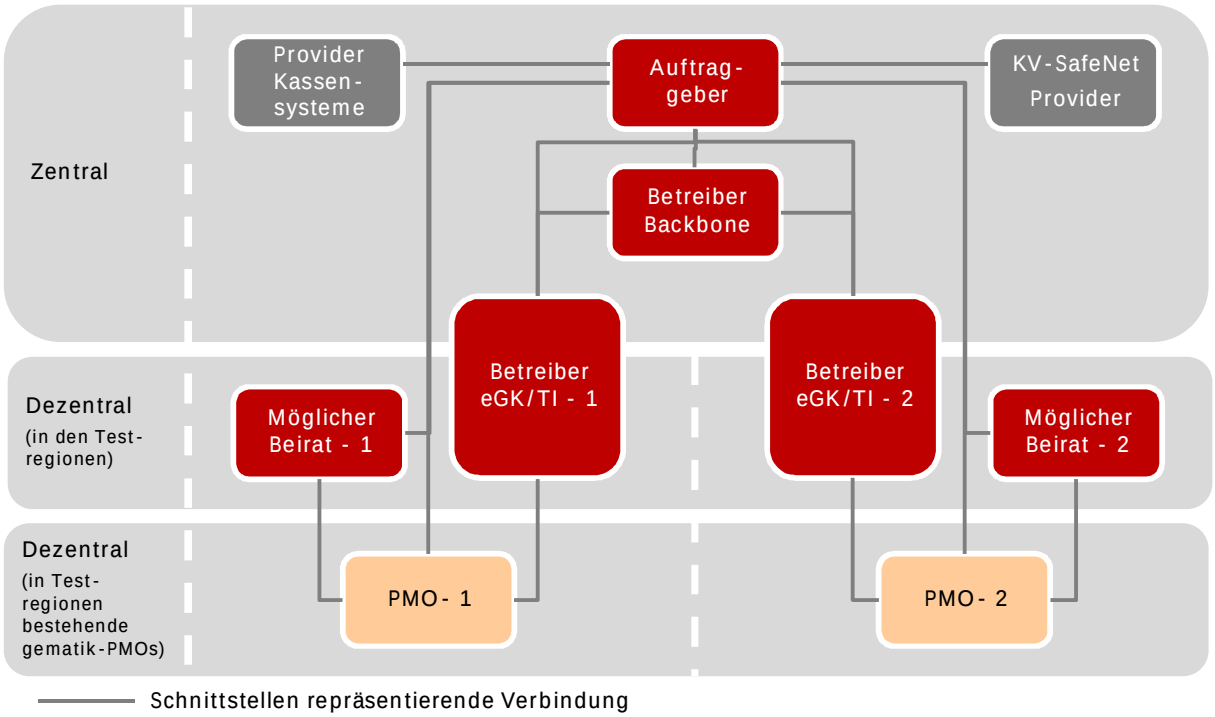


Abbildung 11: Beteiligte und Schnittstellen im fachlichen Konzept

Die dargestellte Struktur ist nicht abschließend. Insbesondere die Koordinierungs- und Managementaufgaben sollten während des Verhandlungsverfahrens in enger Zusammenarbeit mit den potenziellen Auftragnehmern weiter detailliert werden.

Die Auftragnehmer für den eGK/TI-Testbetrieb besitzen eine Schlüsselrolle im Rahmen der Testung. Diese müssen sich gleichermaßen eng mit den Projektbüros in den Testregionen und dem Auftragnehmer für den Betrieb des Backbones, unter Einhaltung der festgesetzten Betriebs-, Service- und Projektlevel, abstimmen. Sie kümmern sich ebenso um den Aufbau der technischen Schnittstellen.

Die bereits durch die 10.000er Tests bestehenden regionalen Projektbüros unterstützen bei der Umsetzungskoordination vor Ort. Laufendes Reporting über die Aktivitäten der Betreiber o.ä. gehört genauso zu ihren Aufgaben wie beratende Tätigkeiten in Gremien.

Gemäß der Verordnung über Testmaßnahmen ist die Bildung von Beiräten in den Testregionen möglich. Vertreter der Leistungserbringer, der Kostenträger, der Versicherten und ggf. weitere können Mitglieder werden. Die tatsächliche Besetzung der Beiräte ist abhängig von den in den Testregionen zuständigen Leistungserbringerorganisationen, Kostenträgern und den obersten Landesbehörden. Die Beiräte kön-

nen die Praxistauglichkeit der Anwendung sichern helfen und geben Empfehlungen im Rahmen der Tests.

Zur Wahrnehmung der Aufgaben im Testbetrieb sind durch die Beteiligten Ansprechpartner zu benennen (zu Themen wie Integration, Projektkommunikation, Eskalation, Gremienteilnahme etc.).

2.4 Ausblick

Bundesweiter Rollout:

Bereits während der regionalen Tests wird das Detailkonzept zum bundesweiten Rollout vollständig ausgearbeitet. Diese Detailkonzeption setzt auf den Erfahrungen aus den regionalen Tests auf. Die gematik-Gesellschafter entscheiden nach der regionalen Testung der vorgezogenen Lösung und deren Evaluation über die Umsetzung des bundesweiten Rollouts. Der bundesweite Rollout beinhaltet die Umsetzung der Online-Anbindung der Leistungserbringer (Ärzte, Zahnärzte und Krankenhäuser) in Verbindung mit der Anwendung VSDM (VSDM mit korrespondierender Infrastruktur und QES). Für den bundesweiten Rollout und die spätere Migration in die Ziellösung bleibt wiederum eine zeitlich schnelle Umsetzung eine wesentliche Anforderung. Dies ist bei der zukünftig anstehenden Ausgestaltung der formalisierten Vergabeverfahren bzw. Zulassungen (ggf. auch ergänzend für einzelne Komponenten) zu berücksichtigen.

3 Bewertung der vorgezogenen Lösung aus der Perspektive der Datensicherheit und des Datenschutzes

3.1 Datensicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Vorgaben für die Spezifikationen der Telematikinfrastruktur erarbeitet. Diese Vorgaben sind in Schutzprofilen (Protection Profiles; PP) formuliert und gelten als Sicherheitsstandards. Die Vorgaben betreffen u. a. den Konnektor und die Kartenterminals. Der Konnektor besitzt als wesentliche Bestandteile den Netzkonnektor, der Paketfilterfunktionalitäten und die Leistungen eines VPN-Clients zur Verfügung stellt, und einen Anwendungskonnektor, der Anwendungslogik und Managementfunktionen enthält. Das PP für den Netzkonnektor kann durch das BSI veröffentlicht werden (PP-NK), die PPs für den vollumfänglichen Konnektor sind noch in Bearbeitung; die PPs müssen den Einsatz von Einbox- und Mehrkomponentenkonnektoren beschreiben. Zukünftig sollen alle am Markt erhältlichen Konnektoren anhand der PPs evaluiert werden.

Der Konnektor der vorgezogenen Lösung ist konform zu den Vorgaben des BSI aufgebaut. Seine funktionalen Bestandteile sind in folgender Abbildung dargestellt.

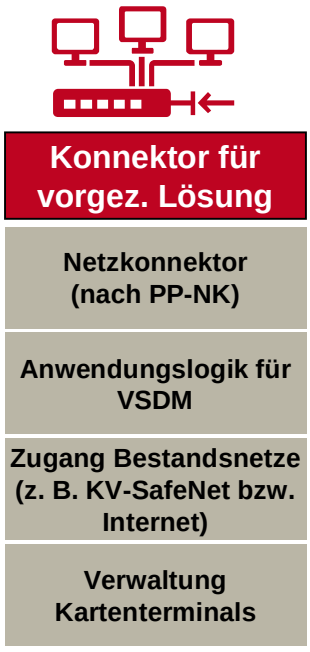


Abbildung 12: Funktionale Bestandteile des Konnektors der vorgezogenen Lösung

Die Lösung sieht einen reduzierten Funktionsumfang im Vergleich zur Konnektorbeschreibung der gematik im Release 4.0.0 vor und ermöglicht eine Anbindung der Leistungserbringer. Zum Einsatz kommt ein Netzkonnektor und ein Anwendungskonnektor „light“ mit Anwendungslogik. , der zunächst ausschließlich VSDM

abbildet (VSDM mit korrespondierender Infrastruktur und QES gemäß Anlage 4 des Berichts der Arbeitsgruppe).

Darüber hinaus bezieht die Lösung die Möglichkeit mit ein, Bestandsnetze, wie z.B. KV-SafeNet, integrieren zu können. Die Anbindung dieser Bestandsnetze soll über ein Sicherheitsgateway der Netzwerkinfrastruktur erfolgen und somit das Sicherheitsniveau von KV-SafeNet deutlich erhöhen.

Die Funktionen zur Verwaltung des Kartenterminals erlauben das Schreiben und Lesen von Daten (z.B. auch von bereits signierten Daten) der Karte und die Echtheitsprüfung der beteiligten Karten (Card-to-Card Authentifizierung).

Die Konzeption der vorgezogenen Lösung setzt die folgenden Anforderungen des BSI zur Integration von Bestandsnetzen um.

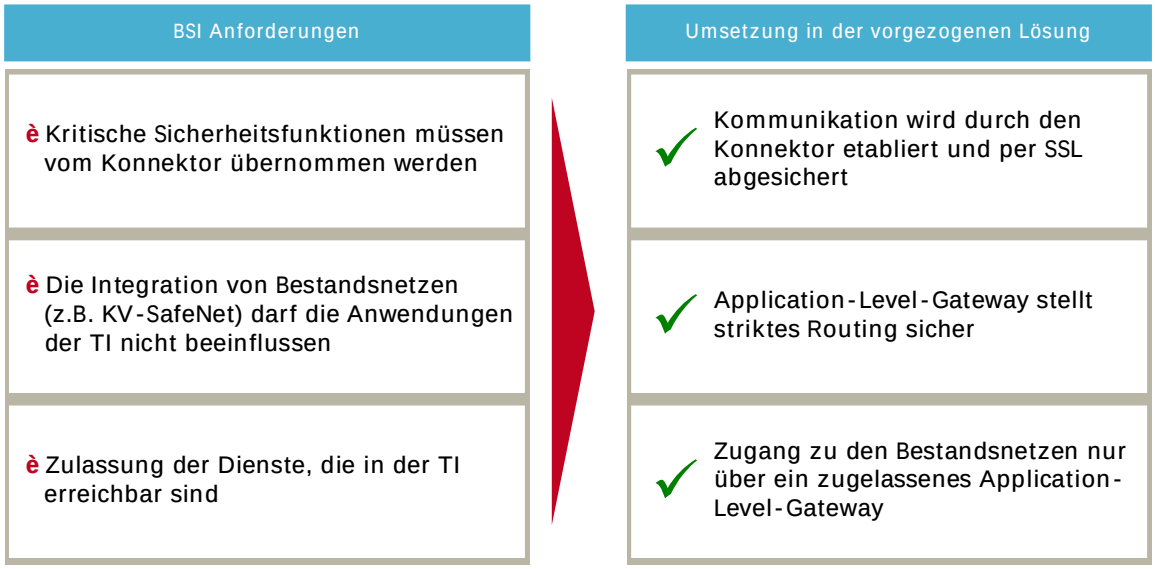


Abbildung 13: In der vorgezogenen Lösung berücksichtigte Kernanforderungen des BSI

Über die Anforderungen an die Netzintegration hinaus waren hinsichtlich der Vorgaben für das Vorhaben der vorgezogenen Lösung noch folgende Punkte mit dem BSI abzuklären:

- Zertifizierungsfähigkeit des Netzkonnektors für den bundesweiten Rollout auf Grundlage des Protection Profiles für den Netzkonnektor (PP-NK)
- Einsetzbarkeit des Anwendungskonnektors „light“ in der vorgezogenen Lösung mit einer späteren Evaluierung nach PP-AK-EB
- Einstufung der vorläufigen Zulassung der gematik für den Netzkonnektor mit Anwendungskonnektor „light“ innerhalb der regionalen Tests als ausreichend
-

- Einrichtung eines Zugangs ins Internet, z.B. über ein zentrales Sicherheits-Gateway oder über ein integriertes Bestandsnetz (z.B. KV-SafeNet)

3.2 Datenschutz

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat in der Vergangenheit immer wieder das Problem der nicht geschützten Versichertenstammdaten auf der Krankenversichertenkarte (KVK) kritisiert und eine baldige Beanstandung angekündigt. Durch den Basis-Rollout wird nun damit begonnen, die KVK durch die eGK zu ersetzen, so dass ein flächendeckender Rollout in 1-2 Jahren zu erwarten ist. Die eGK verwahrt im Zielszenario zu schützende Versichertendaten in einem geschützten Datencontainer. Bis alle Versicherten mit einer eGK ausgestattet sind und die Terminals den SICCT-Standard erreicht haben, verbleiben die zu schützenden Versichertendaten (z.B. besondere Personengruppe, Zuzahlungsstatus) jedoch redundant im geschützten Bereich und zusätzlich im Container allgemeiner Versicherungsdaten, welcher weiterhin ungeschützt ist. Dadurch bleibt bis zum vollständigen Abschluss des Rollouts der Ziellösung die gleiche datenschutzrechtlich problematische Situation wie zu Zeiten der KVK bestehen. Diese Problemstellung hat ebenfalls das BMG aufgegriffen und in einer schriftlichen Stellungnahme den BfDI um datenschutzrechtliche Flankierung sowie Abhilfe aufgefordert.

Durch die bundesweite Umsetzung der vorgezogenen Lösung wäre die Platzierung der Versichertendaten im geschützten Bereich der eGK unmittelbar möglich. Somit wären die Forderungen des BMG und des BfDI mit dieser Lösung im Anschluss an die flächendeckende Kartenausgabe möglich. Die SGB-konforme Protokollierung des Lesens und der Aktualisierung der geschützten Versichertenstammdaten erlaubt, die Versicherten vollständig über den Umgang mit ihren personenbezogenen Daten zu informieren.

Wenngleich der BfDI einer Internetanbindung einer Arztpraxis grundsätzlich äußerst kritisch gegenüber steht, wird einerseits die faktische Notwendigkeit erkannt und andererseits die Erhöhung des Sicherheitsniveaus durch Einbindung des Zugangs über die Infrastruktur der vorgezogenen Lösung positiv beurteilt. Der BfDI hat nach internen Beratungen eine Umsetzung der vorgezogenen Lösung aus Perspektive des Datenschutzes in einer schriftlichen Stellungnahme ausdrücklich begrüßt.

4 Beschaffung

Der Aufbau, die Testung und der Betrieb der Telematikinfrastruktur im Rahmen der vorgezogenen Lösung bedürfen eines gezielten Einsatzes externer Dienstleister. Unmittelbar steht dabei die Beschaffung der erforderlichen Leistungen für die regionalen Tests an. Angesichts der Komplexität, der Kritikalität, der Vorerfahrungen früherer Beschaffungen der gematik und der besonderen Charakteristika des Vorhabens, insbesondere seiner Neuartigkeit, ist das Beschaffungsverfahren sorgfältig auszugestalten. Im Folgenden werden die wesentlichen Eckpunkte des vorgesehenen Verfahrens dargestellt. Leitgedanke der Vergabe ist das Prinzip der Ende-zu-Ende-Verantwortung, mit dem die angesprochenen Anforderungen adressiert werden.

Diese sind auch konstitutiv für die Wahl des formalisierten Verfahrens, eines Verhandlungsverfahrens mit vorgeschaltetem Teilnahmewettbewerb in drei Losen. Sichergestellt wird dabei, dass den spezifischen Vergabeerfordernissen Rechnung getragen wird. Die Neutralität wird gewährleistet, mit der spezifischen Aufteilung in drei Lose wird dem Losgebot auch unter Wahrung des Grundsatzes des Mittelstandsgebots entsprochen. Flankierend zu dieser Vergabe sind die notwendigen auftraggeberseitigen Unterstützungsleistungen Gegenstand eines formalisierten Beschaffungsverfahrens. Im Ausblick kann es auch für zukünftige Entwicklungen, d.h. den Rollout bzw. die Migration zur Ziellösung, zu Beschaffungen mit einem formalisierten Verfahren bzw. Zulassungen (ggf. auch ergänzend für einzelne Komponenten) kommen. Hierzu liefern das anstehende Verfahren für die regionalen Tests und die Durchführung der Tests wichtige Erkenntnisse.

Leitgedanke der Vergabe: Ende-zu-Ende-Verantwortung der Auftragnehmer mit Risikoübernahme

Der vorgesehene Beschaffungsansatz ist dadurch geprägt, dass nicht Einzelkomponenten beschafft werden, sondern die Sicherstellung eines funktionierenden Gesamtsystems in den Testregionen gewährleistet werden muss. Dieser Ansatz unterscheidet sich damit von der bisherigen Beschaffungsstrategie der gematik ganz wesentlich: Beim bislang verfolgten Weg einer Beschaffung einzelner Komponenten verbleibt auftraggeberseitig das Risiko, dass diese Einzelkomponenten auch tatsächlich miteinander funktionieren. Die Übernahme der Ende-zu-Ende-Verantwortung durch die Auftragnehmer verlagert dagegen die Anforderungen an Integration, Interoperabilität und Schnittstellen-Management. Ende-zu-Ende-Verantwortung beschreibt die Gesamtverantwortung für die ganzheitliche Funktionsfähigkeit aller betrieblichen Prozesse, die für übergreifende Anwendungen im Rahmen der Telematikinfrastruktur erforderlich sind. Hierbei ist zwischen der Ende-

zu-Ende-Verantwortung für die beiden Auftragnehmer „eGK/TI Testbetrieb“ und „Backbone-Testbetrieb“ zu unterscheiden, da ihr Verantwortungsbereich jeweils verschiedene, definierte Abschnitte der Telematikinfrastruktur betrifft (siehe hierzu 2.3 in diesem Dokument).

Mit dem ganzheitlichen Ansatz erfolgt eine Risikoübernahme durch die Anbieter. Dadurch soll für die regionalen Tests mit der Möglichkeit des späteren Wirkbetriebs ein sicheres und wirtschaftliches Funktionieren bei niedrigen Betriebs- und Instandhaltungskosten erzielt werden. Der Aufbau der notwendigen technischen Infrastruktur, der zwingend am Anfang des Projekts steht, tritt hinter den hauptsächlichen Zweck, nämlich der Schaffung der Verfügbarkeit einer Telematikinfrastruktur, mit der bestimmte Anwendungen ausgeführt werden können, zurück. Es sollen dazu sach- und zeitgerechte Vergabeverfahren durchgeführt werden, welche den Besonderheiten der vorgezogenen Lösung gerecht werden und deshalb insbesondere folgende Eckpunkte erfüllen müssen:

- die Ende-zu-Ende-Verantwortung bildet den Hauptgegenstand. Die Ausrichtung auf den Leistungserfolg generiert Leistungsanreize bei den Erstellern;
- die Einstehung der Industriepartner für Funktionen, Verfügbarkeit und Betriebskosten;
- die Sicherstellung des Projekterfolgs durch klare Rollenverteilung und klare Verantwortungsstruktur unter Beachtung, dass die technische Verantwortung und Systemintegration im gesamten Erstellungsprozess bei den Industriepartnern verbleiben;
- die Berücksichtigung der Vorgaben hinsichtlich Datenschutz und Datensicherheit.

<u>Verfahrensart: Verhandlungsverfahren mit vorgeschaltetem Teilnahmewettbewerb</u>

Für die Ausgestaltung des Vergabeverfahrens im Zusammenhang mit den regionalen Tests wird ein Verhandlungsverfahren mit vorgeschaltetem Teilnahmewettbewerb vorgesehen.

Dieses Verhandlungsverfahren wird so ausgestaltet, dass in drei Losen im Rahmen von Leistungsbeschreibungen die wesentlichen fachlichen und technischen Eckpunkte vorgegeben werden. Im Zuge der Verhandlungen mit den auf der Basis des Teilnahmewettbewerbs als geeignet ausgewählten Bietern wird die zu erbringende Leistung konkretisiert und die Anforderungen weiterentwickelt. In diesem Rahmen wird den Bietern auch Gelegenheit gegeben, in vertraglicher und preislicher Hinsicht auf diese Entwicklungen zu reagieren. Die Verhandlungsverfahren werden so ausgestaltet, dass die Bieter ihre Vorstellungen von der Art und Weise der Leistungs-

erbringung darzulegen haben und den anzugebenden Angebotspreis unter die Bedingung stellen können, dass über eine „Liste mit verhandlungsbedürftigen Aspekten“ im Rahmen der Verhandlungen Einigkeit erzielt wird.

Bei der Entscheidung über die Zulässigkeit des Verhandlungsverfahrens ist auch der Umstand eingeflossen, dass in der Vergangenheit einzelne Komponenten zum Teil auch in anderen Verfahrensarten (z.B. auch im offenen Verfahren) ausgeschrieben und vergeben wurden. Mit Blick auf die neue Situation, wonach der Ansatz verfolgt wird, eine Gesamtverfügbarkeit des Systems in den Testregionen zu erreichen, ist jedoch eine neue Würdigung der Sachlage durchaus gerechtfertigt. Der wesentliche Unterschied besteht darin, dass nunmehr nicht einzelne Komponenten eindeutig und erschöpfend beschrieben und somit folgerichtig über Verfahren ohne Verhandlungsmöglichkeit beschafft werden. Jetzt geht es darum, die Vertragspartner in eine Gesamtverantwortung für die integrale Verfügbarkeit des Systems in der jeweiligen Testregion zu nehmen. Dies ist ein viel komplexerer Ansatz, der neben der Beschaffung von technischen Komponenten insbesondere einen erheblichen Koordinierungsbedarf und Managementaufgaben umfasst, die wiederum erst sukzessiv im Rahmen von Verhandlungsrunden gemeinsam mit den Bietern entwickelt werden können. Bei Bestimmung der richtigen Verfahrensart wurde auch der wettbewerbliche Dialog gewürdigt, im Ergebnis jedoch abgelehnt, da dieser nach Angebotsabgabe nicht die notwendigen Verhandlungsmöglichkeiten vorsieht.

Konformität mit und Ausgestaltung der Vergabeanforderungen

Das vorgesehene Verfahren trägt den spezifischen Vergabeerfordernissen eindeutig Rechnung. Prägend für die spezifische Ausgestaltung sind auch dabei der Leitgedanke der Ende-zu-Ende-Verantwortung sowie die Besonderheiten des Beschaffungsgegenstands.

Neutralität des Verfahrens

Die Sicherstellung eines ordnungsgemäßen Wettbewerbs und die Diskriminierungsfreiheit des Vergabeverfahrens haben oberste Priorität. Insgesamt wird während des gesamten Vergabeverfahrens darauf geachtet, dass auch solche Unternehmen, die sich in der Vergangenheit an Ausschreibungsverfahren der gematik beteiligt haben, bzw. in diesem Zusammenhang auch Aufträge erhielten, keinen Vorteil durch einen Wissensvorsprung besitzen. Diejenigen Unternehmen, die sich nun erstmalig um die entsprechenden Leistungen bemühen, sollen dieselben Wettbewerbsvoraussetzungen erhalten. Dies wird insbesondere durch Offenlegung sämtlicher vorliegender Spezifikationen gewährleistet.

Konformität des Verfahrens mit dem Los- und dem Mittelstandsgebot angesichts des Beschaffungsziels

Das übergeordnete Ziel der Beschaffung besteht darin, kurzfristig in zwei Testregionen eine definierte Anzahl von Leistungserbringern in eine tragfähige Telematikinfrastruktur einzubinden und damit Erfahrungen mit Transaktionen der eGK zu generieren. Die Erfolgsmessung würde dann in Zukunft in der Testphase nicht darin bestehen, dass Einzelkomponenten, also Hardware oder Software bzw. Dienstleistungen für Teilaspekte, zur Verfügung gestellt werden, sondern die Vertragspartner die Gesamtverantwortung dafür tragen, dass die Leistungserbringer definierte Vorgänge über das System abwickeln können. Die Einhaltung der Zielparameter könnte z.B. über die Zielerreichung hinsichtlich folgender Aspekte kontrolliert werden:

- Anzahl aktualisierter Versichertenkarten
- Update-Dauer
- Menge der angebundenen Leistungserbringer
- etc.

Der nunmehr verfolgte Ansatz besteht daher darin, diese Gesamtverantwortung in den Vordergrund zu stellen und das Ausschreibungsverfahren so zu konzipieren, dass auch tatsächlich eine Gesamtverantwortungsübernahme der Privatwirtschaft möglich erscheint.

Dabei ist auch von zentraler Bedeutung, dass nach Abschluss einer Testphase eine Systemöffnung – zumindest für Teilkomponenten – erfolgen muss und soll, damit auftraggeberseitig keine zu starke Abhängigkeit besteht und im Übrigen auch die Grundsätze des Mittelstandsgebotes gewahrt werden können.

Bei dieser Konzeption wurde der Ausnahmecharakter der einzelnen Gesamtvergaben aufgegriffen und die Ausnahmetatbestände von § 2 EG Abs. 2 VOL/A in Verbindung mit § 97 Abs. 3 GWB unter Beachtung der Auslegung der Rechtsprechung und Literatur herangezogen. Sie führten zu einer Vergabe in drei Losen: nämlich zwei Lose für jeweils eine Testregion und ein Los für den Backbone (vgl. Kapitel 2.3). Dabei wurde beachtet, dass ein öffentlicher Auftraggeber grundsätzlich einen erhöhten Koordinierungsaufwand aufgrund der mittelstandsfördernden Entscheidung des Gesetzgebers zugunsten des Vorrangs der Losvergabe hinzunehmen hat. Eine Koordinierung von Einzelvergaben würde jedoch zu einem erheblichen Mehraufwand führen. Ferner ist zu beachten, dass die Gesamtverantwortung des Auftragnehmers im Vordergrund steht und diese nur mit dem Loszuschnitt auf drei Lose erreicht werden kann.

„Vorgezogene Lösung“

Strukturierte Markterkundung

Im Rahmen der Ausgestaltung des Beschaffungsansatzes wurde eine strukturierte Markterkundung durchgeführt. Sie setzt sich aus zwei Teilen zusammen: erstens der Untersuchung, inwiefern für die gesuchten Komponenten ein Markt existiert, und zweitens strukturierten Gesprächen mit Marktteilnehmern, um zu erkennen, inwiefern ein Markt für die gesuchte Gesamtverantwortung geschaffen werden kann. Zugleich wurden einzelne Planungsparameter geprüft und dabei die Sicht der potenziellen Bieter ermittelt.

Im Ergebnis zeigte sich, dass für alle Komponenten Märkte existieren, jedoch die Beteiligung mehrerer Unternehmen zur Umsetzung der Testinfrastruktur zwingend erforderlich ist. Es gibt potenzielle Bieterkonsortien, welche die Ende-zu-Ende-Verantwortung übernehmen würden. Die Zeit- und Umsetzungsplanungen der vorgezogenen Lösung konnten durch die Gespräche erhärtet werden.

Anforderungen an die Bieter

Die Eignungsprognose wird sich generell an der Struktur der wirtschaftlichen und finanziellen Leistungsfähigkeit einerseits sowie der technischen und fachlichen Leistungsfähigkeit andererseits orientieren. Im Vordergrund wird dabei die Überprüfung der Anbieter dahingehend stehen, inwieweit diese auch tatsächlich in der Lage sind, die Ende-zu-Ende-Verantwortung zu übernehmen. Dies setzt neben den Fähigkeiten der technischen Komponenten auch Fähigkeiten des Verständnisses des Gesamtsystems, des Multiprojektmanagements sowie die Anbindungsmöglichkeit der Primärsysteme der Leistungserbringer voraus.

5 Glossar

ABDA	Bundesvereinigung Deutscher Apothekerverbände
AIS	Arztinformationssystem
AK	Anwendungskonnektor
AK-EB	Teile des Anwendungskonnektors, die gegen das Angriffspotential „enhanced basic“ zu evaluieren sind
AMTS	Arzneimitteltherapiesicherheit: Kontrolle verschiedener Verschreibungen auf Unverträglichkeiten
BÄK	Bundesärztekammer
Basis-Rollout	Ausgabe der eGK-Kartenterminals 2011
BCS	Basic Command Set - Kartenterminal für KVK und eGK, durch Firmware-Update auf SICCT erweiterbar
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGH	Bundesgerichtshof
BMG	Bundesministerium für Gesundheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
CMS	Card Management System
DKG	Deutsche Krankenhausgesellschaft
DMP	Disease Management Programme
DNS	Domain Name Sytsem, Bereichsnamensystem
DSL	Digital Subscriber Line - Breitbandtechnologie auf Basis normaler Telefonleitungen
EC	Eurocard, heute girocard
eFA	elektronische Fallakte
eGK	Elektronische Gesundheitskarte
Feldtests	Begriff aus der RVO für regionale Tests
GKV	Gesetzliche Krankenversicherung
GKV-SV	Spitzenverband der Gesetzlichen Krankenversicherungen und Pflegekassen
GPRS	General Packet Radio Service - Funktechnologie zur Datenübertragung
GSV	Gesellschafterversammlung
GWB	Gesetz gegen Wettbewerbsbeschränkungen
HBA	Heilberufsausweis
IGeL	Individuelle Gesundheitsleistungen - Leistungen außerhalb des gesetzlichen Leistungsumfangs, in der Regel direkt durch den Patienten an den Arzt zu bezahlen
KBV	Kassenärztliche Bundesvereinigung
KIS	Krankenhausinformationssystem
KNA 2006	Kosten/Nutzen-Analyse 2006, erstellt durch Booz Allen Hamilton

KOM-LE	Gerichtete Kommunikation der Leistungserbringer
KTDD	Kostenträgerdatendienste
KV	Kassenärztliche Vereinigung
KVK	Krankenversicherungskarte
KV-SafeNet	Online-Lösung der Kassenärztlichen Vereinigungen zur Nutzung zentraler Leistungen, sicheren Kommunikation und Übertragung von Abrechnungsdaten
KZBV	Kassenzahnärztliche Bundesvereinigung
LAN	Local Area Network
LTE	Long Term Evolution - Funktechnologie im Frequenzbereich des ehemaligen analogen Fernsehens für die Breitbanddatenübertragung speziell in ländlichen Gebieten
MPLS	Multiprotocol Label Switching - Vermittlungsverfahren zur verbindungsorienterten Übertragung von Datenpaketen in verbindungslosen Netzen
NFD	Notfalldaten
NFDM	Notfalldatenmanagement
NHS	National Health Service - staatliche Gesundheitsorganisation in Großbritannien
PKI	Public Key Infrastruktur - zentrales Verzeichnis für die öffentlichen Schlüssel in asymmetrischen Verschlüsselungsverfahren
PMO	Projekt Management Office
PP	Protection Profile
PS	Primärsystem der Leistungserbringer
PVS	Praxisverwaltungssystem (in Arzt- oder Zahnarztpraxis)
QES	Qualifizierte elektronische Signatur gemäß Signaturgesetzt
RVO	Rechtsverordnung
SAK	Signaturanwendungskomponente
SGB	Sozialgesetzbuch
SICCT	Secure Interoperable Chip Card Terminal - Kartenterminal mit erweiterter Funktionalität
SMC-B	Security Module Card, Typ B - Authentifizierungskarte für Institutionen im Gesundheitswesen mit Signaturschlüsseln
SMC-K	Security Module Card (Konnektor)
SMC-KT	Security Module Card (Kartenterminal)
TestV	Testverordnung
TI	Telematikinfrastruktur
UFS	Update Flag Service - Service welcher Informationen zu Zugriffsanfragen anderer Systeme (z.B. für das Update der VSD) konsolidiert
UMTS	Universal Media Telecommunications Systems - Mobilfunkstandard zur Datenübertragung
USB	Universal Serial Bus - standardisierte serielle Schnittstelle zur Anbindung externer Geräte an Computer
VOL	Verdingungsordnung für Leistungen
VPN	Virtual Private Network
VSD	Versichertenstammdaten im Kontext der eGK

VSDD	Versichertenstammdatendienst
VSDM	Versichertenstammdatenmanagement
Ziellösung	Lösung des gematik Hauptprojekts
ZKA	Zentraler Kreditausschuss - Zentrale Einrichtung der deutschen Kreditinstitute ohne eigene Rechtspersönlichkeit
ZOD	Zahnärzte Online Deutschland - Online-Lösung zum Datenaustausch der Kassenzahnärztlichen Bundesvereinigung

Anlage 2

Governance

1. Operative Ebene

- In der gematik wird ein Technischer Leiter verantwortlich für die Organisation, die Steuerung und die Kontrolle der Entwicklungsprojekte sein.
- Der Leiter muss in jedem Fall eine kompetente und entsprechend erfahrene Person sein. Diese Person sollte von außen rekrutiert werden. Wenn die Stelle des Technischen Leiters nicht rechtzeitig mit einem neuen Mitarbeiter besetzt werden kann, soll diese übergangsweise an einen externen Mitarbeiter vergeben werden.
- Der Leiter und sein Stab müssen Kompetenzen mindestens in den Bereichen:
  - Kenntnisse der Ausschreibungsunterlagen („Lastenhefte“),
  - Ausschreibungs- und Vergaberecht,
  - Qualitätssicherung- und steuerung,
  - Terminmanagement,
  - Abnahme von (Teil-) Ergebnissen und
  - Verhandlungskompetenz mit den Auftraggebern, den Testregionen und anderen Beteiligten in ausgeprägter Form haben.
- Die Verantwortung für die Realisierung aller notwendigen Schritte zur Umsetzung des Vorgehens in Stufen ist auf der operativen Ebene angesiedelt.
- Innerhalb des Haushalts der gematik ist ein (Gesamt-) Budget für die Projekte zu bilden, so dass Beschaffungen etc. ohne großen Aufwand erfolgen können; Einzelfallentscheidungen sollten die Ausnahme bleiben.
- Die etablierten Budget- und Finanzcontrolling-Maßnahmen der gematik werden auf die Projekte angewandt.

2. Steuerungsebene

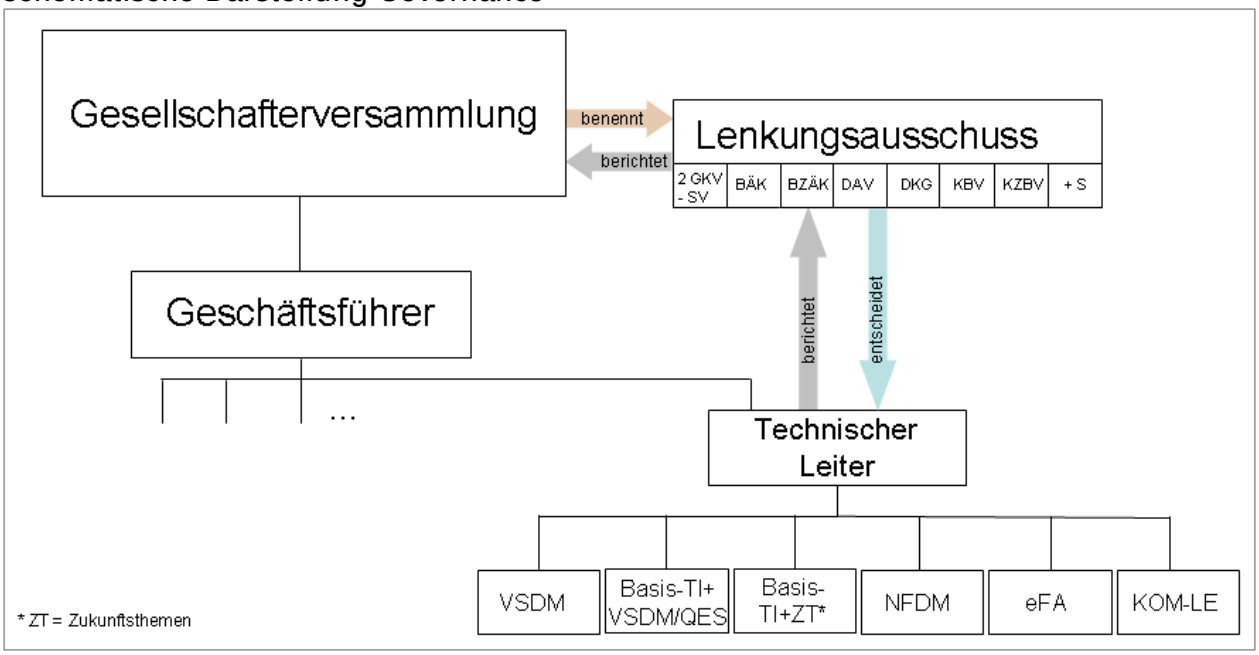
- Es wird ein Lenkungsausschuss gebildet. Der Lenkungsausschuss besteht aus acht Mitgliedern, gebildet mit je einem stimmberechtigten Verantwortlichen der Leistungserbringerseite, einem stimmberechtigten Verantwortlichen des GKV-Spitzenverbands sowie einem zusätzlichen Mitglied vom GKV-Spitzenverband ohne Stimmrecht.

- Jeder Gesellschafter benennt ein Mitglied des Lenkungsausschusses und einen Stellvertreter. Der GKV-Spitzenverband darf ein zusätzliches Mitglied und einen weiteren Stellvertreter ohne Stimmrecht benennen.
- Der Technische Leiter hat den Vorsitz im Lenkungsausschuss. Der Vorsitzende moderiert die Sitzungen und erstellt die entscheidungsreifen Vorlagen.
- Der Lenkungsausschuss tagt mindestens einmal pro Monat.
- Zu den Aufgaben des Lenkungsausschusses gehören u. a. Entscheidung (auch auf Antrag) über auftretende Probleme, die strategische Steuerung der Projekte sowie deren Kontrolle (z. B. Zeitpläne, Integration der Anwendungsprojekte etc.) und die Bestätigung der Ausschreibungstexte und (Zwischen-) Ergebnisse.
- Der Lenkungsausschuss berichtet der Gesellschafterversammlung über den Stand und den Fortgang der Arbeiten.
- Entscheidungen im Lenkungsausschuss werden von den Mitgliedern einstimmig getroffen.
- Wenn es im Lenkungsausschuss keine einstimmige Entscheidung gibt, wird der Beschlussgegenstand in der nächsten Sitzung ein weiteres Mal besprochen und abgestimmt. Die Zeit zwischen den Sitzungen soll der aktiven Lösungsfindung mit Hilfe einer Vermittlung durch den Vorsitzenden des Lenkungsausschusses dienen.

3. Schlichtungsebene

- Wird im Lenkungsausschuss keine Einigung erzielt, kann in der ersten Sitzung, welche sich mit dem Beschlussgegenstand beschäftigt, einstimmig eine Schlichtung einberufen werden. Ansonsten kann in der zweiten Sitzung analog der Schlichtungsordnung mit mindestens 50% der Stimmrechtsanteile die Schlichtung anberaumt werden. Bei Einberufung einer Schlichtung ist die Gesellschafterversammlung umgehend in Kenntnis zu setzen.
- Die Bestimmungen der Schlichtungsordnung vom 25.03.2011, insbesondere § 3 „Ablauf des Schlichtungsverfahren“, werden analog angewandt.

Schematische Darstellung Governance



Anlage 3

Fortentwicklung der Projekte

- Neben den bereits laufenden Projekten wird das Projekte Basis-TI neu aufgestellt.
- Die (Anwendungs-) Projekte bleiben wie bisher Teil der Aufgabe der gematik und unterliegen der fachlichen Steuerung durch den jeweilig beauftragten Gesellschafter.
- Das Basis-TI-Projekt wird zunächst in zwei Teilprojekte Basis-TI für VSDM und Basis-TI Infrastruktur umgewandelt. Dem Projekt Basis-TI für VSDM wird die Aufgabe qualifizierte elektronische Signatur (QES) zugeordnet.
- Während für VSDM der Projektleiter (PL) gesetzt ist, soll der Teil der Basis-TI, der für die 1. Stufe (VSDM mit korrespondierender Infrastruktur und QES) verantwortlich ist, mit einem PL der gematik besetzt werden.
- Der Teil der Basis-TI der sich mit der Infrastruktur und den Zukunftsthemen beschäftigt bleibt zunächst mit den bestehenden PL besetzt, soll aber unter der Projektleitung der gematik vereint werden.
- Die Anwendungsprojekte bzw. deren Gesellschafter entscheiden wann und unter welchen Bedingungen die Projekte nach außen vergeben werden.
- Die Projekte stimmen sich untereinander, mit dem Technischen Leiter und mit dem Lenkungsausschuss für mögliche Vergaben bzw. die damit korrespondierenden Entscheidungen ab.
- Alle Projekte sind gehalten, die Arbeiten so zügig wie möglich zu erledigen. Nach Fertigstellung der Arbeiten und der Schlussabnahme durch den LA und die GSV werden die entsprechenden Anwendungen im System getestet und schließlich für den Wirkbetrieb implementiert.
- Der Technische Leiter schlägt in Abstimmung mit der Geschäftsführung dem Lenkungsausschuss zu gegebener Zeit eine Fortentwicklung der Aufbauorganisation für die Entwicklungsprojekte vor.

Anlage 4

Teilnahmewettbewerb und Ausschreibungsbedingungen

1. Allgemeines

- Bei den Bewerbern ist sicherzustellen, dass sie die wesentlichen Abläufe innerhalb der gesetzlichen Krankenkasse und bei den Leistungserbringern (Ärzte, Zahnärzte, Krankenhäuser, Apotheker und psychologische Psychotherapeuten) kennen und wissen, welche Funktionen mit den Systemen unterstützt werden sollen.
- Die gematik sichert auch weiterhin die Interoperabilität und die Sicherheit des Systems. Bei der gematik bleiben auch die Funktionen Testung von Komponenten, Zulassung etc. angesiedelt.
- Alle Ergebnisse müssen gemeinfrei zur Verfügung stehen bzw. an die gematik übergehen.
- Das Verfahren muss diskriminierungsfrei durchgeführt werden.

2. Besonderes

- In der Ausschreibung wird dargestellt, dass es sich um ein stufenweises Vorgehen zum Einsatz und zur Nutzung der elektronischen Gesundheitskarte für verschiedene Zwecke im Gesundheitswesen handelt.
- Die erste Stufe (VSDM mit korrespondierender Infrastruktur und QES) wird verbindlich ausgeschrieben. Die Bieter werden verpflichtet, gleichzeitig eine qualifizierte elektronische Signatur (QES) anzubieten, deren Realisierung auch zeitlich versetzt aber so zeitnah wie möglich erfolgen kann. Der zeitliche Abstand zwischen Zuschlag zur ersten Stufe und VSDM-Testbeginn darf maximal 10 Monate, zwischen VSDM-Testbeginn und QES-Testbeginn maximal 10 Monate betragen.
- Die Ausschreibungen finden im Wettbewerb mit anschließender Verhandlungsphase statt.
- Es sollen mindestens zwei Konsortien als Wettbewerber beauftragt werden. Eine Monopolsituation ist zu vermeiden.
- In den Tests sind in der ersten Stufe Arzt-, Zahnarzt-, Psychotherapeutenpraxen, Berufsausübungsgemeinschaften und Krankenhäuser einzubeziehen.
- Die Tests sollen zumindest in zwei Regionen und mit jeweils mindestens fünf verschiedenen Arzt- und Zahnarztpraxisverwaltungssystemen sowie Krankenhausinformationssystemen durchgeführt werden. Die Krankenhäuser sollen unterschiedliche Versorgungsstufen zugeordnet sein. Es muss eine Universitätsklinik beteiligt sein.

- In der Ausschreibung ist sicherzustellen, dass:
  - die Nutzung einer QES für medizinische Anwendungen verbindlich festgelegt ist. Hierbei könnte ein Kriterium für die Vergabe die Angaben zur zeitlichen Einführung der QES sein;
  - die Mandantenfähigkeit der Konnektoren entsprechend der vorliegenden Konzeption gewährleistet wird;
  - das sogenannte Stand allone-Szenario auch in Zukunft realisiert werden kann;
  - Bestandsnetze mit ihren zugehörigen Anwendungen erreicht werden können;
  - eine Revision von Teilsystemen ebenso erfolgen kann, wie der Austausch wesentlicher Komponenten ohne größere Beeinträchtigung der Arbeitsprozesse für Leistungserbringer und Krankenkassen.
- Die Anbieter haben auch Zeitpläne mit wesentlichen Meilensteinen vorzulegen.

Anlage 5

Sonstige Festlegungen

- Die gematik muss die Konnektorspezifikation für eine erste Ausbaustufe (Netzkonnektor, Anwendungskonnektor, sichere Nachladeoption, Fachmodul VSDM, Umgebungsverwaltung, SAK) sowie die Kartenterminalspezifikation und die Spezifikationen der erforderlichen Sicherheitsmodule (SMC-K, ggf. modularisiert als SM-NK, SM-AK, SM-SAK, SM-KT) zügig fertigstellen.
- Parallel zur Fertigstellung der Spezifikationen müssen in enger Zusammenarbeit zwischen gematik (Projekte) und BSI die Zulassungsverfahren festgelegt und die entsprechenden Schutzprofile durch das BSI abgeschlossen und evaluiert werden.
- Bereitstellung und Ausgabe von HBAs und SMCs müssen für den Beginn des Testbetriebs sicher gestellt sein.
- Rechtzeitig vor dem Rollout zum Wirkbetrieb – also ca. Mitte der geplanten Tests – müssen alle Bedingungen zwischen den Beteiligten geklärt und die Verträge etc. abgeschlossen sein.
- Der GKV-SV sagt zu, dass die Finanzierungsvereinbarung für die gesamte 1. Stufe abgeschlossen werden kann.
- Neue Projekte die von der Gesellschafterversammlung beschlossen werden können jeder Zeit aufgesetzt und in die Aufbauorganisation integriert werden.