

## Einführung der elektronischen Gesundheitskarte

# Informationsbroschüre Erprobung Online-Rollout (Stufe 1)

Version: 1.0.0  
Stand: 04.04.2012  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: [gemInfo\_OnIRO1]  
Autor: Vergabeteam

---

## Dokumentinformationen

---

### Dokumentenhistorie

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	04.04.12		freigegeben durch den Lenkungsausschuss der gematik am 28.03.2012	gematik

---

## Inhaltsverzeichnis

---

<b>Dokumentinformationen .....</b>	<b>2</b>
<b>Inhaltsverzeichnis.....</b>	<b>3</b>
<b>1 Überblick zum Ausschreibungsgegenstand.....</b>	<b>5</b>
1.1 Ausgangssituation und Rahmenbedingungen.....	5
1.2 Überblick über die Telematikinfrastuktur .....	7
1.3 Test- und Erprobungsphasen.....	8
1.4 Fachbegriffe zur Telematikinfrastuktur .....	11
<b>2 Einbindung der Akteure.....</b>	<b>12</b>
<b>3 Testregionen.....</b>	<b>14</b>
<b>4 Funktionsumfang .....</b>	<b>15</b>
4.1 Funktionsübergreifender Datenaustausch VSDM.....	15
4.2 QES und digitale Signatur / Verschlüsselung .....	16
4.3 Anbindung über VPN-Zugangsdienst .....	18
4.4 Einbindung Bestandsnetze.....	18
4.5 Betrieb und übergreifendes IT Service Management der TI .....	19
4.6 Erprobung weiterer Anwendungen .....	20
4.7 Verlängerungsoptionen .....	20
<b>5 Beachtung systembedingter Anforderungen .....</b>	<b>21</b>
5.1 Produkttypen .....	21
5.1.1 Produkttypen der dezentralen Telematikinfrastuktur.....	21
5.1.2 Produkttypen der zentralen Telematikinfrastuktur.....	22
5.1.3 Produkttypen der fachanwendungsspezifischen Dienste .....	24
5.2 Losbezogene Leistungen.....	24
<b>6 Definierter Erprobungsumfang .....</b>	<b>30</b>
<b>7 Projektspezifische rechtliche Rahmenbedingungen .....</b>	<b>31</b>
7.1 SGB V.....	31
7.2 TestV .....	31
7.3 Datenschutz und Informationssicherheit .....	31
7.3.1 Sicherheitszertifizierungen der Auftragnehmer .....	32

7.3.2	Anforderungen an das Datenschutz- und Informationssicherheitsmanagement der Auftragnehmer .....	32
<b>8</b>	<b>Gesamtprojektverantwortung der Auftragnehmer .....</b>	<b>33</b>
<b>9</b>	<b>Memoranden.....</b>	<b>34</b>
9.1	Lose 1 & 2 .....	34
9.2	Los 3.....	35
	<b>Abkürzungsverzeichnis .....</b>	<b>37</b>

---

## 1 Überblick zum Ausschreibungsgegenstand

---

### 1.1 Ausgangssituation und Rahmenbedingungen

Im Zuge der Einführung der elektronischen Gesundheitskarte (eGK) nach § 291a SGB V (Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung) wird eine hierfür erforderliche interoperable und kompatible Informations-, Kommunikations- und Sicherheitsinfrastruktur (Telematikinfrastuktur i. S. v. § 291a Abs. 7 S.1 SGB V) als bundesweite „Gesundheitstelematik“ im deutschen Gesundheitswesen etabliert. Die Verantwortung für den Aufbau und den Betrieb dieser Telematikinfrastuktur sowie den Betrieb der Testinfrastruktur und der Testmaßnahmen obliegt der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH - gematik (§ 291a Abs. 7 S.2, § 291b SGB V, §§ 1 ff. Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte - TestV).

Die 37. Gesellschafterversammlung der gematik hat am 05. Dezember 2011 beschlossen, eine erste Stufe der Telematikinfrastuktur zu erproben (Online-Rollout (Stufe 1)).

Der Ausschreibungsgegenstand umfasst die Entwicklung, den Aufbau und den Betrieb einer Telematikinfrastuktur unter Einbindung der Akteure

- Leistungserbringer (Ärzte, Zahnärzte, Psychotherapeutenpraxen, Berufsausübungsgemeinschaften und Krankenhäuser) mit Primärsystemen
- Versicherte mit eGK
- Kostenträger und ihre Dienstleister
- Leistungserbringerorganisationen
- Hersteller von Komponenten und Diensten
- die gematik und deren Dienstleister mit Aufgabenstellungen in und für die Telematikinfrastuktur

in zwei Testregionen mit einem definierten (und ggf. erweiterbaren) Funktionsumfang. Im Vordergrund stehen der funktionsübergreifende Datenaustausch Versichertenstammdatenmanagement (VSDM), der Basisdienst QES und die Anbindung von Bestandsnetzen unter Beachtung systembedingter Anforderungen in drei Losen:

- Lose 1 / 2: Aufbau und Betrieb der dezentralen Komponenten und notwendiger Infrastrukturdienste sowie Durchführung der Erprobung in Testregionen,
- Los 3: Aufbau und Betrieb der zentralen Infrastrukturdienste und -umgebungen.

Der Erprobungsumfang bezieht alle gesetzlich Versicherten und eine definierte Auswahl von Leistungserbringern (Ärzte und Psychotherapeuten, Zahnärzte sowie Krankenhäuser) unter Beachtung projektspezifischer rechtlicher Rahmenbedingungen, insbesondere

- SGB V, insbesondere §§ 291 ff.,
- TestV,

ein.

Die Auftragnehmer tragen eine Gesamtprojektverantwortung im Sinne einer Ende-zu-Ende-Verantwortung für die ausgeschriebenen Leistungen und Funktionen, deren Verfügbarkeit und den Betrieb.

Die Rahmenbedingungen der Telematikinfrastruktur (TI) sind insbesondere:

- Datenschutz und Informationssicherheit
- Verfügbarkeit
- Skalierbarkeit
- Erweiterbarkeit
- Migrationsfähigkeit

Die im Rahmen der Erbringung der ausgeschriebenen Leistung zu überprüfenden Qualitätsziele sind insbesondere:

- Praxistauglichkeit
- Akzeptanz der Telematikinfrastruktur bei Versicherten und Leistungserbringern
- Funktionsfähigkeit der Betriebsprozesse in der konkreten Betriebsumgebung (Betriebstauglichkeit)
- Datenschutz
- Funktionalität (Funktionsfähigkeit des Systems und der Fachanwendungen)
- Interoperabilität
- Kompatibilität
- Stabilität und
- Sicherheit

der einzelnen Komponenten und Dienste sowie deren funktionales und technisches Zusammenwirken innerhalb der Telematikinfrastruktur.

Folgende Aspekte sind dabei für den Auftraggeber zusätzlich von zentraler Bedeutung:

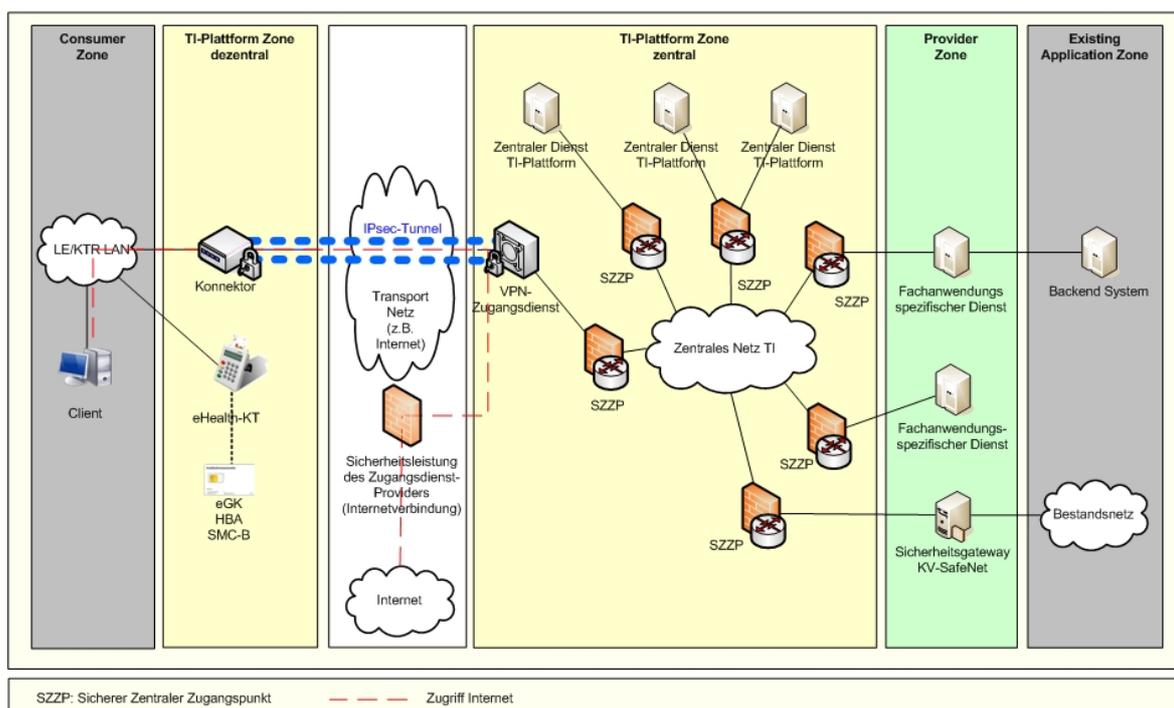
- Unterstützung bestehender Anwendungen und Netze durch die Leistungserbringer an den Beispielen Zugriff auf KZV-Portal über abgesicherte Internetverbindungen (Zahnärzte) und KV-Safenet (Ärzte)
- Einsatzfähigkeit des Lösungsansatzes im Umfeld größerer Leistungserbringerinstitutionen (wie z.B. Krankenhäuser oder medizinische Versorgungszentren), insbesondere durch den mandantenfähigen Konnektor
- Integration der QES im Konnektor
- Bereitstellung einer für den Leistungserbringer optionalen „Standalone-Lösung“ im Leistungserbringer-Einsatzbereich

## 1.2 Überblick über die Telematikinfrastruktur

Die Telematikinfrastruktur ist die bevorzugte Informations-, Kommunikations- und Sicherheitsinfrastruktur des deutschen Gesundheitswesens mit allen technischen und organisatorischen Anteilen. Die Telematikinfrastruktur vernetzt alle Akteure und Institutionen des Gesundheitswesens miteinander und ermöglicht dadurch einen organisationsübergreifenden Datenaustausch innerhalb des Gesundheitswesens. Die Telematikinfrastruktur unterstützt die Anwendungen der Versicherten gemäß §291a SGB V und bildet darüber hinaus die Plattform für weitere interoperable und kompatible IT-Anwendungen im deutschen Gesundheitswesen. Die TI enthält die Komponenten und Dienste der TI-Plattform, die Fachdienste und die Fachmodule.

Die TI-Plattform als anwendungsunabhängiger Teil der TI dient der Unterstützung der Fachanwendungen mit allen nötigen technischen und organisatorischen Anteilen (z.B. Betrieb). Enthalten sind alle nötigen Schnittstellen- und Ablaufdefinitionen für die Fachanwendungen auf den Schichten Netzwerk, Infrastruktur und Anwendungsunterstützung.

Um die Architektur der Telematikinfrastruktur darzustellen, wird im Folgenden die Netzwerk-Sicht des Gesamtsystems grob vereinfacht dargestellt. Abbildung 1 zeigt über die Architektur-Zonen hinweg die Netzsegmente und Verbindungen.



**Abbildung 1: Logische Darstellung der Netzwerktopologie der TI über die Zonen**

Die Schnittstelle der TI zum Clientsystem liegt in der Verantwortung der Fachanwendungen. Clientsysteme sind in diesem Kontext Primärsysteme (Praxisverwaltungssysteme (PVS) und Krankenhausinformationssysteme (KIS)), welche mit dem Konnektor und dem Mobilten Kartenterminal interagieren, um fachliche Anwendungsfälle durchzuführen. Dabei greifen sie entweder direkt auf die dezentralen Außenschnittstellen der TI-Plattform oder auf ein Fachmodul zu.

Ein fachanwendungsspezifischer Dienst ist ein System, das an die TI-Plattform angeschlossen ist und im Rahmen fachlicher Anwendungsfälle als Provider auftritt. Der fachanwendungsspezifische Dienst nutzt Infrastruktur- und Netzwerkdienste der TI-Plattform. Fachanwendungsspezifische Dienste stellen die Integrationsschicht für Backendsysteme und Bestandsnetze (Existing Application Zone) dar.

Der nachfolgend skizzierte Informationsfluss beschreibt ein typisches Kommunikationsmuster in der Telematikinfrastruktur.

- Clientsysteme (Consumer Zone) kommunizieren über das LAN des Leistungserbringers mit dem Konnektor, welcher auf verschiedenen Ebenen Aufgaben wahrnimmt.
  - Auf Netzwerk-/ Infrastrukturebene werden Leistungen erbracht wie z.B. Routing, Etablierung von VPN Tunnels, Zeitsynchronisation, DNS.
  - Auf der anwendungsunterstützenden Ebene werden anwendungsnahe, gekapselte Funktionen bereitgestellt, wie z.B. der kontrollierte Zugriff auf Kartenfunktionalität oder Sicherheitsleistungen wie Signatur- und Verschlüsselung.
  - Auf der Ebene der Fachanwendungen beinhaltet der Konnektor auch rein fachliche Logik, welche die fachlichen Anwendungsfälle umsetzt.
- Der Konnektor (TI-Plattform Zone dezentral) baut einen IPSec-Tunnel zu einem VPN-Zugangsdienst auf und verbindet damit das Leistungserbringer-LAN mit der zentralen TI, im Standardfall über das Internet.
- Über den Zugangsdienst wird das Zentrale Netz der TI erreicht, welches als Backbone Zugang zu den zentralen Diensten (TI-Plattform Zone zentral) und den fachanwendungsspezifischen Diensten (Provider Zone) bietet.

Im Rahmen einer Systemzerlegung ist die Telematikinfrastruktur in einzelne Produkttypen zerlegt worden. Die Produkttypen werden in Kapitel 5 im Zusammenhang mit der Zuordnung zu den Losen 1-3 dargestellt.

### **1.3 Test- und Erprobungsphasen**

Die ausgeschriebenen Leistungen sind ein Teil der umfänglichen Einführung der Telematikinfrastruktur und bieten eine vorgezogene Erprobung des Produktivbetriebs mit eingeschränkter Teilnehmerzahl unter Verwendung von Echtdaten. Ziel dieser Erprobungsphase ist die Prüfung der Betriebseignung unter realen Bedingungen, so dass gravierende Interoperabilitäts- und Betriebsprobleme bereits vor der Aufnahme des Produktivbetriebs entdeckt und behoben werden können. Die Erprobung bildet den Teil der Testmaßnahmen nach TestV ab, der mit Echtdaten durchgeführt wird.

Die Erprobung erfolgt in der Wirkbetriebsumgebung und sieht Smartcards (z. B. eGK/HBA) mit Echtdaten und die Einbindung der Versicherten im regulären Geschäftsprozess bei den Leistungserbringern vor.

Als Wirkbetrieb wird die reguläre Betriebsphase bezeichnet, in der für Anwender die geplanten Funktionen zur Verfügung gestellt werden und der Einsatz von Echtdaten erfolgt. Voraussetzung für die Erprobung ist der Abschluss von Tests durch den Auftragnehmer und anschließenden Produkt-Zulassungen bei der gematik.

Der Produktivbetrieb der TI ist die finale Phase des Wirkbetriebs, in der allen Anwendern die geplanten Anwendungen zur Verfügung gestellt werden und für die der vollständige uneingeschränkte Betrieb vorgesehen ist. Alle Komponenten und Dienste der TI und Fachanwendungen müssen in der Produktivphase vollständig zugelassen sein.

Die Erkenntnisse aus der Erprobung bilden die Grundlage für die fachliche, technische und logistische Umsetzung des bundesweiten Rollouts der Online-Anwendungen der eGK. Gegenstand dieses Vergabeverfahrens ist nicht der bundesweite Rollout der Telematikinfrastruktur.

Die ausgeschriebenen Projektteile werden in verschiedenen Phasen umgesetzt. Die wesentlichen Phasen sind:

- Aufbauphase (Entwicklungs- und Testphase)
- Erprobungsphase

Abbildung 2 gibt einen Überblick über die Phasen und verwendeten Begriffe.

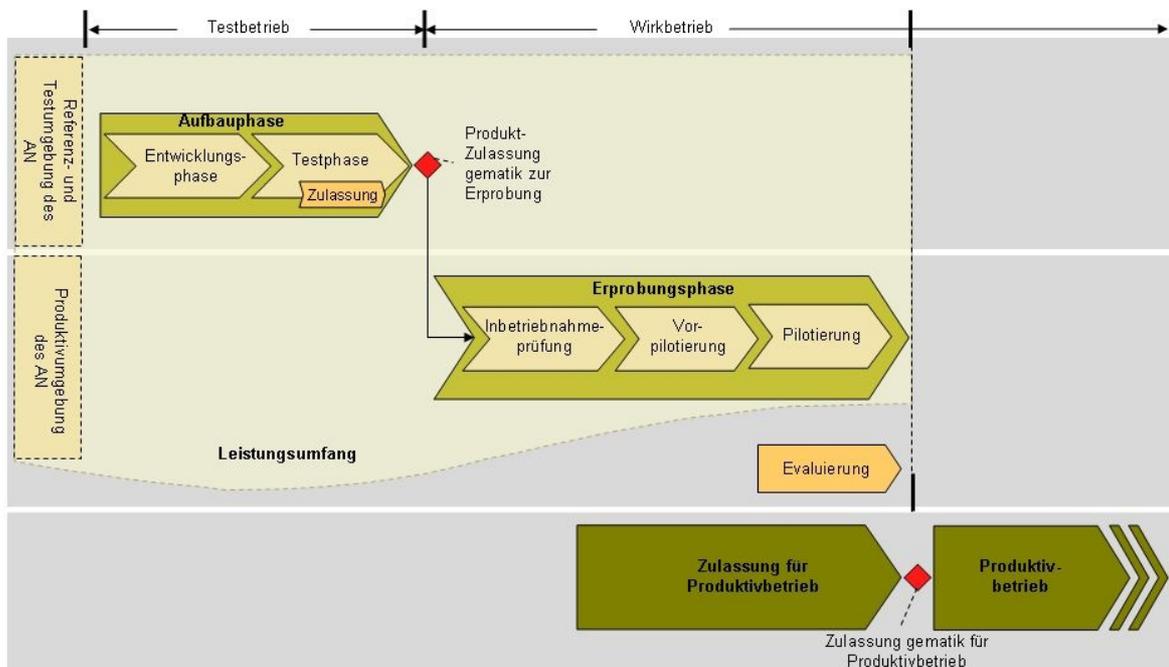


Abbildung 2: Phasendarstellung Test und Erprobung

## Aufbauphase

Um die Qualitätsziele zu überprüfen, müssen die Komponenten und Dienste im Vorfeld der Erprobung getestet werden. Die Tests vor der Erprobung sind eigenverantwortlich durch den Auftragnehmer nach Vorgaben des Auftraggebers durchzuführen. Der Auftragnehmer muss der gematik die Erfüllung der Qualitätsziele nachweisen.

Der Umfang der Tests vor der Erprobung wird in spezifischen Testkonzepten durch den Auftraggeber in den Vergabeunterlagen festgelegt. Typischerweise umfassen diese

- Funktionstests,
- Interoperabilitätstests,

- Leistungstests und
- Sicherheitsrobustheitstests.

Der Nachweis der Testdurchführung und die Testergebnisse sind dem Auftraggeber nach Abschluss jedes Tests zu erbringen bzw. zu übergeben.

Die Tests sollen in einer oder mehreren Umgebungen (Referenz- und Testumgebung) erfolgen, die der Auftragnehmer aufbaut und betreibt. An diese Umgebungen müssen Dritte durch den Auftragnehmer angebunden werden, wie z. B. die Fachdienste der Kostenträger. Um die Vorgaben der gematik zu erfüllen, sind voraussichtlich Testtreiber, Testwerkzeuge, Simulatoren und Referenzimplementierungen einzusetzen. Diese Vorgaben werden in den Vergabeunterlagen definiert.

### **Erprobungsphase**

Die Aufgaben des Auftragnehmers in der Erprobung werden in spezifischen Testkonzepten durch den Auftraggeber in den Vergabeunterlagen festgelegt. Typischerweise umfassen diese:

- Inbetriebnahmeprüfung,
- Vorpilotierung und
- Pilotierung.

Die Pilotierung ist Teil der Erprobungsphase, in dem für eine größere Anzahl von Anwendern neue Funktionen bereit gestellt werden, die sie im gewohnten Umfeld und ohne besondere Vorkenntnisse in Anspruch nehmen.

Ziel der Pilotierung ist u. a. die Untersuchung des Betriebsverhaltens (z. B. Wartung) und Lastverhaltens (z. B. Antwortzeitverhalten und Stabilität) der neuen Funktionen und der damit verbundenen Infrastruktur. Voraussetzung für die Pilotierung sind stabile Entwicklungen und Umsetzungen, deren Reife in Tests zuvor nachgewiesen werden konnten, und dass für diese eine Produkt-Zulassung für die Erprobung erteilt wurde.

Der Pilotbetrieb legt den Schwerpunkt nicht auf die Fehlerermittlung, sondern soll Erkenntnisse zur Stabilität und Betriebbarkeit unter realen Bedingungen liefern. Trotzdem können in Ausnahmefällen Erkenntnisse aus der Erprobungsphase dazu führen, dass Anpassungen an Komponenten, Diensten und Anwendungen notwendig sind.

Die Erprobung findet in der vom Auftragnehmer zu schaffenden Wirkbetriebsumgebung statt, in der Echtdateien in realen fachlichen Abläufen verarbeitet werden. In dieser Umgebung müssen das notwendige Datenschutz- und angemessene Sicherheitsniveau sichergestellt sein. Es werden keine Testfälle gezielt zur Ausführung gebracht.

### **Zulassung und Durchführung von Tests und Zulassung durch den Auftraggeber**

Der Auftraggeber behält sich vor, die vom Auftragnehmer durchgeführten Tests zu wiederholen und weitere eigene Tests durchzuführen. Der Auftragnehmer muss ihm dies ermöglichen und ihn im angemessenen Rahmen dabei unterstützen.

Der Auftraggeber wird im Zuge der Zulassung von Komponenten und Diensten Tests durchführen. Der Auftragnehmer ist verpflichtet, diese Tests in angemessenem Umfang zu unterstützen.

Eine Bereitstellung bzw. Übergabe der vom Auftragnehmer beschafften Mittel für die Durchführung der Testmaßnahmen an den Auftraggeber zur (Weiter-)Nutzung ist in geeigneter Form und Umfang erforderlich.

Die Form der Unterstützung und möglicher Zulieferungen des Auftragnehmers werden in den Vergabeunterlagen näher beschrieben.

Für den Betrieb der Dienste und Komponenten erteilt gemäß der TestV die gematik eine Zulassung auf Basis der erbrachten Nachweise (§ 3a TestV). Die Zulassung wird erteilt, wenn die Komponenten und Dienste für die Erprobung funktional, interoperabel und sicher sind. Die Zulassung kann im Ermessen der gematik ggf. unter den Voraussetzungen des § 3a Abs. 3 TestV vorläufig und befristet erteilt werden; es besteht kein Anspruch auf Erteilung einer befristeten vorläufigen Zulassung. Die Sicherheitszertifizierungen erfolgen hierbei durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) (vgl. § 3a Abs. 2 S. 3 TestV).

### **Vorbereitung Übergang bundesweiter Rollout**

Die Konzepte und Spezifikation der Komponenten und Dienste werden nach Fertigstellung durch die gematik veröffentlicht und allen Interessierten zugänglich gemacht. Parallel dazu werden Zulassungsverfahren für Komponenten und Dienste (Produkttypen) veröffentlicht. Im Zuge der Aufbau- und Erprobungsphase kann es ggf. zu Anpassungen der Spezifikationen aufgrund von Verbesserungen oder Fehlern kommen. Diese Anpassungen werden veröffentlicht. Während der Auswertung der Erprobungsmaßnahmen wird die Anbieterzulassung hinsichtlich der gewonnenen Erkenntnisse finalisiert. Vor dem bundesweiten Rollout werden die Zulassungsverfahren für die einzelnen Produkttypen durchgeführt.

## **1.4 Fachbegriffe zur Telematikinfrastruktur**

Erläuterungen der Fachbegriffe zur TI sind zu finden unter  
[http://www.gematik.de/cms/de/spezifikation/erlaeuterungen\\_nutzer/glossar/glossar.jsp](http://www.gematik.de/cms/de/spezifikation/erlaeuterungen_nutzer/glossar/glossar.jsp)

---

## 2 Einbindung der Akteure

---

Das übergeordnete Ziel der Beschaffung besteht darin, kurzfristig in zwei Testregionen eine definierte Anzahl von Akteuren in eine tragfähige Telematikinfrastuktur einzubinden und damit Erfahrungen mit dem definierten Funktionsumfang der eGK zu sammeln. Bei diesen Akteuren handelt es sich um

- Leistungserbringer (Ärzte, Zahnärzte, Psychotherapeutenpraxen, Berufsausübungsgemeinschaften und Krankenhäuser) mit Primärsystemen,
- Versicherte mit eGK,
- Kostenträger und ihre Dienstleister,
- Leistungserbringerorganisationen,
- Hersteller von Komponenten und Diensten,
- die gematik und deren Dienstleister mit Aufgabenstellungen in und für die Telematikinfrastuktur.

Die geplante Vergabe erfolgt in drei Losen: zwei Lose für den Aufbau und Betrieb für jeweils eine Testregion sowie ein Los für den Aufbau und Betrieb des zentralen Netzes und der einmaligen Dienste. Der Aufbau und der Betrieb umfassen die vollständige Bereitstellung aller erforderlichen Komponenten und Dienste für die Erprobung zumindest der Fachanwendung VSDM sowie des Basisdienstes QES in den Testregionen. Der Auftragnehmer verantwortet dabei auch den operativen IT-Betrieb der Komponenten und Dienste. Konkrete Vorgaben werden in den Vergabeunterlagen dargestellt.

Der Inhalt der Lose setzt sich im Wesentlichen wie folgt zusammen:

Die zwei Lose für die Testregionen beinhalten jeweils Konzeption, Aufbau und Umsetzung von Erprobungsverfahren mit definierter Anzahl von Leistungserbringern. Die späteren Auftragnehmer haben eine ganzheitliche Aufgabenstellung zu erfüllen, die insbesondere

- die Betreuung der Testteilnehmer und Testregionen,
- die Bereitstellung und den Betrieb der notwendigen dezentralen Komponenten (inklusive QES-Funktionalität),
- die Nutzung der Fachanwendung VSDM,
- die Bereitstellung und den Betrieb des Zugangsnetzes inklusive Infrastrukturdienste,
- die Bereitstellung und den Betrieb des Intermediärs sowie
- die Sicherstellung der Nutzungsoption eines sicheren Internetzugangs durch die Testteilnehmer

umschließt. Zur Bereitstellung der Infrastruktur für die Teilnehmer wird es zudem erforderlich sein, an den bestehenden Anwendungen und Komponenten für dezentrale Einsatzumgebungen Anpassungen vorzunehmen.

Das dritte Los umfasst die Konzeption, den Aufbau und den Betrieb der zentralen Infrastrukturdienste, wie das Zentrale Netz mit Infrastrukturleistungen (z. B. NTP, DNS), PKI und ggf. weitere zentrale Dienste. Weiterhin ist die Anbindung der Betreiber der Fachdienste VSDM der Krankenkassen sowie die Anbindung des KV-SafeNet-Backbones als Beispiel für bestehende Netze der Leistungserbringer Bestandteil dieses Loses. In diesem Kontext ist die ganzheitliche Aufgabenstellung des Auftragnehmers für Los 3, eine skalierbare und stabile Infrastruktur zur Nutzung in den beteiligten Testregionen für die Krankenkassen und deren beauftragte Dienstleister sowie der Auftragnehmer der Lose 1 und 2 bereitzustellen.

Die Betriebsführung und das betriebliche Monitoring ist Bestandteil aller drei Lose. Die Auftragnehmer sind zudem verantwortlich für die Bereitstellung von Supportleistungen für die von ihnen bereitgestellten Dienste und Komponenten. Darüber hinaus müssen die Auftragnehmer im Rahmen des geschuldeten Funktionsumfangs eine Ende-zu-Ende-Support-Verantwortung gegenüber den Akteuren übernehmen.

---

## 3 Testregionen

---

Gemäß § 7 TestV (alte Fassung) wurden durch das BMG im Benehmen mit den obersten Landesbehörden (also den jeweils zuständigen Landesministerien) Testregionen bestimmt, in denen die Erprobung der elektronischen Gesundheitskarte und ihrer Anwendungen erfolgen soll.

Die heute vorhandenen 6 Testregionen sind:

- Bochum-Essen (Nordrhein-Westfalen)
- Flensburg (Schleswig-Holstein)
- Wolfsburg (Niedersachsen)
- Ingolstadt (Bayern)
- Löbau-Zittau (Sachsen)
- Trier (Rheinland-Pfalz)

Die Auswahl der Testregion für die ausgeschriebenen Leistungen in Los 1 und 2 erfolgt basierend auf dem Beschluss der 37. GSV der gematik und unter Beachtung der Regelungen der TestV. Die Erprobungsmaßnahmen sollen in zwei Testregionen durchgeführt werden (Los 1 & Los 2). Jeder Bewerber muss in zwei Testregionen die definierten Testziele erfüllen können. Wenn die definierten Testziele nicht anders erreicht werden können, ist auch die Verbindung von mehreren Testregionen möglich. Eine Beauftragung kann nur für eine Testregion oder Testregionsverbindung je Bewerber erfolgen. Für ein und dieselbe Testregion können nicht zwei Bewerber den Zuschlag erhalten.

Los 3 ist übergeordnet und ist unabhängig von der Auswahl der Testregionen.

---

## 4 Funktionsumfang

---

Die zu erprobende Fachanwendung der Stufe 1 ist das Versichertenstammdatenmanagement (VSDM) mit korrespondierender Infrastruktur. Darüber hinaus muss die Nutzung eines Basisdienstes „Qualifizierte elektronische Signatur (QES)“ erprobt werden. Der grundsätzlich vorgesehene Funktionsumfang wird in den nachfolgenden Abschnitten dargestellt.

Die Architektur der dezentralen Komponenten der Telematikinfrastruktur ist so gestaltet, dass ein gesicherter Internetzugang über die Telematikinfrastruktur (VPN-Zugangsnetz) möglich ist. Die Auftragnehmer der Lose 1 & 2 müssen den teilnehmenden Leistungserbringern einen entsprechenden sicheren Internetzugang anbieten.

### 4.1 Funktionsübergreifender Datenaustausch 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 Prüfung wird durch das Primärsystem des Leistungserbringers initiiert. Das Primärsystem ist ein IT-System, das bei einem Leistungserbringer eingesetzt wird. Dabei wird im Rahmen der Erprobung zwischen den beiden Ausprägungsformen Praxisverwaltungssystem (PVS) für niedergelassene Ärzte, Psychotherapeuten und Zahnärzte sowie Krankenhausinformationssystem (KIS) differenziert.

Die Onlineprüfung umfasst folgende drei Schritte:

1. Prüfung der Gültigkeit der eGK (Prüfung Authentifizierungszertifikat)
2. Prüfung der Aktualität der Daten auf der eGK
3. Aktualisierung der Daten auf der eGK, sofern neuere Daten durch den Kostenträger bereitstehen

Sofern der Versuch zur Onlineprüfung fehlschlägt, muss dieser entsprechend der gesetzlichen Zielsetzung (SGB V) 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 wird zusätzlich zur Speicherung auf der eGK auch direkt dem PVS des Leistungserbringers bereitgestellt.

Die Überprüfungsmöglichkeit des Status des Authentifizierungszertifikats der eGK Gen 1plus muss zudem gegeben sein. 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 und -zahnärztlichen Versorgungsbereich besteht für den stationären Bereich keine gesetzliche Verpflichtung zur Onlineprüfung der Versichertenstammdaten auf der eGK. Die Krankenhäuser mit ihren Krankenhausinformationssystemen (KIS) 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 der Leistungserbringer nicht an das Netz der Telematikinfrastruktur angebunden ist (§ 291 Abs. 2b S. 2 SGB V), wird durch die Umsetzung eines sogenannten Standalone-Szenarios Rechnung getragen. Die Wahl, das Standalone-Szenario zu nutzen, obliegt dem Leistungserbringer. Eine repräsentative Anzahl von Leistungserbringern muss das Standalone-Szenario erproben. Die Anzahl wird in der Leistungsbeschreibung festgelegt. Die Umsetzung des Standalone-Szenarios muss grundsätzlich die Anforderung an eine Trennung des Primärsystems zur TI erfüllen. Dabei kann der Leistungserbringer zwischen echter physischer Trennung und rein logischer Trennung wählen. Die eGK Gen 1plus dient bei Nutzung des Standalone-Szenarios als Transportmedium zur Übergabe des Prüfungsnachweises und der aktualisierten Versichertenstammdaten an das Primärsystem.

Es muss zudem zur Abbildung der Fachanwendung VSDM mit folgenden Funktionen zur Verfügung stehen:

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

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

## **4.2 QES und digitale Signatur / Verschlüsselung**

### **QES**

Bei vielen Dokumenten im Gesundheitswesen wird Rechtssicherheit (hier insbesondere Beweissicherheit) benötigt. Aufgrund dessen ermöglicht die Telematikinfrastruktur (TI) sowohl die Erstellung von qualifizierten elektronischen Signaturen mit dem HBA als auch die Prüfung von qualifizierten elektronischen Signaturen gemäß § 2 Nr. 3 des Gesetzes über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG). Die

Unterstützung für den HBA umfasst auch die HBA-Vorläuferkarten (HBAqsig und ZOD-Karten ab Version 2.0).

Die folgenden Funktionen der TI-Plattform müssen den Leistungserbringern zur Nutzung durch Primärsysteme (Praxisverwaltungssoftware (PVS) und Krankenhausinformationssysteme (KIS)) und spätere Fachanwendungen zur Verfügung gestellt werden.

- Signaturerstellung und -prüfung mit HBA und HBA-Vorläuferkarten sowie Signaturprüfung für die Dokumentformate PDF/A, TEXT, TIFF und XML (gemäß zu benennender XML-Schemata)
- Darstellung des Inhalts der zu signierenden / signierten Daten (Trusted Viewer)
- Nachladbarkeit weiterer durch QES zu unterstützender XML-Schemata
- Signieren und Prüfen von Dokumenten in den genannten Formaten durch mehrere Personen (Parallel- / Gegensignatur)

Falls keine Online-Prüfung der verwendeten Zertifikate möglich ist, muss die Erstellung und Prüfung von Signaturen trotzdem möglich sein. Es werden dann alle Schritte ausgeführt, die ohne Zugang zu den zentralen Diensten der TI-Plattform möglich sind. Der Anwender wird durch die Anwendung in geeigneter Form (z. B. per Anzeige etc.) darüber informiert, welche Schritte nicht geprüft werden konnten.

Dem Signaturersteller muss die Möglichkeit gegeben werden, die Erstellung einer QES ohne Anzeige im Trusted Viewer auszulösen.

Die Signaturanwendungskomponente (SAK) i. S. v. § 2 Nr. 11 SigG muss zentral auf dem Konnektor betrieben werden, die sicheren Anzeigeeinheiten sind auf den Arbeitsplätzen zu betreiben, die verwendeten Kartenterminals sind LAN-gebunden.

Diese SAK muss mandanten- und multiusertauglich sein, wobei auf eine eigene Benutzerwaltung zu verzichten ist.

Für die Signaturerstellung und -prüfung müssen Standardverfahren eingesetzt werden.

### **QES Stapelsignatur (gemäß TR-03114)**

Um reibungslose geschäftliche Abläufe zu unterstützen, stellt die TI für die Erstellung qualifizierter elektronischer Signaturen (QES) gemäß SigG / SigV Mechanismen zur Stapelsignatur bereit. Dadurch wird ermöglicht, dass mehrere Dokumente durch einen HBA mit nur einer PIN-Eingabe (ohne wiederholte PIN-Eingabe) in direkter zeitlicher Abfolge jeweils mit einer eigenen qualifizierten Signatur signiert werden können.

Folgende Funktionalitäten müssen hierbei gegeben sein:

- Erstellung und Prüfung von QES für in Stapeln organisierte Dokumente
- Vor dem Auslösen des Signaturlaufs können die Dokumente einzeln im Trusted Viewer angezeigt und in den Signaturlauf ein- oder ausgeschlossen werden.
- Ein Stapel muss Dokumente aller unterstützter Dokumentformate gleichzeitig enthalten können.

## **Einfache digitale, elektronische Signatur**

Digitale Signaturen gewährleisten die Integrität und Authentizität von Daten. Die folgenden Funktionen der TI-Plattform sollen im Online-Rollout (Stufe 1) durch Primärsysteme und Fachmodule genutzt werden können:

- Erstellung einer einfachen digitalen, elektronischen Signatur von XML-Dokumenten, MIME-Objekten, PDF/A-Objekten, TEXT, Binärdaten
- Prüfung einer einfachen digitalen, elektronischen Signatur von XML-Dokumenten, S/MIME-Objekten, PDF/A-Objekten, TEXT, Binärdaten

Falls keine Online-Prüfung der verwendeten Zertifikate möglich ist, muss die Erstellung und Prüfung von Signaturen dennoch möglich sein. Für die Signaturerstellung und -prüfung müssen Standardverfahren eingesetzt werden. Die Software zur Signaturerstellung muss im Konnektor ablaufen.

## **Verschlüsselung**

Zum Schutz der Vertraulichkeit von Daten werden diese verschlüsselt. Hierzu sollen hybride Verfahren basierend auf X.509-Zertifikaten genutzt werden.

Die folgenden Funktionen der TI-Plattform können durch Primärsysteme der Leistungserbringer und Fachmodule genutzt werden:

- Verschlüsselung von XML-Dokumenten, MIME-Objekten, PDF/A-Objekten und bei konkretem Bedarf von Binärdaten (hybrides Verfahren).
- Entschlüsselung von XML-Dokumenten, S/MIME-Objekten, PDF/A-Objekten und bei konkretem Bedarf von Binärdaten (hybrides Verfahren).

Für die Verschlüsselung müssen Standardverfahren gemäß der TR-03116 des BSI eingesetzt werden. Es ist möglich, im Rahmen der hybriden Verschlüsselung die Objekte für mehrere X.509-Zertifikate zu verschlüsseln. Die Verschlüsselung von Objekten muss auch möglich sein, falls keine Verbindung zur zentralen TI besteht, sofern alle dazu notwendigen Informationen offline zur Verfügung stehen.

## **4.3 Anbindung über VPN-Zugangsdienst**

Ein VPN-Zugangsdienst ermöglicht Leistungserbringern unter Verwendung des Konnektors und der dazu nötigen Telekommunikationskomponenten den Zugang zu dem geschlossenen Netz der TI über ein VPN und damit die Nutzung der zentralen und fachanwendungsspezifischen Dienste sowie die Nutzungsoption für einen gesicherten Internetzugang.

## **4.4 Einbindung Bestandsnetze**

Während der Erprobung soll die Nutzung bestehender Anwendungen und Netze durch die Leistungserbringer an den Beispielen KZV-Portal Zahnärzte über abgesicherte Internetverbindungen und KV-Safenet realisiert werden. Die Anbindung des KV-SafeNet-Backbones erfolgt über ein Sicherheitsgateway aus dem zentralen Netz der TI. Die

Leistungserbringer sollen die sichere Internetanbindung als Leistungsbestandteil der Zugangsnetz-Provider der TI nutzen können.

Die Nutzung bestehender Anwendungen durch die Leistungserbringer – wie zum Beispiel KZV-Portal Zahnärzte – soll weiterhin auf der Basis bestehender Internetzugänge möglich sein.

## **4.5 Betrieb und übergreifendes IT Service Management der TI**

Es wird ein an ITILv3 angelehntes übergreifendes IT Service Management (ITSM) mit übergreifenden Betriebsprozessen in den Vergabeunterlagen definiert, das die Interaktion zwischen den beteiligten Akteuren untereinander regelt. Die Einzelheiten werden im Verhandlungsverfahren bestimmt.

Im Rahmen des übergreifenden IT Service Managements der Telematikinfrastruktur sind betriebsunterstützende Systeme vorgesehen, diese umfassen insbesondere:

- Ein Informationssystem zur Bereitstellung aktueller Informationen über die Verfügbarkeit und Leistungsfähigkeit der TI und derer Bestandteile zur Lokalisierung von Störungsursachen

Die Störungsampel dient allen Supportleistenden der TI zur Lokalisierung der Ursache von Störungen. Sie zeigt Nichtverfügbarkeiten, Performanceeinbrüche und Störungen der zentralen TI-Plattform an und unterstützt damit die für den Betrieb Verantwortlichen bei der Fehleranalyse einer aufgetretenen Störung. Die Anbieter von Diensten sind für die aktuelle Bereitstellung von Daten über den Funktionsstatus und die Leistungsfähigkeit ihrer Dienste zur Störungsampel verantwortlich. Dazu müssen sie ihre Dienste technisch überwachen.

- Informationsquelle zur effizienten Behandlung TI-übergreifender Störungen beim Anwender (Wissensdatenbank)

Die Wissensdatenbank enthält eine Aufschlüsselung der in den Spezifikationen enthaltenen Fehlermeldungen, die dem Nutzer oder dessen Supportpartner für die dezentralen Komponenten im Störfall angezeigt werden oder die in technischen Logfiles enthalten sind. Die Bedeutung der Fehlermeldung und die möglichen Ursachen werden erklärt und der Lösungsverantwortliche benannt.

- Informationssystem zur Auswirkungsanalyse von Änderungen und Störungen an der TI (Configuration Management System)

Die Konfigurationsdatenbank dient als Informationsquelle u. a. für die Planung größerer Änderungen, um beispielsweise zu ermitteln, welche Produkte welcher Hersteller und Anbieter von einer Änderung betroffen sind und wie viele Produktinstanzen betroffener Produktversionen produktiv sind. Sie wird durch den Auftraggeber genutzt.

- Informationssystem über geplante und durchgeführte Changes und Releasewechsel (Change- und Release-Kalender)

Im Change- und Release-Kalender werden alle in Planung, Prüfung oder Umsetzung befindlichen sowie abgeschlossene übergreifende Changes und Releasewechsel hinsichtlich ihrer zeitlichen Umsetzungsplanung vermerkt. Damit dient der Kalender sowohl als Planungsinstrument im übergreifenden Change

Management, um Prioritäten oder Abhängigkeiten von Changes untereinander bewerten zu können, als auch als Unterstützung für das anbieterspezifische Change Management.

Die Einzelheiten werden im Verhandlungsverfahren geklärt.

#### **4.6 Erprobung weiterer Anwendungen**

Der Auftraggeber behält sich vor, weitere Anwendungen auf der aufgebauten Infrastruktur zu erproben. Dies erfolgt durch Einzelabruf aus der jeweils zu schließenden Rahmenvereinbarung. Die Einzelheiten werden im Verhandlungsverfahren festgelegt.

#### **4.7 Verlängerungsoptionen**

Der Auftraggeber behält sich vor, bei Bedarf nach Abschluss der Erprobung bestimmte Bestandteile der Telematikinfrastruktur für eine Übergangszeit im Produktivbetrieb weiter betreiben zu lassen.

---

## 5 Beachtung systembedingter Anforderungen

---

Auf Basis der Beschreibung der Telematikinfrastuktur in Kapitel 1.2 erfolgt nun die Beschreibung der einzelnen Produkttypen und deren Zuordnung zu den Losen als Bestandteil der Leistung.

### 5.1 Produkttypen

Im Rahmen einer Systemzerlegung ist die Telematikinfrastuktur in einzelne Produkttypen aufgeteilt worden. Im Folgenden werden die einzelnen Produkttypen kurz beschrieben und in die Bereiche Produkttypen

- der dezentralen Telematikinfrastuktur,
- der zentralen Telematikinfrastuktur sowie
- der fachanwendungsspezifischen Dienste

gruppiert.

#### 5.1.1 Produkttypen der dezentralen Telematikinfrastuktur

Der **Konnektor** stellt Dienste für die Authentisierung, die Ansteuerung der Kartenterminals, den Zugriff auf Kartenterminals, den Zugriff auf beteiligte Karten und die Prüfung von Zertifikaten bereit. Er verfügt über Schnittstellen zu den Client-Systemen (u. a. Primärsystem). Der Konnektor stellt die Verbindung zum zentralen Netz der TI über ein VPN her und ermöglicht die Nutzung von zentralen Diensten und fachanwendungsspezifischen Diensten der TI und die Nutzung bestehender Anwendungen der Leistungserbringer. Dafür realisiert der Konnektor Schnittstellen zum VPN-Zugangsdienst, den OCSP-Respondern, dem TSL-Dienst, dem Namensdienst und dem Zeitdienst. Die Signaturanwendungskomponente (SAK) ist integraler Bestandteil des Konnektors und stellt die erforderliche Umgebung für die Erstellung von qualifizierten Signaturen unter Verwendung einer geeigneten Karte (z. B. HBA) dar. Die Signaturanwendungskomponente muss in einer Umgebung betrieben werden, die durch den Leistungserbringer kontrolliert werden kann. Im Kontext der Erweiterbarkeit muss insbesondere die Nachladefähigkeit des Konnektors umgesetzt werden. Diese enthält eine Nachladefunktionalität für neue Konnektorsoftware, über die jegliche Funktionalität des Konnektors, auch die Nachladefunktionalität selber, aktualisiert werden kann. Im Falle einer Aktualisierung wird die neue Konnektorsoftware evaluiert. Der Konnektor muss ein sicheres Nachladen z. B. der SAK und weiterer Anwendungskomponenten (Fachmodul) ermöglichen.

Der Konnektor beinhaltet ebenfalls das Fachmodul VSDM, welches dem Primärsystem die Funktionalität der Fachanwendung VSDM bereitstellt. Das Fachmodul VSDM wird als logisches Modul auf dem Konnektor betrieben und nutzt die interne Funktionalität des Konnektors

Das **eHealth-Kartenterminal** basiert auf der Hardware des ab dem Basis-Rollout verwendeten BCS-Kartenterminals und erweitert dieses durch eine Aktualisierung der

Firmware um eine Kommunikationsschnittstelle zum Konnektor. Dieser Produkttyp wird durch Leistungserbringer in deren Umgebung betrieben.

Das **Mobile Kartenterminal (Ausbaustufe 2)** basiert auf der Hardware der ab dem Basis-Rollout genutzten mobilen Kartenterminals der Ausbaustufe 1 und ermöglicht durch eine Aktualisierung der Firmware die Nutzung der Fachanwendungen VSDM (offline) in mobilen Einsatzszenarien. Das Mobile Kartenterminal beinhaltet ebenfalls das mobile Fachmodul VSDM mobil, welches die Funktionalität der Fachanwendung VSDM für mobile Anwendungen bereitstellt. Das mobile Fachmodul VSDM wird als logisches Modul auf dem Mobilien Kartenterminal betrieben und nutzt die interne Funktionalität des Mobilien Kartenterminals.

Die **eGK** in der Generation 1 wird seit Oktober 2011 stufenweise an alle Versicherten ausgegeben. Die eGK stellt für bestimmte Fachanwendungen Container für die Speicherung von Daten der Fachanwendungen bereit. Die eGK G1 wurde bereits spezifiziert und zugelassen. Die Bereitstellung der Karten erfolgt durch die Kostenträger. Für die Erprobung wird die eGK in der Ausprägung eGK Gen 1plus verwendet.

Das **gSMC-KT** implementiert die Identität des eHealth-Kartenterminals durch ein Sicherheitsmodul. Das Sicherheitsmodul dient der sicheren Kommunikation mit anderen Komponenten der TI (auch Remote-PIN) und kommt in Form einer Chipkarte zum Einsatz.

Das **gSMC-K** implementiert die Identität des Konnektors durch ein Sicherheitsmodul. Das Sicherheitsmodul ist Bestandteil des Konnektors und dient u. a. der sicheren Kommunikation mit anderen Komponenten der TI.

Der **HBA** in der Generation 1 wird für die Authentisierung und Signaturerstellung von Heilberuflern verwendet. Der HBA verfügt über ein qualifiziertes Signaturzertifikat.

Die **SMC-B** in der Generation 1 dient der Authentisierung und Signatur (DSIG) durch Organisationen des Gesundheitswesens.

Das **HSM-B** kann alternativ zur SMC-B die kryptografischen Identitäten medizinischer Institutionen bzw. Kostenträger-Geschäftsstellen enthalten und die Aufgaben einer SMC-B übernehmen. Das HSM-B kann in größeren Organisationen des Gesundheitswesens anstatt der SMC-B zum Einsatz kommen, falls die Performance der SMC-B nicht ausreichend ist.

### 5.1.2 Produkttypen der zentralen Telematikinfrastruktur

Der **Konfigurationsdienst** dient der Bereitstellung von Aktualisierungen (Software und Konfigurationen) von dezentralen Komponenten (ausgenommen Karten) im Wirkbetrieb.

Der **Namensdienst** dient Auflösung von Fully Qualified Domain Names (FQDN) in IP-Adressen für die TI. Weiterhin wird der Namensdienst zur Lokalisierung von Diensten (DNS-Service Discovery) genutzt.

Der **OCSP-Responder BNetzA-Proxy** dient dem Caching von Statusinformationen zu qualifizierten Zertifikaten der Bundesnetzagentur (BNetzA).

Ein **Trust Service Provider (TSP) X.509** stellt X.509-Zertifikate für berechnigte Personen (z. B. Zertifikate des HBA und der eGK), Organisationen und technische Komponenten aus und ermöglicht die Abfrage des Sperrstatus (OCSP-Responder) von durch ihn

ausgestellten X.509-Zertifikaten. Hierbei kommen die folgenden Ausprägungen des TSP vor:

- Der **TSP X.509 eGK** stellt Statusinformationen zu Zertifikaten des Kartentyps eGK bereit. Für die Bereitstellung der PKI einschließlich der OCSP-Responder ist der für die Ausgabe der Karte zuständige Kostenträger verantwortlich.
- Der **TSP X.509 HBA non QES** stellt Statusinformationen zu nicht-qualifizierten Zertifikaten des Kartentyps HBA bereit. Für die Bereitstellung der PKI einschließlich der OCSP-Responder ist die für die Ausgabe der Karte verantwortliche berufsständische Organisation verantwortlich.
- Der **TSP X.509 HBA QES** stellt Statusinformationen zu qualifizierten Zertifikaten des Kartentyps HBA bereit. Für die Bereitstellung der PKI einschließlich der OCSP-Responder ist die für die Ausgabe der Karte verantwortliche berufsständische Organisation verantwortlich.
- Der **TSP X.509 SMC-B** stellt Statusinformationen zu Zertifikaten des Kartentyps SMC-B bereit. Für die Bereitstellung der PKI einschließlich der OCSP-Responder sind die für die Ausgabe der Karte zuständigen Organisationen verantwortlich.
- Der **TSP X.509 Komponenten** stellt Statusinformation zu Zertifikaten bereit, die durch die Komponenten und Dienste der TI genutzt werden, um sichere Kommunikationskanäle (VPN, SSL/TLS) zu etablieren, die Identität von Komponenten nachzuweisen (gSMC-K, gSMC-KT) und Konfigurationsdateien und Softwarepakete zu signieren.

Der **Zentrale OCSP-Responder** ermöglicht die Abfrage des Sperrstatus von in der TI ausgestellten X.509-Zertifikaten. Ein TSP kann diesen zentralen OCSP-Dienst nutzen. Die Sperrstatusinformationen müssen von den teilnehmenden TSP bei Änderung bereitgestellt werden.

Der **Trust Service Provider CVC** betreibt eine von der gematik CVC-Root-CA abgeleitete CVC-Sub-CA (CA der zweiten Ebene) nach den Regularien der gematik und erstellt CV-Zertifikate mit den spezifizierten Rollenattributen für berechnigte Akteure.

Die **CVC-Root** stellt die zentrale Root CA der PKI für CV-Zertifikate in der TI dar und dient der Zertifizierung von CVC-Sub-CAs und der damit verbundenen Ausstellung von CVC-Sub-CA-Zertifikaten.

Das **Sicherheitsgateway KV-SafeNet** ermöglicht eine sichere Kopplung von Bestandsnetzen des Gesundheitswesens, in diesem Falle des KV-SafeNet-Backbones mit der TI.

Der **TSL-Dienst** dient der Bereitstellung des zentralen Vertrauensraums der X.509-PKI der TI mittels einer signierten Liste vertrauenswürdiger Zertifikatsherausgeber.

Ein **VPN-Zugangsdienst** ermöglicht Leistungserbringern unter Verwendung des Konnektors und der dazu nötigen Telekommunikationskomponenten den Zugang zu dem geschlossenen Netz der TI über ein VPN und damit die Nutzung der zentralen und fachanwendungsspezifischen Dienste sowie die Nutzungsoption für einen gesicherten Internetzugang.

Der **Zeitdienst** stellt allen relevanten Produkttypen eine zentrale Zeitinformation zur Verfügung.

Das **Zentrale Netz TI** dient der performanten Kommunikation zwischen VPN-Zugangsdiensten, zentralen Diensten und fachanwendungsspezifischen Diensten.

Die **Störungssampel** aggregiert und korreliert den Betriebsstatus der Zentralen Dienste der TI-Plattform und der fachanwendungsspezifischen Dienste.

### 5.1.3 Produkttypen der fachanwendungsspezifischen Dienste

Die **Fachdienste VSDM** (VSDD, UFS und CMS) dienen der Prüfung der Aktualität des Versichertenstammdatensatzes auf der eGK und der Aktualisierung der Versichertenstammdaten auf der eGK sowie der Sperrung / Entsperrung der Gesundheitsanwendung DF.HCA über CMS. Die Fachdienste VSDM wurden bereits von den Kostenträgern entwickelt und haben Bestandsschutz. Sie dürfen nur in Abstimmung mit den Kostenträgern verändert werden.

Der **Intermediär VSDM** dient als Proxy für die Fachdienste VSDM der einzelnen Kostenträger. Im Gegensatz zum Broker aus dem Release 4.0 fallen Funktionalitäten wie Nachrichtensignatur, Anonymisierung und Umschlüsselung beim neuen Intermediär VSDM weg.

## 5.2 Losbezogene Leistungen

Nachdem im vorangegangenen Kapitel die Produkttypen vorgestellt wurden, zeigt das vorliegende Kapitel die Zuordnung von Produkttypen zu den drei Losen. Zum Teil handelt es sich dabei um Produkttypen, die nicht durch das Los bereitgestellt werden, sondern in dieses integriert werden müssen. Dies ist entsprechend ausgewiesen.

Online Rollout Stufe 1  
Losschnitt

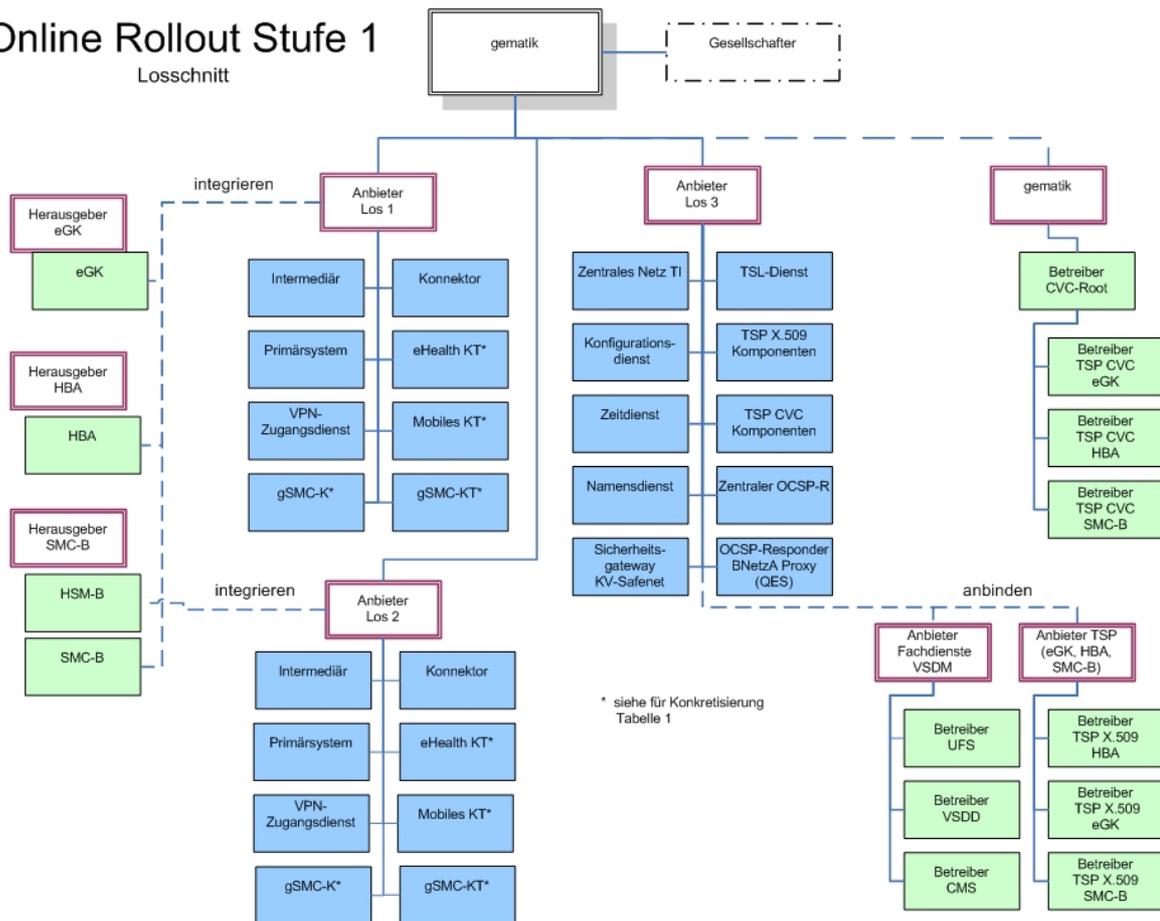


Abbildung 3: Grafische Darstellung des Losschnittes

Die nachfolgende Tabelle zeigt die relevanten Produkttypen (ggf. mit ihren weiteren Ausprägungen) und ihre Zuordnung zu den Losen. Die Produkttypen / Ausprägungen sind Liefer- und Leistungsgegenstände der entsprechenden Lose bzw. Beistellungen des Auftraggebers. Die folgenden Leistungsarten sind für die Produkttypen in unterschiedlicher Tiefe durch den AN durchzuführen:

- Auftragnehmerbezogenes Konzept / Dokumentationen: Erstellung, Abstimmung von Konzepten wie Implementierungskonzepte, Spezifische Betriebskonzepte, Betriebshandbücher, Leitfäden etc., die auch unabhängig von Spezifikations-erstellungen erforderlich sind.
- Spezifikation: Mögliche Vervollständigung / Erweiterung / Anpassung von Spezifikationen für Komponenten oder Dienste
- Entwicklung: Software- oder Hardware-technische Erstellung, Produktion, Testung von Komponenten und Diensten
- Lieferung: Logistische Bereitstellung der vorgegebenen Mengengerüste für Software- und Hardware-Komponenten einschl. erforderlicher Peripherie, Verkabelung und Installation bei den in der Leistungsbeschreibung benannten Zielgruppen (Testteilnehmer, VSDM-Betreiber, Auftraggeber, etc.)

- **Aufbau:** Installation und Test aller Komponenten und Dienste entsprechend den Vorgaben der Leistungsbeschreibung und unter Beachtung der „Ende-zu-Ende-Support-Verantwortung“
- **Betrieb:** Durchführung, Betreuung, Support der in der Leistungsbeschreibung definierten Erprobungsphasen und Unterstützung aller beteiligten Betriebsinstanzen mit den geforderten Supportleistungen einschl. Support für die teilnehmenden Leistungserbringer / Provider im Sinne der „Ende-zu-Ende-Support-Verantwortung“.
- **Integration:** Bereits in den Testregionen vorhandene Produkttypen müssen durch den Auftragnehmer zur Nutzung des geschuldeten Funktionsumfangs integriert werden. (Diese Produkttypen sind in der nachfolgenden Tabelle *kursiv* dargestellt)

**Tabelle 1: Übersicht der relevanten Produkttypen und die Zuordnung der Liefer- und Leistungsgegenstände zu den ausgeschriebenen Losen.**

<b>Produkttyp (und Ausprägung)</b>	<b>Los 1 &amp; 2</b>	<b>Los 3</b>	<b>Erläuterung</b>
Konnektor	X		Der Konnektor muss entwickelt, zugelassen, evaluiert und betrieben werden. Er enthält die Signaturanwendungskomponente, das Fachmodul VSDM, das Anwendungskonnektormodul und das Netzkonnektormodul.
eHealth KT	X		Die Geräte sind in der Testregion als BCS-Kartenterminals vorhanden. Die zugelassenen Updates der Kartenterminalhersteller, die Geräte bei den Teilnehmern haben, müssen installiert und integriert werden. Die Geräte müssen ebenso über eine Herstellererklärung oder Bestätigung durch die BNetzA für die Erstellung von QES zulässig sein. Die vorhandenen KT müssen verwendet werden. Ein Austausch ist nicht vorgesehen.
Mobiles KT	X		Die Geräte sind als Mobile KTs der Ausbaustufe 1 in der Testregion vorhanden. Die zugelassenen Updates der Kartenterminalhersteller, die Geräte bei den Teilnehmern haben, müssen installiert und integriert werden. Die vorhandenen KT müssen verwendet werden. Ein Austausch ist nicht vorgesehen.
Primärsystem	X		Die Primärsysteme sind in den Testregionen vorhanden und zur Nutzung des geschuldeten Funktionsumfangs weiterzuentwickeln und anzubinden.
Intermediär	X		Der Intermediär muss aufgebaut und betrieben werden.

Produkttyp (und Ausprägung)	Los 1 & 2	Los 3	Erläuterung
VPN-Zugangsdienst	X		Der VPN-Zugangsdienst inkl. gesichertem Internetzugang muss aufgebaut und betrieben werden.
Konfigurationsdienst		X	Der Konfigurationsdienst muss entwickelt, aufgebaut und betrieben werden.
Sicherheitsgateway KV-Safenet		X	Das Sicherheitsgateway KV-Safenet muss entwickelt, aufgebaut und betrieben werden. Bestandteil der Leistung des AN ist zudem die Anbindung und Integration der Provider des Bestandsnetzes von KV-Safenet an das zentrale Netz bzw. das Sicherheitsgateway.
Namensdienst		X	Der Namensdienst muss aufgebaut und betrieben werden.
Zeitdienst		X	Der Zeitdienst muss aufgebaut und betrieben werden.
Zentrales Netz TI		X	Das Zentrale Netz TI muss aufgebaut und betrieben werden.
TSP X.509 Komponenten / TSP CVC Komponenten		X	Der TSP X.509 Komponenten/ CVC Komponenten muss entwickelt, aufgebaut und betrieben werden.
TSL-Dienst		X	Der TSL-Dienst muss entwickelt, aufgebaut und betrieben werden.
OCSP-Responder BNetzA-Proxy		X	Der OCSP-Responder BNetzA-Proxy soll entwickelt, aufgebaut und betrieben werden.  Im Rahmen des Verhandlungsverfahrens wird bestimmt, ob dieser Dienst benötigt wird.
gSMC-KT	X	X	Die Evaluierung der gSMC-KT muss nicht durch den AN durchgeführt werden. Herausgeber der gSMC-KT ist der Hersteller der Kartenterminals. Die notwendigen Zertifikate werden durch den TSP Komponenten aus Los 3 erstellt. In Los 1 & 2 erfolgt die Installation und Integration der gSMC-KT.
gSMC-K	X	X	Die Evaluierung der gSMC-K muss nicht durch den AN durchgeführt werden. Herausgeber der gSMC-K ist der Hersteller des Konnektors. Die notwendigen Zertifikate werden durch den TSP Komponenten aus Los 3 erstellt. In Los 1 & 2 erfolgt die Installation und Integration der gSMC-K.

Produkttyp (und Ausprägung)	Los 1 & 2	Los 3	Erläuterung
HSM-B	X	X	Einsatz noch nicht abschließend geklärt Die Evaluierung des HSM-B muss nicht durch den AN durchgeführt werden. Die notwendigen Zertifikate werden durch den TSP Komponenten aus Los 3 erstellt. In Los 1 & 2 erfolgt die Installation und Integration des HSM-B.
Zentraler OCSP-Responder		X	Der Zentrale OCSP-Responder soll entwickelt, aufgebaut und betrieben werden. Im Rahmen des Verhandlungsverfahrens wird bestimmt, ob dieser Dienst benötigt wird.

Die nachfolgende Tabelle zeigt die durch den Auftragnehmer zu integrierenden Systembestandteile der Telematikinfrastruktur. Die Bereitstellung dieser Systembestandteile ist nicht Bestandteil dieser Ausschreibung.

**Tabelle 2: Übersicht der relevanten zu integrierenden Produkttypen und ihre Zuordnung zu den ausgeschriebenen Losen**

Produkttyp (und Ausprägung)	Los 1 & 2	Los 3	Erläuterung
<i>eGK Gen 1plus</i>	X		Die eGK ist in den Testregionen vorhanden. Die Versicherten verfügen in den Testregionen über eine eGK. Die eGK ist zur Nutzung der Fachanwendung VSDM zu <u>integrieren</u> .
<i>Heilberufsausweis (HBA)</i>	X		Die Ausgabe des HBA erfolgt über die verantwortlichen Herausgeber (Landes(zahn-)ärztekammer(n), KZVn (ZOD-Karten) sowie die Landespsychotherapeutenkammer(n) in der Testregion) bzw. über ihre Dienstleister. Der HBA muss zur Authentisierung gegenüber der eGK und zur Nutzung der QES <u>integriert</u> werden.
<i>SMC-B</i>	X		Die Ausgabe der SMC-B erfolgt über die verantwortlichen Herausgeber (Kassen(zahn-)ärztliche(n) Vereinigung(en) in der Testregion bzw. die zuständigen DKTIG) bzw. über ihre Dienstleister. Die SMC-B muss zur Authentisierung gegenüber der eGK und zum Verbindungsaufbau in die TI <u>integriert</u> werden.
<i>Fachdienste VSDM (inkl. UFS, VSDD und CMS)</i>		X	Die Fachdienste VSDM werden von den Kostenträgern (bzw. ihren Dienstleistern) entwickelt, zugelassen und betrieben. Bestandteil der Leistung

			des AN ist die Anbindung und Integration der Fachdienste an das zentrale Netz.
<i>TSP X.509 SMC-B</i>		X	Die OCSP-Responder der SMC-B werden durch die Kartenherausgeber bzw. ihre Dienstleister betrieben. Bestandteil der Leistung des AN ist die Anbindung und Integration der OCSP-Responder an das zentrale Netz.
<i>TSP X.509 eGK</i>		X	Die OCSP-Responder der eGK werden durch die Kartenherausgeber bzw. ihre Dienstleister betrieben. Bestandteil der Leistung des AN ist die Anbindung und Integration der OCSP-Responder an das zentrale Netz.
<i>TSP X.509 HBA non QES</i>		X	Die OCSP-Responder der HBA für non QES werden durch die Kartenherausgeber bzw. ihre Dienstleister betrieben. Bestandteil der Leistung des AN ist die Anbindung und Integration der OCSP-Responder an das zentrale Netz.
<i>TSP X.509 HBA QES</i>		X	Die OCSP-Responder der HBA für QES werden durch die Kartenherausgeber bzw. ihre Dienstleister betrieben. Bestandteil der Leistung des AN ist die Anbindung und Integration der OCSP-Responder an das zentrale Netz.
<i>CVC Root CA</i>		X	Die CVC-Root ist vorhanden. Der AN muss für die Erstellung der CV-Zertifikate der Komponenten eine CV-CA vom Betreiber der CVC-Root beantragen.

---

## 6 Definierter Erprobungsumfang

---

Für die Erprobung muss eine geeignete Anzahl Leistungserbringer ausgestattet und eingebunden werden. Unter den Krankenhäusern müssen unterschiedliche Versorgungsstufen (Regelversorgung, Schwerpunktversorgung und Maximalversorgung) mit mindestens einer Universitätsklinik vertreten sein. Die Erprobung muss die Nutzung eines sog. „Mehrkomponentenkonnektors“ für den Einsatz im Krankenhaus ermöglichen. Hierbei wird vorausgesetzt, dass die Versicherten zum Großteil bereits mit eGK Gen 1plus ausgestattet sind und die Fachdienste für die Anwendung VSDM der Kassen funktionsfähig sind.

Pro Los (Los 1 & 2) muss das nachfolgende Mengengerüst **mindestens** eingehalten werden:

**Tabelle 3: Mengengerüst pro Los (Los 1 & 2)**

Dimension	Wert
Anzahl einzubindender Leistungserbringerinstitutionen (Ärzte, Zahnärzte, Psychotherapeutenpraxen, Berufsausübungsgemeinschaften) mit Primärsystemen	500
Anzahl unterschiedlicher Primärsysteme (PVS) für Arztpraxen, wobei mindestens 3 der Hersteller dieser Produkte nicht gesellschaftsrechtlich verbunden sind, sondern (konzern-)unabhängig sein müssen.	5
Anzahl unterschiedlicher Primärsysteme (PVS) für Zahnarztpraxen, wobei mindestens 3 der Hersteller dieser Produkte nicht gesellschaftsrechtlich verbunden sind, sondern (konzern-)unabhängig sein müssen.	5
Anzahl unterschiedlicher Primärsysteme (KIS) für Krankenhäuser	5
Anzahl einzubindender Krankenhäuser	5
In der Anzahl der einzubindenden Krankenhäuser enthaltene Anzahl von Universitätskliniken	1

---

## 7 Projektspezifische rechtliche Rahmenbedingungen

---

### 7.1 SGB V

Bei dem Aufbau und Betrieb der für die Einführung und Anwendung erforderlichen Telematikinfrastruktur sind die Regelungen des SGB V, insbesondere §§291 ff. SGB V (vgl. Anlage) zu beachten.

### 7.2 TestV

Die Testmaßnahmen (Tests und Erprobung) sind nach den Maßgaben der Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte in der Fassung der Bekanntmachung vom 23.09.2009 (BGBl. I S. 3162), zuletzt geändert durch Art. 1 Dritte ÄndVO vom 11.01.2011 (BGBl. I S. 39) - kurz TestV - (siehe Anlage) durchzuführen.

### 7.3 Datenschutz und Informationssicherheit

Die Sicherstellung des informationellen Selbstbestimmungsrechtes der Patienten sowie des (Sozial-)Datenschutzes bei der Nutzung ihrer elektronischen Gesundheitskarte stellt eine der Kernaufgaben der gematik dar. §291b Abs. 1 S. 2 SGB V bestimmt, dass die gematik „die Interessen von Patientinnen und Patienten zu wahren und die Einhaltung der Vorschriften zum Schutz personenbezogener Daten sicherzustellen“ hat. Auch bei der Erprobung der Telematikinfrastruktur und ihrer Anwendungen ist der Datenschutz sicherzustellen (§ 2 Abs. 1 S. 4 TestV). Nicht zuletzt sind Datenschutzkonformität und Informationssicherheit auf einem angemessenen Niveau wesentliche Voraussetzungen für die Akzeptanz der elektronischen Gesundheitskarte und ihrer Anwendungen.

Die Erreichung des notwendigen Datenschutz- und angemessenen Sicherheitsniveaus erfolgt durch drei strategische Festlegungen:

- **Privacy und Security by Design:** Für das Design werden einheitliche Methoden zum Datenschutz und zur Informationssicherheit von der gematik vorgegeben. Die Anwendung der einheitlichen Methoden stellt sicher, dass eine nachvollziehbare Datenschutz- und Sicherheitskonzeption für die jeweilige Fachanwendung, die TI-Plattform und ihre Bestandteile (Komponenten und Dienste) entsteht und Anforderungen des Datenschutzes und der Informationssicherheit bereits im Design angemessen berücksichtigt werden.
- **Prüfung vor Inbetriebnahme:** Bevor ein Produkt in Betrieb genommen wird, findet im Rahmen der Zulassung eine Prüfung statt, ob die im Design vorgegebenen Anforderungen erfüllt wurden. Es können keine Produkte in der TI betrieben werden, die nicht durch die gematik zugelassen wurden. Analog hierzu können keine Betreiber oder Anbieter ihre Dienstleistungen für die TI erbringen, die nicht durch die gematik zugelassen wurden.

- **Aufrechterhaltung** des notwendigen Datenschutz- und angemessenen Sicherheitsniveaus **im laufenden Betrieb**: Alle an der TI beteiligten Anbieter und Betreiber zentraler Produkte der TI etablieren ein Datenschutzmanagementsystem (DSMS) und ein Informationssicherheitsmanagementsystem (ISMS). Die einheitlichen Methoden zu Datenschutz und Informationssicherheit werden angewendet.

Im Rahmen des Verhandlungsverfahrens werden übergreifende Regelungen definiert, die durch den Auftragnehmer zu berücksichtigen sind.

Die Telematikinfrastruktur muss auf der einen Seite dem Schutzbedarf personenbezogener, medizinischer Daten gerecht werden und auf der anderen Seite praktikabel bleiben, um von den Anwendern genutzt werden zu können (Akzeptanz). Durch eine risikobasierte Sicherheitsbetrachtung wird diesem Zielkonflikt begegnet.

Die Komponenten und Dienste müssen einer risikobasierten Sicherheitsbetrachtung unterzogen werden und dadurch der tolerierbare Bereich der Risiken auf der Basis der Risikopolicy der TI eingeschätzt werden. Restrisiken werden zwischen Auftragnehmer und Auftraggeber transparent gemacht, damit die Aufrechterhaltung des notwendigen Datenschutz- und angemessenen Sicherheitsniveaus im laufenden Betrieb sichergestellt ist.

### 7.3.1 Sicherheitszertifizierungen der Auftragnehmer

Dezentrale Komponenten, die die Auftragnehmer entwickeln, herstellen oder bereitstellen, müssen ggf. eine erfolgreiche Evaluation nach Common Criteria auf der Grundlage eines vom BSI erstellten Protection Profiles nachweisen.

### 7.3.2 Anforderungen an das Datenschutz- und Informationssicherheitsmanagement der Auftragnehmer

Die Auftragnehmer müssen ein Datenschutzmanagement- und Informationssicherheitsmanagementsystem für die von ihnen gelieferten Produkte und zu erbringenden Leistungen etablieren und aufrechterhalten.

Die Auftragnehmer müssen einen zuständigen Datenschutzbeauftragten und einen zuständigen Sicherheitsbeauftragten gegenüber dem Auftraggeber benennen. Diese bilden die Schnittstelle zum DSMS bzw. ISMS der gematik und berichten regelmäßig und anlassbezogen an die gematik.

Die Leistungserbringung erfordert organisatorische Schnittstellen zum BSI und zum BfDI, die die Auftragnehmer jeweils etablieren sollen. Die gematik unterstützt die Auftragnehmer in der Zusammenarbeit mit diesen Behörden nach Möglichkeit.

Die Auftragnehmer müssen die an der Erprobung der Telematikinfrastruktur Beteiligten bei der Wahrnehmung ihrer jeweiligen Betroffenenrechte i. S. d. Bundesdatenschutzgesetzes bzw. des Sozialdatenschutzes unterstützen. Erste Anlaufstelle für Karteninhaber (Versicherte und Leistungserbringer) sind die jeweiligen Kartenherausgeber. Anfragen müssen ggf. dorthin weitergeleitet werden.

---

## 8 Gesamtprojektverantwortung der Auftragnehmer

---

Die Auftragnehmer tragen die Gesamtprojektverantwortung für Aufbau und Erprobung einer funktionierenden Telematikinfrastruktur. Diese umfasst insbesondere auch die Planung und die Steuerung mehrerer, unterschiedlicher Arbeitspakete, Leistungsarten (Konzept, Spezifikation, Entwicklung, Lieferung, Aufbau, Betrieb) und Planungsstränge im Sinne eines Multiprojektmanagements. Im gesamten Projektverlauf sind alle Akteure einschließlich der Kartenherausgeber von den Auftragnehmern organisatorisch und technisch einzubinden und zu koordinieren. Eine genaue Zuordnung – auch zu den einzelnen Losen – wird im Rahmen des Verhandlungsverfahrens detailliert festgelegt. Die Gesamtverantwortung im Sinne einer Ende-zu-Ende-Verantwortung umfasst dabei insbesondere Folgendes:

### **Entwicklungs-, Aufbau- und Testverantwortung**

In diesem Projektabschnitt haben die Auftragnehmer eine funktionsfähige, interoperable und sichere Telematikinfrastruktur mit dem beschriebenen Funktionsumfang zu entwickeln, aufzubauen und zu testen.

### **Verantwortung für den Rollout in den Testregionen**

Im weiteren Projektverlauf sind alle Akteure für die Erprobung der Telematikinfrastruktur technisch anzubinden und insbesondere die Installation der notwendigen Komponenten bei den zuvor identifizierten und akquirierten Leistungserbringern für die Erprobung durchzuführen.

### **Verantwortung für die Erprobung**

In diesem Projektabschnitt tragen die Auftragnehmer die technische und die organisatorisch-prozessuale Betriebsverantwortung. Des Weiteren sind die Leistungserbringer bei der Onlineprüfung der eGK (VSDM) und der Durchführung / Nutzung von QES zu unterstützen. Die Betriebsverantwortung umfasst im Wesentlichen:

- die Sicherstellung der Verfügbarkeit und des Betriebs in allen beauftragten Betriebsumgebungen,
- die Erbringung von Support- und Serviceleistungen für die eingesetzten Komponenten einschl. Austausch bei Defekt, Firmware-Updates,
- das Monitoring der technischen Schnittstellen, Komponenten und Dienste,
- Bereitstellung der Support-Instanzen für alle Teilnehmer (Servicedesk, Hotline, Vor-Ort-Service),
- Aufbau und Durchführung der vorgegebenen ITIL V3 – Prozesse,
- Bereitstellung von Daten für die Evaluation.

---

## **9 Memoranden**

---

Die Bewerber werden gebeten, bereits im Rahmen des Teilnahmewettbewerbs die folgenden Memoranden – jeweils für das konkrete Los, auf das sich deren Bewerbung bezieht - zu erstellen und mit dem Teilnahmeantrag informativ einzureichen. Die Konzepte werden nicht Gegenstand der Bewertung der Eignung sein. Ziel ist es, ein gemeinsames Grundverständnis vom Umfang und der Art und Weise der zu erbringenden Leistungen bereits zu diesem frühen Zeitpunkt herbeizuführen.

### **9.1 Lose 1 & 2**

#### **Memorandum 1:**

Die Bewerber werden gebeten, auf Basis der Informationen der Informationsbroschüre darzustellen, wie das Gesamtvorhaben der Entwicklung sowie des Aufbaus und Betriebs einer Telematikinfrastruktur unter Einbindung der genannten Akteure (Kapitel 1 und 2) in den losbezogenen Testregionen mit dem definierten (und ggf. erweiterbaren) Funktionsumfang unter Beachtung der systembedingten Anforderungen (Kapitel 3, 4, 5) und unter Beachtung des Erprobungsumfangs (alle gesetzlich Versicherten und eine definierte Auswahl von Leistungserbringern (Ärzte, Zahnärzte, Psychotherapeutenpraxen, Berufsausübungsgemeinschaften und Krankenhäuser mit Primärsystemen)) unter Berücksichtigung projektspezifischer rechtlicher Rahmenbedingungen (Kapitel 6, 7) realisiert werden soll.

Dabei ist folgende Gliederungsstruktur einzuhalten:

1. Planung, Projekt- und Qualitätsmanagement einschließlich Darstellung der Organisation (Organigramm des Bewerbers) und Koordinationsplanung der Einbindung sämtlicher Akteure und der einzubindenden Behörden (z.B. BSI)
2. Entwicklung, Aufbau und Test
  - a. Darstellung der Entwicklung des Bewerbers inklusive der Einbindung aller Entwicklungspartner
  - b. Vorgehen zum Aufbau und zur Testung unter frühzeitiger Einbindung von Endnutzern
  - c. Vorgehen bei der Einbindung der Akteure in den Testregionen vor dem Hintergrund der geforderten Testziele
3. Rollout
  - a. Identifikation und Akquise der Leistungserbringer unter Beachtung des definierten Erprobungsumfangs
  - b. Verteilung und Installation der Lösung bei den Leistungserbringern
  - c. Umsetzung der Rollout-Logistik (Management und Schulung)
4. Erprobung

- a. Darstellung des Supports für die teilnehmenden Akteure (insbesondere der Leistungserbringer) unter Berücksichtigung der vorhandenen Strukturen

In der Darstellung muss die vom Auftragnehmer zu übernehmende Gesamtprojektverantwortung (entsprechend Kapitel 8) deutlich herausgestellt werden.

Gesamtumfang: max. 30 Seiten (Schriftgröße 12; Zeilenabstand 1,5).

#### **Memorandum 2:**

Die Bewerber werden gebeten zu beschreiben, wie sich die zeitliche Planung der Entwicklung und Bereitstellung der Fachanwendung VSDM und der QES (inkl. Stapelsignatur, einfacher digitaler, elektronischer Signatur und Verschlüsselung) zur Erprobung nach einer möglichen Zuschlagserteilung darstellt.

- Der geschuldete Funktionsumfang umfasst die beiden Teile VSDM mit korrespondierender Infrastruktur und QES. Idealerweise erfolgt die Realisierung in einer Phase, kann jedoch – wenn erforderlich – in 2 Phasen umgesetzt und so weit getestet werden, dass sie ggf. separat für den Produktivbetrieb freigegeben werden können.
- Der zeitliche Abstand zwischen Zuschlag zum gesamten Funktionsumfang und VSDM-Erprobungsbeginn darf maximal 10 Monate, zwischen VSDM-Erprobungsbeginn und QES-Erprobungsbeginn maximal 10 Monate betragen.
- Der Bewerber hat hierbei jeweils für die Fachanwendung VSDM und den Basisdienst QES die durch ihn vorzunehmende Einbindung der Akteure und Behörden (z. B. BSI) darzulegen.

Gesamtumfang: max. 20 Seiten (Schriftgröße 12; Zeilenabstand 1,5).

## **9.2 Los 3**

#### **Memorandum 1:**

Die Bewerber werden gebeten, auf Basis der Informationen der Informationsbroschüre darzustellen, wie das Gesamtvorhaben der Entwicklung sowie des Aufbaus und Betriebs einer Telematikinfrastuktur unter Einbindung der genannten Akteure (Kapitel 1 und 2) in den losbezogenen Testregionen mit dem definierten (und ggf. erweiterbaren) Funktionsumfang unter Beachtung der systembedingten Anforderungen (Kapitel 3, 4, 5) und unter Beachtung des Erprobungsumfangs (alle gesetzlich Versicherten und eine definierte Auswahl von Leistungserbringern (Ärzte, Zahnärzte, Psychotherapeutenpraxen, Berufsausübungsgemeinschaften und Krankenhäuser mit Primärsystemen) unter Berücksichtigung projektspezifischer rechtlicher Rahmenbedingungen (Kapitel 6, 7) realisiert werden soll.

Dabei ist folgende Gliederungsstruktur einzuhalten:

1. Planung, Projekt- und Qualitätsmanagement einschließlich Darstellung der Organisation (Organigramm des Bewerbers) und Koordinationsplanung der Einbindung sämtlicher Akteure und der einzubindenden Behörden (z.B. BSI)
2. Entwicklung, Aufbau und Test

- a. Planung und Umsetzung der Infrastrukturdienste, insbesondere des Konfigurations- und Software-Repositories und des Sicherheitsgateways
  - b. Aufbau des zentralen Netzes der TI
  - c. Aufbau der PKI, insbesondere Herausgabe und Bereitstellung erforderlicher Zertifikate an die Akteure
  - d. Aufteilung von mehreren Umgebungen
  - e. Vorgehen zum Aufbau und zur Testung der Produkttypen inklusive Zulassung
3. Rollout
- a. Unterstützung der Lose 1 & 2, der Kostenträger mit ihren Fachdiensten bzw. deren Dienstleister sowie des KV-SafeNet-Backbones (über das Sicherheitsgateway) bei der erforderlichen Anbindungen an das zentrale Netz und der Inbetriebnahme
4. Erprobung
- a. Darstellung der Ansätze für die Betriebsprozesse, insbesondere Incident- / Problem Management, Monitoring und Reporting
  - b. Darstellung des Supports für die angebundenen Akteure

In der Darstellung muss die vom Auftragnehmer zu übernehmende Gesamtprojektverantwortung (entsprechend Kapitel 8) deutlich herausgestellt werden.

Gesamtumfang: max. 30 Seiten (Schriftgröße 12; Zeilenabstand 1,5).

---

## Abkürzungsverzeichnis

---

Erläuterungen der Fachbegriffe und Abkürzungen zur TI sind zu finden im Glossar der gematik, veröffentlicht unter [http://www.gematik.de/cms/de/spezifikation/erlaeuterungen\\_nutzer/glossar/glossar.jsp](http://www.gematik.de/cms/de/spezifikation/erlaeuterungen_nutzer/glossar/glossar.jsp).

Nachfolgend werden einige weitere, für das Verständnis wesentliche Begriffe erläutert:

Begriff	Erläuterung
ÄndVO	Änderungsverordnung
Basis-Rollout	Ausgabe der eGK-Kartenterminals 2011
BGBI	Bundesgesetzblatt
BMG	Bundesministerium für Gesundheit
BnetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
DKG	Deutsche Krankenhausgesellschaft
DKTIG	Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH
DL	Dienstleistung, Dienstleister
GKV	Gesetzliche Krankenversicherung
GKV-SV	Spitzenverband der Gesetzlichen Krankenversicherungen und Pflegekassen
gSMC	Gerätespezifische Secure Module Card
GSV	Gesellschafterversammlung
KBV	Kassenärztliche Bundesvereinigung
KIS	Krankenhausinformationssystem
KV	Kassenärztliche Vereinigung
KZBV	Kassenzahnärztliche Bundesvereinigung
PP	Protection Profile
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SigV	Signaturverordnung
TestV	Verordnung über Testmaßnahmen (siehe Kap. 7.2)