

Telematikinfrastruktur 2.0

Einzureichende Konzepte

Los 2 – Cloud Services

Anlage-11 der Vergabeunterlagen

2026-0030 TI-Flow - Entwicklung, Bereitstellung und Betrieb eines Workflow Fachdienstes, sowie der Aufbau und Betrieb einer sicheren Infrastruktur-Plattform in der TI

Version: 1.0.0
Stand: 14.10.2026
Klassifizierung: öffentlich

Inhaltsverzeichnis

1	Überblick.....	4
2	Einzureichende Konzepte	6
2.1	Konzept 1 (K-01): Umsetzungskonzept HCC (max. 33 Seiten)	6
2.1.1	Praktikabilität der RZ-Infrastruktur für die Umsetzung von HCC	6
2.1.2	Umsetzung der HCC-Komponenten	7
2.1.3	Einbindung von HCC in die Cloud-Governance	8
2.2	Konzept 2 (K-02): Umsetzungskonzept CI/CD (max. 13 Seiten)	9
2.2.1	Systemarchitektur, Organisations- und Berechtigungsmodell (Architekturbild).....	9
2.2.2	Repository-, Pipeline- und Runner-Konzept	10
2.2.3	Artefakt-, Registry- und Supply-Chain-Konzept.....	10
2.2.4	Integration, Freigabe, Promotion und Deployment zwischen CI/CD- Plattform und HCC-Cloud.....	10
2.2.5	Umsetzung, technische Betriebsbefähigung und Portabilität der CI/CD- Plattform.....	10
2.3	Konzept 3 (K-03): Testkonzept HCC_Bietername (max. 15 Seiten) ..	11
2.4	Konzept 4 (K-04): Testkonzept CI/CD-Plattform (max. 5 Seiten)	12
2.4.1	Teststrategie und Teststufen.....	12
2.4.2	Testvorgehen und Nachweisführung	12
2.4.3	Anbindung der Testumgebung	13
2.5	Konzept 5 (K-05): Betriebskonzept HCC (max. 30 Seiten)	13
2.5.1	Betriebsorganisation	13
2.5.2	Reporting- und Eskalationsmanagement	14
2.5.3	Monitoring, Telemetrie und Betriebsdaten	14
2.5.4	Capacity Management.....	15
2.5.5	IT-Service-Management	15
2.5.6	Change- und Release-Management	16
2.5.7	SLA-Konzept.....	17
2.5.8	Abrechnungsmodell	18
2.5.9	Eigenmonitoring und Anomalieerkennung	19
2.6	Konzept 6 (K-06): Betriebskonzept CI/CD-Plattform (max. 15 Seiten)	20
2.6.1	Betriebsmodell, Organisation und Verantwortlichkeiten	20
2.6.2	Betriebsprozesse und Service Management	20
2.6.3	Überwachung, Ereignis- und Störungsmanagement	21
2.6.4	Sicherheits-, Schwachstellen- und Änderungsbetrieb	21
2.6.5	Kapazität, Kontinuität, Datensicherung und Exit.....	21
2.7	Konzept 7 (K-07): Souveränitätskonzept (max. 10 Seiten)	21
2.7.1	Governance-, Eigentums- und Kontrollstrukturen	22
2.7.2	Drittstaaten- und Jurisdiktionsrisiken	22
2.7.3	EU-basierter Betrieb, Betriebsautonomie und Disconnect-Fähigkeit	23
2.7.4	Lieferkettensouveränität und Unterauftragnehmereinbindung	23
2.8	Konzept 8 (K-08): Konzept gemeinsame datenschutzrechtliche Verantwortung (max. 3 Seiten)	24

2.8.1	Vorgehen zum Abschluss der Vereinbarung gem. Art. 26 DSGVO.....	24
2.8.2	Standardprozesse und organisatorische Verfahren.....	24
2.8.3	Aufteilung der datenschutzrechtlichen Verpflichtungen und Zuständigkeiten	24
2.8.4	Operative Umsetzung und Zusammenarbeit	25
2.8.5	Umgang mit Änderungen	25
2.9	Konzept 9 (K-09): Umsetzung der Use-Cases aus Anlage_09b (max. 10 Seiten).....	25
2.10	Konzept 10 (K-10): Security Monitoring Konzept (max. 5 Seiten)	26
2.10.1	Mechanismen und Prozesse des Security Monitorings.....	26
2.10.2	Use-Cases bezogene Systematik:	26
2.11	Konzept 11 (K-11): Projektvorgehen (max. 15 Seiten, zzgl. einer Excel-Liste der Projektbeteiligten)	27
2.11.1	Projektorganisation.....	27
2.11.2	Projektdurchführung	27
2.11.3	Risikomanagement	28
2.11.4	Agile Projektdurchführung	28
2.11.5	Gutachten	28
2.12	Konzept 12 (K-12): Projektplan (MSP-Datei und max. 5 Seiten)	28
2.12.1	Planungsgrundlagen	29
2.12.2	Spezifische Erläuterungen.....	29

1 Überblick

In diesem Dokument werden die Themen benannt, die der Bieter des Verfahrens mit Abgabe seines Angebotes im einzureichenden Konzept näher auszuführen und darzustellen hat. Die einzureichenden Grobkonzepte müssen bei Zuschlag vom Auftragnehmer gemäß Leistungsbeschreibung fortgeschrieben werden. Zur besseren Lesbarkeit wird in diesem Dokument anstelle von "Grobkonzept" nur "Konzept" verwendet.

Alle Konzepte sind in dem vorgegebenen Konzepttemplate gemäß der vorgegebenen Kapitelstruktur zu erstellen und als Word-Datei (.docx) einzureichen. Sie haben nachfolgende Formatanforderungen zu erfüllen. Diese Anforderungen gelten nicht für die weiteren, zusätzlich einzureichenden Dateien (z.B. MS Project, Excel, o.Ä.), die im Folgenden beschrieben sind. Zur Darstellung bzw. Beantwortung der Themen sind auch ergänzende Abbildungen im Rahmen des jeweiligen Konzepts erwünscht.

Die Bieter müssen für die Konzepte die vorgegebenen Templates verwenden. Alle Konzepte haben die vorgegebene Schriftart Verdana mit der Schriftgröße 10 sowie voreingestellten Seitenabstände aufzuweisen. Für den Fall, dass diese Anforderungen nicht erfüllt bzw. nicht eingehalten worden sind, wird der Auftraggeber diese Formatierung eigenständig umsetzen. Gewertet werden ausschließlich die Konzeptausführungen innerhalb der jeweiligen Maximalseitenanzahl (exkl. Deckblatt, Dokumentinformationen und Inhaltsverzeichnis). Über die maximale Seitenanzahl hinausgehende Ausführungen des Bieters werden bei der Bewertung nicht berücksichtigt.

Die geforderten Konzepte haben folgende Dateibezeichnungen aufzuweisen:

- Anlage-11 - K-01 Umsetzungskonzept_HCC_Bietername
- Anlage-11 - K-02 Umsetzungskonzept_CI-CD_Bietername
- Anlage-11 - K-03 Testkonzept_HCC_Bietername
- Anlage-11 - K-04 Testkonzept_CI-CD_Bietername
- Anlage-11 - K-05 Betriebskonzept_HCC_Bietername
- Anlage-11 - K-06 Betriebskonzept_CI-CD_Bietername
- Anlage-11 - K-07 Souveränitätskonzept_Bietername
- Anlage-11 - K-08 Konzept gemeinsame datenschutzrechtliche Verantwortung_Bietername
- Anlage-11 - K-09 Umsetzung der Use-Cases aus Anlage_09b_Bietername
- Anlage-11 - K-10 Security_Monitoring_Konzept_Bietername
- Anlage-11 - K-11 Projektvorgehen_Bietername
- Anlage-11 - K-11 Anlage Projektbeteiligte_Bietername
- Anlage-11 - K-12 Projektplan_Bietername
- Anlage-11 - K-12 Projektplan Anlage_Bietername

Hinweis

Die Bewertung der Konzepte ergibt sich aus der Bewertungsmatrix (Anlage-10 - Bewertungsmatrix Angebotsphase Los 2). Der Bieter hat die Dokumente "Anlage-11 - K-XX_Konzeptname_Bieterame.docx" (für alle folgenden Konzepte K-xx im unten beschriebenen Umfang) mit den eigenen Konzeptinhalten auszufüllen (alle gemeinsam nachfolgend als "Vorlagen der Vergabestelle" bezeichnet).

Die einzureichenden Konzepte sind Bestandteil der Angebote. Die nachfolgend geforderten Inhalte und Strukturen sind einzuhalten. Ein nicht eingereichtes (fehlendes) Konzept wird gemäß der Bewertungsmatrix mit 0 Punkten bewertet.

Im Fall von Widersprüchen zwischen der Leistungsbeschreibung (inkl. Anlagen) und den nachfolgenden Ausführungen gehen die Ausführungen der Leistungsbeschreibung inkl. ihrer Anlagen vor.

Erwartete Darstellung

Die Darstellung der geforderten Inhalte der einzureichenden Konzepte soll folgende Merkmale aufweisen:

- Die Darstellungen sollen verständlich und präzise sein und in Form und Umfang angemessen bzgl. der Komplexität der darzustellenden Sachverhalte.
- Für bestimmte Themen kann dabei eine Aufzählung genutzter Technologien o. Ä. (soweit diese allgemein bekannt sind) ausreichen.
- Für qualifizierte Personen sollen die Konzepte in sich aussagekräftig sein, d. h., es soll für die Bewertung nicht vorausgesetzt werden, dass weitere Informationen aus Links auf weitere Dokumente herangezogen werden.
- Beschreibungen sollen ohne produktspezifische ("proprietäre") Vorkenntnisse verständlich sein.
- Grafische, textuelle oder tabellarische Beschreibungen sind dort zu verwenden, wo es zweckdienlich ist.
- Bei grafischen Darstellungen sollen bevorzugt gängige, standardisierte Mittel eingesetzt werden (z.B. UML, BPMN o.ä.)

2 Einzureichende Konzepte

In diesem Kapitel werden die einzureichenden Konzepte beschrieben.

2.1 Konzept 1 (K-01): Umsetzungskonzept HCC (max. 33 Seiten)

Zielsetzung: Die Ausführungen sollen es dem AG ermöglichen, die grundsätzliche Lösungskompetenz des Bieters in Bezug auf die HCC-Cloud einzuschätzen, die vom Bieter geplante Umsetzung auf Plausibilität zu prüfen sowie die seitens des Bieters eingebrachten Kompetenzen, Technologien und Möglichkeiten zu bewerten.

Der Bieter stellt in seinem Konzept die geplante technische und organisatorische Realisierung der HCC-Cloud dar.

Das Konzept soll die Umsetzung von HCC beim Bieter im Hinblick auf die aufgeführten Aspekte und Themen in jeweils kompakter Form darstellen und es der gematik damit ermöglichen, die resultierende Plattform unter den Gesichtspunkten

- Sicherheit
- Verfügbarkeit
- Prozessreife und -stabilität
- Niveau der Cloud-Integration bzw. der Automatisierung

nachzuvollziehen und zu bewerten.

Das Konzept muss folgendermaßen strukturiert sein, mindestens die geforderten Inhalte darstellen und die nachfolgenden Fragestellungen beantworten:

2.1.1 Praktikabilität der RZ-Infrastruktur für die Umsetzung von HCC

Standorte und Anbindung

- An welchen Rechenzentrumsstandorten wird HCC für TI-Flow implementiert und welche Abstände haben diese untereinander?
- Wie ist die Internet-Anbindung dieser Standorte mit Kapazitäten und Redundanzen?

Physische Sicherheit

- Welche wesentlichen Elemente der physischen Sicherheit (technisch, organisatorisch) insb. hinsichtlich Vermeidung bzw. Erkennung von Manipulationen an HCC-Hosts sind in den Rechenzentren umgesetzt?

Zertifizierungen

- Welche der durch gemSpec_HCC vorgegebenen Zertifizierungen liegen vor oder werden angestrebt (mit Zeitplan)?

Request /Response Delivery aus dem / in das Internet

- Wie wird DDoS-Protection umgesetzt?
- Wie sind SDN-Topologie und Gateways zum Mandantenkontext für eingehende Requests und ausgehende Responses umgesetzt?

HSM-Cluster

- Wie wird ein Mandantenkontext im HSM abgebildet?
- Wie wird Skalierung, Redundanz und Erweiterbarkeit des HSM-Clusters umgesetzt?

2.1.2 Umsetzung der HCC-Komponenten

2.1.2.1 Lösungsübersicht

Gesamtarchitektur

- Architekturbild der HCC-Plattform auf einer Seite
- Hauptkomponenten: HCC-Hosts, Managed Kubernetes, TDCAS, HSM-Cluster, Deployment Repository
- Managed Services der Cloud: SQL-Datenbanken, Object Storage, Message Broker, Caching, Secrets Management
- Abgrenzung Confidential und Non-Confidential: Welche Komponenten laufen im HCC-Vertrauensraum, welche in der regulären Cloud?
- Einbettung in die Gesamt-Cloud des Anbieters

Geplante Softwarearchitektur

- Welche Anteile der HCC-Funktionalität sind bereits vorhanden, werden durch Standardkomponenten abgedeckt oder werden im Projekt entwickelt?
- Welche Teile der HCC-Funktionalität werden in die Cloud-Funktionalität integriert bzw. sind als individuelle Funktionserweiterungen bereitgestellt?

2.1.2.2 HCC-Stack

Host-Technologie:

- Welche Hardware-Plattform und CC-Technologie kommen bei den HCC-Hosts zum Einsatz?
- Supply-Chain Sicherheit bei der Beschaffung von HCC-Hosts
- Abweichende Technologie der Non-Confidential-Hosts, sofern vorhanden

HCC-Stack und Host-Provisionierung:

- Wie ist der HCC-Stack aufgebaut (alle Komponenten unterhalb der Workload, wie Bootloader, Hypervisor, Provider-Komponenten, Netzwerk-Stack)?
- Wie sind die Prozesse für Änderungen am HCC-Stack definiert?
- Aus welchen Quellsystemen werden Komponenten des HCC-Stacks bezogen?
- Wie häufig ändern sich Komponenten des HCC-Stacks im zeitlichen Mittel?
- Wie wird eine temporär exklusive Provisionierung in einen Vertrauensraum durchgesetzt?

Attestationskette

- Wie erfolgen Onboarding und Registrierung (der Signer-Keys) von Hosts?
- Wie und auf welcher Basis erfolgt die Attestation von Host-Hardware?
- Wie und auf welcher Basis erfolgt die Attestation des Hypervisors?
- Wie und auf welcher Basis erfolgt die Attestation des Host-OS?
- Wie und auf welcher Basis erfolgt die Workload-Attestation?

- Welche Attestationsschritte stellen eine Verknüpfung mit einem HCC-Vertrauensraum her?
- Wie ist die kryptographische Verkettung der Attestationsschritte?
- Wie werden Kuckucksangriffe abgewehrt?

2.1.2.3 HCC-Komponenten

Deployment Repository

- Mit welcher Technologie wird das Deployment Repository umgesetzt?
- Über welche Schnittstellen wird das Deployment Repository befüllt (UI, API)?
- Wie ist die Zuordnung von Workloads zu einem HCC-Vertrauensraum umgesetzt?

TDCAS

- Wie werden Sicherheit und Manipulationsschutz des TDCAS umgesetzt (z. B. Betriebsmodus auf Dedicated Hosts, HSM-Pairing, Sealing, Rollback-Schutz für die Konfigurationsdatenbank)?
- Wie ist die Schnittstelle zur Einbringung von Policies gestaltet (Format, Autorisierung, Funktionsumfang, ...)?

HSM-Cluster

- Wie erfolgt die Initialisierung einer HCC-Partition?
- Wie wird der HSM-Cluster von anderen HCC-Komponenten genutzt?

2.1.2.4 Workload-Integration

Workload Provisionierung

- Aus welchen Quellsystemen werden Workload-Images und Konfigurationsdaten in einen Vertrauensraum provisioniert?

Container-Runtime/cVM-Runtime/Kubernetes

- Wie werden Workload OCI-Container in die Kubernetes-Umgebung eingebunden? In der Darstellung zu dieser Frage sind folgende Aspekte besonders zu berücksichtigen:
 - Minimierung der Trusted Computing Base
 - Betreiberausschluss und Kubernetes Control Plane
 - Integration von Workloads in cVMs
- Welche Skalierungs- und Verfügbarkeitsfunktionen stehen für HCC zur Verfügung?

HSM-Integration:

- Wie können Workloads Schlüssel aus dem HSM-Cluster nutzen oder beziehen?

2.1.3 Einbindung von HCC in die Cloud-Governance

Mandantenkontext (Cloud-Kunde)

- Einordnung des Mandanten als Kunde der Cloud
- Beziehung des Mandanten zum HCC-Vertrauensraum
- Sicht des Mandanten auf Confidential und Non-Confidential Ressourcen

Kapazitätsmanagement

- Welche Prozesse sind für das Kapazitätsmanagement der Rechenzentren bereits etabliert?
- Wie wird das Kapazitätsmanagement spezifisch für die HCC-Infrastruktur umgesetzt?
- Welches Sizing ist für HCC-Hosts vorgesehen (CPU-Cores, Arbeitsspeicher)?

Trust Domain Provider

- Wie verwaltet der Trust Domain Provider (gematik) seinen Vertrauensraum?

Mandantenkontext

- Welche Konfigurationsmöglichkeiten hat ein Mandant für HCC-Ressourcen?
- Welche Rollen sind für einen Mandanten definiert?
- Wie werden Nutzer eines Mandanten authentisiert und autorisiert?

2.2 Konzept 2 (K-02): Umsetzungskonzept CI/CD (max. 13 Seiten)

Zielsetzung: Die Ausführungen sollen es dem AG ermöglichen, die grundsätzliche Lösungskompetenz des Bieters in Bezug auf die CI/CD-Plattform einzuschätzen, die vom Bieter geplante Umsetzung auf Plausibilität zu prüfen sowie seitens des Bieters eingebrachte Kompetenzen, Technologien und Möglichkeiten zu bewerten.

Das Konzept muss folgendermaßen strukturiert sein und mindestens die geforderten Inhalte darstellen und die nachfolgenden Fragestellungen beantworten:

2.2.1 Systemarchitektur, Organisations- und Berechtigungsmodell (Architekturbild)

- Was sind wesentliche Software- und Plattformkomponenten und wie werden sie bereitgestellt?
- Welche Interaktionen und Datenflüsse gibt es zwischen Komponenten und Nachbarsystemen?
- Welches sind die Schnittstellen zwischen CI/CD-Plattform und HCC-Cloud?
- Welche Technologien, Frameworks, Werkzeuge und Standardprodukte werden verwendet?
- Welche Komponenten sind vorhanden, zu konfigurieren, neu zu entwickeln oder werden von Drittanbietern bereitgestellt?
- Wie sind Organisations-, Mandanten-, Projekt- und Namespace-Modell aufgebaut?
- Wie ist das Rollen- und Berechtigungsmodell einschließlich administrativer Rechte des AG aufgebaut?
- Wie kann der AG eigenständig weitere Fachdiensthersteller und Nutzer berechtigen?
- Wie werden nichtfunktionale Eigenschaften, SCS-Prinzipien, Sicherheit, Verfügbarkeit, Skalierbarkeit und Überwachbarkeit, umgesetzt?

2.2.2 Repository-, Pipeline- und Runner-Konzept

- Welche Funktionen für die Ablage und Versionierung der vom AG oder von berechtigten Dritten bereitgestellten Quellen sind vorhanden?
- Wer kann die fachliche Struktur, Reihenfolge und Logik der Pipelines festlegen?
- Welche Branch-, Merge-/Pull-Request-, Review- und Freigabeverfahren stehen dem AG zur Verfügung?

2.2.3 Artefakt-, Registry- und Supply-Chain-Konzept

- Ist die Registry OCI-konform?
- Wie werden Nutzungskontexte der Registry-Instanzen auf CI/CD-Plattform und HCC-Cloud abgegrenzt?
- Wie werden Rollen-, Projekt-, Mandanten- und Stagebezüge abgesichert?
- Wie werden Stage-Repositories bzw. HCC Trust Domain Repositories berücksichtigt?
- Wie werden die Aufbewahrung, Bereinigung und Löschung von Artefakten umgesetzt?
- Wie werden Sicherheits- und Nachweisartefakten zu Hauptartefakten zugeordnet?
- Werden SBOM, Signaturen, Attestierungen, Build-Attestations, VEX und Vulnerability Reports unterstützt?

2.2.4 Integration, Freigabe, Promotion und Deployment zwischen CI/CD-Plattform und HCC-Cloud

- Wie sind Verantwortlichkeiten zwischen CI/CD-Plattform und HCC-Cloud aufgeteilt?
- Welche Authentifizierungs- und Autorisierungsverfahren kommen an den Schnittstellen zur Anwendung?
- Wie werden Artefakte an die HCC-Cloud-Umgebungen übergeben und deployed?
- Wie werden Laufzeit-, Versions- und Attestierungsinformationen verarbeitet?
- Wie werden Status-, Fehler- und Ergebnismeldungen verarbeitet?
- Welche Test-, Prüf-, Freigabe-, Promotion- und Deploymentprozesse werden unterstützt?
- Sind mehrstufige Freigaberegeln, Vier-Augen-Prinzip und Rollentrennung möglich?
- Wird die Ablage von Testergebnissen, Logs und Testartefakten unterstützt?
- Wie ist eine eindeutige Zuordnung von Quellstand, Pipeline-Lauf, Artefakt, Nachweisen, Freigabe und Zielumgebung gewährleistet?
- Welche Audit-, Such-, Filter- und Exportmöglichkeiten sind möglich?

2.2.5 Umsetzung, technische Betriebsfähigkeit und Portabilität der CI/CD-Plattform

- Wie wird die CI/CD-Plattform bereitgestellt, konfiguriert und abgesichert?

- Wie kann die CI/CD-Plattform stufenweise vom Prototyp bis zur vollständigen Plattform umgesetzt werden?
- Welche Abhängigkeiten, Voraussetzungen und Meilensteine bestehen für die Umsetzung?
- Welche Funktion zum Monitoring, Logging, Metriken, Tracing, Alarmierung und zur technische Fehleranalyse sind vorhanden?
- Wie können Plattform- und Runner-Ressourcen skaliert werden?
- Welche Funktionen zur Datensicherung, Wiederherstellung und Wiederanlauf sind vorhanden?
- Wie ist die CI/CD-Plattform Betriebs-, Support-, Monitoring- und Auditprozesse technisch integriert?
- Wie können Repositories, Pipelines, Konfigurationen, Artefakten und Betriebsinformationen zu einem anderen Anbieter portiert werden?
- Welche Hersteller- und Plattformabhängigkeiten bestehen für die CI/CD-Plattform?
- Welche Risiken, Einschränkungen und offene Architekturentscheidungen sind für die CI/CD-Plattform bekannt?

2.3 Konzept 3 (K-03): Testkonzept HCC_Bietername (max. 15 Seiten)

Zielsetzung: Die Ausführungen sollen es dem AG ermöglichen, die geplante Testvorgehensweise des Auftragnehmers zu bewerten und zu beurteilen, ob alle relevanten Anforderungen berücksichtigt werden, die an den Test gestellt werden. Das Testkonzept soll eine transparente Grundlage für die Konzeption, Planung, Durchführung und Nachverfolgung der Testaktivitäten schaffen und dabei die Nachvollziehbarkeit der Ergebnisse sowie die frühzeitige Identifikation und Minimierung von Projektrisiken gewährleisten.

Das vom Auftragnehmer in der Projektphase weiter auszuarbeitende Testkonzept ist auf Grundlage der vom Auftraggeber bereitgestellten Vorlage zu erstellen, die auf der Standard-Vorlage gemäß [gemKPT Test] basiert. Für das im Rahmen des Angebots einzureichende Testkonzept HCC sind die nachfolgend aufgeführten Kapitel dieser Vorlage vom Bieter auszufüllen:

Der AN muss in der vorgegebenen Vorlage die folgenden Kapitel befüllen:

- Prüfgegenstand und Vorgehen (Kapitel 3 und 4)
 - 3.1 Testobjekte und ihre Identifizierung,
 - 3.3 Abgrenzung der Testgegenstände (generische Cloud / HCC / CI/CD-Plattform / Fachdienst),
 - 4.1 Herangehensweise und geplante Teststufen
 - 4.3 Einbindung in die CI/CD-Strecke,
- Prüfschwerpunkte und Nachweisführung (Kapitel 5 und 8)
 - 5.1 Funktionale Prüfschwerpunkte
 - 5.2 Nichtfunktionale Prüfschwerpunkte

- 8.1 Nachweisführung und Traceability,
- 8.2 Ablage von Testreports in der Artefakt-Registry,
- Attestierung und Bereitstellungsprozess (Kapitel 9)
 - 9 Attestierung und Bereitstellungsprozess
- Testumgebung und Unterstützung Dritter (Kapitel 10 und 11)
 - 10.1 Werkzeuge und Simulatoren,
 - 10.2 Mocks sowie die Anforderungen an die Testumgebung
 - 11 Unterstützung des AG und Dritter – Maßnahmen zur Unterstützung des AG und Dritter, geplante Integrationstests

Alle weiteren Kapitel des vorgegebenen Testkonzept-Templates müssen durch den AN erst nach Beauftragung geliefert werden. Ausfüllhinweise für das jeweilige Kapitel sind in der Vorlage hinterlegt.

2.4 Konzept 4 (K-04): Testkonzept CI/CD-Plattform (max. 5 Seiten)

Zielsetzung: Das Testkonzept CI/CD-Plattform legt die für die CI/CD-Plattform spezifischen Testgegenstände, Prüfschwerpunkte, Nachweisformen und Abgrenzungen der Testkonzeption fest. Es ermöglicht dem Auftraggeber die Bewertung und Beurteilung der geplanten Testvorgehensweise des Auftragnehmers. Das Testkonzept schafft eine transparente Grundlage für die Konzeption, Planung, Durchführung und Nachverfolgung der Testaktivitäten und gewährleistet dabei die Nachvollziehbarkeit der Ergebnisse sowie die frühzeitige Identifikation und Minimierung von Projektrisiken.

Das Konzept muss folgendermaßen strukturiert sein und mindestens die geforderten Inhalte darstellen:

2.4.1 Teststrategie und Teststufen

- Die grundsätzliche Herangehensweise an die Prüfung der CI/CD-Plattform, die vorgesehenen Teststufen und ihre Einbindung in die CI/CD-Strecke.

2.4.2 Testvorgehen und Nachweisführung

- Abgrenzung des Testvorgehens – die Abgrenzung zwischen generischen Cloud-Funktionalitäten, HCC-spezifischen Funktionalitäten, Funktionen der CI/CD-Plattform und fachlichen Fachdienstthemen.
- Nachweisführung und Traceability – die vorgesehene Nachweisform, die Zuordnung von Prüfnachweisen zu Quellcode-, Build-, Artefakt-, Konfigurations- und Release-Ständen sowie der Zugriff des AG auf die Nachweise.
- Verwendung von Standardnachweisen – Darstellung, in welchem Umfang für Standardprodukte auf Hersteller-, Betriebs-, Sicherheits- oder Zertifizierungsnachweise zurückgegriffen wird und für welche Prüfgegenstände eigene Nachweise vorgesehen sind.

2.4.3 Anbindung der Testumgebung

- Die Anbindung der Testumgebung an die CI/CD-Strecke einschließlich des Deployment-Pfades sowie die Unterscheidung, welche Gegenstellen durch Mocks ersetzt und welche real angebunden werden.

2.5 Konzept 5 (K-05): Betriebskonzept HCC (max. 30 Seiten)

Zielsetzung: Die Ausführungen sollen es dem AG ermöglichen, die Betriebsreife, Servicequalität, Leistungsfähigkeit, Skalierbarkeit und Resilienz der angebotenen HCC-Cloud-Plattform zu bewerten. Der Bieter hat darzustellen, wie ein sicherer, stabiler, hochverfügbarer und leistungsfähiger Betrieb der angebotenen Infrastruktur- und Plattformdienste gewährleistet wird und wie diese Dienste den Betrieb geschäftskritischer Fachanwendungen unterstützen.

Das Betriebskonzept beschreibt die wesentlichen Bestandteile und Leistungsmerkmale der Betriebsorganisation des Bieters sowie die Prozesse und Verfahren zur Sicherstellung eines ordnungsgemäßen, sicheren, stabilen, hochverfügbaren und leistungsfähigen Betriebs der angebotenen HCC-Cloud-Plattform.

Der Schwerpunkt des Betriebskonzepts liegt auf den organisatorischen, prozessualen und operativen Aspekten des Betriebs. Technische Architekturdetails, die bereits im Umsetzungskonzept HCC (K-01) dargestellt werden, sind nur insoweit aufzugreifen, wie dies zum Verständnis der Betriebsprozesse erforderlich ist.

Das Betriebskonzept soll insbesondere darlegen, wie der Bieter die Servicequalität, Betriebsstabilität, Verfügbarkeit, Leistungsfähigkeit, Skalierbarkeit und Resilienz der angebotenen Infrastruktur- und Plattformdienste sicherstellt, überwacht und kontinuierlich verbessert.

Das Betriebskonzept muss folgendermaßen strukturiert sein, mindestens die geforderten Inhalte darstellen und die nachfolgenden Fragestellungen beantworten:

2.5.1 Betriebsorganisation

Betriebsorganisation

- Wie ist die Betriebsorganisation einschließlich Rollen, Verantwortlichkeiten, Vertretungsregelungen und Eskalationsstufen aufgebaut?
- Welche Betriebsleistungen werden durch eigenes Personal und welche durch Unterauftragnehmer erbracht?
- Welche Betriebsfunktionen werden 24/7/365 bereitgestellt?
- Welche organisatorischen Maßnahmen stellen die Handlungsfähigkeit bei Ausfall einzelner Schlüsselpersonen sicher?

Zusammenarbeit mit Auftraggeber und Diensteanbietern

- Wie erfolgt die Zusammenarbeit zwischen Auftragnehmer, Auftraggeber und den Mandanten der auf der HCC-Cloud betriebenen Dienste?
- Welche Kommunikations-, Melde- und Eskalationswege werden genutzt?
- Welche betrieblichen Schnittstellen und Übergabepunkte bestehen zwischen den beteiligten Organisationen?

Qualitätsnachweise

- Welche verbindlichen internen Reaktionszeiten gelten für kritische Betriebsereignisse und wie wird deren Einhaltung überwacht?
- Wie hoch war die tatsächliche Einhaltung dieser Reaktionszeiten in den letzten 12 Monaten für vergleichbare produktive Plattformdienste?
- Wie werden Verbesserungspotenziale identifiziert, priorisiert und nachverfolgt und welche messbaren Verbesserungen wurden hierdurch in den letzten 12 Monaten erzielt?

2.5.2 Reporting- und Eskalationsmanagement

- Welche Betriebs-, Qualitäts- und Serviceberichte werden bereitgestellt?
- Welche Kennzahlen werden standardmäßig ausgewertet und berichtet?
- In welchen Intervallen werden diese Kennzahlen ausgewertet und die Berichte bereitgestellt?

Eskalationsmanagement

- Welche internen Eskalationsstufen & -mechanismen sind definiert?
- Wie erfolgt die Eskalation bei Störungen, SLA-Verletzungen und Sicherheitsereignissen?
- Wie werden Auftraggeber und Mandanten informiert?

Qualitätsnachweise

- Welche Kennzahlen werden zur Bewertung der Servicequalität verwendet und welchen Zielwerten unterliegen diese?
- Wie werden wiederkehrende Betriebsprobleme identifiziert, priorisiert und nachhaltig beseitigt?
- Innerhalb welcher Fristen werden Ursachenanalysen für kritische Betriebsstörungen erstellt und wie hoch war die Einhaltungquote dieser Fristen in den letzten 12 Monaten?

2.5.3 Monitoring, Telemetrie und Betriebsdaten

Monitoring

- Welche Infrastruktur-, Plattform-, Netzwerk- und Sicherheitsmetriken werden standardmäßig überwacht?
- Welche Monitoring-Werkzeuge kommen zum Einsatz?
- Welche Messpunkte existieren entlang der Servicekette?

Telemetrie

- Welche Betriebs- und Telemetriedaten stehen Mandanten zur Verfügung?
- In welcher Granularität und Aktualität werden diese Daten bereitgestellt?
- Welche Schnittstellen für den Abruf dieser Daten werden unterstützt?

Integration

- Wie erfolgt die Bereitstellung von Monitoring- und Telemetriedaten für Systeme der gematik?

- Welche Möglichkeiten bestehen zur Integration in Monitoring-Lösungen?

Qualitätsnachweise

- Welche mittlere Zeitspanne zwischen Auftreten und Erkennung kritischer Infrastruktur- oder Plattformstörungen wurde in den letzten 12 Monaten für vergleichbare produktive Plattformdienste erreicht (Mean Time to Detect)?
- Welche Betriebs-, Kapazitäts-, Verfügbarkeits- und Performancekennzahlen stehen Mandanten standardmäßig zur Verfügung und in welcher zeitlichen Auflösung?
- Welche Monitoring-, Analyse- und Exportfunktionen können Mandanten eigenständig nutzen und welche Einschränkungen bestehen hierbei?
- Welche Metriken unterstützen die Abgrenzung von Infrastruktur-, Plattform- und Anwendungsproblemen?

2.5.4 Capacity Management

Kapazitätsplanung

- Wie erfolgen Kapazitätsplanung, Kapazitätsüberwachung und Bedarfsprognosen?
- Welche Planungszeiträume und Prognoseverfahren werden verwendet?
- Welche Kennzahlen fließen in die Kapazitätsplanung ein?

Skalierung

- Wie erfolgt die Bereitstellung zusätzlicher Kapazitäten?
- Welche automatisierten Skalierungsmechanismen werden unterstützt?
- Wie werden Lastspitzen erkannt und verarbeitet?

Kapazitätsreserven

- Welche Kapazitätsreserven werden dauerhaft vorgehalten?
- Wie werden Ressourcenengpässe vermieden?
- Wie erfolgt die Priorisierung bei konkurrierenden Ressourcenanforderungen?

Qualitätsnachweise

- Welche zusätzlichen Compute-, Storage- und Netzwerkressourcen können innerhalb von 15, 30 und 60 Minuten bereitgestellt werden?
- Welche maximale Laststeigerung kann ohne manuelle Eingriffe verarbeitet werden?
- Welche tatsächlichen Skalierungszeiten wurden in den letzten 12 Monaten für vergleichbare Plattformdienste erreicht?
- Wie wird sichergestellt, dass Plattformdienste auch bei außergewöhnlichen Lastsituationen die vereinbarten Leistungswerte erreichen?

2.5.5 IT-Service-Management

ITSM-Prozesse

- Welche ITSM-Prozesse werden eingesetzt?
- Welche Rollen, Verantwortlichkeiten und Werkzeuge unterstützen die Prozesse?

- Wie werden Incidents, Problems, Changes, Releases und Configuration Items verwaltet?
- Welche Service Level werden für ITSM-Prozesse zugesichert?
- Welche Eskalationsmöglichkeiten werden dem AG und den Mandanten geboten?

Integration

- Wie erfolgt die Integration der ITSM-Prozesse mit den Prozessen von gematik und Mandanten?
- Welche Schnittstellen und Integrationsmechanismen werden hierfür bereitgestellt?

Qualitätsnachweise

- Welcher Anteil der Incident-, Change-, Provisionierungs- und Wiederherstellungsprozesse erfolgt automatisiert?
- Welche Service-Management-Kennzahlen werden erhoben und welche Zielwerte gelten hierfür?
- Welche Mean Time to Detect (MTTD) und Mean Time to Restore (MTTR) wurden im letzten Kalenderjahr für kritische Betriebsstörungen erreicht?
- Wie wird die dauerhafte Beseitigung wiederkehrender Störungen sichergestellt?

2.5.6 Change- und Release-Management

Change-Management

- Wie werden Infrastruktur- und Plattformänderungen geplant, bewertet, freigegeben und umgesetzt?
- Welche Verfahren zur Risikobewertung kommen zum Einsatz?
- Wie werden Auswirkungen auf Mandanten und Plattformnutzer berücksichtigt?

Release Management

- Wie werden Releases vorbereitet, getestet und eingeführt?
- Welche Rückfallverfahren stehen zur Verfügung?

Beteiligung

- Wie werden Auftraggeber und Mandanten in Change- und Release-Prozesse eingebunden?
- Welche Vorankündigungsfristen werden angewendet?

Qualitätsnachweise

- Wie hoch war die Erfolgsquote produktiver Changes im letzten Kalenderjahr für vergleichbare Plattformdienste?
- Wie hoch war die Rollback-Quote produktiver Changes im letzten Kalenderjahr?
- Welcher Anteil produktiver Änderungen erfolgt ohne geplante Betriebsunterbrechung?
- Welcher Anteil produktiver Änderungen wird vollständig automatisiert durchgeführt?

2.5.7 SLA-Konzept

KPI- und SLA-Modell

- Welche Leistungs-, Verfügbarkeits-, Kapazitäts- und Betriebskennzahlen empfiehlt der Bieter für die vertragliche Steuerung und Überwachung der angebotenen Infrastruktur- und Plattformdienste?
- Welche der vorgeschlagenen Kennzahlen empfiehlt der Bieter als SLA-relevante Kennzahlen?
- Welche Zielwerte empfiehlt der Bieter für die vorgeschlagenen Kennzahlen?
- Welche Schwellwerte und Eskalationsgrenzen empfiehlt der Bieter für die vorgeschlagenen Kennzahlen?
- Wie werden die vorgeschlagenen Kennzahlen gemessen, berechnet und nachgewiesen?
- Welche Messpunkte werden für die Erhebung der Kennzahlen verwendet?
- Welche Kennzahlen können durch den Auftraggeber oder die Mandanten unabhängig überprüft werden?
- Welche Kennzahlen eignen sich aus Sicht des Bieters zur frühzeitigen Erkennung von Verfügbarkeits-, Performance- oder Kapazitätsproblemen?
- Welche Kennzahlen verwendet der Bieter selbst zur operativen Steuerung vergleichbarer produktiver Plattformdienste?
- Welche Zusammenhänge bestehen zwischen den vorgeschlagenen Kennzahlen und den angebotenen Service Levels?

Zusätzlich hat der Bieter die aus seiner Sicht zehn wichtigsten SLA-relevanten Kennzahlen für den Betrieb geschäftskritischer Anwendungen auf der angebotenen Plattform zu benennen. Für jede Kennzahl sind Zweck, Messmethode, Messpunkt, Messintervall, Zielwert, Schwellwert, Eskalationsgrenze sowie die betriebliche Aussagekraft darzustellen.

Hochverfügbarkeit und Resilienz

- Wie unterstützen die angebotenen Dienste den Betrieb hochverfügbarer und geschäftskritischer Fachanwendungen?
- Welche Architekturannahmen liegen den Verfügbarkeitszusagen zugrunde?
- Welche automatisch wirksamen Failover-Mechanismen bestehen?
- Innerhalb welcher Zeit erfolgt ein Failover bei Ausfall einzelner Infrastrukturkomponenten, Availability Zones oder Standorte?
- Welche technischen und organisatorischen Maßnahmen werden eingesetzt, um ungeplante Ausfälle zu vermeiden?
- Welche Abhängigkeiten bestehen zwischen den angebotenen Diensten hinsichtlich ihrer Verfügbarkeit?

Desaster Recovery

- Welche RPO- und RTO-Werte gelten für die angebotenen Dienste?
- Welche Wiederanlauf- und Wiederherstellungsverfahren kommen zum Einsatz?
- Wann wurden die letzten Tests zur Überprüfung der Wiederherstellungsfähigkeit durchgeführt?
- Welche Wiederherstellungszeiten und Datenverlustzeiträume wurden hierbei tatsächlich erreicht?
- Wie häufig werden Wiederherstellungstests durchgeführt?

- Welche Einschränkungen bestehen während eines Disaster-Falls für die angebotenen Dienste?

Leistungskennzahlen und Performance

- Welche Leistungskennzahlen werden für Compute-, Storage-, Netzwerk-, Datenbank-, Kubernetes-, HSM- sowie weitere Plattformdienste vertraglich zugesichert?
- Welche Latenz-, Durchsatz-, Antwortzeit- und Kapazitätswerte werden garantiert?
- Welche Leistungswerte werden für die Kommunikation zwischen Availability Zones und Standorten erreicht?
- Welche Auswirkungen haben Lastsituationen, Ressourcenauslastungen und Kapazitätsengpässe auf die zugesicherten Leistungswerte?
- Welche Maßnahmen werden zur Sicherstellung der Leistungsfähigkeit bei Laststeigerungen und Skalierungsvorgängen eingesetzt?
- Welche Mechanismen werden eingesetzt, um Performance-Degradation frühzeitig zu erkennen und zu verhindern?

Messung und Nachweis

- Wie werden Leistungs-, Verfügbarkeits- und Kapazitätskennzahlen gemessen, überwacht und nachgewiesen?
- Welche Messpunkte werden genutzt?
- Welche Datenquellen liegen den Nachweisen zugrunde?
- Welche Leistungskennzahlen können Mandanten selbst überwachen?
- Welche Berichte, Dashboards oder Schnittstellen werden zur Verfügung gestellt?
- Wie wird sichergestellt, dass die Messwerte nachvollziehbar, revisionssicher und reproduzierbar sind?

Qualitätsnachweise

- Welche tatsächlichen Verfügbarkeiten wurden für vergleichbare produktive Plattformdienste in den letzten 12 Monaten erreicht?
- Welche tatsächlichen Performancewerte werden regelmäßig gemessen und ausgewertet?
- Welche P95- und P99-Leistungswerte werden für die angebotenen Plattformdienste kontinuierlich gemessen?
- Welche Zielwerte gelten für diese Kennzahlen?
- Welche Maßnahmen werden bei Performanceverschlechterungen automatisch oder manuell eingeleitet?
- Welche tatsächlichen RPO- und RTO-Werte wurden bei Wiederherstellungstests erreicht?
- Wann wurde zuletzt ein Ausfall einer Availability Zone oder eines Rechenzentrums getestet und welche wesentlichen Ergebnisse wurden dabei erzielt?
- Welche Erkenntnisse aus den gewonnenen Betriebskennzahlen haben in den vergangenen 12 Monaten zu konkreten Verbesserungsmaßnahmen geführt?

Die Aussagen sind anhand konkreter Betriebskennzahlen, Erfahrungswerte aus produktiven Umgebungen oder etablierter Betriebsverfahren nachvollziehbar zu begründen.

2.5.8 Abrechnungsmodell

Abrechnungsverfahren

- Wie erfolgt die Abrechnung der angebotenen Services sowie deren Serviceklassen und ggf. vorhandenen Leistungsklassen?
- Welche Messpunkte und Messwerte liegen der Abrechnung zugrunde?
- Welche Preisparameter bestimmen die Kosten?

Verbrauchsnachweis

- Wie werden mandantenspezifischen Verbrauchsdaten erfasst und nachgewiesen?
- Wie erfolgt die revisionssichere Speicherung der Abrechnungsdaten?

Planbarkeit

- Welche Möglichkeiten bestehen zur Kostenprognose?
- Welche Modelle für reservierte und verbrauchsabhängige Ressourcen werden angeboten?

Qualitätsnachweise

- Welche Maßnahmen stellen die Nachvollziehbarkeit und Revisionssicherheit der Abrechnung sicher?
- Welche Mechanismen verhindern unerwartete Kostensteigerungen?
- Welche unabhängigen Prüfungen oder Zertifizierungen existieren für das Abrechnungsverfahren?
- Welche Abweichung zwischen prognostizierten und tatsächlichen Kosten wird für vergleichbare Nutzungsszenarien typischerweise beobachtet?

2.5.9 Eigenmonitoring und Anomalieerkennung

Anomalieerkennung

- Welche Verfahren zur automatisierten Erkennung von Betriebs-, Sicherheits- und Performanceanomalien werden eingesetzt?
- Welche Datenquellen werden ausgewertet?

Alarmierung

- Welche Schwellwerte, Regeln und Alarmierungsmechanismen kommen zum Einsatz?
- Wie werden kritische Ereignisse priorisiert?

Maßnahmen

- Welche automatisierten Gegenmaßnahmen können ausgelöst werden?
- Welche manuellen Maßnahmen sind vorgesehen?

Qualitätsnachweise

- Welche Arten von Anomalien können automatisiert erkannt werden?
- Welche mittlere Zeitspanne zwischen Auftreten und Erkennung einer Anomalie wird erreicht?
- Welcher Anteil kritischer Betriebsereignisse wird automatisiert erkannt?
- Wie hoch ist die Fehlalarmquote der eingesetzten Verfahren?
- Wie wird die Qualität der Anomalieerkennung kontinuierlich verbessert?

2.6 Konzept 6 (K-06): Betriebskonzept CI/CD-Plattform (max. 15 Seiten)

Zielsetzung: Die Ausführungen sollen es dem AG ermöglichen die Betriebsreife, Servicequalität, Leistungsfähigkeit und Resilienz der angebotenen CI/CD-Plattform zu bewerten. Der Bieter hat darzustellen, wie der sichere, stabile, nachvollziehbare und für berechnigte Nutzergruppen verfügbare Betrieb der Plattform gewährleistet und wie die Plattform für die Prozesse des AG bereitgestellt, überwacht und kontinuierlich verbessert wird.

Das Betriebskonzept beschreibt den Betrieb der CI/CD-Plattform als eigenständige Plattform. Es stellt dar, wie der sichere, stabile, nachvollziehbare und für berechnigte Nutzergruppen verfügbare Betrieb sichergestellt wird. Soweit für den Betrieb der CI/CD-Plattform dieselben Strukturen, Prozesse und Organisationseinheiten genutzt werden wie für die HCC-Cloud, kann auf das Betriebskonzept HCC verwiesen werden. Die Verweise auf das HCC-Betriebskonzept und die daraus genutzten Strukturen, Prozesse und Organisationseinheiten sind eindeutig zu referenzieren. Abweichungen und CI/CD-spezifische Besonderheiten sind eigenständig darzustellen.

Das Betriebskonzept CI/CD-Plattform muss folgendermaßen strukturiert sein, mindestens die geforderten Inhalte darstellen:

2.6.1 Betriebsmodell, Organisation und Verantwortlichkeiten

- Betriebsmodell mit Leistungsumfang, Betriebszeiten und Abgrenzung zu Projekt- und Umsetzungsleistungen
- Betriebsorganisation mit Rollen, Verantwortlichkeiten, Vertretungen und Ansprechpartnern
- Abgrenzung der Verantwortlichkeiten zwischen AN, AG, HCC-Cloud-Betrieb und weiteren Beteiligten
- Governance-, Entscheidungs-, Abstimmungs-, Berichts- und Eskalationswege
- Regelungen für administrative Zugriffe, Übergaben, Dokumentation und Mitwirkungspflichten

2.6.2 Betriebsprozesse und Service Management

- Prozesse für Incident-, Problem-, Change-, Release- und Configuration-Management
- Service-Request- und Zugriffsmanagement einschließlich Nachverfolgung und Genehmigung
- SLAs bzw. Serviceziele, Prioritäten, Reaktions-, Wiederherstellungs- und Lösungszeiten
- Wartungsfenster, geplante Änderungen, Kommunikation und Abstimmung mit dem AG
- Dokumentation, Ticketing, Wissensmanagement sowie regelmäßige Serviceberichte und Reviews

2.6.3 Überwachung, Ereignis- und Störungsmanagement

- Monitoring von Verfügbarkeit, Zustand, Kapazität, Performance und zentralen Plattformdiensten
- Zentrale Erfassung und Korrelation von Logs, Metriken, Traces und sicherheitsrelevanten Ereignissen
- Alarmierung mit Schwellwerten, Prioritäten, Bereitschaften und Eskalationsketten
- Erkennung, Analyse, Behebung und Dokumentation von Störungen einschließlich Root-Cause-Analyse
- Verfügbarkeit von Betriebsinformationen, Dashboards, Berichten und Auditnachweisen für den AG

2.6.4 Sicherheits-, Schwachstellen- und Änderungsbetrieb

- Betriebliche Umsetzung von Identitäts-, Berechtigungs-, Geheimnis- und Schlüsselmanagement
- Vulnerability-, Patch- und Update-Management für Plattform, Runner, Images und Abhängigkeiten
- Sicherheitsmonitoring, Behandlung von Sicherheitsvorfällen und Einbindung des AG
- Härtung, Konfigurationskontrolle, regelmäßige Überprüfung und Nachweisführung
- Kontrollierte Behandlung von Ausnahmen, Risiken, Findings und technischen Schulden

2.6.5 Kapazität, Kontinuität, Datensicherung und Exit

- Kapazitäts-, Performance- und Skalierungsmanagement für Plattform- und Runner-Ressourcen
- Datensicherungs-, Wiederherstellungs- und Wiederanlaufverfahren einschließlich RPO und RTO
- Notfallvorsorge, Ausfall- und Wiederanlaufszszenarien sowie regelmäßige Übungen und Tests
- Lebenszyklus, Aufbewahrung und Wiederherstellung von Repositories, Konfigurationen, Artefakten und Betriebsdaten
- Portabilität, Datenexport, Betriebsübergabe, Exit-Unterstützung und geordnete Beendigung des Betriebs

2.7 Konzept 7 (K-07): Souveränitätskonzept (max. 10 Seiten)

Zielsetzung: Die Ausführungen im Souveränitätskonzept dienen der Darstellung, wie der Bieter die in der Leistungsbeschreibung festgelegten Souveränitätsanforderungen umsetzt. Die Ausführungen sollen es dem AG insbesondere ermöglichen, die rechtlichen, technischen und wirtschaftlichen Abhängigkeiten der angebotenen Services sowie die hieraus resultierenden Risiken für einen selbstbestimmten und autonomen Betrieb zu bewerten.

Das Souveränitätskonzept ersetzt oder modifiziert die in der Leistungsbeschreibung festgelegten Souveränitätsanforderungen nicht. Bei etwaigen Abweichungen im Souveränitätskonzept gehen die Anforderungen der Leistungsbeschreibung vor.

Der Bieter hat bei der Konzepterstellung nachfolgende Gliederung einzuhalten und die geforderten Inhalte nachvollziehbar und bezogen auf die angebotene Lösung darzustellen:

2.7.1 Governance-, Eigentums- und Kontrollstrukturen

Der Bieter erläutert die für die angebotene Leistung relevanten Governance-, Eigentums- und Kontrollstrukturen.

Die Darstellung umfasst mindestens:

- Konzernstrukturen, in die der Bieter und gegebenenfalls die Mitglieder der etwaigen Bietergemeinschaft (im Folgenden: "Konsortialpartner") eingebunden sind und wie diese aufgebaut sind
- unmittelbare und mittelbare Eigentums- und Beteiligungsverhältnisse einschließlich der wirtschaftlich Berechtigten
- bestehende Weisungs-, Kontroll-, Veto- oder vergleichbare Einflussrechte Dritter auf den Bieter und/oder seine Konsortialpartner
- Für die Leistungserbringung relevante Mutter-, Tochter- und Schwesterunternehmen sowie deren Funktion bei der Leistungserbringung
- Weitere Beteiligungs- und Kontrollverhältnisse, soweit diese Einfluss auf die digitale Souveränität oder die Leistungserbringung haben können

2.7.2 Drittstaaten- und Jurisdiktionsrisiken

Der Bieter erläutert die für die angebotene Leistung bestehenden Drittstaaten- und Jurisdiktionsrisiken sowie die vorgesehenen Maßnahmen zu deren Beherrschung.

Die Darstellung beinhaltet mindestens:

- Rechtsordnungen und sonstige Regelungen von Staaten außerhalb der EU/des EWR, denen der Bieter, etwaige Konsortialpartner, relevante verbundene Unternehmen oder sonstige für die Leistungserbringung wesentliche Unternehmen unterliegen
- daraus ggf. Resultierende rechtliche oder tatsächliche Einflussmöglichkeiten auf Daten, Systeme, betriebliche Prozesse oder die Fortführung der Leistungserbringung
- die vom Bieter identifizierten Auswirkungen und Risiken für die Leistungserbringung
- technische, organisatorische und rechtliche Maßnahmen zur Verhinderung, Abwehr oder Begrenzung extraterritorialer Zugriffe und Störungen oder sonstiger Drittstaateneinflüsse
- Vorgehensweise für den Fall staatlicher Zugriffs-, Herausgabe-, Unterlassungs- oder sonstiger Maßnahmen eines Drittstaates, soweit diese die Leistungserbringung beeinträchtigen können

Dabei ist insbesondere darzustellen, durch welche technischen und organisatorischen Maßnahmen die Anforderungen der Leistungsbeschreibung erfüllt werden. Bloße Verweise auf vertragliche Regelungen oder allgemeine Risikoanalysen sind nicht ausreichend.

2.7.3 EU-basierter Betrieb, Betriebsautonomie und Disconnect-Fähigkeit

a) EU-basierter Betrieb und Betriebsautonomie

Der Bieter legt dar, durch welche technischen und organisatorischen Maßnahmen der EU-basierte Betrieb und die Betriebsautonomie der angebotenen Lösung unter Berücksichtigung der Vorgaben der Leistungsbeschreibung gewährleistet werden kann.

Das umfasst mindestens:

- Betriebsmodell, Standorte der für Betrieb, Administration, Wartung etc. eingesetzten Einheiten
- techn. und org. Maßnahmen zur Verhinderung privilegierter Admin-Zugriffe von außerhalb der EU
- eingesetzte Dienste für Schlüssel- und Zertifikatsmanagement, Monitoring, Sicherheitsüberwachung, Authentifizierung etc. und Standorte sowie externe Abhängigkeiten

b) Disconnect-Fähigkeiten und Disconnect-Tests

Der Bieter beschreibt ein Disconnect-Szenario und stellt insbesondere folgendes dar:

- Durch welche technischen und organisatorischen Maßnahmen wird die Betriebsfähigkeit im Falle einer dauerhaften Unterbrechung sämtlicher Verbindungen zu Organisationseinheiten, Dienstleistern und Infrastrukturen außerhalb der EU aufrechterhalten?
- Welche Funktionen stehen im Disconnect-Fall unverändert, eingeschränkt oder ggf. gar nicht mehr zur Verfügung?
- Wie wird die Disconnect-Fähigkeit nachgewiesen?

2.7.4 Lieferkettensouveränität und Unterauftragnehmereinbindung

- Der Bieter stellt dar, inwieweit er ein dokumentiertes Inventar der Hardware-Komponenten führt, die zur Bereitstellung der Cloud-Dienste verwendet werden, eine Liste der relevanten Hardware-Lieferanten sowie deren Herkunftsländer erstellt und diese dem Auftraggeber auf Anfrage zur Verfügung stellt.
- Der Bieter stellt dar, inwieweit er Prozesse zur Identifikation und Minderung von Risiken im Zusammenhang mit Exportbeschränkungen oder Lieferkettenunterbrechungen für Software, externe Dienste und Hardware etabliert hat, die zur Bereitstellung des Cloud-Dienstes eingesetzt werden. Er stellt zudem dar, inwieweit er sich verpflichtet, bei möglichen Beeinträchtigungen des Betriebs den Auftraggeber zu informieren.

2.8 Konzept 8 (K-08): gemeinsame datenschutzrechtliche Verantwortung (max. 3 Seiten)

Hinweis: Nach der in der Leistungsbeschreibung dargelegten Auffassung des Auftraggebers liegt zwischen den Auftragnehmern des Loses 1 und des Loses 2 eine gemeinsame datenschutzrechtliche Verantwortung für den TI-Flow-Fachdienst vor. Gemäß Art. 26 DSGVO ist daher zwischen beiden Auftragnehmern als gemeinsam Verantwortliche in einer Vereinbarung in transparenter Form festzulegen, wer von ihnen welche Verpflichtung nach der DSGVO erfüllt. Das betrifft insbesondere die Wahrnehmung der Rechte betroffener Personen und die Erfüllung der Informationspflichten gem. Art. 13 und 14 DSGVO. Die Vereinbarung hat die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend zu berücksichtigen.

Zielsetzung: Die Ausführungen im Konzept zur gemeinsamen datenschutzrechtlichen Verantwortung sollen es dem AG ermöglichen, die vorgesehenen Maßnahmen und Schritte zur Sicherstellung der Einhaltung der Anforderungen an die gemeinsame Datenschutzverantwortlichkeit zu bewerten.

Der Bieter hat darzustellen, wie er die vertragliche und operative Ausgestaltung der gemeinsamen datenschutzrechtlichen Verantwortlichkeit mit dem künftigen Auftragnehmer des Loses 1 sicherstellen würde.

Der Bieter hat bei der Darstellung folgende Gliederung einzuhalten und das Konzept soll insbesondere folgende Aspekte umfassen:

2.8.1 Vorgehen zum Abschluss der Vereinbarung gem. Art. 26 DSGVO

- Wie wird der Bieter bei der Abstimmung und dem Abschluss der Vereinbarung gemäß Art. 26 DSGVO mit dem zukünftigen Auftragnehmer des Loses 1 vorgehen?

2.8.2 Standardprozesse und organisatorische Verfahren

- Welche Standardprozesse, Muster oder organisatorische Verfahren zur Ausgestaltung und Umsetzung einer gemeinsamen Verantwortlichkeit bestehen beim Bieter bzw. müssten noch aufgesetzt werden und wie sollen diese im vorliegenden Fall zum Einsatz kommen?

2.8.3 Aufteilung der datenschutzrechtlichen Verpflichtungen und Zuständigkeiten

- Was ist aus Sicht des Bieters eine sachgerechte Aufteilung der datenschutzrechtlichen Verpflichtungen, Aufgaben und Zuständigkeiten zwischen den gemeinsam datenschutzrechtlichen Verantwortlichen und wie sollte sie ausgestaltet werden, insbesondere hinsichtlich der Wahrnehmung von Betroffenenrechten sowie der Erfüllung der Informationspflichten gemäß Art. 13 und 14 DSGVO?

2.8.4 Operative Umsetzung und Zusammenarbeit

- Welche organisatorische und operative Zusammenarbeit der gemeinsam datenschutzrechtlich Verantwortlichen ist vorgesehen und wie soll sie ausgestaltet werden, insbesondere die vorgesehenen Zuständigkeiten, Ansprechpartner, Kommunikations- und Abstimmungswege?

2.8.5 Umgang mit Änderungen

- Wie soll mit Änderungen der für die gemeinsame datenschutzrechtliche Verantwortlichkeit maßgeblichen Verarbeitungsvorgänge oder sonstiger für die Aufgaben- und Verantwortungsverteilung relevanter Umstände umgegangen werden?

Die Darstellung hat sich auf die konkrete Ausgestaltung und operative Umsetzung der vom Auftraggeber zugrunde gelegten gemeinsamen datenschutzrechtlichen Verantwortlichkeit zu beziehen. Allgemeine Ausführungen zur DSGVO oder eine rechtliche Bewertung der Einordnung des Auftraggebers sind nicht erforderlich.

2.9 Konzept 9 (K-09): Umsetzung der Use-Cases aus Anlage-09b (max. 10 Seiten)

Zielsetzung: Die Ausführungen solle es dem AG ermöglichen

- nachzuvollziehen, wie der für die angegebenen Use-Cases aus Anlage-09b ermittelte Preis aus dem Servicekatalog errechnet wird,
- die Auswahl und Ausprägung der eingesetzten Servicekomponenten (z.B. vCPU/Kernanzahl, Arbeitsspeicher, Speicherklassen und Plattformservices) nachzuvollziehen und
- zu bewerten, wie geeignet, vollständig und plausibel die ausgewählten Konfigurationen sind.

Der Bieter hat dazu je Use-Case die technische Umsetzung auf Basis der angebotenen Services zu beschreiben sowie eine nachvollziehbare Herleitung der Preisbestandteile auf Grundlage des eingereichten Servicekatalogs darzustellen. Anschließend sind die vorgegebenen Konfigurationen hinsichtlich ihrer Eignung für den jeweiligen Anwendungsfall zu bewerten. Die Vorgaben aus Anlage-09b sind zu beachten.

Der Bieter hat bei der Darstellung folgende Gliederung einzuhalten:

1. Use-Case PU
2. Use-Case RU
3. Use-Case RU-DEV
4. Use-Case CI/CD

Der Bieter kann dem Konzept bei Bedarf zur Erläuterung seiner Kalkulation eine MS-Excel-Datei beifügen ("Anlage-11 - K-09 Use-Cases Anlage_Bietername.xls").

2.10 Konzept 10 (K-10): Security Monitoring Konzept (max. 5 Seiten)

Zielsetzung: Die Ausführungen sollen es dem AG ermöglichen, die Kompetenz des Bieters im Security Monitoring einzuschätzen. Hierzu soll der Bieter im Rahmen der folgenden Struktur sein Konzept zum Security Monitoring darstellen.

Das Konzept muss folgendermaßen strukturiert sein, mindestens die geforderten Inhalte darstellen und die nachfolgenden Fragestellungen beantworten::

2.10.1 Mechanismen und Prozesse des Security Monitorings

- Darstellung der bestehenden Mechanismen und Prozesse des Security Monitorings beim Bieter.

2.10.2 Use-Cases bezogene Systematik:

Der Bieter soll darüber hinaus darstellen, wie er eine auf Detection Use-Cases bezogene Systematik für das Security Monitoring unter Berücksichtigung der folgenden Anforderungen entwickelt.

- Der Bieter muss Attestierungsreports aus dem TDCAS an die gematik ausleiten, zusammen mit Logs über die Bereitstellung von Credentials zur Nutzung von Schlüsselmateriale aus dem HSM-Cluster sowie den Bezug von Workload Images aus dem Deployment Repository. Grundsätzlich sind in dieser Hinsicht alle Ergebnisse von Prüfungen relevant, die zum Zwecke der Attestierung der Vertrauenswürdigkeit einer cVM und ihrer Berechtigung zum Zugriff auf bestimmte Ressourcen durchgeführt werden.
- Der Bieter stellt dar, wie er in Zusammenarbeit mit dem AG die im Hinblick auf seine technische und organisatorische Umsetzung von HCC notwendige Konkretisierung der für das Security Monitoring relevanten Informationen erarbeitet und abstimmt.
- Darstellung der spezifischen für die sicherheitstechnische Beurteilung der Kernfunktionen der HCC-Plattform durch den AG benötigten Informationen. Assets, die im Kontext der Dienstleistung eingesetzt werden:
 - i. Ergebnisse authentisierter Schwachstellenscans
 - ii. Alerts aus dem Anbieter-eigenen Security Monitoring
- Darüber hinaus beschreibt der Bieter eigene sicherheitsrelevante Detection Use-Cases, die spezifische Aspekte seiner vorgeschlagenen Lösung adressieren. Diese Use-Cases sollen Ereignisse aus der generellen Cloud-Infrastruktur abdecken, Ereignisse aus dem Identity & Access Management für die Verwaltung der Cloud Ressourcen und HCC sowie Ereignisse aus weiteren Bereichen, in denen die Erkennung sicherheitsrelevanter Anomalien eine Rolle spielt.

Details zum Umfang der zu liefernden Daten sind dem TI-Security-Standard zu entnehmen (vgl. Leistungsbeschreibung (Anlage-02), Kap. 3.3.5). Das Format dieser Daten sowie die weiteren Inhalte dienstspezifischer Reports sind vom AN im Rahmen der Projektdurchführung mit dem Cyber Defense Center des AG abzustimmen.

Die gelieferten sicherheitsrelevanten Informationen werden von der gematik für die Umsetzung konkreter Detection Use-Cases genutzt, z. B. indem anhand der Attestierungsreports Fehler in der Umgebungskonfiguration erkannt werden.

2.11 Konzept 11 (K-11): Projektvorgehen (max. 15 Seiten, zzgl. einer Excel-Liste der Projektbeteiligten)

Zielsetzung: Die Ausführungen sollen es dem AG ermöglichen, die grundsätzliche Planungs-, Steuerungs- und Umsetzungskompetenz des Bieters einzuschätzen und seitens des Bieters getroffene Planannahmen und erkannte Risiken nachzuvollziehen. Die Ausführungen sollen dem AG zusätzlich ermöglichen, das Verständnis des Bieters für die Anforderungen des AG an die Zusammenarbeit und für die zu erstellenden Gutachten einzuschätzen.

Der Bieter stellt seine geplante Projektorganisation und die geplante Produktdurchführung dar.

Das Projektvorgehen muss folgendermaßen strukturiert sein, mindestens die geforderten Inhalte darstellen:

2.11.1 Projektorganisation

- Der Bieter stellt in Form eines Organigramms seine **Projektorganisationsstruktur** dar. Das Organigramm muss neben der Projektleitung auch ggf. definierte Querschnittsfunktionen (wie z.B. Risiko- und Qualitätsmanagement), Teilprojekte, involvierte Projektpartner (Subunternehmer), beteiligte Instanzen bzw. Gremien der internen Unternehmensorganisation des Bieters und spezifisch beteiligte Rollen berücksichtigen. Der Bieter beschreibt die Rollen und Funktionen der Organisationseinheiten. Die Aufnahme aller Projektmitarbeiter des Bieters in das Organigramm ist dabei nicht erforderlich.
- Der Bieter stellt in einer tabellarischen Auflistung (als Excel-Datei K-11 – Anlage Projektbeteiligte_Bietername.xlsx) die **Projektbeteiligten** gemäß Projektorganigramm des Bieters mit Zuordnung der Aufgabenbereiche, Rollen und Verantwortlichkeiten dar. Schnittstellen gegenüber dem AG sind zu beschreiben.

2.11.2 Projektdurchführung

- Der Bieter stellt grundlegende sowie liefergegenstandsbezogene Planungsannahmen dar
- Der Bieter stellt die von ihm geplanten **Umsetzungsphasen** einschließlich wesentlicher Meilensteine und Abhängigkeiten zur vollständigen Erbringung der Werkleistung innerhalb der Projektphase dar.
- Der Bieter stellt in einer tabellarischen Übersicht den geplanten **Ressourceneinsatz** in der Größeneinheit FTE (Full Time Equivalent) für alle Rollen nach den Qualifikationsstufen des Preisblatts für die Projekt- und Betriebsphase dar. Sie kann in der Excel-Tabelle "K-11 Anlage Projektbeteiligte_Bietername.xlsx" erfolgen.

2.11.3 Risikomanagement

- Der Bieter beschreibt die Aufgaben und Prozesse des geplanten **Risikomanagements** inkl. involvierter Rollen.
- Der Bieter beschreibt initiale **Projektrisiken**, insbesondere bezogen auf Abhängigkeiten zu anderen in der Leistungsbeschreibung benannten Projekten und die Inbetriebnahme. Risiken können dabei beispielsweise zeitlich, technisch, organisatorisch oder kommerzieller Natur sein.

2.11.4 Agile Projektdurchführung

- Der Bieter beschreibt die agile Projektdurchführung in Zusammenarbeit mit dem AG sowie die geplanten Fortschrittsberichte an den AG insbesondere mit Bezug auf die konkreten Anforderungen der Leistungsbeschreibung.

2.11.5 Gutachten

- Der Bieter stellt die gegebenen Voraussetzungen und die wesentlichen Schritte zur Erlangung des Sicherheitsgutachtens und Produktgutachtens dar

2.12 Konzept 12 (K-12): Projektplan (MS-Project-Datei und max. 5 Seiten)

Zielsetzung: Die Ausführungen sollen es dem AG ermöglichen, die konkrete Projektplanung des Bieters hinsichtlich Erreichbarkeit des vertraglichen Fertigstellungstermins in Form von Vollständigkeit, Konsistenz und Realisierbarkeit einzuschätzen und zu bewerten.

Der Bieter stellt in einem verbindlichen Projektplan im MS Project (MSP) Dateiformat und als PDF- und Excel-Export ("K-12 – Projektplan_Bietername.mpp" sowie *.pdf, *.xlsx) das geplante Vorgehen zur vollständigen Umsetzung der geforderten Lieferungen und Leistungen dar. Der Bieter ergänzt in einer Anlage zum Projektplan ("K-12 – Projektplan Anlage_Bietername.docx") wesentliche Erläuterungen zum Verständnis und zur Nachvollziehbarkeit des Projektplans.

Der Projektplan muss eine nachvollziehbare Ergebnis-, Zeit- und Ressourceneinsatzplanung für alle zur Erfüllung des Leistungsgegenstandes erforderlichen Aktivitäten in der Projektphase und bis zum Beginn der Betriebsphase beinhalten. Die Aktivitäten sind vom Bieter detailliert unter Berücksichtigung der nachfolgenden Punkte im Projektplan zu planen und darzustellen.

1. Planung und Darstellung aller Aktivitäten ausgehend von den Bestimmungen der Leistungsbeschreibung (Anfangs- und Endtermin, Abhängigkeiten, durchführende Rollen)
2. Planung und Darstellung aller Meilensteine des AG und Einordnung zu wesentlichen Umsetzungsphasen, Aktivitäten und zusätzlichen Meilensteinen des Bieters.
3. Planung und Darstellung aller Liefergegenstände der Leistungsbeschreibung inkl. Aktivitäten zur Erstellung durch den AN und zur Güteprüfung und Kenntnisnahme durch den AG sowie Zuordnung zu den Meilensteinen des AG

4. Darstellung aller vom AG zu leistenden Beistellungen gemäß Leistungsbeschreibung

Der Projektplan muss unter den folgenden Planungsvorgaben des AG erstellt werden:

- Der kalkulatorische Projektstart ist auf den avisierten Zuschlagstermin (gemäß Angebotsaufforderung Angebotsphase (Anlage-08)) anzusetzen.
- Die Produktivsetzung und stabile Bereitstellung der Lösung sowie die verbindlich vorgegeben Meilensteine müssen spätestens zu den in der Leistungsbeschreibung vorgegebenen Terminen erfolgen.
- Der Projektplan ist auf Basis einer realistischen Termin- und Ressourcenplanung zu erstellen und muss angemessene sowie nachvollziehbar begründete Pufferzeiten enthalten.
- Liefergegenstände sollen mit der LG-Nummer und LG-Namen gemäß Leistungsbeschreibung eindeutig gekennzeichnet sein.
- Für Güteprüfungen und Kenntnisnahmen von Liefergegenständen sind die in der Leistungsbeschreibung festgelegten Mitwirkungen des AG und Fristen verbindlich einzuplanen. Dabei ist mindestens eine Nachbesserungsiteration zu berücksichtigen. Sofern hiervon abgewichen wird, ist dies nachvollziehbar zu begründen.
- Kontrollpunktlieferungen sollen eingeplant werden.
- Aktivitäten müssen dem AG und AN bzw. UAN eindeutig zuordbar sein.

Der Bieter soll im Anhang zum Projektplan wesentliche Aspekte seiner Projektplan erläutern. Dazu zählen insbesondere:

2.12.1 Planungsgrundlagen

- Erläuterung des grundsätzlichen Planungsvorgehens und von zentralen Planungsgrundlagen zur Nachvollziehbarkeit der Planung
- Erläuterung von bieterspezifischen Planungsannahmen, die über die in diesem Abschnitt vorgegebenen Planungsvorgaben hinausgehen

2.12.2 Spezifische Erläuterungen

- Erläuterung von Pufferzeiten, Erläuterung der Aktivitäten, bei denen durch erhöhten Ressourceneinsatz oder Parallelisierung einzelne Umsetzungsphasen verkürzt werden können.
- Erläuterung des kritischen Pfads, der sich aus der MS-Projekt-Ansicht der kritischen Vorgänge ergibt sowie Darstellung von Risiken und Maßnahmen zur Vermeidung oder Kompensation von Terminverzögerungen

Mit Einreichung des Projektplans erkennt der Bieter die vorgegebenen Meilensteine und Termine des AG entsprechend der Leistungsbeschreibung als verbindlich an. Die Termine aller Meilensteine werden verbindlicher Bestandteil des Angebots. Anpassungen des Projektplans bedürfen der Zustimmung des AG. Anpassungen an den Lieferterminen der Meilensteine werden als Change Request behandelt.