

Telematikinfrastruktur 2.0

Leistungsbeschreibung

Los 2 – Cloud Services

Anlage 02 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
Referenzierung:	[gemLB_TI-Flow_Los2_Anlage2]

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
1 Rahmenbedingungen und Überblick	8
1.1 Überblick über die Telematikinfrastuktur.....	8
1.2 Ausgangssituation.....	8
1.3 Übersicht und Abgrenzung	9
1.4 Zusammenhang der Dokumente/Anforderungen	10
1.5 Vertragslaufzeit, Regelungen zum Vertragsende/ zur Migrationsfähigkeit	10
1.6 Hinweis zur Zulassung	10
2 Zielsetzung und Inhalt.....	12
2.1 Leistungen des AN im Überblick	13
2.2 Verantwortung des AN.....	14
3 Lieferungen und Leistungen des AN.....	16
3.1 Projektphase.....	16
3.1.1 Allgemeine Dokumentenanforderungen	16
3.1.2 Arbeitspaket 1: Konzeptionsleistungen des AN	17
3.1.2.1 Umsetzungskonzept HCC.....	17
3.1.2.1.1 Umgebungen und Instanzen	18
3.1.2.2 Umsetzungskonzept CI/CD	19
3.1.2.3 Testkonzepte HCC-Cloud und CI/CD.....	20
3.1.2.3.1 Übergreifende Vorgaben für Testkonzepte.....	20
3.1.2.3.2 Testkonzept CI/CD	22
3.1.2.4 Betriebliche Konzepte ITSM, SLA und Governance	23
3.1.2.5 Betriebskonzept CI/CD.....	24
3.1.3 Arbeitspaket 2: Entwicklung und Bereitstellung der HCC-Cloud	25
3.1.3.1 Prototyp zur Clientintegration.....	26
3.1.3.2 Prototyp-HCC und Testnachweise der HCC-Funktionalität	27
3.1.3.3 Entwicklung der vollständigen HCC-Funktionalität.....	28
3.1.3.4 Entwicklungsartefakte.....	28
3.1.3.5 Dokumentation HCC	29
3.1.3.6 Bereitzustellende Umgebungen	30

3.1.3.7	Erklärung zur funktionalen, betrieblichen und sicherheitstechnischen Eignung	32
3.1.4	Arbeitspaket 3: Entwicklung und Bereitstellung der CI/CD-Plattform	32
3.1.4.1	Organisationsmodell, Mandantenfähigkeit und Zugriffsstruktur	35
3.1.4.2	Identitäts- und Zugriffsmanagement	35
3.1.4.3	Source-Code-Repository-Funktion.....	36
3.1.4.4	Pipeline-Orchestrierung und Pipeline-Ausführung.....	37
3.1.4.5	Verarbeitung von HCC-Laufzeit-, Versions- und Attestierungsinformationen.....	38
3.1.4.6	Ausführung und Auswertung bereitgestellter Testsuiten.....	39
3.1.4.7	Artefakt- und OCI-Registry	39
3.1.4.8	Supply-Chain-Security / Nachweise.....	41
3.1.4.9	Freigaben, Promotion und Deployment-Governance	42
3.1.4.10	Runner-Ausführungsumgebungen	42
3.1.4.11	APIs, Integration und Automatisierung	43
3.1.4.12	Audit, Nachvollziehbarkeit und Compliance.....	44
3.1.4.13	Technische Betriebsbefähigung der CI/CD-Plattform	45
3.1.4.14	Datensicherung und Wiederherstellung	46
3.1.4.15	Prototyp CI/CD-Plattform	46
3.1.4.16	Betriebshandbuch CI/CD-Plattform	48
3.1.4.17	Dokumentation CI/CD-Plattform	49
3.1.4.18	Schulungen	51
3.1.5	Arbeitspaket 4: Vorbereitung und Durchführung von Tests der HCC-Cloud	51
3.1.5.1	Referenz-Container	51
3.1.5.2	Testautomatisierung.....	57
3.1.5.3	Testnachweise	57
3.1.5.4	Testarchitektur, Nachweisführung und operative Testumsetzung	58
3.1.5.5	Testreports und Artefakt-Registry	58
3.1.5.6	Testfallentwicklung.....	58
3.1.5.7	Unterstützung bei Testaktivitäten	58
3.1.5.8	Testphasen und HCC Testumgebungen	59
3.1.5.9	Ermöglichung der Produktübergreifenden Tests / HCC-Cloud-Tests (PüT)	60
3.1.5.10	Mitwirkung an Gesamtintegrationstests (GIT-HCC)	60
3.1.6	Arbeitspaket 5: Vorbereitung und Durchführung von Tests der CI/CD-Plattform	61
3.1.7	Arbeitspaket 6: Aufbau Service-Management und Inbetriebnahme	61
3.1.7.1	Aufbau der Betriebsorganisation	62
3.1.7.2	Nachweis der betrieblichen Leistungsfähigkeit.....	62
3.1.7.3	Bereitstellung der Betriebsdokumentation	62

3.1.7.4	Aufbau von Monitoring und Alarmierung	62
3.1.7.5	Vorbereitung des Multi-Provider-Betriebs	63
3.1.7.6	Nachweis der Datensicherung und Wiederherstellung	63
3.1.7.7	Nachweis der Notfall- und Wiederanlauffähigkeit	64
3.1.7.8	Betriebsbereitschaftsnachweis	64
3.1.8	Arbeitspaket 7: Übergabestrategie	64
3.1.8.1	Übergabestrategie HCC Cloud	64
3.1.8.1.1	Datenmigration	65
3.1.8.1.2	Risiken	66
3.1.8.1.3	Kosten	66
3.1.8.2	Übergabestrategie CI/CD Pipeline	66
3.1.9	Arbeitspaket 8: Beratungs- und Unterstützungsleistungen	67
3.2	Betriebsphase	69
3.2.1	Anforderungen an den Dienst und Leistungsumfang	69
3.2.2	Serviceportfolio und Servicekatalog	70
3.2.2.1	Allgemeine Anforderungen	70
3.2.2.2	Umfang des Servicekatalogs	71
3.2.2.3	Bereitstellung und Skalierung	71
3.2.2.4	Verbrauchsmodell	72
3.2.2.5	Verfügbarkeit der Leistungen	73
3.2.2.6	Kapazitäts- und Ressourcenreporting	73
3.2.2.7	Verbrauchs-, Billing- und Kostentransparenz	74
3.2.2.8	Preis- und Abrechnungsmodell	75
3.2.2.9	Servicekatalogpflege	76
3.2.3	Betrieb und IT-Service Management	76
3.2.3.1	Service Desk und Anwenderbetreuung	77
3.2.3.2	Supportmodell	78
3.2.3.3	Notfall- und Wiederanlaufmanagement	79
3.2.3.4	Tooling und Schnittstellenintegration	80
3.2.3.5	Datenliefermodell	80
3.2.4	Service Level und Verfügbarkeit	82
3.2.4.1	Service-Level-Kennzahlen	82
3.2.4.2	Mess- und Nachweisverfahren	83
3.2.4.3	Verfügbarkeit und Betriebsstabilität	84
3.2.4.4	Redundanz und Nachweisführung	84
3.2.4.5	Wartung	85
3.2.4.6	Reporting	85
3.2.4.7	Umgang mit Schlechtleistung	86
3.2.4.8	Governance, Steuerung und Zusammenarbeit	86
3.2.4.9	Rollen und Verantwortlichkeiten	86
3.2.4.10	Gremien- und Steuerungsmodell	87
3.2.4.11	Leistungs- und Änderungsmanagement	88

3.2.4.12	Eskalations- und Konfliktmanagement	89
3.2.4.13	Zusammenarbeit in einer Multi-Provider-Betriebsumgebung	89
3.2.4.14	Kontinuierliche Verbesserung und Innovation	90
3.2.4.15	Reporting	91
3.2.4.16	Bezug zu Support und Eskalation.....	91
3.2.5	Transition, Transformation und Exit	92
3.2.5.1	Transition	92
3.2.5.2	Transformation	92
3.2.5.3	Exit und Betreiberwechsel	93
3.2.6	Nachweis der erfolgreich durchgeführten Betriebs- und Schnittstellenprüfung	94
3.2.7	Betrieb CI/CD-Plattform	94
3.2.8	Begleitende Dokumentation	96
3.2.8.1	Sicherheitskonzept.....	97
3.2.8.2	Vorlage der Vereinbarung über die gemeinsame datenschutzrechtliche Verantwortung	98
3.2.8.3	Security Monitoring Konzept	98
3.2.8.4	Notfallkonzept	98
3.3	Datenschutz und Informationssicherheit	98
3.3.1	Datenschutz- und Informationssicherheitspflichten als Hersteller... ..	99
3.3.2	Sicherheitsgutachten Softwareentwicklungsprozesse	99
3.3.3	Produktgutachten HCC	99
3.3.4	Sicherheitsanalysen und Audits.....	100
3.3.5	Datenschutz- und Informationssicherheitspflichten als Anbieter ...	100
3.3.5.1	TI Security Standard	101
3.3.5.2	Controls des TI Security Standards	101
3.3.5.3	Prozessprüfung sicherheitstechnische Eignung	101
3.3.6	Sicherheitsgutachten HCC.....	102
3.3.7	IT-Security Management Meetings	102
3.3.8	Sicherheitsanalysen und Audits.....	103
4	Durchführung	104
4.1	Phasen, Meilensteine und Liefertermine im Überblick	104
4.2	Meilensteine mit verbindlichen Zielterminen	106
4.3	Bereitstellung Liefergegenstände zu Meilensteinen	107
4.4	MS1: Prototypen erstellt	111
4.5	MS2: Planung und Konzeption abgeschlossen	111
4.6	MS3.1: Entwicklung CI/CD-Plattform abgeschlossen	111
4.7	MS3.2: Entwicklung HCC abgeschlossen	112

4.8	MS4.1: Hersteller-Tests CI/CD-Plattform abgeschlossen	112
4.9	MS4.2: Hersteller-Tests HCC abgeschlossen	112
4.10	MS5.1: Integration CI/CD-Plattform mit der PU abgeschlossen	112
4.11	MS5.2: Integration HCC auf PU abgeschlossen	112
4.12	MS6: Inbetriebnahme für die PU abgeschlossen	113
4.13	MS7: Projektphase abgeschlossen	113
5	Übergreifende Vorgaben und Leistungen	114
5.1	Souveränitätsanforderungen	114
5.1.1	Souveränitätskonzept	115
5.1.2	Strategische und rechtliche Souveränität	115
5.1.2.1	Eigentums- und Kontrollstrukturen	115
5.1.2.2	Schutz vor Drittstaateneinflüssen	116
5.1.2.3	Änderungen der Souveränitätsarchitektur	117
5.1.3	EU-basierter Betrieb der Cloud-Infrastruktur	118
5.1.3.1	Disconnect-Fähigkeit	119
5.1.4	Datensouveränität	120
5.1.4.1	Datenlokalisierung	120
5.1.4.2	Datenzugriff und Daten-Portabilität	121
5.1.4.3	Kryptographische Souveränität	121
5.1.5	Lieferketten- und Infrastruktursouveränität	122
5.1.5.1	Dokumentation	122
5.1.5.2	Transparenz der Lieferkette	122
5.1.5.3	Hardware	123
5.1.5.4	Software-Lieferkette	123
5.1.6	Technologische Souveränität und Exit-Fähigkeit/ Vermeidung von Vendor Lock-in	123
5.2	Beistellungen des Auftraggebers	124
5.3	Mitwirkung des Auftraggebers	124
5.3.1	Allgemeine Mitwirkungsleistungen des AG	125
5.3.2	Übergreifende Steuerungsmaßnahmen des AG	125
5.3.3	Prüfmaßnahmen des AG	125
5.4	Koordinierungsverantwortung des Auftragnehmers	127
5.5	Projektmanagement	127
5.5.1	Anforderungen an das Projektmanagement	128
5.5.2	Anforderungen an die agile Zusammenarbeit	129
5.5.3	Mitwirkung an übergreifenden Steuerungsmaßnahmen des AG	130
5.5.4	Projekttrollen- und Gremien	130

5.6	Qualitätsmanagement	132
5.7	Eskalationsmanagement	132
5.8	Produktivfreigabe.....	133
6	Mitgeltende Dokumente.....	134
Anhang A – Verzeichnisse	136	
A1 – Abkürzungen	136	
A2 – Glossar	136	
A3 – Abbildungsverzeichnis	137	
A4 – Tabellenverzeichnis	137	
A5 – Referenzierte Dokumente.....	138	

1 Rahmenbedingungen und Überblick

1.1 Überblick über die Telematikinfrastruktur

Die Digitalisierung wird das Gesundheitswesen künftig weiter und nachhaltig verändern.

Die Erfassung, Verarbeitung und Nutzung medizinischer Daten beflügelt die Forschung, revolutioniert Therapien und sorgt dafür, dass wir individueller und besser versorgt werden können. Diesen Prozess in Deutschland entschlossen voranzutreiben und konstruktiv mitzugestalten, ist Ziel, Aufgabe und Mission der gematik.

Die gematik trägt die Gesamtverantwortung für die Telematikinfrastruktur (TI), die zentrale Plattform für digitale Anwendungen im deutschen Gesundheitswesen. Mit der Definition und der Durchsetzung verbindlicher Standards für Dienste, Komponenten und Anwendungen in der TI gewährleistet die gematik, dass diese zentrale Infrastruktur sicher, leistungsfähig und nutzerfreundlich ist und bleibt.

Die Arbeit der gematik als Digitalagentur Gesundheit reicht weit über Landesgrenzen hinaus – für die beste medizinische Versorgung der Menschen kooperiert sie international mit e-Health-Kompetenzzentren anderer Länder. Sie ist Kompetenzzentrum für Interoperabilität im Gesundheitswesen (KIG) und versteht sich dabei nicht nur als Prüferin und Standardgeberin, sondern auch als Vermittlerin, Moderatorin und Beraterin.

1.2 Ausgangssituation

Mit dem E-Rezept wurde eine flächendeckende digitale Lösung für den Verordnungsprozess eingeführt, welche papiergebundene Prozesse abgelöst, Medienbrüche reduziert und die Patientensicherheit erhöht hat. Die gesetzlichen Vorgaben sehen eine verpflichtende Nutzung des E-Rezepts für verordnungspflichtige Arzneimittel vor, mit perspektivischer Erweiterung auf weitere Verordnungstypen wie Heil- und Hilfsmittel, Betäubungsmittel, T-Rezepte sowie digitale Gesundheitsanwendungen.

Der E-Rezept-Fachdienst ist dabei als zentraler Infrastrukturdienst der TI produktiv im Einsatz und wird durch Ärzte, Apotheken, Versicherte und weitere Akteure des Gesundheitswesens genutzt. Der Dienst stellt eine hochverfügbare, performante und sichere Umgebung bereit, die die Ende-zu-Ende-Sicherheit medizinischer Verordnungsdaten, die Verwaltung des Verordnungslebenszyklus (Erstellung, Einlösung, Storno, Ablauf) sowie das Zugriffsmanagement für alle beteiligten Akteure (Versicherte, Vertreter, Apotheken, verordnende Einrichtungen, Kostenträger und ggf. Pflegeeinrichtungen) gewährleistet.

Der E-Rezept-Fachdienst basiert auf den Spezifikationen der gematik, insbesondere gemSpec_FD_eRp. Die technische Umsetzung umfasst RESTful FHIR-Schnittstellen für Primärsysteme (ambulant, stationär, Apotheke) und Krankenkassen, die Anbindung an zentrale TI-Dienste (Zeitdienst, Namensdienst, Verzeichnisdienst, Identitätsdienste via HBA/SMC-B), die Interoperabilität mit Standards (FHIR-Profiles, PZN, ICD/ATC) sowie die Einbindung externer Dienste wie den BfArM Webservices (BTM, T-Rezepte) und dem Terminologie-Server. Der Betrieb erfolgt im 24/7-Modus mit definierten Service Level Agreements (SLAs) für Verfügbarkeit, Latenz und Durchsatz.

1.3 Übersicht und Abgrenzung

Mit der Weiterentwicklung der Telematikinfrastruktur zur TI 2.0 und der Einführung der Zero Trust Architektur ergeben sich neue technische und sicherheitsbezogene Anforderungen. Die Integration der Zero Trust Komponenten (ZETA Guard gemäß gemSpec_ZETA), die Unterstützung neuer Authentifizierungsmechanismen (GesundheitsID), die Anbindung an das zentrale Monitoring- und Überwachungssystem der gematik sowie die kontinuierliche Umsetzung regulatorischer Änderungen und fachlicher Erweiterungen erfordern eine Weiterentwicklung und Neuausrichtung des Dienstes. Mit den genannten funktionalen Erweiterungen der Ablaufsteuerungsprozesse wird die Fachlichkeit des E-Rezept-Fachdienstes in Zukunft unter der Bezeichnung TI-Flow-Fachdienst weitergeführt und um die Fachlichkeit eines neuen TI-Dienstes, der E-Überweisung, erweitert. Diese Weiterentwicklung wird in Los 1 des vorliegenden Vergabeverfahrens abgebildet.

Die Bereitstellung und der Betrieb der Infrastruktur für den TI-Flow-Fachdienst werden über das Los 2 abgebildet. Die vorliegende Leistungsbeschreibung beschreibt die vom Auftragnehmer (AN) im Los 2 zu erbringenden Leistungen. Dabei erfüllt der AN die Rolle des HCC-Providers aus der zugrundeliegenden Spezifikation [gemSpec_HCC].

Die Leistungen, die der AN gegenüber dem Auftraggeber (AG) zu erbringen hat, teilt sich in die in Kapitel 3 weiter ausgeführten Arbeitspakete auf:

1. Konzeptionsleistungen (je weiteres Arbeitspaket),
2. Entwicklung und Bereitstellung der Cloud-Infrastruktur (gemäß der vorliegenden Leistungsbeschreibung sowie gemäß [gemSpec_HCC]),
3. Entwicklung und Bereitstellung der CI/CD-Plattform (gemäß der vorliegenden Leistungsbeschreibung),
4. Vorbereitung und Durchführung von Tests für die Cloud-Infrastruktur sowie für die CI/CD-Plattform,
5. Aufbau Service Management und Inbetriebnahme für die Cloud-Infrastruktur,
6. Entwicklung einer Übergabestrategie zur Absicherung der Fortführbarkeit des Betriebs der auf der HCC-Cloud betriebenen Dienste (bspw. des TI-Flow-Fachdienstes) nach Vertragsende bei einem anderen Cloud-Anbieter sowie
7. Unterstützungs- und Beratungsleistungen (für den AG sowie für den Anbieter des TI-Flow-Fachdienstes).

Die Cloud-Infrastruktur ("HCC-Cloud") muss vom AN so umgesetzt werden, dass die durch sie bereitgestellten Funktionalitäten (HCC, HSMs, Datenbank-Services, etc.) zukünftig für eine Nutzung durch weitere Dienste der TI nachnutzbar sind. Sie muss dabei den Betrieb der anwendungsübergreifend durch den AG umgesetzten Zero Trust Komponenten ("ZETA Guard") und anwendungsübergreifend die Integration in das kontinuierliche Monitoring, das ITSM und das SIEM des AG für die Dienste unterstützen.

Mit den Funktionalitäten zur Unterstützung von Tests für Dienste ermöglicht der AN den Diensteanbietern die Erreichung ihrer Qualitätsziele. Die Durchführung der Tests für die (Fach-)Dienste ist die Aufgabe des jeweiligen Diensteanbieters.

Mit der Bereitstellung der CI/CD-Funktionalitäten für den AG unterstützt der AN die Umsetzung und Integration von Diensten in die HCC-Cloud und die Steuerung von HCC durch den AG. Die redaktionellen CI/CD-Funktionalitäten (z. B. Veränderungen an Policies, Einbringen von Code) müssen so umgesetzt werden, dass sie nicht fest an einen Betrieb in der Cloud-Infrastruktur des AN gebunden sind, d. h., dass sie ggf. auch in einer anderen Infrastruktur betrieben werden könnten, indem die direkten Bezüge zur spezifischen HCC-Infrastruktur des AN auf einen anderen Betreiber portiert werden.

1.4 Zusammenhang der Dokumente/Anforderungen

Für das Los 2 „HCC-Cloud“ besteht das für die Leistungserbringung gültige Dokumentenpaket aus der Spezifikation der HCC-Cloud [gemSpec_HCC], aus den Produkttypsteckbriefen [gemProdT_HCC_PTV] und den Anbietertypsteckbriefen [gemAnbT_HCC_ATV], den dort aufgeführten Anforderungen sowie den im Kapitel 6 aufgeführten mitgeltenden Dokumenten.

Die Spezifikation [gemSpec_HCC] und die zugehörigen Steckbriefe sind im Kontext der vorliegenden Leistungsbeschreibung als Anforderungssammlungen zu interpretieren. Darüber hinaus soll die Umsetzung von HCC im Rahmen der vorliegenden Beauftragung auch dazu beitragen, die Spezifikationen für HCC in Zusammenarbeit mit dem AN weiter zu verfeinern und zu konkretisieren.

1.5 Vertragslaufzeit, Regelungen zum Vertragsende/ zur Migrationsfähigkeit

Die Vertragslaufzeit beträgt ab Zuschlagserteilung drei Jahre und kann durch den Auftraggeber fünfmal um jeweils ein weiteres Jahr verlängert werden.

Der AN muss dafür sorgen, dass nach Ablauf der Laufzeit des gegenständlichen Vertrages oder bei einer Vertragsbeendigung aus anderen Gründen die auf der HCC-Cloud betriebenen TI-Dienste mit ihren Nutzdaten sowie die Inhalte der CI/CD-Plattform auf eine andere HCC-Cloud unterbrechungsfrei migriert werden können. Dazu erstellt der AN eine Übergabestrategie gemäß Kapitel 3.1.8.

Das Verfahren richtet sich nach den in Kapitel 3.1.8 aufgeführten Vorgaben.

1.6 Hinweis zur Zulassung

Aufgrund des zum Zeitpunkt der Auftragsbekanntmachung im Entwurf vorliegenden Gesetzes für Daten und digitale Innovation im Gesundheitswesen (GeDIG), welches bestimmt, dass für Komponenten und Dienste der TI, die von der gematik beauftragt wurden, eine Zulassung nicht erforderlich ist, geht der Auftraggeber davon aus, dass dies auch für die hier gegenständlichen Leistungen zur Schaffung von Komponenten oder Diensten der TI gilt.

Soweit in dieser Leistungsbeschreibung oder in referenzierten Spezifikationsdokumenten auf eine Zulassung Bezug genommen wird, ist dies entsprechend auf die Produktivfreigabe anzuwenden, sofern aufgrund der dann gegebenenfalls geltenden Gesetzeslage keine Zulassungspflicht besteht. Es gelten dann die Festlegungen zur Produktivfreigabe (siehe Kapitel 5.8).

Sollte wider Erwarten die avisierte gesetzliche Regelung nicht oder nicht mit der vorstehend beschriebenen Wirkung in Kraft treten, ist der Auftragnehmer verpflichtet, neben der Abnahmereife seiner Leistungen auch eine Zulassung für die von ihm geschaffenen Komponenten oder Dienstes der TI zu erlangen.

2 Zielsetzung und Inhalt

Zielsetzung des Projekts ist die Bereitstellung einer souveränen, vertrauenswürdigen Managed Cloud-Infrastruktur für Dienste der Telematikinfrastruktur. Die Cloud-Infrastruktur dient als Ausführungsumgebung für den TI-Flow-Fachdienst mit den Anwendungen E-Rezept und E-Überweisung sowie ggf. zukünftig für weitere Fachdienste. Die Cloud-Infrastruktur beinhaltet Services, welche die Anforderungen für HCC erfüllen, und wird nachfolgend als „HCC-Cloud“ bezeichnet.

Die HCC-Cloud muss vom AN sowohl für den AG als auch für im Auftrag des AG handelnde und von ihm benannte Anbieter von Fachdiensten bereitgestellt werden. Diese werden im Folgenden als Mandanten des AN bzw. kurz Mandanten bezeichnet. Die Bereitstellung durch den AN muss derart erfolgen, dass die Mandanten mittels eines ihnen zur Verfügung gestellten User Interfaces und über eine API eigenständig die für ihre auszuführende Software („Workloads“) erforderlichen Umgebungsparameter einbringen und die für ihre Ausführung erforderlichen Ressourcen der HCC-Cloud konfigurieren und überwachen können.

Der AN muss alle für den Betrieb der Fachdienste (und den von diesen benötigten weiteren Services, wie Datenbanken, Storage, etc.) notwendigen Werkzeuge bereitstellen. Das umfasst Werkzeuge zur Einbringung der Workloads, ihrer Konfiguration, ihrer Überwachung und Protokollierung sowie zur Bereitstellung von Ressourcen der HCC-Cloud für die Nutzung durch die Workloads (produktiv), für die Testung der Workloads, sowohl in statischen Testumgebungen als auch in bedarfsgesteuert instanziierten Testkonfigurationen. Die Werkzeuge müssen im Regelfall über APIs angesprochen werden können, z. B. um als Instrumente in Build-Pipelines des jeweiligen Mandanten integriert werden zu können.

Die vom AN bereitgestellte HCC-Cloud muss insbesondere Confidential-Compute-Ressourcen zur Verfügung stellen, die gemäß [gemSpec_HCC] in einen kryptographischen Vertrauensraum für die TI eingebunden sind. Sie muss weiterhin Cloud-native Services für die Bereitstellung von Funktionen einer relationalen Datenbank, Block Storage, Backup Services, KMS, Hardware Security Module sowie reguläre Compute-Ressourcen umfassen. Die HCC-Cloud kann darüber hinaus weitere Services und Ressourcen aus dem Standard-Servicekatalog des AN bereitstellen.

Sämtliche Funktionen der vom AN bereitgestellten HCC-Cloud müssen darauf ausgelegt sein, die Hochverfügbarkeitsanforderungen des AG zu erfüllen. Sie müssen dazu auf mindestens zwei georedundante Standorte gemäß BSI-Anforderungen [BSI-Standortkriterien] verteilt verfügbar sein, die den Anforderungen an kritische Infrastruktur [BSI-Kritis] genügen. Die Funktionen müssen über Standorte synchronisiert bereitgestellt werden und mit Mechanismen zur Kompensation von Ausfällen auf Komponenten-, Service- und Standortebene ausgestattet werden.

Die Lösung muss spätestens zum 01.05.2028 mit MS6 produktiv und stabil in der Telematikinfrastruktur (TI) zur Verfügung gestellt und anschließend betrieben werden.

Die Beauftragung umfasst die Planung und den Aufbau sowie den 24/7-Betrieb der HCC-Cloud in verschiedenen Betriebsumgebungen der TI (Referenz-, Test- und Produktivumgebungen) und schließt die kontinuierliche Weiterentwicklung im Rahmen regulatorischer Anforderungen und fachlicher Erweiterungen ein.

2.1 Leistungen des AN im Überblick

Die wesentlichen Leistungen des Auftragnehmers umfassen insbesondere:

- Konzeption, Entwicklung, Test, Weiterentwicklung und Bereitstellung der HCC-Cloud gemäß den Vorgaben dieser Leistungsbeschreibung und den geltenden Spezifikationen der gematik. Die Ergebnisse der Konzeption und der Weiterentwicklung werden seitens des AG bei Bedarf in die Weiterentwicklung der Spezifikationen eingebracht.
- Konzeption, Entwicklung, Test, Weiterentwicklung und Bereitstellung der CI/CD-Pipeline gemäß den Vorgaben dieser Leistungsbeschreibung und den geltenden Spezifikationen der gematik.
- Betrieb der HCC-Cloud inklusive Sicherstellung definierter SLAs (Verfügbarkeit, Latenz, Durchsatz) sowie Notfall und Disaster Recovery.
- Betrieb der CI/CD-Plattform inklusive Sicherstellung definierter SLAs (Verfügbarkeit, Latenz, Durchsatz) sowie Notfall und Disaster Recovery.
- Unterstützung der Nutzung der vom AG bereitgestellten Zero-Trust-Komponenten (ZETA Guard) seitens der Dienstanbieter durch Bereitstellung der von diesen Komponenten benötigten Ressourcen in der Cloud. Hierzu gehören die Hilfskomponenten/Funktionen Admission Controller und Service Mesh und die austauschbaren Komponenten PDP Datenbank, HSM-Proxy, Local Artifact Registry Cache und Gateway oder Ingress/Egress. Zur Unterstützung der Georedundanz wird ein globaler Load Balancer benötigt (siehe auch [gemSpec_ZETA]).
- Unterstützung der Anbindung der HCC-Dienste an andere Dienste der TI (u. a. ePA-Aktensysteme, Verzeichnisdienst, PoPP-Service und PKI-Dienste) oder externer Dienste (z. B. BfArM-Webservice) mittels Bereitstellung entsprechender Konfigurationsmöglichkeiten für die Netzwerk-Umgebung der HCC-Dienste (z. B. Einrichtung von erlaubten Routen).
- Bereitstellung und Test interoperabler Schnittstellen gemäß gematik-Vorgaben.
- Anbindung an das zentrale Monitoring und Überwachungssystem der gematik einschließlich Lieferung von Betriebs- und Qualitätskennzahlen.
- Aufbau und Betrieb des TI-IT-Service Managements (TI-ITSM) für die verantworteten Betriebsleistungen.
- Anbindung an und Integration in das zentrale SIEM der gematik.
- Konzeption, Vorbereitung und Durchführung der Tests in den definierten Testphasen, Bereitstellung der notwendigen Testartefakte und Implementierungen aller für einen möglichst automatisierten System- und Integrationstest benötigten Komponenten sowie Mitwirkung an Abnahme- und Freigabeverfahren.
- Projekt-, Qualitäts- und Releasemanagement, einschließlich Versions-, Roll-back- und Migrationsfähigkeit.

- Bereitstellung vollständiger Dokumentationen, insbesondere Betriebs-, Sicherheits-, Schnittstellen- und Supportdokumentation.

Der AN muss sicherstellen, dass die erbrachten Leistungen im Rahmen dieser Beauftragung alle Anforderungen und Festlegungen aus:

- dem Vertrag inkl. Anhängen,
- dieser Leistungsbeschreibung inkl. Anhängen und mitgeltenden Dokumenten
- der Spezifikation [gemSpec_HCC] mit den zugehörigen Produkttypsteckbrief [gemProdT_HCC_PTV] und Anbietertypsteckbriefen [gemAnbT_HCC_ATV] einschließlich der dort referenzierten Dokumente sowie
- den Dokumenten, die als Grundlage für die Bereitstellung spezifischer Liefergegenstände in den jeweiligen Kapiteln dieser Leistungsbeschreibung aufgeführt sind,

erfüllen. Die Leistungen des AN sind im Kapitel 3 detailliert aufgeführt und beschrieben.

2.2 Verantwortung des AN

Aufbau- und Betriebsverantwortung

Der Auftragnehmer trägt für sämtliche im Rahmen dieser Beauftragung zu erbringenden Leistungen (Konzeption, Dokumentation, Entwicklung, Integration, Test, Bereitstellung, Betrieb und Weiterentwicklung) eine umfassende Ende-zu-Ende- sowie **Erfolgsverantwortung**. Diese umfasst insbesondere auch die eigenverantwortliche Planung, Steuerung und Qualitätssicherung seiner Leistungen.

Koordinierungsverantwortung

Darüber hinaus übernimmt der Auftragnehmer eine Koordinierungsverantwortung. Diese beinhaltet die fachliche und technische Abstimmung mit dem AG, mit weiteren vom Auftraggeber beauftragten Auftragnehmern sowie sonstigen beteiligten Akteuren, insbesondere an Schnittstellen und Übergabepunkten (z. B. Zero-Trust-Komponenten, Fachdienst-Hersteller und -Anbieter, Dienste der TI). Ziel ist die Sicherstellung der Kompatibilität und des stabilen Zusammenspiels aller beteiligten Systeme und Dienste. Dies umfasst die Projektphase und die Betriebsphasen. In der Betriebsphase gelten federführend, jedoch nicht abschließend, die entsprechenden Aufgaben im Rahmen des übergreifenden IT-Service Managements (siehe Kapitel 3.1.7 und speziell Kapitel 3.2.3 sowie 5.4).

Datenschutzrechtliche Verantwortung

Der Auftragnehmer ist Verantwortlicher im Sinne von Art. 4 Nr. 7 und Art. 24 DSGVO in Verbindung mit den §§ 306 Absatz 2 Nr. 3, 307 Absatz 4 SGB V für die Verarbeitung personenbezogener Daten im Rahmen der HCC-Cloud. Er ist insbesondere verantwortlich für die datenschutzkonforme Ausgestaltung der Verarbeitungsvorgänge sowie für die Durchführung und Pflege erforderlicher Datenschutz-Folgenabschätzungen.

Nach Auffassung des Auftraggebers besteht ferner eine **gemeinsame Verantwortlichkeit** zusammen mit dem Auftragnehmer für den TI-Flow-Fachdienst-Anbieter gemäß Art. 26 DSGVO. Somit verteilt sich auch die zuvor in einem einzigen Verantwortlichen gebündelte datenschutzrechtliche Verantwortlichkeit – gemeinschaftlich – auf perspektivisch zwei Verantwortliche. Der Auftragnehmer muss daher sämtliche Pflichten, die sich aus dieser gemeinsamen Verantwortlichkeit mit dem Fachdienst-Anbieter ergeben, ordnungsgemäß erfüllen, einschließlich dem Abschluss einer **Vereinbarung gemäß Art. 26 Abs. 1 DSGVO**, welche dem Auftraggeber vor Abschluss zur Freigabe vorzulegen ist.

Hinweispflicht

Sofern der Auftragnehmer erkennt, dass Anforderungen dieser Leistungsbeschreibung, der zugrunde liegenden Konzepte oder Spezifikationen sich gegenseitig widersprechen oder nicht bzw. nur mit unverhältnismäßigem Aufwand umsetzbar sind, besteht eine unverzügliche Hinweispflicht gegenüber dem Auftraggeber. In diesem Fall hat der Auftragnehmer konkrete Vorschläge zur Anpassung der betreffenden Anforderungen oder Dokumente zu unterbreiten.

Kontinuität der Verantwortung

Die Pflichten und Obliegenheiten des hiesigen Auftragnehmers in Bezug auf den in dieser Leistungsbeschreibung dargestellten Auftragnehmer des Loses 1 (TI-Flow Fachdienst) gelten während der Vertragslaufzeit fort, auch wenn der Auftragnehmer des Los 1 wechseln oder die Leistungsinhalte des Loses 1 auf mehrere Auftragnehmer aufgeteilt werden sollten (z.B. eRezept und eÜberweisung getrennt). Sollten sich daraus nachweislich Mehraufwände bzw. zusätzliche Leistungen ergeben, die dem Grunde oder der Höhe nach nicht ohne eine Nachtragsvereinbarung für den hiesigen Auftragnehmer zumutbar sind, werden sich die Vertragsparteien unter Berücksichtigung der beiderseitigen Interessen im vertraglichen Change Request Verfahren über einen angemessenen Ausgleich abstimmen.

3 Lieferungen und Leistungen des AN

3.1 Projektphase

3.1.1 Allgemeine Dokumentenanforderungen

Alle zu liefernden Dokumentationen sind auf die Bedürfnisse des potenziellen Nutzers anzupassen. Sie müssen so erstellt werden, dass ihre Form sprachlich und inhaltlich verständlich ist. Sie müssen dem Nutzer und einem entsprechend qualifizierten Dritten ein Selbststudium ermöglichen. Beispielsweise sollen Abläufe durch Grafiken veranschaulicht werden.

Die Dokumentationen müssen den jeweils aktuellen Entwicklungsstand des HCC-Services widerspiegeln. Hierzu gehört u.a. auch die Beschreibung bedienungsrelevanter Funktionen und sicherheitstechnischer und organisatorischer Prozesse.

Dokumentationen sind grundsätzlich in deutscher Sprache zu verfassen.

- Alle allgemeinen Dokumentationen, die sich an Nutzer, Betreiber und Administratoren richten (wie Betriebs- und Installationsanleitungen, Konzepte, Testdokumente usw.), sind in deutscher Sprache zu verfassen.
- Quellcode, Kommentare im Code und die direkt mit dem Code zusammenhängende technische Dokumentation (API-Dokumentation, Entwicklerdokumentation) sind in englischer Sprache zu verfassen.
- Dokumentationen (z.B. Zertifizierungen) können in Englisch bereitgestellt werden, wenn dies der übliche Standard ist.
- Müssen allerdings aufgrund gesetzlicher Bestimmungen oder Spezifikationen des AG diese Unterlagen in Deutsch vorliegen, so hat der Auftragnehmer zusätzlich eine entsprechende Übersetzung bereitzustellen.
- Wichtige Entscheidungen müssen sowohl im Code (in englischer Sprache) als auch in der allgemeinen Dokumentation (in deutscher Sprache) dokumentiert werden.

Dokumentationen sind grundsätzlich in einem MS Office-Dateiformat in einem vom AG vorgegebenen Repository (s. Kapitel 4.2) bereitzustellen (z.B. MS Word, MS Excel). Dokumentation müssen vom AN in der Form übergeben werden, dass sie vom AG bei Bedarf fortgeschrieben werden können. Sollte der AN Dokumentationen z.B. auf Confluence-Seiten erstellen, so muss er dem AG Zugriff auf diese ermöglichen und zusätzlich revisionssicher als PDF-Dokument bereitstellen.

Für alle Dokumente muss die Änderungshistorie verfügbar sein. Es muss möglich sein, Änderungen zwischen Versionen mittels Hervorhebung im Dokument sichtbar zu machen.

Testdokumente (insbesondere Testkonzept, Testspezifikation, Testprotokoll und Testbericht) unterliegen einer vollständigen Versionierung. Jede Änderung ist mit Versionsnummer, Datum, Grund der Änderung und Bearbeiter zu kennzeichnen. Ältere Versionen müssen im vom AG vorgegebenen Repository nachvollziehbar erhalten bleiben.

3.1.2 Arbeitspaket 1: Konzeptionsleistungen des AN

Dieses Arbeitspaket beinhaltet die Erstellung der nachfolgend aufgeführten Konzepte und Prozessbeschreibungen auf Basis der vom AG in den zugehörigen Unterkapiteln definierten Festlegungen.

Folgende Grobkonzepte hat der AN bereits mit seinem Angebot eingereicht:

- K-01: Umsetzungskonzept HCC
- K-02: Umsetzungskonzept CI/CD
- K-03: Testkonzept HCC
- K-04: Testkonzept CI/CD
- K-05: Betriebskonzept HCC
- K-06: Betriebskonzept CI/CD
- K-07: Souveränitätskonzept
- K-08: Datenschutzkonzept gemeinsame datenschutzrechtliche Verantwortung
- K-09: Umsetzung der Use-Cases aus Anlage_09b
- K-10: Security_Monitoring_Konzept
- K-11: Projektvorgehen
- K-11: Anlage Projektbeteiligte
- K-12: Projektplan
- K-12: Projektplan Anlage

Der AN muss die Grobkonzepte K-01 bis K-12 während der Projektphase, wie in den folgenden Kapiteln vorgegeben, fortschreiben und finalisieren. Um Verzögerungen bei der Güteprüfung und Freigabe der Konzepte zu vermeiden, muss der AN den AG bei der Fortschreibung der Konzepte in geeigneter Weise einbinden und die vorgesehenen Anpassungen mit dem AG abstimmen. Der AN legt die Konzepte dem AG gemäß Meilensteinplan (s. Kapitel 4) zur Prüfung und Freigabe vor. Abweichungen von den freigegebenen Konzepten sind nur in Abstimmung mit dem AG möglich. In diesem Falle sind betroffene Konzepte auch nach Freigabe anzupassen und im Rahmen des Projektabschlusses MS7 erneut zur Freigabe vorzulegen.

3.1.2.1 Umsetzungskonzept HCC

Das Umsetzungskonzept HCC muss die vom AN geplante technische und organisatorische Realisierung des Produktes auf Basis des Produkttyps und des Anbietertyps HCC sowie dieser Leistungsbeschreibung beschreiben.

Das Umsetzungskonzept HCC ist die Fortführung und Detaillierung des bereits mit dem Angebot des AN eingereichten Grob-Umsetzungskonzepts HCC. Es muss bis zum MS2 final fertiggestellt, um die in diesem Kapitel beschriebenen Themen und Inhalte konkretisiert, ergänzt oder erweitert und an den Projektfortschritt sowie den aktuellen Stand der Abstimmung mit dem AG angepasst werden. Teile des Umsetzungskonzepts HCC werden in die Dokumentation HCC übernommen und dort fortgeschrieben.

Die Arbeit an dem Umsetzungskonzept HCC, insbesondere konzeptionelle Änderungen, muss der AN mit dem AG abstimmen.

Folgende Inhalte sind in der Überarbeitung besonders zu berücksichtigen:

- Im Zusammenwirken mit dem AG erstellte Vervollständigungen, Änderungen und Verfeinerungen zu den für das ursprüngliche Grob-Umsetzungskonzept HCC geforderten Inhalten,
- Schnittstellenbeschreibung für alle Schnittstellen, welche eine HCC-Workload nutzen oder bedienen müssen, z.B. des TDACS, des KMS und des HSM,
- Schnittstellenbeschreibungen für alle Schnittstellen, die zur Bereitstellung der Testumgebungen erforderlich sind,
- Schnittstellenbeschreibungen für das Einbringen von Artefakten (z. B. cVM-Images) und Policies für die Attestation,
- Schnittstellenbeschreibungen für die von der CI/CD-Plattform benötigten Funktionen der HCC-Cloud zur Ausführung und Auswertung von Tests,
- Änderungen gegenüber dem Grob-Umsetzungskonzept HCC mit Auswirkungen auf betriebliche oder andere Prozesse sowie
- Darstellung der Umsetzung des Umgebungskonzeptes der gematik wie in 3.1.2.1.1 beschrieben

Der AN muss seine Entwicklung auf die im Umsetzungskonzept HCC beschriebene projekthafte Umsetzung ausrichten.

Der AN kann weitere, notwendige Themen im Umsetzungskonzept HCC ergänzen.

3.1.2.1.1 Umgebungen und Instanzen

Die HCC-Cloud bildet die technische Plattform, auf der HCC-Dienste getestet und betrieben werden. Es müssen für die Produktion und Test- und Entwicklungstätigkeiten zwei streng getrennte Trust Domains vorgesehen und eingerichtet werden mit unterschiedlichen kryptographischen Wurzeln, Policies und Servicelevels. In der Trust Domain Produktion müssen eine Produktionsumgebung (PU) unterstützt und exklusive HCC-Hosts verwendet werden. In der TrustDomain für Test- und Entwicklungstätigkeiten müssen verschiedene, logisch getrennte Umgebungen unterstützt werden, entsprechend ihrer Position im Stagingprozess:

- RU DEV: Einstiegspunkt für Entwicklungsstände und externe Integration.
- TU: Durchführung der zentralen, übergreifenden Integrationstests.
- RU: Finale Validierung als PU-Abbild vor der Freigabe.

Im logischen Rahmen dieser Umgebungen muss es möglich sein in Verbindung mit der CI/CD-Plattform und Infrastructure as Code separate Instanzen eines HCC-Dienstes mit eigenen Ressourcen und Konfigurationen zu starten und zu beenden.

Die Trust Domain für Test und Entwicklung kann HCC-Hosts mit anderen Mandanten teilen.

Je nach Einsatzzweck können Instanzen permanent betrieben oder nach dem pay-as-you-go Prinzip bei Bedarf gestartet werden.

Das Starten und Beenden von Instanzen muss der AG an HCC-Diensthersteller bzw. -Betreiber delegieren können. Der AG muss dabei Möglichkeiten zur Kontrolle des Ressourcenverbrauchs haben.

3.1.2.2 Umsetzungskonzept CI/CD

Das Umsetzungskonzept CI/CD muss die vom AN geplante technische und organisatorische Realisierung der in Kapitel 3.1.4 beschriebenen CI/CD-Plattform beschreiben. Das Umsetzungskonzept CI/CD ist die Fortführung und Detaillierung des bereits mit dem Angebot des AN eingereichten Grob-Umsetzungskonzepts CI/CD. Es muss bis zum MS2 um die in diesem Kapitel beschriebenen Themen und Inhalte konkretisiert, ergänzt oder erweitert und an den Projektfortschritt angepasst werden. Die Arbeit an dem Umsetzungskonzept CI/CD, insbesondere konzeptionelle Änderungen, muss der AN mit dem AG abstimmen.

Das Umsetzungskonzept CI/CD muss insbesondere folgende Inhalte beschreiben:

- die Systemarchitektur der CI/CD-Plattform einschließlich Laufzeitumgebungen, Mandantenmodell, Repository-Funktionen, Artefakt-Verwaltung, Runner-Ausführungsumgebungen, Sicherheitsfunktionen, Monitoring, Protokollierung sowie Datensicherung und Wiederherstellung,
- die Bereitstellung, Konfiguration, Integration, Absicherung, Skalierung, Überwachung sowie Datensicherung und Wiederherstellung der CI/CD-Plattform,
- die Abgrenzung zwischen CI/CD-Plattform und HCC-Cloud sowie deren Zusammenwirken über definierte Schnittstellen,
- die Ablage, Versionierung, Berechtigung, Ausführung, Überwachung und Auswertung von Pipeline-Definitionen, Testsuiten, Testfällen, Testskripten und Stage-Übergangslogiken,
- die Unterstützung der Ausführung, Berechtigung, Protokollierung und Nachvollziehbarkeit von Pipeline-Definitionen, Testsuiten sowie Prüf-, Signatur-, Freigabe-, Promotion- und Deployment-Prozessen,
- die Registry-Instanzen der CI/CD-Plattform und der HCC-Cloud einschließlich Nutzungskontext, Berechtigungsmodell, Freigabeprozessen und Betriebsverantwortung,
- die Schnittstellen zur HCC-Cloud, insbesondere zur Verarbeitung von Laufzeit-, Versions- und Attestierungsinformationen sowie zur Überführung freigegebener Artefakte in Stage-Repositories der HCC-Cloud,
- die Abgrenzung zwischen vorhandenen, zu konfigurierenden und gegebenenfalls zu entwickelnden Komponenten
- die Verwendung von Komponenten Dritter einschließlich erforderlicher Lizenzen.

Komponenten Dritter, Konfigurationen und zu entwickelnde Komponenten sind als Entwicklungsartefakte der CI/CD-Plattform aufzulisten und zu beschreiben.

Der AN kann weitere, notwendige Themen im Umsetzungskonzept CI/CD ergänzen.

3.1.2.3 Testkonzepte HCC-Cloud und CI/CD

3.1.2.3.1 Übergreifende Vorgaben für Testkonzepte

Der AN muss für die HCC-Cloud und für die CI/CD-Plattform jeweils ein Testkonzept erstellen und dem AG zur Freigabe vorlegen.

Grundlage für die Testkonzepte sind die Vorgaben dieser Leistungsbeschreibung. Spezifische Regelungen für die Anwendungsfälle HCC und CI/CD, die in dieser Leistungsbeschreibung und in den mitgeltenden Dokumenten enthalten sind, sind bei der Erstellung und Fortschreibung der Testkonzepte verbindlich zu berücksichtigen. Generische Vorgaben zum Testvorgehen, insbesondere zu Testphasen, Rollen und Verantwortlichkeiten, Ein- und Ausgangskriterien, Fehlermanagement, Testdokumentation, Quality Gates und Reporting, enthalten die Festlegungen aus [gemKPT_Test] und [C_12813_Anlage_CC].

Die Testkonzepte sind unter Fortführung der mit dem Angebot des AN eingereichten Grob-Testkonzepte zu erstellen. Der AG stellt für die Grob-Testkonzepte sowie für die fortzuschreibenden Testkonzepte der HCC-Cloud und der CI/CD-Plattform verbindliche Templates zur Verfügung.

Die Testkonzepte müssen die in dieser Leistungsbeschreibung geforderten spezifischen Inhalte vollständig abdecken und bis zu den maßgeblichen Meilensteinen entsprechend dem jeweiligen Umsetzungsstand konkretisiert werden.

Der AN muss die Testkonzepte im Projektverlauf fortschreiben, wenn sich infolge fachlicher, technischer oder organisatorischer Änderungen Auswirkungen auf die Testkonzeption ergeben. Dies gilt insbesondere bei Änderungen von Liefergegenständen, Testumgebungen, Spezifikationen, Schnittstellen oder sonstigen Randbedingungen sowie bei Erkenntnissen aus Testphasen oder sonstigen im Rahmen der Auftragserfüllung gewonnenen Erkenntnissen mit Auswirkungen auf die Testkonzeption.

Die Arbeit an den Testkonzepten, insbesondere konzeptionelle Änderungen, muss der AN mit dem AG abstimmen. Der AN muss zum MS 1 eine Kontrollpunktlieferung der Testkonzepte bereitstellen. In dieser Kontrollpunktlieferung muss mindestens enthalten sein:

- Mindestens zu liefernden Inhalten im Testkonzept CI/CD
 - Kapitel 1–4 final
 - Restliche Kapitel zu 50% fertiggestellt
- Mindestens zu liefernden Inhalten im Testkonzept HCC
 - Kapitel 1–4 zu 80% fertiggestellt
 - Restliche Kapitel zu 50% fertiggestellt

Die jeweils einzureichenden Fassungen müssen den zu diesem Zeitpunkt maßgeblichen Umsetzungsstand und die hierfür relevanten Testinhalte vollständig und nachvollziehbar abbilden.

Die Mitwirkung, Prüfung, Abstimmung oder Freigabe durch den AG entbinden den AN nicht von seiner Verantwortung für die inhaltliche Vollständigkeit, fachliche Eignung und konkrete Ausgestaltung der Testkonzepte. Testkonzept HCC

Zusätzlich zu den übergreifenden Vorgaben für Testkonzepte gemäß Kapitel 3.1.2.3.1 muss das Testkonzept HCC die für die HCC-Cloud spezifischen Testgegenstände, Prüfungsschwerpunkte und Abgrenzungen der Testkonzeption festlegen. Es muss insbesondere festlegen:

- die Testgegenstände, Teststufen, Testarten, Testumgebungen, Prüfnachweise, Quality Gates sowie Ein- und Ausgangskriterien für die Prüfung der HCC-Cloud,
- die Regressionsteststrategie sowie den Umgang mit Breaking Changes, insbesondere in Bezug auf die Container- Laufzeitumgebung, das Attestierungsprotokoll sowie plattformrelevante Schnittstellen,
- die funktionalen Prüfungsschwerpunkte einschließlich der hierfür vorgesehenen Funktions-, Integrations-, Schnittstellen-, Attestierungs-, Mandantenisolations-, Negativ- und Regressionstests,
- die HCC-spezifischen nichtfunktionalen Schwerpunktbereiche, insbesondere zu Performance, Skalierbarkeit, Resilienz, Hochverfügbarkeit, Wiederanlauf, Fehler-toleranz, Mandantenisolation, Verhalten von HSM-Clustern, Autoscaling sowie zum Verhalten bei Standortausfall, Failover und Rollback,
- die HCC-spezifischen Risiken, Annahmen, Abhängigkeiten und Einschränkungen des Testvorgehens,
- den Einsatz eines fachlich neutralen Referenz-Containers als Referenz-Workload sowie geeigneter Varianten für Edge-Case-, Fehlerfall- und Negativtests,
- die konzeptionelle Abdeckung des vollständigen Attestierungs- und Bereitstellungsprozesses, insbesondere des Starts einer cVM-Workload, der Host- und Workload-Attestation, des Bezugs einer Dienst-Identität, des Aufbaus durchgängiger HTTPS-/TLS-Verbindungen sowie des Trust-Domain-Build-Prozesses einschließlich der Überführung von Container-Images in cVM-Workload-Images, der Berechnung und Hinterlegung von Referenz-Hashes sowie eines nachvollziehbaren Build-Prozesses.

Das Testkonzept HCC muss festlegen, dass Standortausfälle, Failover, die erneute Attestierung von Host und Workload nach Wiederanlauf sowie die Wahrung der Datenkonsistenz als eigenständige Testkategorie berücksichtigt und geprüft werden.

Das Testkonzept HCC muss ferner die Abgrenzung zwischen generischen Cloud-Funktionalitäten, HCC-spezifischen Funktionalitäten, den Funktionen der CI/CD-Plattform sowie fachlichen Fachdienstthemen im Testvorgehen festlegen.

Das Testkonzept HCC muss das konkrete Zusammenwirken generischer Cloud Funktionalitäten mit der HCC-Funktionalität an den jeweiligen Schnittstellen sowie die HCC-seitigen Voraussetzungen für die Integration von Fachdiensten beschreiben und deren Prüfung und Nachweis im Testvorgehen festlegen.

Nachweisführung, Traceability und providerneutrale Bereitstellung

Ergänzend zu den Vorgaben des [gemKPT_Test] muss das Testkonzept festlegen, wie HCC-spezifische Prüfnachweise, deren Nachvollziehbarkeit und ihre Zuordnung zu Container-, cVM-, Attestierungs-, Trust-Domain-, Build- und Release-Ständen sichergestellt werden.

Soweit Prüfnachweise automatisiert erbracht werden, muss das Testkonzept deren konzeptionelle Einbindung in die internen CI/CD-Prozesse des AN festlegen.

Testarchitektur und Testeinbindung in übergreifende Teststufen

Das Testkonzept muss die geplante Testarchitektur und das eingesetzte Testframework beschreiben. Hierzu gehören insbesondere die für die Prüfung der HCC-Cloud eingesetzten Testsuiten, die Testinfrastruktur, deren Schnittstellen sowie die verwendeten Testwerkzeuge.

Das Testkonzept muss ferner die teststrategischen Schwerpunkte der eigenverantwortlichen Tests des AN festlegen. Diese liegen insbesondere auf dem Nachweis der korrekten Umsetzung und des korrekten Betriebs der HCC-Funktionalitäten auf Basis des ReferenzContainers sowie der administrativen HCC-Dienste.

Testreports und Artefakt-Registry

Die Testreports müssen die für die HCC-Cloud erzielten Testergebnisse, den Stand der Testabdeckung sowie die Einhaltung der festgelegten Quality Gates dokumentieren.

Testreports müssen durch den AN signiert und versioniert in einer Artefakt-Registry abgelegt werden. Die Ablage muss so erfolgen, dass die Testreports den jeweils zugrunde liegenden Testläufen, Prüfnachweisen sowie den zugehörigen Build-, Artefakt-, Commit-, Container-, cVM-Image-, Infrastructure-as-Code-(IaC)-, Konfigurations- und Versionsständen eindeutig zugeordnet werden können.

Der AN muss dem AG lesenden Zugriff auf die in der Artefakt-Registry abgelegten Testreports und die für deren Nachvollziehbarkeit erforderlichen Artefakte ermöglichen

Quality Gates

Das Testkonzept muss darstellen, wie die Quality Gates im Testvorgehen berücksichtigt und anhand geeigneter Prüfnachweise nachgewiesen werden. Es muss hierzu insbesondere die Testmaßnahmen und Nachweisformen beschreiben, mit denen die vollständige Abdeckung aller prüfrelevanten HCC-Funktionalitäten, Schnittstellen und administrativen HCC-Dienste sichergestellt wird.

3.1.2.3.2 Testkonzept CI/CD

Das Testkonzept CI/CD muss die für die CI/CD-Plattform spezifischen Testgegenstände, Prüfungsschwerpunkte, Nachweisformen und Abgrenzungen der Testkonzeption festlegen.

Zusätzlich zu den übergreifenden Vorgaben für Testkonzepte gemäß Kapitel 3.1.2.3.1 muss das Testkonzept CI/CD insbesondere festlegen:

- die Testgegenstände, Teststufen, und Testumgebungen für die Prüfung der CI/CD-Plattform,
- die Prüfschwerpunkte für die CI/CD-Plattform,
- die testkonzeptionelle Berücksichtigung von Fehlerfällen, Abbrüchen, Wiederanläufen und Recovery-Szenarien innerhalb der CI/CD-Prozesse,
- die konzeptionelle Abdeckung der Prozesse gemäß Kapitel 3.1.4, einschließlich der Ausführung, Berechtigung, Protokollierung und Nachvollziehbarkeit,
- die Anbindung der Testumgebung an die CI/CD-Strecke, einschließlich des Deployment-Pfades und der Unterscheidung zwischen Mocks und realen Gegenständen sowie die Abgrenzung zwischen der Testverantwortung des AN für die CI/CD-Plattform und der Verantwortung anderer Beteiligter für die fachliche Korrektheit der über die Plattform bereitgestellten Artefakte.

Das Testkonzept CI/CD muss zudem festlegen, wie Prüfnachweise innerhalb der CI/CD-Prozesse den jeweiligen Quellcode-, Build-, Artefakt-, Konfigurations- und Release-Ständen eindeutig zugeordnet werden.

Für Funktionen von Standardprodukten oder Standardplattformen, die ohne wesentliche funktionale Änderungen bereitgestellt werden, sind geeignete Nachweise des Herstellers, der Community oder aus dem Betrieb als Nachweis für die Produktbasisfunktionen ausreichend, sofern Funktionsumfang, Version und Versionsstand eindeutig benannt und für den AG zugänglich sind. Unabhängig davon muss der AN für die von ihm vorgenommene Bereitstellung, Integration, sicherheitsrelevante Konfiguration, Mandantenisolation, Schnittstellenanbindung sowie für HCC-spezifische Erweiterungen und Anpassungen geeignete Testnachweise erbringen.

Der AN kann das Testkonzept CI/CD um weitere, notwendige CI/CD-spezifische testrelevante Themen ergänzen.

3.1.2.4 Betriebliche Konzepte ITSM, SLA und Governance

Das im Rahmen der Angebotsphase eingereichte Betriebskonzept HCC dient der Darstellung des grundsätzlichen Betriebsansatzes des AN und wird nach Zuschlagserteilung nicht als eigenständiges Dokument fortgeschrieben.

Die im Betriebskonzept beschriebenen Inhalte müssen nach Zuschlagserteilung in die im Rahmen dieses Arbeitspakets zu erstellenden und fortzuschreibenden Detailkonzepte durch den AN überführt und dort konkretisiert werden.

Hierzu muss der AN insbesondere ein IT-Service-Management-Konzept (ITSM-Konzept) gemäß Kapitel 3.2.3, ein SLA-Konzept gemäß Kapitel 3.2.4 sowie ein Governance-Konzept gemäß Kapitel 3.2.5 erstellen und dem AG zur Prüfung und Freigabe vorlegen.

Die vorgenannten Konzepte bilden gemeinsam die Grundlage für die spätere Betriebsphase und müssen während der Vertragslaufzeit fortgeschrieben werden.

3.1.2.5 Betriebskonzept CI/CD

Der AN muss für die CI/CD-Plattform das im Angebot erstellte Betriebskonzept fortschreiben und dem AG für MS2 zur Freigabe vorlegen. Die Inhalte des Betriebskonzepts CI/CD werden anschließend über das Betriebshandbuch CI/CD und die Dokumentation CI/CD fortgeschrieben.

Das Betriebskonzept CI/CD muss insbesondere darstellen, wie der sichere, stabile, nachvollziehbare und für die berechtigten Nutzergruppen verfügbare Betrieb der Plattform sichergestellt wird.

Das Betriebskonzept muss insbesondere Festlegungen enthalten:

- zum Betriebsmodell der CI/CD-Plattform einschließlich der Abgrenzung zwischen Plattformbetrieb, Plattformadministration, Nutzung der Plattform durch berechnigte Nutzer sowie der Schnittstellen zum Betrieb der HCC-Cloud,
- zu Rollen, Verantwortlichkeiten und Berechtigungen für den Betrieb, die Administration, die Nutzung von Repositories, Pipelines, Runnern, Artefakt Ablagen, Freigaben und Signaturprozessen,
- zu den Betriebszeiten, Wartungsfenstern, Verfügbarkeitszielen und den für die CI/CD-Plattform geltenden Service Levels,
- zu Monitoring, Protokollierung, Metriken, Traces, Alarmierung und Eskalation für die Plattformkomponenten, die Runner-Ausführungsumgebungen, Repositories, Artefakt Ablagen und die Schnittstellen zur HCC-Cloud,
- zum Incident-, Problem-, Change- und Release-Management für die CI/CD-Plattform einschließlich des Umgangs mit Störungen, Fehlerbildern, Abbrüchen, Wiederanläufen, Recovery-Szenarien sowie sicherheitsrelevanten Updates, Patches und Hotfixes,
- zu Notfall- und Ausweichverfahren für den Fall der Nichtverfügbarkeit der CI/CD-Plattform, insbesondere hinsichtlich der kontrollierten Durchführung notwendiger Hotfixes einschließlich Voraussetzungen, Verantwortlichkeiten, Freigaben und Nachvollziehbarkeit,
- zu Backup, Restore, Wiederanlauf und Recovery der betriebsrelevanten Plattformkomponenten, Konfigurationen, Repositories, Artefakte und Protokolldaten,
- zum Betrieb und zur Skalierung der Runner- und Ausführungsumgebungen einschließlich Kapazitätsmanagement, Lastverteilung und Verhalten bei hoher Parallelisierung,
- zum Betrieb der Repository-, Artefakt- und Registry-Komponenten einschließlich Versionierung, Freigabe, Berechtigungsmodell und Nachvollziehbarkeit,
- zur sicheren Verwaltung von Identitäten, Berechtigungen, Secrets, Schlüsseln, Signaturen und sonstigen sicherheitsrelevanten Betriebsobjekten,
- zur Auditierbarkeit und Nachvollziehbarkeit des Plattformbetriebs, insbesondere hinsichtlich Änderungen an Pipeline-Definitionen, Pipeline-Templates, Berechtigungen, Freigaben, Artefakten, Runner-Konfigurationen und Schnittstellenkonfigurationen,

- zur organisatorischen und technischen Trennung unterschiedlicher Verantwortungsbereiche innerhalb der CI/CD-Plattform,
- zum Zusammenwirken der CI/CD-Plattform mit der HCC-Cloud, insbesondere hinsichtlich der Übergabe freigegebener Artefakte, der Nutzung definierter Schnittstellen, der Verarbeitung von Laufzeit-, Versions- und Attestierungsinformationen sowie der Nachvollziehbarkeit dieser Übergänge.

Das Betriebskonzept muss ferner beschreiben, wie die CI/CD-Plattform den AG sowie berechnete Nutzergruppen im Betrieb unterstützt und wie Betriebs-, Support- und Eskalationsprozesse für die Nutzung der Plattform ausgestaltet sind.

Soweit für die CI/CD-Plattform bereits Festlegungen in Umsetzungskonzepten, Testkonzepten, Sicherheitskonzepten oder sonstigen mitgeltenden Dokumenten getroffen werden, muss das Betriebskonzept diese konsistent aufnehmen und betriebsbezogen konkretisieren. Es gilt die Hinweispflicht des AN gem. Kapitel 2.2, sofern der AN Widersprüche in den Konzepten erkennt.

Die Mitwirkung, Prüfung, Abstimmung oder Freigabe durch den AG entbinden den AN nicht von seiner Verantwortung für die inhaltliche Vollständigkeit, fachliche Eignung und konkrete Ausgestaltung des Betriebskonzepts.

3.1.3 Arbeitspaket 2: Entwicklung und Bereitstellung der HCC-Cloud

Die Bereitstellung der HCC-Cloud setzt voraus, dass die Sicherheitsarchitektur gemäß [gemProdT_HCC_PTV] und [gemAnbT_HCC_ATV] in der HCC-Cloud umgesetzt ist, da diese die sicherheitstechnischen Anforderungen für den Betrieb der vertrauenswürdigen TI-Dienste darstellt.

Die Implementierung von HCC stellt eine projekthafte Leistung des AN in Zusammenarbeit mit dem AG dar. Die Anforderungslage für die Implementierung ist durch die vorliegende Leistungsbeschreibung, die Spezifikation [gemSpec_HCC], die Verfeinerungen bzw. Konkretisierungen im Umsetzungskonzept HCC des AN sowie die weiteren Konzepte des AN vorgegeben.

Das Arbeitspaket umfasst für die Entwicklung der HCC-Cloud die folgenden Umsetzungsleistungen:

- Projekthafte Umsetzung der beim AN benötigten Services für HCC nach den Vorgaben von [gemSpec_HCC]. Die Umsetzung soll in der ersten produktiv eingesetzten Version zum MS6 bereits so weit wie möglich auf das Ziel der Bereitstellung von HCC als Cloud-natives Produkt ausgerichtet sein. Der Übergang von dieser ersten, im Sinne der Anforderungen des TI-Flow-Fachdienstes voll funktionsfähigen, aber spezifisch für den TI-Flow-Fachdienst implementierten Form von HCC zu einer zukünftigen Cloud-nativen Form soll in Schritten entlang der im eingereichten Umsetzungskonzept HCC dargestellten Roadmap erfolgen.
- Aufbau und Bereitstellung des HCC-Stacks und der zugehörigen administrativen Services für die gematik in ihrer Rolle als Governance Authority (Trust Domain Provider) für ihre HCC-Vertrauensräume (Trust Domains).

- Aufbau der für HCC erforderlichen Konfigurationsmöglichkeiten im Mandantenkontext für Dienstanbieter.
- Entwicklung und Bereitstellung eines Confidential Virtual Machine Templates (cVM-Template), einer Test-Workload (Test-Container) sowie der Funktionalität zur Integration von Workloads und cVM-Template in für das Deployment innerhalb der HCC-Cloud geeignete cVM-Images.
- Bereitstellung der Test-Pipeline einschließlich der für die vollständige Prüfung der Funktionalität und der Sicherheitseigenschaften der HCC-Cloud erforderlichen Logs, Metriken und Traces für die Auswertung von Testergebnissen.
- Unterstützung des AG bei der Initialisierung der HCC-Trust-Domains für die Produktivumgebung (PU), Referenzumgebung (RU) bzw. Testumgebungen (TU und RU-DEV). In der PU müssen HCC-Hosts zur exklusiven Nutzung in dieser Trust Domain provisioniert werden. Die virtuellen Maschinen der Trust Domains RU und RU-DEV können beliebig auf attestierte Hosts verteilt werden. Einige Umgebungen werden permanent betrieben, darüber hinaus werden weitere Umgebungen bei Bedarf instanziiert und wieder beendet.
- Für Last-, Failover- und Resilienztests muss der AN die vorgesehenen Workload-Instanzen auf für die Dauer der Tests exklusiv provisionierten HCC-Hosts bereitstellen, sodass Performance-Ergebnisse nicht durch konkurrierende Workloads und das getestete Systemverhalten nicht durch andere als in der PU vorgesehene Konfigurationen beeinflusst werden.
- Nachweis der Anforderungskonformität über Tests und beauftragte Gutachten durch den AN.

3.1.3.1 Prototyp zur Clientintegration

Der Prototyp zur Clientintegration dient dazu, dass zu einem möglichst frühen Zeitpunkt ein Prototyp des TI-Flow-Fachdienstes aus Los 1 und die Komponente ZETA Guard über den Prototyp der CI/CD-Plattform deployed und getestet werden können. Dieser Prototyp muss eine geeignete Laufzeitumgebung für die Komponente ZETA-Guard bieten und eine Container-Runtime für den Prototyp des TI-Flow Fachdienstes. Spezifische HCC-Funktionalität wird für diesen Prototyp nicht gefordert. Wenn es dem Zeitplan des AN entspricht, kann dieser Prototyp mit dem Prototyp der HCC-Funktionalität zusammengelegt werden.

Der Prototyp Clientintegration umfasst:

- Die Möglichkeit für gematik und Los 1 Cloud-Ressourcen im Self-Service für die Workloads nutzbar zu machen
- Netzwerkservices (Ingress, Egress, Load Balancer, DNS etc.)
- Managed Kubernetes
- Managed SQL-Datenbank
- Compute- und Storage Ressourcen

Der Prototyp gilt als erfolgreich bereitgestellt, wenn:

- Eine Beispielworkload über den Prototypen CI/CD deployed wurde
- Die Workload über das Internet kommunizieren konnte
- Datenbankfunktionalität nachgewiesen wurde.

3.1.3.2 Prototyp-HCC und Testnachweise der HCC-Funktionalität

Der Prototyp-HCC ist der erste Kontrollpunkt für die Umsetzung der HCC-Funktionalität. Er dient zum einen als Proof of Concept für das Umsetzungskonzept HCC und um Informationen zur Finalisierung des Umsetzungskonzepts HCC zu ermitteln. Zum anderen soll er Integrationstests mit ZETA Guard und den Entwicklungsergebnissen aus Los 1 ermöglichen, indem alle Schnittstellen nutzbar sind, die für die Ausführung dieser Workloads benötigen werden. Die Funktionalität dieser Schnittstellen kann dabei gemocked werden.

Im Prototyp vom AN umzusetzende Funktionalität:

- Herstellen des cVM-Templates nach den Vorgaben von [gemSpec_HCC]
- Herstellen eines Referenz-Containers nach den Vorgaben von Kapitel 3.1.5.1
- Integration von ZETA Guard mit dem Referenz-Container
- Erstellen eines Deployable Workload durch den Trust Domain Build Service mit Artifact Signing und Ermittlung der Attestation Reference Values
- Instanziierung des Deployable Workload als cVM inkl. ZETA Guard und Referenz-Container aus dem Deployment Repository mit Attestation und Schlüssel-Provisionierung für den Zugriff auf Redis-DB, Block Storage, SQL-DB
- Prototypische Umsetzung oder Mockup des HSM-Proxys nach [gemSpec_ZETA]
- Prototypische Umsetzung der für die Prüfung des vollständigen Verifikations- und Deployment-Prozesses erforderlichen Funktionalitäten

Die Entwicklung hat in einem separaten Prototyp-Mandanten zu erfolgen, so dass der Prototyp HCC für Tests genutzt werden kann. Die HCC-Funktionalität wird kontinuierlich weiterentwickelt, wobei stabile Entwicklungsstände dem Mandanten so zur Verfügung gestellt werden, dass sie von gematik bzw. dem Anbieter von Los1 in den Prototypen HCC übernommen werden können, sobald die Entwicklung des TI-Flow-Fachdienstes darauf vorbereitet ist.

Der Prototyp gilt als erfolgreich abgeschlossen, wenn alle in diesem Kapitel genannten Funktionalitäten in der Entwicklungsumgebung des AN nachweislich ausgeführt und die Ergebnisse in der Artefakt-Registry dokumentiert wurden, und der AG die Ergebnisse im Prototypen HCC nachvollziehen konnte.

Die im Prototyp-HCC gewonnenen Testergebnisse und Erkenntnisse sind verpflichtend in das Testkonzept HCC einzuarbeiten. Der AG erhält Zugriff auf alle Testergebnisse des Prototyp-Mandanten und prüft im Rahmen der Freigabe, ob die Erkenntnisse aus dem Prototyp eingeflossen sind.

3.1.3.3 Entwicklung der vollständigen HCC-Funktionalität

Die Entwicklung der HCC-Funktionalität und HCC-Dienste, wie im freigegebenen Umsetzungskonzept HCC beschrieben, ist abgeschlossen und integriert den HSM-Proxy nach [gemSpec_ZETA]. Die Trust Domain RU ist angelegt und hat den Prototypen HCC als Test- und Integrationsumgebung abgelöst. Die Entwicklung erfolgt in einem separaten Mandanten, so dass die Entwicklung und Testtätigkeiten der Trust Domain RU nicht behindert werden. Stabile Entwicklungsstände werden dem Mandanten der Trust Domain RU zur Verfügung gestellt.

Für jeden der in diesem Kapitel genannten administrativen HCC-Dienste sind dedizierte Testfälle zu definieren. Die Freigabe jedes Dienstes setzt den erfolgreichen Abschluss der zugehörigen Eigenverantwortlichen Tests (EvT) und die Vorlage der Testdokumentation gemäß [gemKPT_Test#4.4] voraus.

Alle HTTP-/REST-Schnittstellen der HCC-Cloud-Leistung, die durch Komponenten außerhalb der HCC-Cloud genutzt werden oder für eine Nutzung durch solche Komponenten vorgesehen sind, sind im Format OpenAPI Specification (OAS) Version 3.0 oder höher zu dokumentieren. Dies umfasst insbesondere Schnittstellen zu Fachdiensten, TI-Diensten sowie zu Governance-, Betriebs-, Monitoring- und Testsystemen der gematik sowie sonstige externe Service-APIs.

Die Dokumentation muss realitätsnahe, implementierungskonforme Beispiele enthalten; generische Platzhalter sind unzulässig. Die OpenAPI-Spezifikationen sind maschinenlesbar über einen HTTP-GET-Endpunkt bereitzustellen und über CI/CD-Pipelines kontinuierlich aktuell zu halten. Dokumentationsrelevante Änderungen an REST-Schnittstellen (insbesondere an Ressourcen, Endpunkten, Parametern, Schemata, Authentifizierung oder Fehlercodes) sind spätestens mit Bereitstellung der Änderung versioniert nachzuführen.

Für die Versionierung ist Semantic Versioning anzuwenden, um Breaking Changes eindeutig zu kennzeichnen. Zudem ist durch geeignete API-Tests, insbesondere Contract Tests zwischen In-Scope- und Out-of-Scope-Komponenten, jederzeit die Übereinstimmung zwischen OpenAPI-Spezifikation und Implementierung sicherzustellen.

3.1.3.4 Entwicklungsartefakte

Bei verschiedenen Meilensteinen werden Entwicklungsartefakte als Liefergegenstände gefordert. Die Entwicklungsartefakte umfassen:

- Entwickelter Softwarestand integriert in die HCC-Cloud des Anbieters und nutzbar für gematik-Trustdomains.
- Entwickelte Individualsoftware als Quellcode und Individualkonfiguration in einem vom AG vorgegebenen Repository

3.1.3.5 Dokumentation HCC

Die konzeptionellen Anforderungen an Struktur, Inhalt und Bereitstellung der Testdokumentation und -berichte (Reporting) sind im Kapitel 3.1.2.3 festgelegt. Die nachfolgende Aufzählung benennt die hierauf aufbauenden konkreten Liefergegenstände (gemäß gem-KPT_Test):

- Testkonzepte (Testkonzept HCC und Testkonzept CI/CD)
- Release Notes mit
 - Liste der pro Umsetzungspaket umgesetzten Anwendungsfälle
 - Versionen der bereitgestellten Komponenten
 - Beschreibung und Auswirkungen der Änderungen zur Vorversion (Auswirkungsanalyse) sowie Risikoanalyse
- Fehler und Abweichungen:
 - Offene und bekannte Fehler mit den aus ihnen resultierenden Beeinträchtigungen. Als Fehler gilt eine Abweichung des Verhaltens von den Anforderungen der Spezifikation oder des Umsetzungskonzepts HCC.
 - Abweichungen: vom erwarteten Verhalten abweichende Beobachtungen, die spezifikationskonform sind, weil die Spezifikation den Sachverhalt nicht regelt oder ihrerseits fehlerhaft ist. Solche Beobachtungen sind unabhängig von der Einordnung als Fehler zu dokumentieren.
 - Über die Anforderungen der Spezifikation oder des Umsetzungskonzepts hinausgehende Änderungen
- Testspezifikation (für die umgesetzten Anwendungsfälle aus den Umsetzungspaketen)
- Testprotokoll (für die umgesetzten Anwendungsfälle aus den Umsetzungspaketen)
- Testbericht: Der Testbericht muss die zusammenfassende Auswertung der Testprotokolle pro Umsetzungspaket sowie die Zuordnung zu Anforderungen, Testfällen, Defekten und Freigabeständen enthalten. Er muss in der Artefakt-Registry abgelegt werden.
- Produktdokumentation (Fortschreibung des Umsetzungskonzepts HCC) *)

Die Dokumentation HCC stellt zu den Kontrollpunktlieferungen den jeweils aktuellen Entwicklungsstand dar. Die mit *) markierten Bestandteile müssen zum MS4.2 vollständig bereitgestellt werden.

Die im Rahmen der CI/CD-Pipelines automatisiert erzeugten, kryptographisch signierten und versionierten Testreports gelten als Testprotokoll im Sinne dieser Leistungsbeschreibung; sie ersetzen nicht den Testbericht. Der Testbericht ist als zusammenfassende, anforderungsbezogene Auswertung gemäß den vorstehenden Anforderungen an den Testbericht (Zuordnung zu Anforderungen, Testfällen, Defekten und Freigabeständen) abzuleiten. Testreport und Testprotokoll können vollständig automatisiert aus den CI/CD-Pipelines erzeugt werden; eine über die Pipeline-Artefakte hinausgehende manuelle Testdokumentation wird nicht gefordert. Der Testbericht muss als aus den Testreports automatisiert aggregierte Auswertung (Anforderungsabdeckung, Quality-Gate-Status, offene Defekte, Freigabestand) je Umsetzungspaket oder je Freigabeeinheit bzw. Pipeline-Lauf bereitgestellt

werden. Alle vorgenannten Artefakte müssen versioniert in der Artefakt-Registry abgelegt werden.

Das Admin-Handbuch enthält Anleitungen und Informationen für Systemadministratoren, um den HCC-Service effektiv zu verwalten, zu konfigurieren, zu warten und zu überwachen.

3.1.3.6 Bereitstellende Umgebungen

Der AN muss die in der Tabelle: "Übersicht der geplanten Umgebungen" genannten Umgebungen als HCC-Trust-Domains bereitstellen, betreiben und dem AG sowie berechtigten Dritten zur Verfügung stellen. Die Bereitstellungspflicht umfasst:

Tabelle 1: Bereitstellungsanforderungen der Umgebungen

Anforderung	Beschreibung
Bereitstellung	Der AN muss alle Umgebungen innerhalb der vereinbarten Fristen nach Anforderung durch den AG bereitstellen.
Betrieb	Der AN betreibt alle Umgebungen gemäß den in Kapitel 3.2.4 definierten SLAs.
Skalierung	Der AN muss die dynamische Instanziierung und Abbau temporärer Umgebungen ermöglichen.
Monitoring	Der AN stellt Monitoring und Logging für alle Umgebungen bereit.

Auslösung der Bereitstellung durch den AG

Die Auslösung der Bereitstellung und des Abbaus erfolgt durch den AG oder durch von ihm beauftragte Dritte. Grundlage hierfür sind der Provider gemäß Kapitel 3.2.2.3 (Bereitstellung und Skalierung) sowie die Steuerungsschnittstellen gemäß Kapitel 3.1.4.11 (APIs, Integration und Automatisierung). Die CI/CD-Plattform dient dabei als Steuerungsebene für die Auslösung der Bereitstellungs- und Abbauprozesse. Der AN muss hierfür sicherstellen, dass

- die Bereitstellung und der Abbau über die vom AG genutzten Steuerungswege auslösbar sind, insbesondere über Self-Service, Infrastructure as Code sowie die Provisionierungs- und Steuerungsschnittstellen,
- die Bereitstellungs- und Abbauprozesse einschließlich der Allokation und Freigabe der zugeordneten Ressourcen vollständig automatisiert auf Grundlage der bereitgestellten Provisionierungs-Schnittstellen ablaufen und keine manuelle Einzeltätigkeit des AN erfordern,
- die hierfür erforderlichen Schnittstellen während der vereinbarten Servicelevels verfügbar sind.

Die folgende Übersicht zeigt die geplanten Umgebungen, deren Zweck sowie die Eigenschaften der benötigten Instanzen:

Tabelle 2: Übersicht der geplanten Umgebungen

Umgebung	Anzahl Instanzen	Lebensdauer	Hauptzweck
RU Dev permanent	1 Instanz	permanent	Integrationstests mit Dritten (FdVs, Primärsysteme)
RU Dev- temporär	Bis zu 5 Instanzen	Temporär	Isolierte HCC Tests (Failover, Lasttests, ggf. mit TI Flow) zur Vorbereitung und Dimensionierung; der verbindliche Nachweis erfolgt in der RU
TU	1 Instanz	Temporär	Durchführung der übergreifenden Gesamt-Integrationstests (GIT-TI-Tests) durch die gematik.
RU	1 Instanz	Permanent	Referenzumgebung für Fehler- nachtests sowie einzelne GIT-TI Testarten wie die Generalprobe und Bestätigungsverfahren

Der AN muss sicherstellen, dass die permanenten Umgebungen dauerhaft verfügbar sind. Temporäre Umgebungen muss der AN auf Anforderung bereitstellen. Die Bereitstellung erfolgt zweistufig:

- Technische Bereitschaft: Die Workload-Instanzen sind innerhalb von 30 Minuten nach Anforderung verfügbar.
- Testbereitschaft: Die Umgebung ist innerhalb von einer Stunde nach Anforderung für die vorgesehenen Tests nutzbar. Dies umfasst die vollständige Konfiguration einschließlich des Datenimports gemäß Vorgabe sowie der erforderlichen internen Netz- und Namensauflösungseinträge.
- Der AN muss die temporären Umgebungen nach Erreichen des jeweiligen Testzwecks abbauen und die zugeordneten Ressourcen freigeben. Der Abbau muss durch den AG ohne Mitwirkung des AN auslösbar sein.

Anbindungen an Systeme Dritter – insbesondere Fachdienste, Primärsysteme und weitere Testpartner – erfolgen in Abstimmung mit dem jeweiligen Betreiber und richten sich nach den hierfür geltenden Mitwirkungsregelungen.

Für temporäre Umgebungen, die der Integration mit Systemen Dritter dienen – insbesondere Fachdienste und Primärsysteme – muss der AN die hierfür erforderlichen Anbindungen für die Dauer des Testzwecks bereitstellen und mit dem Abbau der Umgebung zurückführen. Die Mitwirkung der jeweiligen Betreiber richtet sich nach den hierfür geltenden Mitwirkungsregelungen.

3.1.3.7 Erklärung zur funktionalen, betrieblichen und sicherheitstechnischen Eignung

Der AN muss gegenüber dem AG eine schriftliche Erklärung abgeben, dass die Leistung alle Anforderungen aus [gemAnbT_HCC_ATV] erfüllt, die den Prüfverfahren:

- Anbietererklärung funktionale Eignung
- Anbietererklärung betriebliche Eignung
- Anbietererklärung sicherheitstechnische Eignung

zugeordnet sind.

Der AN muss gegenüber dem AG eine schriftliche Erklärung abgeben, dass die Leistung alle Anforderungen aus [gemProdT_HCC_PTV] erfüllt, die den Prüfverfahren:

- Herstellererklärung funktionale Eignung
- Herstellererklärung sicherheitstechnische Eignung

zugeordnet sind.

3.1.4 Arbeitspaket 3: Entwicklung und Bereitstellung der CI/CD-Plattform

Die Leistung des AN in Bezug auf Test-, CI- und CD-Funktionalitäten besteht in der Bereitstellung einer CI/CD-Plattform für die Ausführung von Pipelines und ihrer Anbindung an die verschiedenen Umgebungen (gemäß Kapitel 3.1.3.6) in der HCC-Cloud (die als Stages genutzt werden). Zur CI/CD-Plattform gehören entsprechende Repositories zur Verwaltung der Pipeline-Definitions-Artefakte sowie je Umgebung (RU, TU, etc.) eine eigene Runner-Umgebung zur Ausführung von Pipeline-Skripten und -Funktionen.

Die CI/CD-Plattform wird für automatisierte Test-, Prüf-, Signatur-, Freigabe-, Promotion- und Deployment-Prozesse im Kontext der Bereitstellung und des Betriebs von Fachdiensten innerhalb der HCC-Cloud genutzt. Sie wird durch den AG und durch von ihm beauftragte Dritte genutzt und durch den AN betrieben. Sie ist nicht als primäre Entwicklungsplattform der Fachdiensthersteller zu verstehen. Die fachliche Entwicklung, die Quellcodeverwaltung und herstellerspezifische interne Build-Prozesse der Fachdiensthersteller müssen außerhalb der CI/CD-Plattform erfolgen.

Die CI/CD-Plattform besitzt integrierte Funktionen für

- Repository-Zugriff und -Verwaltung
- Pipeline-Orchestrierung
- Runner-Ausführung und -Steuerung
- Identitäts-, Schlüssel- und Zugriffsmanagement
- Auditierung und Protokollierung
- OCI-Artefakt- und Image-Verwaltung
- Schnittstellen zur HCC-Cloud

Sie muss über diese Funktionen ein Staging und den Stage-Übergang von Fachdienstanwendungen innerhalb der Pipelines ermöglichen. Die Entwicklung der Pipelines und deren Stage-Übergangslogiken erfolgt durch den AG.

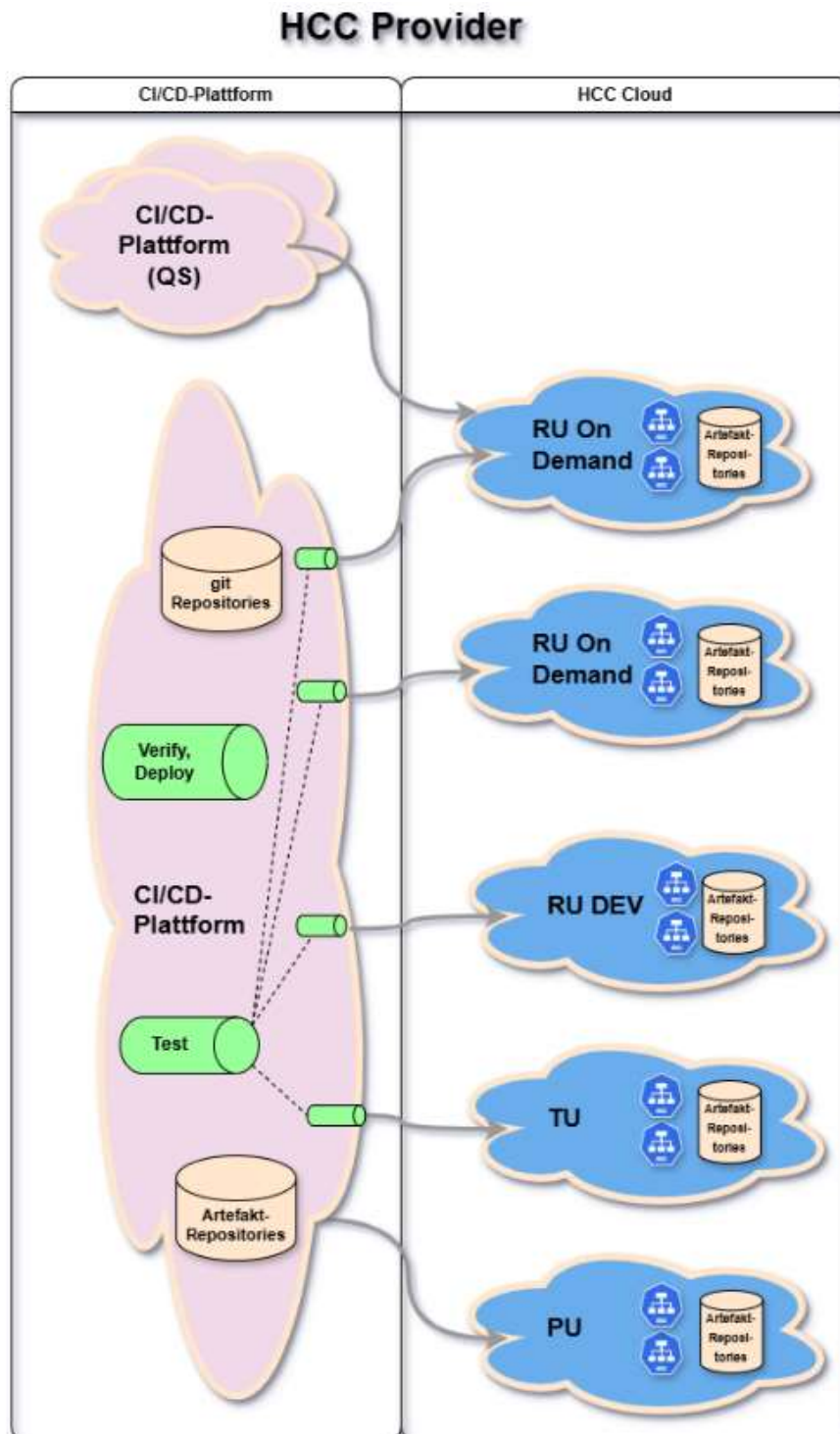


Abbildung 1: Staging und Stageübergänge beim HCC-Provider

Soweit in diesem Kapitel und dessen Unterkapiteln von Quellcodeverwaltung die Rede ist, bezieht sich dies auf Quellcode, Konfigurationen und textbasierte Artefakte, die für die auf der CI/CD-Plattform abgebildeten Prozesse erforderlich sind. Hierzu zählen insbesondere, jedoch nicht ausschließlich, Pipeline-Definitionen, Pipeline-Templates, Testsuiten, Testfälle, Testskripte, testbezogene Konfigurationen und Automatisierungsartefakte.

Soweit Funktionen des TI Design & Configuration Repository oder des TI Verification & Build Service nach [gemSpec_HCC] betroffen sind, stellt die CI/CD-Plattform diese nur insoweit bereit oder integriert sie, wie dies für Test-, Prüf-, Signatur-, Freigabe-, Promotion- und Deployment-Prozesse erforderlich ist. HCC-spezifische Runtime-Funktionen, insbesondere die Ausführung von Workloads, Attestierung zur Laufzeit, Schlüsselbereitstellung, Trust-Domain-Konfiguration und der Betrieb freigegebener Workloads, verbleiben in der HCC-Cloud.

Die CI/CD-Plattform ersetzt die HCC-Cloud nicht als Runtime-Umgebung für TI-Flow-Fachdienste. Deployments in die HCC-Cloud erfolgen ausschließlich über definierte Schnittstellen, Freigabeprozesse und Stage-Repositories der HCC-Cloud.

Soweit in diesem Kapitel auf SCS Bezug genommen wird, ist hierunter der Sovereign Cloud Stack (SCS)¹ zu verstehen.

Die Anforderungen zum SCS in diesem Kapitel beziehen sich ausschließlich auf die CI/CD-Plattform und deren Architektur, Schnittstellen, Betriebsprozesse und Portabilität. Sie begründen keine unmittelbare SCS-Konformitätsanforderung an die HCC-Cloud.

Die CI/CD-Plattform soll sich hinsichtlich ihrer Architektur, Schnittstellen, Betriebsprozesse und Portabilität an den Vorgaben und Prinzipien des SCS orientieren. Der AN muss im Umsetzungskonzept CI/CD nachvollziehbar darstellen, welche relevanten SCS-Vorgaben, Referenzarchitekturen, Schnittstellen und Betriebsprozesse bei der Konzeption und Umsetzung der CI/CD-Plattform berücksichtigt werden und an welchen Stellen hiervon abgewichen wird. Der AG behält sich vor, SCS oder ausgewählte SCS-Vorgaben in zukünftigen Ausbaustufen als verbindlichen Standard vorzugeben.

Die konkreten Anforderungen an die Funktionalität der CI/CD-Plattform werden in den nachfolgenden Unterkapiteln detaillierter beschrieben.

¹ <https://sovereigncloudstack.org/>

3.1.4.1 Organisationsmodell, Mandantenfähigkeit und Zugriffsstruktur

Die CI/CD-Plattform muss über ein integriertes Namespace- bzw. Organisationsmodell verfügen. Dieses:

- muss eine Gruppen- und Projektstruktur mit getrennten Verantwortungsbereichen und Berechtigungen unterstützen,
- soll eine hierarchische Gruppen- und Projektstruktur mit obersten Organisationseinheiten, Untereinheiten/Subgruppen/Projekten und klar getrennten Verantwortungsbereichen unterstützen,
- muss Hersteller, interne Prüforganisationen und Betriebs- bzw. Plattformpartner logisch und administrativ voneinander isolieren,
- soll vererbte und granulare Berechtigungen ermöglichen,
- muss Mandanten und Organisationseinheiten getrennt auswertbar halten; Artefakte, Pipelines und Deployments müssen eindeutig zuordenbar sein,
- muss so konfiguriert werden können, dass unterschiedliche Rollen- und Zugriffsmodelle nutzbar sind und die Ausführung von Pipeline-Runnern im konfigurierbaren HCC-Mandantenraum unterstützt wird,
- muss Cloud-Nutzern ermöglichen, auf der CI/CD-Plattform bereitgestellte Pipeline-Templates zu nutzen und darüber Test-, Prüf-, Freigabe-, Promotion- und Deployment-Prozesse für berechtigte HCC-Cloud-Mandantenräume über definierte Schnittstellen auszulösen,
- muss eine Abbildung von Berechtigungsstrukturen für die verwalteten Artefakte und Pipelines ermöglichen sowie
- muss eine mindestens dreistellige Anzahl von Anwendern sowie mehrere organisatorisch getrennte Verantwortungsbereiche unterstützen.

Die fachliche und organisatorische Ausgestaltung (u. a. Gruppen- und Projekt-Modell, Rollenmodelle, Naming-Konventionen, Onboarding-Prozesse) liegt in der Verantwortung des AG.

3.1.4.2 Identitäts- und Zugriffsmanagement

Die CI/CD-Plattform muss sich an ein durch den AG vorgegebenes zentrales Identitätsmanagement anbinden können. Sie muss dabei OpenID Connect bzw. OAuth 2.0 und optional die folgenden Standards unterstützen:

- Microsoft Entra ID / Azure AD,
- SAML 2.0.

Die CI/CD-Plattform soll SCIM zur Benutzer- und Gruppen-Provisionierung unterstützen.

Es muss eine rollenbasierte Zugriffskontrolle (RBAC) realisiert werden, die mindestens folgende unterschiedliche Rollen abbilden kann:

- Lese-Rolle,
- Entwicklungs-/Änderungs-Rolle,
- Maintainer-/Administrations-Rolle,
- Deployment-/Freigabe-Rolle,
- Sicherheits-/Audit-Rolle.

Darüber hinaus muss die CI/CD-Plattform:

- Benutzer und Gruppen zentral zuordenbar und entziehbar halten,
- eine lückenlose Nachvollziehbarkeit von Benutzeraktionen sicherstellen, insbesondere für Code-Änderungen, Pipeline-Ausführungen, Freigaben sowie Berechtigungs- und Konfigurationsänderungen,
- Pipeline-based Access Control (PBAC) oder ein gleichwertiges Konzept zur kontrollierten, rollen- und kontextabhängigen Ausführung von Pipeline-Schritten unterstützen.

3.1.4.3 Source-Code-Repository-Funktion

Die CI/CD-Plattform muss eine Git-basierte, verteilte Repository-Funktion bereitstellen, in der mehrere Repositories innerhalb einer übergeordneten Organisationsstruktur verwaltet werden können.

Die Repository-Funktion dient der versionierten Verwaltung aller Quellcode-, Konfigurations- und Automatisierungsartefakte, die für die auf der CI/CD-Plattform abgebildeten Test-, Prüf-, Signatur-, Freigabe-, Promotion- und Deployment-Prozesse erforderlich werden.

Sie muss:

- Branch-Strategien unterstützen,
- Merge-/Pull-Request-basierte Review-Prozesse mit konfigurierbaren Freigaberegeln ermöglichen,
- geschützte Branches und Tags unterstützen,
- Pipeline-as-Code versioniert verwalten,
- standardisierte Pipeline-Bausteine (z. B. Templates, Includes, Komponenten oder Bibliotheken) wiederverwendbar bereitstellen,
- die Ausführung von Pipeline-Runnern für berechnete HCC-Cloud-Mandantenräume über definierte Schnittstellen unterstützen,
- signierte Commits unterstützen und für durch den AG definierte Repositories durchsetzen können.

Für zentrale, durch den AG bereitgestellte Template-Repositories müssen differenzierte Zugriffsrechte unterstützt werden. Der AG muss Templates erstellen, bearbeiten und versionieren können. Andere berechnete Nutzer müssen diese Templates für standardisierte Test-, Prüf-, Freigabe-, Promotion- und Deployment-Prozesse verwenden können, ohne sie verändern zu dürfen.

Das zentrale Repository wird vom AN bereitgestellt und betrieben.

3.1.4.4 Pipeline-Orchestrierung und Pipeline-Ausführung

Die CI/CD-Plattform muss die Orchestrierung und Ausführung von Pipeline-Definitionen für Test-, Analyse-, Prüf-, Signatur-, Freigabe-, Promotion- und Deployment-Prozesse unterstützen.

Build-Schritte sind nur insoweit Bestandteil der CI/CD-Plattform, wie sie für standardisierte Prüf-, Signatur-, Attestierungs-, Transformations- oder Deployment-Prozesse erforderlich sind.

Unterstützt werden müssen mindestens:

- Pipeline-Laufzeitumgebung,
- Konfigurationsmöglichkeiten für Pipeline-Runner,
- Monitoring für Pipeline-Runner,
- Artefakt-Annahme- und Artefakt-Prüfungs-Pipelines,
- Transformations- und Signaturprozesse für deploymentfähige Artefakte,
- Artefakt- und Container-Builds,
- Sicherheits- und Compliance-Prüfungen,
- Freigabe- und Deployment-Pipelines,
- mehrstufige Promotion-, Stage-Übergangs- und Release-Workflows.

Die CI/CD-Plattform muss darüber hinaus:

- mehrstufige und voneinander abhängige Pipelines abbildbar machen,
- Pipelines ereignisgesteuert (z. B. Commit, Tag, Merge-Request, Registry-Event), zeitgesteuert oder per API startbar machen,
- manuelle Freigabeschritte integrierbar halten,
- parallelisierte und seriell gesteuerte Jobausführung erlauben,
- projektübergreifende Standardisierung und Wiederverwendung von Pipeline-Definitionen unterstützen,
- Pipeline-as-Code durchgängig umsetzen.

Die CI/CD-Plattform muss es Pipeline-Stufen ermöglichen, HCC-spezifische Dienste der HCC-Cloud über dokumentierte und abgesicherte Schnittstellen aufzurufen. Dies umfasst insbesondere:

- die Übergabe freigegebener OCI-Artefakte an den Trust Domain Build Service der HCC-Cloud zur Erzeugung deploymentfähiger cVM-Workload-Images,
- die Abfrage von Laufzeit- und Versionsinformationen der bereitgestellten Workloads,
- die Prüfung bereitgestellter Signaturen, Attestierungen und Nachweisartefakte im Rahmen definierter Freigabeprozesse,
- die Überführung freigegebener deploymentfähiger Artefakte in das jeweils zugehörige Stage-Repository der HCC-Cloud,
- das Deployment freigegebener deploymentfähiger Artefakte.

3.1.4.5 Verarbeitung von HCC-Laufzeit-, Versions- und Attestierungsinformationen

Die CI/CD-Plattform muss relevante Laufzeit-, Versions- und Attestierungsinformationen zu instanziierten Workloads einschließlich Informationen zum zugrunde liegenden HCC-Stack automatisiert verarbeiten können. Sie muss diese Informationen während der Testausführung aus der HCC-Cloud abrufen, mit dem jeweiligen Testlauf korrelieren und als Bestandteil der Testlaufauswertung, insbesondere in Testreports und Testartefakten, nachvollziehbar dokumentieren und persistieren können.

Die CI/CD-Plattform soll es ermöglichen, dass eine durch den AG oder durch berechtigte Dritte bereitgestellte Pipeline die Instanziierung des Testobjekts selbst durchführt und dabei die entstehenden Runtime-Informationen unmittelbar erfasst und weiterverarbeitet.

Erfolgt die Instanziierung außerhalb der Pipeline, muss die CI/CD-Plattform die hierfür erforderlichen Informationen über Schnittstellen der HCC-Cloud, insbesondere über den TDCAS, automatisiert abrufen können. Dies umfasst mindestens Endpunkte, Versionsstände und Attestierungsinformationen laufender Workloads.

3.1.4.6 Ausführung und Auswertung bereitgestellter Testsuiten

Die CI/CD-Plattform muss Workflows für die Bereitstellung, Ausführung und Auswertung von Tests unterstützen.

Die Plattform muss insbesondere unterstützen:

- das Laden bereitgestellter Testfälle, Testsuiten, Testdaten und testbezogener Konfigurationen,
- die Ausführung bereitgestellter automatisierter Tests,
- die Bereitstellung von Logs und weiteren Testartefakten einschließlich deren Weitergabe an nachgelagerte Schritte,
- die Zuordnung der Testergebnisse zu Artefakt-Version, Signatur-/Attestierungsstatus, Pipeline-Lauf, Zielumgebung und Freigabeentscheidung.

3.1.4.7 Artefakt- und OCI-Registry

Der AN muss Artefakt- und OCI-Registry-Instanzen bereitstellen, die sowohl im Kontext der CI/CD-Plattform als auch im Kontext der HCC-Cloud genutzt werden können. Die Registry-Instanzen müssen denselben geforderten Funktionsumfang bereitstellen. Die Unterscheidung erfolgt über Nutzungskontext, Zugriffsrechte und Freigabeprozesse.

Die Artefakt-Verwaltung muss eine Artefakt-Registry für generische Artefakte sowie eine OCI-konforme Registry für OCI-Artefakte umfassen. Beide können als gemeinsame technische Lösung umgesetzt werden, sofern sämtliche Anforderungen erfüllt werden.

Artefakt-Registry

Die Artefakt-Registry muss mindestens die folgenden Artefakt-Typen unterstützen:

- Eingangsartefakte der Fachdiensthersteller, des AG oder berechtigter Dritter, soweit sie für Test-, Prüf-, Signatur-, Freigabe-, Promotion- oder Deployment-Prozesse benötigt werden,
- Build-Artefakte, z. B. Build-Ergebnisse, Pakete und Archive,
- Binärartefakte, z. B. JAR-, WAR-, DLL-, EXE-, ZIP-, Maven-, NuGet-, NPM- oder PyPI-Pakete,
- Test- und Qualitätsartefakte, z. B. Testreports, Coverage-Reports und Scan-Ergebnisse,
- Sicherheits- und Nachweisartefakte, z. B. SBOMs, Signaturen, Attestierungen, Build-Attestations, Vulnerability Reports und VEX-Dokumente.

OCI-konforme Registry

Die OCI-konforme Registry muss mindestens die folgenden Artefakt-Typen unterstützen:

- OCI Images,
- OCI Image Indexes, insbesondere Multi-Arch-Images,
- OCI Artifacts gemäß OCI-Spezifikation,
- OCI-Referrer-Artefakte, z. B. SBOMs, Signaturen, Attestierungen und Vulnerability Reports.

Die Artefakt-Registry sowie die OCI-konforme Registry müssen es ermöglichen, Artefakte und OCI-Artefakte:

- versioniert abzulegen,
- mit einer nachvollziehbaren Herkunftszuordnung zu versehen,
- rollen-, projekt-, mandanten- und stagebezogen abzusichern,
- in CI/CD-Pipelines ohne Medienbrüche direkt zu nutzen,
- zwischen definierten Freigabe-, Prüf- oder Releasestufen zu überführen,
- nach Regeln zu löschen bzw. zu bereinigen,
- revisionssicher in ihrer Historie nachzuvollziehen.

Sicherheits- und Nachweisartefakte, insbesondere SBOMs, Signaturen, Attestierungen, Build-Attestationen, VEX-Dokumente und Vulnerability Reports, müssen gemeinsam mit den zugehörigen Artefakten bzw. OCI-Artefakten verwaltet oder über OCI-Referrer eindeutig referenziert werden können.

Im Nutzungskontext der HCC-Cloud muss der AN getrennte Stage-Repositories für die Referenzumgebung (RU), Testumgebungen (TU und RU-DEV) und Produktionsumgebung (PU) bereitstellen. Diese müssen technisch und berechtigungsseitig voneinander getrennt sein.

Die Stage-Repositories der HCC-Cloud müssen so konfiguriert sein, dass ausschließlich die für die jeweilige Stage freigegebenen deploybaren Artefakte einschließlich der zugehörigen Signaturen, Attestierungen, Referenzwerte und sonstigen deploymentrelevanten Nachweise abgelegt werden können.

Die Stage-Repositories der HCC-Cloud müssen so konfiguriert sein, dass Testreports, Testdaten, Build-Zwischenstände, Quellcode und allgemeine Qualitätsartefakte dort nicht abgelegt werden können, sofern sie nicht unmittelbar deploymentrelevant sind.

Die CI/CD-Plattform muss sicherstellen, dass ein Artefakt nur dann aus dem Nutzungskontext der CI/CD-Plattform in ein Stage-Repository der HCC-Cloud überführt werden kann, wenn die hierfür definierten Freigabe-, Signatur-, Attestierungs- und Quality-Gate-Anforderungen erfüllt sind.

Die hierfür erforderlichen Pipeline-Definitionen und Stage-Übergangslogiken können durch den AG oder durch von ihm berechnigte Dritte bereitgestellt werden. Der AN muss sicherstellen, dass die CI/CD-Plattform diese Pipeline-Definitionen und Stage-Übergangslogiken ausführen, berechnigen, protokollieren und überwachen kann.

Die Überführung freigegebener Artefakte in Stage-Repositories der HCC-Cloud muss durch die CI/CD-Plattform technisch unterstützt, nachvollziehbar dokumentiert, auditierbar protokolliert und reproduzierbar ausführbar sein. Direkte Schreibzugriffe auf Stage-Repositories der HCC-Cloud außerhalb definierter Promotion- und Freigabeprozesse müssen technisch ausgeschlossen sein.

3.1.4.8 Supply-Chain-Security / Nachweise

Die CI/CD-Plattform muss unter Berücksichtigung der OWASP Top 10 CI/CD Security Risks in ihrer jeweils aktuellen Fassung umgesetzt und betrieben werden. Risiken der Software-Lieferkette, der Pipeline-Ausführung, der Identitäts- und Zugriffsverwaltung, der Build- und Deployment-Prozesse sowie der Integrität von Artefakten müssen durch geeignete technische und organisatorische Maßnahmen adressiert werden.

Hierzu muss die CI/CD-Plattform insbesondere die folgenden Funktionen und Nachweise unterstützen:

- SBOM,
- Signaturen,
- Weitere generische Attestierungen (in-toto basierend),
- VEX als Nachweisformat für Schwachstellenbewertungen.

Darüber hinaus muss die CI/CD-Plattform:

- Sicherheits- und Nachweisartefakte pipelinebezogen erzeugen, entgegennehmen, speichern, prüfen und revisionssicher zuordnen können,
- signierte Build-Attestations entgegennehmen, prüfen und verwalten können,
- für durch die CI/CD-Plattform selbst erzeugte Artefakte eine signierte Build-Attestation bereitstellen können, die mit den Anforderungen von SLSA Level 3 kompatibel ist und Informationen zum Quellcode, zur Build-Pipeline, zu Build-Werkzeugen, Build-Abhängigkeiten und zur Build-Umgebung enthält,
- es ermöglichen, Sicherheits- und Nachweisartefakte gemeinsam mit den zugehörigen Artefakten bzw. OCI-Artefakten zu verwalten oder eindeutig zu referenzieren,
- Freigabeprozesse so ausgestalten können, dass sicherheitsrelevante Prüfungen zwingende Voraussetzung für nachgelagerte Schritte sind.

3.1.4.9 Freigaben, Promotion und Deployment-Governance

Die CI/CD-Plattform muss geschützte Zielumgebungen oder ein gleichwertiges Konzept zur Absicherung von Deployments unterstützen. Sie muss:

- Deployment-Rechte getrennt von Entwicklungsrechten verwalten,
- mehrstufige Freigabe- und Genehmigungsregeln abbildbar machen, insbesondere:
 - Vier-Augen-Prinzip,
 - approver-basierte Freigaben,
 - getrennte Rollen für Ausführung und Genehmigung,
- Deployments an definierte Bedingungen knüpfen können, insbesondere:
 - Teststatus,
 - Sicherheitsstatus,
 - Signatur-/Attestierungsstatus,
 - manuelle Freigaben,
- sämtliche Freigaben und Deployments auditierbar protokollieren.

Die konkrete fachliche Ausgestaltung der Freigabe-, Promotion- und Stage-Übergangslogiken kann durch den AG oder durch vom AG berechnigte Dritte vorgegeben und als Pipeline-Definition bereitgestellt werden. Der AN muss die technische Ausführung, Berechnigung, Protokollierung und Nachvollziehbarkeit dieser Prozesse über die CI/CD-Plattform ermöglichen.

Die CI/CD-Plattform muss technisch ermöglichen, dass Artefakte erst nach erfolgreicher Prüfung der definierten Freigabekriterien in das jeweils zugehörige Stage-Repository der HCC-Cloud überführt werden. Dies umfasst mindestens die Überführung in die Stage-Repositories RU, TU und PU. Die Überführung in ein Stage-Repository stellt noch nicht zwingend die Ausführung des Artefakts dar; die Ausführung erfolgt ausschließlich innerhalb der HCC-Cloud nach den dort geltenden Deployment- und Runtime-Prozessen.

Jede Überführung muss auditierbar protokolliert und eindeutig auf Source-Stand bzw. Eingangsartefakt, Pipeline-Lauf, Artefakt-Version, Signatur, Attestierung, Freigabeentscheidung, Ziel-Stage und Ziel-Stage-Repository rückführbar sein.

3.1.4.10 Runner-Ausführungsumgebungen

Die CI/CD-Plattform muss den Betrieb von Runnern in containerisierten und – für Spezialanforderungen – in dedizierten Ausführungsumgebungen technisch ermöglichen. Folgende Ausführungstypen müssen bereitgestellt werden:

- Ausführung in Containern (zwingend),
- Ausführung auf Kubernetes (zwingend),

Dedizierte oder statische Ausführungsknoten für technisch begründete Sonderfälle sollen bereitgestellt werden.

Die CI/CD-Plattform muss es dem AG ermöglichen, Runner-Pools organisatorisch und technisch nach Nutzergruppen zu trennen – mindestens nach:

- Fachdienstherstellern (z. B. TI-Flow Los 1),
- Test- und Freigabeeinheiten des AG,
- Plattform- und Betriebspartnern.

Der AG nimmt diese Konfiguration eigenständig vor; der AN muss lediglich sicherstellen, dass die CI/CD-Plattform die erforderlichen Konfigurationsmöglichkeiten bereitstellt.

Die CI/CD-Plattform muss dem AG ferner ermöglichen, jeden Runner-Pool einem konkreten Namespace oder Projekt zuzuordnen, sodass Ausführungsisolation und Zurechenbarkeit der Pipeline-Läufe jederzeit gewährleistet sind. Eine plattformseitige gemeinsame Nutzung von Runnern über Namespace-Grenzen hinweg ohne explizite Konfiguration durch den AG muss technisch ausgeschlossen sein.

Die Ausführungsumgebungen müssen Container-Workloads auf Kubernetes sowie Java-basierte Build- und Testprozesse einschließlich Laufzeitumgebung (JDK), Build-Werkzeug (Maven) und des Nachladens von Dependencies aus den dafür vorgesehenen Repositories unterstützen.

3.1.4.11 APIs, Integration und Automatisierung

Die CI/CD-Plattform muss dokumentierte APIs mindestens für folgende Bereiche bereitstellen:

- Repositories,
- Pipelines,
- Benutzer- und Gruppenverwaltung,
- Übergabe und Abfrage von Artefakten und OCI-Artefakten,
- Übergabe und Abfrage von Signaturen, Attestierungen, SBOMs und weiteren Nachweisartefakten,
- Start, Steuerung und Auswertung von bereitgestellten Testsuiteausführungen,
- Freigabe-, Signatur-, Promotion- und Stage-Übergangsprozesse,
- Überführung freigegebener Artefakte in Stage-Repositories der HCC-Cloud,
- Abfrage von Prüf-, Freigabe-, Promotion- und Deploymentstatus,
- Provisionierung und Abbau der bereitgestellten Umgebungen.

Die Auslösung der Bereitstellung und des Abbaus temporärer Umgebungen gemäß Kapitel 3.1.2.1.1 erfolgt über die API zur Provisionierung und zum Abbau der bereitgestellten Umgebungen.

Die Berechtigung zur Auslösung ist über das Rollen- und Berechtigungsmodell gemäß Kapitel 3.1.4.2 zu steuern

Die CI/CD-Plattform muss Integrationen mit externen Systemen ermöglichen, insbesondere mit:

- Testfallquellen,
- Ticket-/Change-Systemen,
- Sicherheitswerkzeugen,
- Container-/Artefakt-Ökosystemen,
- externen Signatur-/Attestierungsdiensten.

Webhook- oder Event-basierte Integrationsmechanismen müssen vorgesehen werden, um automatisierte Workflows und Kopplungen mit Drittsystemen zu unterstützen.

3.1.4.12 *Audit, Nachvollziehbarkeit und Compliance*

Alle wesentlichen Aktionen müssen vollständig und nachvollziehbar protokolliert werden, darunter:

- Build- und Testausführungen,
- Artefakt-Erzeugung,
- Freigaben,
- Deployment-Aktionen,
- Benutzer- und Rechteänderungen,
- Überführungen von Artefakten aus der CI/CD-Plattform-Registry in Stage-Repositories der HCC-Cloud,
- Änderungen an Stage-Repositories der HCC-Cloud.

Die CI/CD-Plattform muss eine revisionssichere Zuordnung ermöglichen von:

- Source-Stand,
- Pipeline-Lauf,
- erzeugten Artefakten,
- Sicherheits-/Nachweisartefakten,
- Deployment-Ziel,
- Quell-Registry und Ziel-Stage-Repository der HCC-Cloud,
- Freigabeentscheidung und Freigabezeitpunkt.

Audit-Daten müssen über geeignete Such-, Filter- und Auswertungsfunktionen durchsuchbar sein und exportiert werden können, um Prüfungen, Compliance-Nachweise und die Nachvollziehbarkeit von Änderungen und Deployments zu unterstützen. Die CI/CD-Plattform muss hierfür eine benutzerfreundliche grafische Benutzeroberfläche sowie eine Volltextsuche bereitstellen. Die Suche muss mindestens nach Zeitraum, Benutzer, Projekt bzw. Namespace, Pipeline-Lauf, Artefakt, Deployment-Ziel, Ereignistyp und Ergebnisstatus filterbar sein.

3.1.4.13 Technische Betriebsbefähigung der CI/CD-Plattform

Der AN muss die CI/CD-Plattform im Rahmen dieses Arbeitspakets so entwickeln, konfigurieren, integrieren und bereitstellen, dass der spätere Regelbetrieb gemäß Kapitel 3.2.7 technisch ermöglicht wird.

Dieses Kapitel beschreibt ausschließlich die technischen Voraussetzungen, die im Rahmen der Projektphase für die Entwicklung und Bereitstellung der CI/CD-Plattform umzusetzen sind. Die Anforderungen an den Betrieb der CI/CD-Plattform, das Betriebsmodell, die Betriebsprozesse, die Verantwortlichkeiten, die Service Levels sowie die Support- und Eskalationsprozesse ergeben sich aus Kapitel 3.2.7. Die Anforderungen an das Betriebskonzept CI/CD ergeben sich aus Kapitel 3.1.2.5.

Die CI/CD-Plattform muss insbesondere die technischen Voraussetzungen bereitstellen für:

- Monitoring, Metriken, Protokollierung, Tracing, Alarmierung und technische Fehleranalyse der Plattformkomponenten, Nutzung der Runner-Ausführungsumgebungen, Repositories, Artefakt-Ablagen, Registry-Komponenten und der Schnittstellen zur HCC-Cloud,
- die nachvollziehbare und revisionssichere Protokollierung wesentlicher Aktionen, insbesondere Änderungen an Pipeline-Definitionen, Pipeline-Templates, Berechtigungen, Freigaben, Artefakten, Runner-Konfigurationen, Registry-Konfigurationen und Schnittstellenkonfigurationen,
- die eindeutige Zuordnung von Pipeline-Läufen, Artefakten, Test- und Nachweisartefakten, Freigabeentscheidungen, Signaturen, Attestierungen, Quellständen, Zielumgebungen und Stage-Repositories,
- die technische Sicherung und Wiederherstellung von betriebsrelevanten Plattformkomponenten, Konfigurationen, Repositories, Pipeline-Definitionen, Pipeline-Templates, Artefakten, OCI-Artefakten, Sicherheits- und Nachweisartefakten sowie Audit- und Protokolldaten,
- die technische Wiederanlauffähigkeit der CI/CD-Plattform nach Störungen, Abbrüchen, Ausfällen oder fehlgeschlagenen Pipeline-Ausführungen,
- die technische Skalierbarkeit der Runner- und Ausführungsumgebungen einschließlich der Unterstützung paralleler Pipeline-Ausführungen und organisatorisch getrennter Verantwortungsbereiche,
- die technische Umsetzung von Rollen-, Rechte- und Berechtigungsmodellen für Administration, Nutzung, Freigaben, Pipeline-Ausführung, Artefakt-Zugriffe und Auditierung,
- die technische Trennung unterschiedlicher Verantwortungsbereiche, Projekte, Namespaces, Runner-Pools, Artefakt-Ablagen und Zugriffskontexte innerhalb der CI/CD-Plattform,
- die Integration in Betriebs-, Support-, Monitoring-, Logging-, Audit- und Eskalationsprozesse des AN und des AG über geeignete Schnittstellen, APIs, Exportmechanismen oder gleichwertige Verfahren,
- die Bereitstellung von Betriebs-, Audit- und Nachweisinformationen, die eine Fehleranalyse, Betriebsüberwachung, Nachweisführung, Übergabe an den Regelbetrieb sowie spätere Übergabe- und Exit-Szenarien unterstützen.

Die CI/CD-Plattform muss so ausgestaltet sein, dass Störungen im Zusammenspiel zwischen Plattformfunktionen, Pipeline-Ausführung, Repositories, Artefakt-Ablagen, Registry-Komponenten, Runner-Ausführungsumgebungen und Schnittstellen zur HCC-Cloud technisch nachvollzogen und eingegrenzt werden können.

Die hierfür erforderlichen Monitoring-, Telemetrie-, Logging-, Tracing- und Betriebsdaten müssen über dokumentierte Schnittstellen exportierbar sein.

Die bereitgestellten Monitoring-, Telemetrie-, Logging-, Tracing- und Betriebsdaten sowie die zugehörigen Messpunkte müssen eine nachvollziehbare Ursachenanalyse und Verantwortungsabgrenzung zwischen CI/CD-Plattform, HCC-Cloud und den betriebenen Fachanwendungen ermöglichen.

3.1.4.14 *Datensicherung und Wiederherstellung*

Der AN muss für die CI/CD-Plattform Verfahren zur Sicherung und Wiederherstellung von Quellcode-Repositories, Pipeline-Konfigurationen, Artefakten, OCI-Artefakten, Sicherheits- und Nachweisartefakten sowie Audit-Daten bereitstellen. Die Verfahren müssen im Betriebskonzept CI/CD bzw. Betriebshandbuch CI/CD dokumentiert sein. Die Wiederherstellbarkeit muss regelmäßig überprüft und gegenüber dem AG nachgewiesen werden.

3.1.4.15 *Prototyp CI/CD-Plattform*

Ziel des Prototyps ist ein erster durchgängiger technischer Ablauf von der Bereitstellung eines Artefakts über dessen Deployment in eine nichtproduktive Umgebung der HCC-Cloud bis zur automatisierten Ausführung und Auswertung einer Testsuite. Der Prototyp CI/CD-Plattform wird vom AG und Los1 genutzt, um Testruns zu implementieren und durchzuführen und Deployment-Pipelines einzurichten. Der Prototyp CI/CD-Plattform mit seinen Repositories wird im Laufe der Projektphase mit Funktionen angereichert, bis der volle Funktionsumfang der CI/CD-Plattform erreicht ist.

Staging für die CI/CD-Plattform:

- AN entwickelt Funktionen für die CI/CD-Plattform in einer eigenen Umgebung.
- AN stellt der gematik neue Funktionen auf einer CI/CD-Freigabeumgebung bereit.
- AG testet neue Funktionen auf der CI/CD-Freigabeumgebung.
- AG übernimmt neue Funktionen in die CI/CD-Plattform.

Geforderte Funktionalitäten des Prototyps sind:

- ein initiales Organisations-, Rollen- und Berechtigungsmodell gemäß Kapitel 3.1.4.1 und 3.1.4.2, das dem AG die eigenständige Berechtigung weiterer Fachdiensthersteller und Nutzer ermöglicht,
- eine Git-basierte Repository-Funktion gemäß Kapitel 3.1.4.3 zur Ablage und Versionierung von Pipeline-Definitionen, Testsuiten, Testfällen, Testkonfigurationen und weiteren erforderlichen Automatisierungsartefakten,
- eine Pipeline-Laufzeitumgebung gemäß Kapitel 3.1.4.4, in der der AG und berechtigte Nutzer eigene Pipeline-Definitionen anlegen beziehungsweise importieren, konfigurieren, ausführen und auswerten können,
- die für die Ausführung der Pipelines erforderlichen Runner-Ausführungsumgebungen gemäß Kapitel 3.1.4.10,
- eine Artefakt- und OCI-Registry gemäß Kapitel 3.1.4.7 zur Annahme und versionierten Ablage der durch Fachdiensthersteller bereitgestellten Artefakte sowie zur Ablage der bei der Pipeline-Ausführung erzeugten Ergebnisse und Testartefakte,
- die für den Prototyp erforderlichen dokumentierten Schnittstellen gemäß Kapitel 3.1.4.11 zur Übergabe und zum Deployment eines Artefakts in eine nichtproduktive Umgebung der HCC-Cloud (ggf. ohne HCC-Funktionalität),
- die Funktionen gemäß Kapitel 3.1.4.6 zur Ausführung einer durch den AG oder durch berechtigte Dritte bereitgestellten automatisierten Testsuite gegen das deployte Artefakt

Der AN muss einen beispielhaften Pipeline-Ablauf bereitstellen, anhand dessen mindestens folgender technischer Durchstich nachgewiesen werden kann:

- Bereitstellung oder Abruf eines versionierten Artefakts aus der Artefakt- oder OCI-Registry,
- Deployment des Artefakts in eine nichtproduktive Umgebung der HCC-Cloud (ggf. ohne HCC-Funktionalität),
- Prüfung der Erreichbarkeit des deployten Artefakts.

Der beispielhafte Pipeline-Ablauf dient als technischer Nachweis der Funktionsfähigkeit des Prototyps. Die Erstellung und fachliche Ausgestaltung weiterer Pipeline-Definitionen und Testsuiten erfolgt durch den AG oder durch von ihm berechtigte Dritte.

Der technische Durchstich muss wiederholbar ausführbar sein. Die verwendete Pipeline-Version, das eingesetzte Artefakt, die Artefaktversion und die Zielumgebung müssen einander eindeutig zugeordnet werden können. Fehlgeschlagene Pipeline-Schritte müssen erkennbar und anhand der bereitgestellten Protokolle analysierbar sein.

Für den Prototyp sind noch nicht erforderlich:

- Verarbeitung von HCC-Laufzeit-, Versions- und Attestierungsinformationen gemäß Kapitel 3.1.4.5,
- vollständige Umsetzung der Supply-Chain-Security-Anforderungen gemäß Kapitel 3.1.4.8,

- vollständige Umsetzung mehrstufiger Freigabe-, Genehmigungs-, Promotion- und Deployment-Governance-Prozesse gemäß Kapitel 3.1.4.9,
- Überführung von Artefakten in produktive Stage-Repositories oder Deployment in die Produktivumgebung,
- vollständige Umsetzung der HCC-spezifischen Attestierungs- und Vertrauensprozesse,
- Nachweis der vollständigen Betriebsreife der CI/CD-Plattform.

Der Prototyp gilt als erfolgreich bereitgestellt, wenn:

- der AG und die durch ihn berechtigten Nutzer auf die für den Prototyp erforderlichen Funktionen zugreifen können,
- eigene Pipeline-Definitionen angelegt beziehungsweise importiert und ausgeführt werden können,
- der beschriebene technische Durchstich in einer nichtproduktiven Umgebung der HCC-Cloud erfolgreich und wiederholbar ausgeführt wurde,
- eine bereitgestellte Testsuite automatisiert ausgeführt und ausgewertet wurde und
- der AG Zugriff auf die Pipeline-Definitionen, Pipeline-Läufe, Artefakte, Logs, Testergebnisse und Testartefakte besitzt.

Der AN muss die im Rahmen des Prototyps gewonnenen Erkenntnisse, bekannten Einschränkungen und offenen Punkte dokumentieren und bei der weiteren Umsetzung der CI/CD-Plattform sowie bei der Fortschreibung des Umsetzungskonzepts CI/CD berücksichtigen.

3.1.4.16 *Betriebshandbuch CI/CD-Plattform*

Der AN muss ein Betriebshandbuch für die CI/CD-Plattform erstellen, dem AG zur Freigabe vorlegen und während der Vertragslaufzeit aktuell halten.

Das Betriebshandbuch CI/CD muss die konkreten Arbeitsanweisungen, Betriebsverfahren und Runbooks beschreiben, die für den sicheren, stabilen und nachvollziehbaren Betrieb sowie für die Administration und Nutzung der CI/CD-Plattform erforderlich sind.

Das Betriebshandbuch CI/CD muss insbesondere beschreiben:

- die betrieblich relevanten Komponenten, Abhängigkeiten und Schnittstellen der CI/CD-Plattform,
- die operativen Aufgaben, Zuständigkeiten und Verantwortungsgrenzen des AN, des AG sowie der durch den AG berechtigten Dritten,
- den technischen Betrieb und die Administration der Repositories, Pipeline-Orchestrierung, Runner-Ausführungsumgebungen, Artefakt-Ablagen, Registry-Komponenten und Schnittstellen zur HCC-Cloud,
- die durch den AG eigenständig ausführbaren administrativen Tätigkeiten, insbesondere die Verwaltung von Organisationseinheiten, Projekten, Namespaces,

- Repositories, Artefakt-Bereichen, Benutzern, Gruppen, Rollen, Berechtigungen und Runner-Zuordnungen,
- die Verfahren zur Überwachung der Plattformkomponenten und Schnittstellen einschließlich Metriken, Logs, Traces, Zustandsprüfungen und Alarmierungen,
 - die Verfahren zur Analyse und Bearbeitung von Störungen,
 - die Verfahren für Datensicherung, Wiederherstellung, Wiederanlauf und Recovery,
 - die Verfahren für Wartungen, Updates, Patches, Hotfixes und Versionswechsel einschließlich Prüfung, Freigabe, Einführung, Rollback und Nachweisführung,
 - die operative Ausgestaltung des Staging-Verfahrens für Änderungen an der CI/CD-Plattform einschließlich der Entwicklungs- und Testumgebung des AN, der CI/CD-Freigabeumgebung und der produktiv genutzten CI/CD-Plattform,
 - die bei Plattformänderungen anzuwendenden Prüf- und Freigabekriterien, die bereitzustellenden Release Notes und Testnachweise sowie das Vorgehen bei fehlgeschlagenen Prüfungen oder Einführungen,
 - die Verfahren zur Bereitstellung und zum Export von Betriebs-, Audit- und Nachweisinformationen für den AG,
 - die betrieblichen Ansprechpartner, Supportwege, Kommunikationswege und Eskalationsverfahren.

Für wiederkehrende, sicherheitskritische oder zeitkritische Tätigkeiten muss das Betriebshandbuch CI/CD konkrete Runbooks enthalten. Die Runbooks müssen mindestens den Auslöser und Zweck, die Voraussetzungen, die erforderlichen Berechtigungen und beteiligten Rollen, die Arbeitsschritte, die Prüfschritte, die erwarteten Ergebnisse, die Abbruch- und Eskalationskriterien sowie mögliche Rollback-Maßnahmen beschreiben.

Das Betriebshandbuch CI/CD muss eindeutig zwischen dem technischen Plattformbetrieb durch den AN und der fachlichen Administration und Nutzung durch den AG oder berechnigte Dritte unterscheiden. Die fachliche Erstellung und Pflege von Pipeline-Definitionen, Pipeline-Templates, Testsuiten, Testfällen, Stage-Übergangslogiken und fachlichen Freigabekriterien verbleibt beim AG oder bei den durch ihn berechtigten Dritten.

Das Betriebshandbuch CI/CD muss mit dem Umsetzungskonzept CI/CD sowie dem Sicherheits- und Notfallkonzept, den ITSM-, SLA- und Governance-Festlegungen sowie der Übergabestrategie der HCC-Cloud konsistent sein.

Änderungen an Komponenten, Schnittstellen, Administrationsmöglichkeiten oder Betriebsverfahren müssen im Betriebshandbuch CI/CD spätestens mit ihrer Überführung in die produktiv genutzte CI/CD-Plattform nachgeführt werden.

3.1.4.17 Dokumentation CI/CD-Plattform

Der AN muss eine vollständige technische, administrative und nutzungsbezogene Dokumentation der CI/CD-Plattform erstellen, dem AG bereitstellen und während der Vertragslaufzeit aktuell halten.

Die Dokumentation muss den AG und die durch ihn berechtigten Dritten in die Lage versetzen, die bereitgestellten Funktionen der CI/CD-Plattform innerhalb ihres jeweiligen Verantwortungsbereichs eigenständig zu administrieren und zu nutzen.

Die Dokumentation muss insbesondere beschreiben:

- die bereitgestellten Plattformfunktionen, Komponenten, Umgebungen und Schnittstellen,
- die Organisations-, Projekt-, Namespace-, Rollen- und Berechtigungsstrukturen,
- die Erstellung, Verwaltung, Versionierung, Konfiguration und Ausführung von Pipeline-Definitionen, Pipeline-Templates, Testsuiten und Testartefakten,
- die Konfiguration, Zuordnung und Nutzung von Runner-Pools und Runner-Ausführungsumgebungen,
- die Nutzung und Administration der Artefakt-Ablagen sowie der Artefakt- und OCI-Registry,
- die Ablage, Referenzierung und Verwendung von Pipeline-Variablen, Secrets, Schlüsseln und Zertifikaten,
- die Nutzung der APIs, Webhooks und sonstigen Schnittstellen einschließlich der Schnittstellen zur HCC-Cloud,
- die Recherche und Auswertung von Pipeline-Läufen, Protokollen, Testergebnissen, Artefakten, Freigaben, Deployments und Audit-Daten,
- bekannte technische Grenzen, Einschränkungen und Abhängigkeiten der bereitgestellten Plattformfunktionen.

Die Dokumentation muss geeignete Beispiele für die Nutzung und Administration der wesentlichen Plattformfunktionen enthalten.

Die fachliche Erstellung und Pflege konkreter Pipeline-Definitionen, Pipeline-Templates, Testsuiten, Testfälle, Stage-Übergangslogiken und fachlicher Freigabekriterien verbleibt beim AG oder bei den durch ihn berechtigten Dritten. Die Dokumentation des AN muss deren eigenständige Erstellung, Konfiguration, Ausführung und Auswertung ermöglichen.

Die Dokumentation kann in mehrere zielgruppenspezifischen Dokumente, insbesondere eine Administrations-, Nutzungs-, Schnittstellen- und technische Produktdokumentation, gegliedert werden.

Die für eine Änderung relevanten Teile der Dokumentation müssen spätestens mit der Bereitstellung des jeweiligen Änderungsstands auf der CI/CD-Freigabeumgebung aktualisiert und dem AG zur Verfügung gestellt werden. Die Dokumentation muss den auf der CI/CD-Freigabeumgebung bereitgestellten Funktions- und Konfigurationsstand vollständig und nachvollziehbar abbilden.

Erkenntnisse oder Anpassungen, die sich aus der Prüfung auf der CI/CD-Freigabeumgebung ergeben, müssen vor der Übernahme des Änderungsstands in die produktiv genutzte CI/CD-Plattform in die Dokumentation eingearbeitet werden. Zum Zeitpunkt der Übernahme muss die Dokumentation dem freigegebenen und produktiv bereitgestellten Stand entsprechen.

3.1.4.18 Schulungen

Der Auftragnehmer muss für proprietäre oder selbstentwickelte Funktionen eine Schulung mit bis zu 10 Teilnehmern durchführen. Die Schulung ist online durchzuführen und aufzuzeichnen.

3.1.5 Arbeitspaket 4: Vorbereitung und Durchführung von Tests der HCC-Cloud

Dieses Kapitel regelt die operative Vorbereitung, Durchführung und Auswertung der Tests des HCC-Stacks. Die konzeptionellen Vorgaben zu Testgegenstand, Teststrategie, Testumgebungen, Nachweisführung und Quality Gates sind im Kapitel 0 festgelegt.

Die nachfolgenden Anforderungen konkretisieren die operative Umsetzung dieser Vorgaben im Rahmen der Testvorbereitung und Testdurchführung durch den AN.

Der AN muss die im Testkonzept vorgesehenen Tests des HCC-Stacks operativ vorbereiten, durchführen und auswerten. Standortausfälle sind als eigenständige Testkategorie zu prüfen. Hierzu muss der AN insbesondere mittels automatisierter Blackbox-Tests nachweisen, dass der Referenz-Container sowie geeignete repräsentative Prüfvarianten in der HCC-Cloud lauffähig sind und die für sie vorgesehenen Dienste der HCC-Cloud ordnungsgemäß nutzen können. Der AN muss hierfür den Referenz-Container als standardisiertes Prüfmittel einsetzen.

Der AN muss ferner sicherstellen, dass prüfrelevante Mechanismen und Schnittstellen frühzeitig in testbarer Form vorliegen und die vorgesehenen Tests entwicklungs- und integrationsbegleitend implementiert, ausgeführt und ausgewertet werden können.

3.1.5.1 Referenz-Container

Im Rahmen dieses Arbeitspaketes muss der AN einen fachlich neutralen Referenz-Container bereitstellen, der als OCI-konformes Referenz-Container-Image die für HCC erforderlichen technischen Mechanismen implementiert und für sämtliche Testphasen und auch in der PU genutzt werden kann. Der Referenz-Container ist nicht als produktive Workload vorgesehen, sondern dient ausschließlich Test- und Nachweiszwecken. Die HCC-Cloud muss jedoch die dem Referenz-Container zugrunde liegenden Verifikations-, Attestierungs- und Deployment-Mechanismen auch in der Produktionsumgebung für produktive Workloads unterstützen. Der AN muss den Referenz-Container entsprechend den Weiterentwicklungen der Funktionalität von HCC weiterentwickeln. Der AN muss den Quellcode des Referenzcontainers als Open Source zur Verfügung stellen.

Dieses Kapitel konkretisiert operativ den im Kapitel 0 als Konzeptbestandteil benannten Einsatz eines fachlich neutralen Referenz-Containers. Die dortigen konzeptionellen Vorgaben und die nachfolgenden operativen Anforderungen sind gemeinsam zu lesen.

Der Referenz-Container muss als primäres Diagnosemittel zur Abgrenzung von Fehlerursachen zwischen HCC-Cloud und Fachdiensten verwendet werden.

Zur Vermeidung von Zuständigkeitskonflikten bei unklarer Fehlerlage muss die Fehlerursachenabgrenzung zwischen HCC-Cloud und Fachdienst nach dem folgenden verbindlichen

Verfahren erfolgen. Angemessene Fristen für Analyse und Reaktion müssen im Testkonzept verbindlich festgelegt werden.

- Kann ein Fehler mit dem Referenz-Container reproduziert werden, ist dies als wesentliches Indiz für eine mögliche Ursache im Bereich der HCC-Cloud oder ihrer HCC-spezifischen Schnittstellen zu bewerten. Der AN muss in diesem Fall eine vertiefte Fehleranalyse durchführen und dem Auftraggeber das Analyseergebnis fristgerecht bereitstellen.
- Kann ein Fehler ausschließlich mit einem Fachdienst, nicht jedoch mit dem Referenz-Container reproduziert werden, ist dies zunächst als Indiz für eine Ursache außerhalb der HCC-Cloud zu bewerten. Eine HCC-seitige Ursache ist hierdurch jedoch nicht automatisch ausgeschlossen; der AG prüft dies gemeinsam mit dem Fachdiensthersteller und dem AN im Rahmen der weiteren Ursachenanalyse.
- Lässt sich die Ursache nicht eindeutig zuordnen, muss der Auftragnehmer prüfen, ob Änderungen der HCC-Cloud ursächlich sind, und das Ergebnis fristgerecht bereitstellen; Auftragnehmer und Auftraggeber müssen auf dieser Grundlage gemeinsam über das weitere Vorgehen abstimmen, der Auftraggeber entscheidet über das weitere Vorgehen.

Die Beweislastverteilung bei der Fehlerursachenabgrenzung ist verbindlich wie folgt festgelegt:

Tabelle 3: Fehlerursachen Abgrenzung

Fehlerbild	Verantwortlichkeit	Nächster Schritt
Fehler reproduzierbar mit Referenz-Container	HCC-Cloud-AN	Vertiefte Analyse durch AN, Ergebnis an AG
Fehler nur mit Fachdienst, nicht mit Referenz-Container	Fachdienst-Hersteller (zunächst)	Gemeinsame Analyse AG + Fachdienst + AN
Unklare Zuordnung	HCC-Cloud-AN (Prüfung auf HCC-Änderungen)	Ergebnis an AG, AG entscheidet über weiteres Vorgehen

Der Referenz-Container dient der transparenten Fehlereingrenzung. Er begründet weder eine Vermutung gegen den Fachdienst noch entlastet er den HCC-Cloud-AN von seiner Prüf- und Nachweispflicht.

Der Referenz-Container muss insbesondere folgende Funktionalität bereitstellen:

- Der Referenz-Container muss standardisierte HTTP(S)-Endpunkte zur Entgegennahme und Verarbeitung von Test-Requests bereitstellen und die hierfür vorgesehenen HCC-Routing-Mechanismen nutzen.
- Der Referenz-Container muss mit den relevanten HCC-Basisdiensten interagieren, insbesondere TDCAS und dem HSM-Cluster. Ferner muss er die Überführung und Bereitstellung über den Trust Domain Build Service sowie die Erreichbarkeit und Kommunikation der Workload im mandantenbezogenen SDN berücksichtigen. Dabei gilt die allgemeine Anforderung zur Nutzung und zum Nachweis der jeweils vorgesehenen TDCAS-Instanz (siehe Kapitel 3.1.3) entsprechend.
- Der Referenz-Container muss ein deterministisches und reproduzierbares Verhalten aufweisen, sodass Tests über verschiedene Umgebungen hinweg konsistente Ergebnisse liefern. Der AN muss die Reproduzierbarkeit des Referenz-Container-Verhaltens durch dokumentierte Testläufe nachweisen, in denen identische Eingaben auf verschiedenen Umgebungen (RU-DEV, RU) zu identischen, nachvollziehbaren Ergebnissen führen. Die Nachweise müssen in der Artefakt-Registry abgelegt werden.
- Der Referenz-Container muss das Auslösen definierter Fehler- und Grenzfalle Szenarien ermöglichen, um das Verhalten der HCC-Cloud unter Störungen gezielt zu prüfen. Der AN muss eine vollständige Dokumentation aller im Referenz-Container implementierten Fault-Injection-Mechanismen zur Erzeugung dieser Fehlerszenarien bereitstellen. Die Fault-Injection-Mechanismen setzen die im Kapitel 0 konzeptionell geforderten Varianten des Referenz-Containers für Edge-Case-, Fehlerfall- und Negativtests operativ um. Die Dokumentation muss je Fehlerszenario den Auslösemechanismus, das erwartete Verhalten und das Nachweisverfahren benennen. Die Dokumentation muss versioniert in der Registry abgelegt werden.
- Der Referenz-Container muss in einem cVM Workload Image betreibbar sein; das Container Image wird hierzu über den Trust Domain Build Prozess in ein cVM Workload Image eingebettet bzw. überführt, für das Referenz Hashes ermittelt werden und das auf dieser Grundlage in der Attestation wiedererkannt wird. Die Überführung des Container-Images in ein cVM-Workload-Image einschließlich Referenz-Hashes und reproduzierbarem Build ist Bestandteil des in [gemSpec_HCC] beschriebenen Trust Domain Build Services; die nachfolgende Abbildung 2 und die CI/CD-bezogenen Anforderungen konkretisieren diesen Prozess.
- Soweit mit dem Referenz-Container prüf- und nachweisrelevante Aussagen zur HCC-Cloud getroffen werden, muss er auf attestierten HCC-Hosts betrieben werden. Sein Zugriff auf Identität und Credentials müssen insoweit von einer erfolgreichen Host-Attestation und Workload-Attestation abhängen. Tests in anderen Umgebungen sind zulässig, haben jedoch keine nachweisbegründende Wirkung.
- Nach erfolgreicher Attestation muss der Referenz-Container Credentials für die Nutzung seiner Identität mit HTTPS vom TDCAS beziehen. Mit Hilfe des Referenz-Containers muss getestet werden, dass der HCC-Dienst die Credentials ausschließlich aus dem TDCAS bezieht (Positiv/Negativ).

- Der Referenz-Container muss kryptographische Operationen unter Nutzung von im HSM-Cluster verwaltetem Schlüsselmaterial ausführen; der Zugriff erfolgt über das mandantenisolierte interne SDN und unter Verwendung der vom TDCAS ausgestellten Credentials. Der Referenz-Container muss in einem definierten Mandantenkontext betrieben werden. Er muss an die für diesen Kontext geltenden TI-Policies gebunden sein. Attestations- und Betriebsprotokolle müssen so erzeugt werden, dass sie für Monitoring- und Auswertungszwecke der gematik bereitgestellt und genutzt werden können.
- Der Referenz-Container muss Datenbank- und Cache-Zugriffe unterstützen und für Last- und Skalierungstests ausgelegt sein.

Der AN muss dem AG vollumfänglich die für die Durchführung der Tests erforderlichen Testartefakte bereitstellen. Der vollständige Source Code des Referenz-Containers, Source Code der Testsuiten, Testfalld Definitionen und Testkonfigurationen muss versioniert in einem für den AN und die beteiligten Fachdiensthersteller zugänglichen Code-Repository bereitgestellt werden. Die daraus erzeugten ausführbaren Testpakete, Testdaten-Pakete sowie Testreports müssen versioniert in einer gemeinsam genutzten Artefakt-Registry für Testreports und Testartefakte vorgehalten werden.

Der Referenz-Container, sämtliche Testsuiten, Testartefakte und Testdaten müssen möglichst providerneutral bereitgestellt werden, sodass der AG das vollständige Testset bei einem Wechsel zu einem anderen Anbieter grundsätzlich weiterverwenden kann. Provider-spezifische Anpassungen müssen auf das notwendige Mindestmaß begrenzt, dokumentiert und austauschbar gehalten sein. Der AG muss jederzeit lesenden Zugriff auf sämtliche Testartefakte, Testläufe, Pipelines, Logs, Metriken und Traces erhalten.

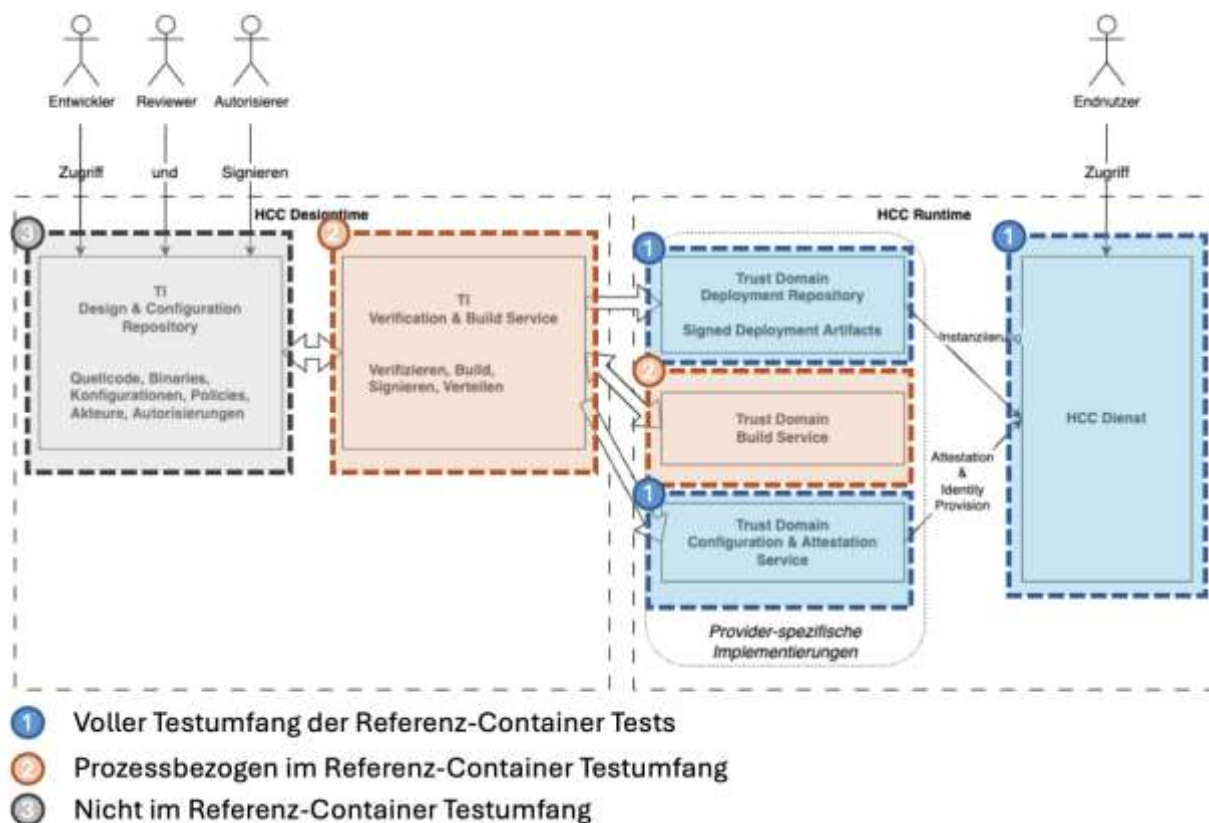


Abbildung 2: Durch Referenz-Container abgedeckter Testumfang

Mit dem Referenz-Container werden die im Testkonzept (Kapitel 3.1.2.3) festgelegten Prüfungsschwerpunkte für die HCC-Funktionalität operativ umgesetzt.

- (1) Voller Testumfang der Referenz-Container Tests: Der Referenz-Container läuft als cVM-Workload auf attestierten Hosts: Host/Workload-Attestation (TDCAS), Identitäts-/Credential-Bezug, HTTPS-Webschnittstelle, HSM-Kryptographische Funktionen, Cache- und Datenbankzugriff, Mandantenisolation, Instanziierung aus Deployment Repository, Fault-Injection, Last-/Resilienz-/Failover Test
- (2) Prozessbezogen im Referenz-Container Testumfang: Getestet wird die Überführung des Container Images ins cVM-Workload-Images, Referenz-Hashes, Signierung und reproduzierbarer Build; technischer Durchstich des Verifikations-/Deploy-Prozesses mit dem Referenz-Container
- (3) Nicht im Referenz-Container Testumfang: TI Design & Configuration Repository: organisatorische Abläufe, Mehraugenprinzip, Akteure (Entwickler, Reviewer, Autorisierer) sind außerhalb des Referenz-Container Testumfangs

Build, Signierung und Test des Referenz-Containers erfolgen vollständig CI/CD-gestützt unter Nutzung der vom AN bereitgestellten Pipeline-Laufzeitumgebung:

- Der AN stellt den vollständigen Source Code des Referenz-Containers einschließlich Konfigurationen und Build-Skripten in einem Git-Repository auf der

HCC-Cloud zur Verfügung und richtet einen vollständig CI/CD-gestützten Build-, Signatur- und Deploy-Prozess ein; Repository und Pipelines sind für die gematik vollständig einsehbar.

- Der AN betreibt einen durchgängigen CI/CD-gestützten Build- und Deploy-Prozess für den Referenz-Container, in dem Änderungen an Source Code oder Basis-Images automatisiert zu einem neuen Container-Artefakt im OCI-Format gebaut, versioniert, validiert und einem Repository zugeführt sowie als OCI-Container für nachgelagerte Umgebungen bereitgestellt werden.
- Der AN muss den Trust Domain Build Service in die CI/CD-Prozesse so einbinden, dass ein Container-Image automatisiert in ein cVM-Workload-Image überführt wird.
- Der AN gestaltet die CI/CD-Pipelines für Tests mit dem Referenz-Container so aus, dass ein vollständiger technischer Durchstich vom OCI-Image über Build-Prozess und Deployment bis hin zum Lauf im Mandantenkontext einschließlich automatisierter Funktionstests abgedeckt wird.
- Der AN führt in den CI/CD-Pipelines automatisierte Tests der HCC-Kernfunktionen durch, insbesondere zum Start des Referenz-Containers als cVM auf attestierten Hosts, zur Ausstellung von Credentials durch TDCAS, zu kryptographischen Operationen mit dem HSM-Cluster und zur Mandantenisolation.
- Der AN führt in den CI/CD-Pipelines Tests der Attestierungsfunktionalität durch. Diese müssen insbesondere abdecken:
 - die Host-Attestation,
 - die Workload-Attestation,
 - das Zusammenwirken von Host- und Workload-Attestation,
 - den Schutz gegen Replay-Angriffe,
 - die Ablehnung nicht zulässiger oder nicht attestierter Workloads,
 - die Nutzung oder die Ausstellung von TLS-Identitäten nach erfolgreicher Attestierung.
- Der AN führt in den CI/CD-Pipelines Tests durch, die versuchen, zur Laufzeit auf eine HCC-Dienst-Workload administrativ zuzugreifen oder Konfigurationen außerhalb der Zero-Trust-Regeln zu ändern. Diese Tests zielen darauf ab, unerwünschtes Verhalten offenzulegen: Der Zugriff bzw. die Änderung muss verweigert werden, und der Versuch muss gemäß den Vorgaben protokolliert und für die Auswertung nachvollziehbar sein. Auswirkungen auf andere Mandanten dürfen dabei nicht entstehen.
- Der AN stellt die kontinuierliche Ausführung von Tests mit dem Referenz-Container in seinen CI/CD-Pipelines sicher und gewährt dem AG Einsicht in diese Pipelines.

Darüber hinaus unterstützt der AN den AG bei der Durchführung von Tests mit dem Referenz-Container, insbesondere durch die Bereitstellung von Fault-Injection-Mechanismen, Monitoring-Informationen und Unterstützung bei der Analyse von Fehlersituationen.

3.1.5.2 Testautomatisierung

CI/CD bildet die Grundlage für kontinuierliches Testen.

Tests sind grundsätzlich automatisiert und in CI/CD-Pipelines auszuführen. Eine nicht automatisierte bzw. nicht pipelinegestützte Durchführung ist nur ausnahmsweise zulässig, wenn dies fachlich oder technisch begründet ist und der AG ausdrücklich zugestimmt hat. Dies kann beispielsweise für Failover-Tests gelten, die aufgrund ihrer Art nicht sinnvoll in einen wiederkehrenden Pipeline-Ablauf integrierbar sind.

Die Testautomatisierung muss insbesondere auf folgende Gegenstände ausgerichtet sein:

- Automatisierte Funktions- und Integrationstests der HCC-Komponenten.
- Automatisierte Negativ-, Fehlerfall-, Last- und Regressionstests, soweit technisch sinnvoll und wirtschaftlich vertretbar.
- Automatisierte Tests der Build-, Signatur-, Deployment- und Rollback-Prozesse.
- Automatisierte Tests unter Nutzung des Referenz-Containers als Referenz-Workload.

Der AN muss sicherstellen, dass automatisierte Testläufe reproduzierbar durchführbar und eindeutig auf den getesteten Softwarestand, die verwendete Infrastrukturdefinition, die Zielumgebung sowie den Mandantenkontext referenzierbar sind.

Soweit Testumgebungen dynamisch bereitgestellt oder betrieben werden, sind auch deren Start, Konfiguration, Rücksetzung und Beendigung – soweit technisch möglich – in die automatisierten Abläufe einzubinden.

Für automatisierte Testsuiten sind im Testkonzept Zielwerte oder Grenzwerte für Laufzeiten, Ausführungsfrequenz und Wiederholbarkeit festzulegen. Der AN muss darstellen, welche Testergebnisse als Quality Gates wirken und unter welchen Voraussetzungen ein automatisierter Lauf oder ein nachgelagerter Deployment-Schritt abubrechen ist.

3.1.5.3 Testnachweise

Prüfnachweise sind, soweit technisch möglich und wirtschaftlich vertretbar, automatisiert zu erbringen.

Automatisiert erbrachte Prüfnachweise müssen in die vom AN bereitgestellten CI/CD-Prozesse integriert werden.

Der AN muss sicherstellen, dass automatisierte Prüfnachweise innerhalb der CI/CD-Prozesse ausgeführt, versioniert, gespeichert und ausgewertet werden.

Der AN muss sicherstellen, dass die Ergebnisse der Prüfnachweise den jeweiligen HCC-Quellcode-, Build-, Container-, cVM-, Infrastruktur-, Trust-Domain- und Release-Ständen eindeutig zugeordnet werden können.

Der AN muss Testsuiten, Testartefakte, Referenz-Container, Testdaten und Prüfnachweise in einer Form bereitstellen, die so weit wie möglich eine providerneutrale Weiterverwendung durch den AG ermöglicht.

Der AN muss dem AG lesenden Zugriff auf die für die Nachvollziehbarkeit relevanten Testartefakte, Testläufe, Pipelines, Logs, Metriken und Traces ermöglichen.

3.1.5.4 Testarchitektur, Nachweisführung und operative Testumsetzung

Der AN muss die im Testkonzept festgelegten Tests der HCC-Cloud operativ vorbereiten, durchführen und auswerten.

Der AN muss hierzu den Referenz-Container sowie geeignete repräsentative Prüfvarianten als standardisierte Prüfmittel einsetzen und mittels automatisierter Blackbox-Tests nachweisen, dass diese in der HCC-Cloud lauffähig sind und die für sie vorgesehenen HCC-Dienste ordnungsgemäß nutzen können.

Der AN muss Standortausfälle, Failover, die erneute Attestierung von Host und Workload nach Wiederanlauf sowie die Wahrung der Datenkonsistenz in geeigneten Testläufen prüfen und auswerten.

3.1.5.5 Testreports und Artefakt-Registry

Die Testreports dokumentieren die für die HCC-Cloud erzielten Testergebnisse, den Stand der Testabdeckung sowie die Einhaltung der festgelegten Quality Gates.

Testreports müssen durch den AN signiert und versioniert in einer Artefakt-Registry abgelegt werden. Die Ablage muss so erfolgen, dass die Testreports den jeweils zugrunde liegenden Testläufen, Prüfnachweisen sowie den zugehörigen Build-, Artefakt-, Commit-, Container-, cVM-Image-, Infrastructure-as-Code-(IaC)-, Konfigurations- und Versionsständen eindeutig zugeordnet werden können.

Der AN muss dem AG lesenden Zugriff auf die in der Artefakt-Registry abgelegten Testreports und die für deren Nachvollziehbarkeit erforderlichen Artefakte ermöglichen

3.1.5.6 Testfallentwicklung

Testfälle müssen aus den prüfrelevanten Anforderungen abgeleitet werden; die maßgeblichen Vorgaben ergeben sich aus dem Kapitel 3.1.2.3.1 im Abschnitt „Nachweisführung, Traceability und providerneutrale Bereitstellung“.

3.1.5.7 Unterstützung bei Testaktivitäten

Der AN dokumentiert die Testausführung in Form von:

- Versionen der getesteten Komponenten
- Liste der eingesetzten Simulatoren / Mocks
- Liste der durchgeführten Testfälle mit Ergebnis der Testausführung
- Liste von bekannten Fehlern und Abweichungen

- lesbaren Logfiles

und unterstützt den AG bei der Analyse der Ergebnisse.

Der AN muss während der gesamten Vertragsdauer Support für alle verwendeten Testartefakte und Tools leisten, indem er Fragen zeitnah beantwortet und gefundene Fehler in diesen Artefakten korrigiert.

3.1.5.8 Testphasen und HCC Testumgebungen

Für die HCC-Cloud müssen die Teststufen Eigenverantwortliche Tests (EvT), produktübergreifende Tests (PÜT) sowie Gesamtintegrationstests im TI-Kontext (GIT-HCC) vorgesehen und so ausgestaltet werden, dass Änderungen am HCC-Stack und seinen Betriebskomponenten vor dem Übergang in die Produktion in einem mehrstufigen Verfahren geprüft und kontrolliert freigegeben werden.

Die inhaltlichen Schwerpunkte der Teststufen ergeben sich aus dem Testkonzept gemäß Kapitel 3.1.2.3.

Der AN muss hierfür logisch getrennte HCC-Testumgebungen für Entwicklungs-, Test- und Referenzzwecke bereitstellen und betreiben. Innerhalb eines Mandanten müssen mindestens eine HCC-Testumgebung mit Entwicklungsfokus (RU-DEV) und eine HCC-Testumgebung mit Referenzfokus (RU) bereitgestellt werden. Die Umgebungen müssen logisch isoliert sein und bei erhöhtem Bedarf horizontal skaliert werden können. Sie müssen so ausgestaltet sein, dass HCC-Komponenten, administrative Dienste, Attestierungsfunktionen und relevante Cloud-Services unter realitätsnahen Bedingungen getestet werden können.

Für den Wechsel zwischen den Teststufen muss der AN Eingangs- und Ausgangskriterien festlegen. Abweichungen von festgelegten Ausgangskriterien müssen im Testkonzept dokumentiert und mit dem AG abgestimmt werden. Ausnahmeregelungen dürfen die betriebliche Stabilität sowie die Sicherheit und Vertraulichkeit der HCC-Cloud nicht in der Weise beeinträchtigen, dass sie über den spezifizierten Testrahmen hinausgehende oder ungeplante Auswirkungen auf nicht explizit dem Test unterliegende Systeme oder Datenbestände verursachen. Im Rahmen definierter und mit dem AG abgestimmter Testszenarien – insbesondere in isolierten HCC-Testumgebungen (RU-DEV) – können kontrollierte Tests zur Prüfung von Sicherheits- und Vertraulichkeitseigenschaften nach Maßgabe des Testkonzepts durchgeführt werden.

Eigenverantwortliche Tests (EvT)

Der AN muss die für die HCC-Cloud vorgesehenen EvT durchführen und die zugehörigen Nachweise bereitstellen. Hierbei muss der Referenz-Container als standardisiertes Prüfmittel eingesetzt werden. Für die Durchführung der EvT muss der AN den Referenz-Container auf temporären, isolierten HCC-Instanzen in RU-DEV betreiben und sicherstellen, dass diese Instanzen die für die jeweiligen Prüfungen erforderlichen Voraussetzungen erfüllen.

Die Ergebnisse der EvT müssen in der im Testkonzept festgelegten Form dokumentiert und dem AG bereitgestellt werden. Dabei muss sichergestellt werden, dass EvT-Ergebnisse, verwendete HCC-Stände, Konfigurationen und Referenz-Container-Versionen eindeutig zueinander zugeordnet und nachvollziehbar gehalten werden.

3.1.5.9 Ermöglichung der Produktübergreifenden Tests / HCC-Cloud-Tests (PüT)

Der AG führt produktübergreifende Tests mit Fachdiensten durch, um Kompatibilitätsprobleme zwischen HCC-Cloud- und Fachdienst-Implementierungen frühzeitig zu erkennen.

Der AN muss den AG hierbei durch folgende Leistungen unterstützen:

- Bereitstellung einer Testinstanz gemäß Kapitel 3.1.5.8
- Bereitstellung der erforderlichen Testartefakte (Referenz-Container, Konfigurationen)
- Unterstützung bei der Fehleranalyse und -eingrenzung
- Bereitstellung von Monitoring-Daten, Logs und Traces während der Tests soweit dies für die Fehleranalyse erforderlich ist

3.1.5.10 Mitwirkung an Gesamtintegrationstests (GIT-HCC)

Der AG kann vor einer Produktionsauslieferung die Durchführung gemeinsamer Gesamtintegrationstests mit realen Fachdiensten (ohne Mocks und Attrappen oder simulierte Gegenstellen) verlangen, sofern dies nach Art, Umfang, Risikoprofil oder potenziellen Auswirkungen der betreffenden Änderung aus Sicht des AG erforderlich ist.

Die Gesamtintegrationstests müssen auf RU durchführbar sein. Der AN muss RU so bereitstellen und betreiben, dass Fachdienste unter produktionsnahen Bedingungen getestet werden können.

Der AG koordiniert die Gesamtintegrationstests. Der AN muss den AG hierbei durch folgende Leistungen unterstützen:

- Bereitstellung einer Testinstanz gemäß Kapitel 3.1.5.8
- Bereitstellung der erforderlichen Testartefakte (Referenz-Container, Konfiguration)
- Technische Unterstützung bei der Fehleranalyse und Fehlereingrenzung sowie bei der Umsetzung erforderlicher Rollback-Maßnahmen
- Bereitstellung von Monitoring-Daten, Logs und Traces während der Tests soweit dies für die Fehleranalyse erforderlich ist

3.1.6 Arbeitspaket 5: Vorbereitung und Durchführung von Tests der CI/CD-Plattform

Der AN muss die Tests der CI/CD-Plattform gemäß den Vorgaben dieser Leistungsbeschreibung durchführen. Prüfnachweise sind, soweit technisch möglich und wirtschaftlich vertretbar, automatisiert zu erbringen.

Automatisiert erbrachte Prüfnachweise müssen in die vom AN bereitgestellten CI/CD-Prozesse integriert werden. Der AN muss sicherstellen, dass diese innerhalb der CI/CD-Prozesse ausgeführt, versioniert, gespeichert und ausgewertet werden.

Der AN muss sicherstellen, dass die Ergebnisse der Prüfnachweise den jeweiligen Quellcode-, Build-, Artefakt-, Konfigurations- und Release-Ständen eindeutig zugeordnet werden können.

Der AN muss die für die Nachvollziehbarkeit der Testdurchführung erforderlichen Testartefakte, Testläufe, Protokolle, Logs, Metriken, Traces und Prüfnachweise in geeigneter Form bereitstellen und versioniert ablegen.

Der AN muss dem AG lesenden Zugriff auf die für die Nachvollziehbarkeit der Testdurchführung erforderlichen Testartefakte, Testläufe, Protokolle, Logs, Metriken, Traces und Prüfnachweise ermöglichen.

Soweit für die CI/CD-Plattform Quality Gates vorgegeben sind, muss der AN deren Einhaltung im Rahmen der Testdurchführung nachweisen. Unterschreitungen von Quality Gates sind zu dokumentieren, zu bewerten und im Hinblick auf ihre Auswirkungen auf Meilensteine und Freigaben zu behandeln.

Ab dem Meilenstein MS4.1 müssen bei Änderungen an bereits abgenommenen Komponenten der CI/CD-Plattform automatisierte Regressionstests durchgeführt werden. Die Ergebnisse dieser Regressionstests müssen nachvollziehbar dokumentiert und den jeweils betroffenen Freigabe- und Versionsständen zugeordnet werden.

3.1.7 Arbeitspaket 6: Aufbau Service-Management und Inbetriebnahme

Dieses Arbeitspaket umfasst die Herstellung der operativen Betriebsbereitschaft der HCC-Cloud sowie die Vorbereitung der Aufnahme des Regelbetriebs.

Ziel des Arbeitspakets ist der Nachweis, dass die durch den Auftragnehmer bereitgestellte HCC-Cloud einschließlich der zugehörigen Betriebsorganisation, Betriebswerkzeuge, Monitoring- und Supportleistungen sowie der Schnittstellen zu weiteren Auftragnehmern und zum Auftraggeber für die Leistungserbringung gemäß Kapitel 3.2 geeignet und betriebsbereit ist.

Die im Rahmen dieses Arbeitspakets erstellten Konzepte, Dokumentationen und Nachweise bilden die Grundlage für die Leistungserbringung des Auftragnehmers in der Betriebsphase. Der Auftragnehmer muss sicherstellen, dass diese die Anforderungen des Kapitels 3.2 erfüllen.

3.1.7.1 Aufbau der Betriebsorganisation

Der Auftragnehmer muss vor Aufnahme des Regelbetriebs die für die Leistungserbringung erforderliche Betriebsorganisation bereitstellen und dokumentieren.

Hierzu muss der Auftragnehmer insbesondere:

- die verantwortlichen Betriebsfunktionen benennen,
- Ansprechpartner und Eskalationsinstanzen festlegen,
- die Kommunikationswege zum Auftraggeber definieren,
- die Servicezeiten bereitstellen,
- die Schnittstellen zu weiteren Auftragnehmern und Dienstleistern dokumentieren.

Der Auftragnehmer muss gegenüber dem Auftraggeber nachweisen, dass die Betriebsorganisation die in Kapitel 3.2 beschriebenen Leistungen erbringen kann.

3.1.7.2 Nachweis der betrieblichen Leistungsfähigkeit

Der Auftragnehmer muss dem Auftraggeber im ITSM-Konzept (siehe Kapitel 3.2.3) darlegen, wie die für die HCC-Cloud vorgesehenen Betriebsprozesse die Anforderungen dieser Leistungsbeschreibung erfüllen.

Vorhandene Standardprozesse des Auftragnehmers können verwendet werden, sofern diese die Anforderungen der Kapitel 3.2.3 und 3.2.4 erfüllen.

Eine projektspezifische Neuentwicklung dieser Prozesse wird nicht gefordert.

3.1.7.3 Bereitstellung der Betriebsdokumentation

Der Auftragnehmer muss die für die Betriebsaufnahme erforderliche Dokumentation erstellen und dem Auftraggeber zur Prüfung zur Verfügung stellen.

Dies umfasst insbesondere:

- ITSM-Konzept,
- Governance-Konzept,
- SLA-Konzept

Die Dokumentation muss die Grundlage für die Leistungserbringung gemäß Kapitel 3.2.1 bis 3.2.7 bilden.

3.1.7.4 Aufbau von Monitoring und Alarmierung

Der Auftragnehmer muss die für den Betrieb der HCC-Cloud erforderlichen Monitoring-, Logging- und Alarmierungsfunktionen bereitstellen und in Betrieb nehmen.

Der Auftragnehmer muss insbesondere nachweisen, dass:

- Verfügbarkeiten überwacht werden,
- Kapazitäten überwacht werden,
- Betriebsstörungen erkannt werden,
- Alarmierungen automatisiert ausgelöst werden,
- Betriebsdaten für den Auftraggeber bereitgestellt werden,

Die erfolgreiche Funktionsprüfung der Monitoring- und Alarmierungsmechanismen ist zu dokumentieren.

3.1.7.5 Vorbereitung des Multi-Provider-Betriebs

Die auf der HCC-Cloud betriebenen Fachanwendungen können durch weitere Auftragnehmer bereitgestellt oder betrieben werden. Der Auftragnehmer muss die organisatorischen und technischen Voraussetzungen für einen Multi-Provider-Betrieb schaffen.

Hierzu muss der Auftragnehmer insbesondere festlegen:

- Verantwortungsabgrenzungen,
- Betriebsübergabepunkte,
- Eskalationswege,
- Kommunikationsverfahren,
- Verfahren zur Fehlerursachenanalyse,
- Verfahren zur Bearbeitung gemeinsamer Incidents,
- Verfahren zur Durchführung von Major-Incident-Prozessen,
- Prozesse für die organisationsübergreifende Zusammenarbeit.

Die Festlegungen müssen mit den Anforderungen der Kapitel 3.2.3, 3.2.4 und 3.2.5 übereinstimmen.

3.1.7.6 Nachweis der Datensicherung und Wiederherstellung

Der Auftragnehmer muss die Datensicherungs- und Wiederherstellungsverfahren für die bereitgestellten Leistungen implementieren und deren Wirksamkeit nachweisen.

Der Nachweis muss mindestens enthalten:

- Durchführung eines Wiederherstellungstests,
- Dokumentation der Wiederherstellungsdauer,
- Nachweis der Datenkonsistenz,
- Bewertung der Ergebnisse,
- gegebenenfalls erforderliche Verbesserungsmaßnahmen.

3.1.7.7 Nachweis der Notfall- und Wiederanlauffähigkeit

Der Auftragnehmer muss vor Aufnahme des Regelbetriebs die Wirksamkeit der vorgesehenen Notfall- und Wiederanlaufverfahren nachweisen.

Der Nachweis muss mindestens geeignete Tests für folgende Szenarien umfassen:

- Ausfall kritischer Infrastrukturkomponenten,
- Ausfall kritischer Plattformdienste,
- Ausfall von Datenbankdiensten,
- Ausfall von HSM-Komponenten,
- Failover-Szenarien,
- Standortausfallszenarien.

Die Testergebnisse sind zu dokumentieren und dem Auftraggeber vorzulegen.

3.1.7.8 Betriebsbereitschaftsnachweis

Vor Aufnahme des Regelbetriebs muss der Auftragnehmer einen Betriebsbereitschaftsnachweis erbringen.

Der Betriebsbereitschaftsnachweis muss auf den Ergebnissen der Betriebs- und Schnittstellenprüfung gemäß Kapitel 3.2.8 basieren und bestätigen, dass die organisatorischen, technischen und prozessualen Voraussetzungen für die Leistungserbringung sind.

Der Nachweis muss insbesondere umfassen:

- Verfügbarkeit der Betriebsorganisation,
- Vollständigkeit der Betriebsdokumentation,
- Funktionsfähigkeit von Monitoring und Alarmierung,
- Nachweis der Datensicherung,
- Nachweis der Wiederherstellbarkeit,
- Nachweis der Notfallverfahren,
- Nachweis der Multi-Provider-Zusammenarbeit,
- Nachweis der Bereitschaft zur Erbringung der vereinbarten Service Levels.

Die erfolgreiche Durchführung der Betriebs- und Schnittstellenprüfung sowie die Vorlage des Betriebsbereitschaftsnachweises sind Voraussetzungen für die Aufnahme des Regelbetriebs.

3.1.8 Arbeitspaket 7: Übergabestrategie

3.1.8.1 Übergabestrategie HCC Cloud

Dieses Arbeitspaket umfasst die Erstellung und Fortschreibung einer Übergabestrategie für die geordnete Übergabe der durch den AN bereitgestellten Leistungen an den AG oder einen durch den AG benannten Dritten.

Die Übergabestrategie muss die Umsetzung der Anforderungen aus Kapitel 3.2.5.3 beschreiben.

Die Übergabestrategie muss ein Leistungsverzeichnis beinhalten, in dem der AN sämtliche Leistungen aufführt, die er im Rahmen einer Übergabe dem betrieblichen Nachfolger im Sinne eines Servicekataloges anbietet. Der betriebliche Nachfolger entscheidet darüber, welche Leistungen er davon beim AN abrufen wird.

Der AN muss die Übergabestrategie dem AG vor Aufnahme des Regelbetriebs zur Freigabe vorlegen. Zudem ist die Übergabestrategie während der kompletten Vertragslaufzeit stets aktuell zu halten und bei Änderungen dem AG erneut zur Freigabe vorzulegen.

Der AN muss erläutern, welche Voraussetzungen ein anderer Cloud-Anbieter mitbringen muss, um mit der beauftragten Entwicklungsleistung eine HCC-Cloud aufzubauen.

Der AN muss ferner beschreiben, welche Voraussetzungen geschaffen werden müssen, damit eine gleiche Betriebsumgebung für den TI-Flow-Fachdienst automatisiert mit minimalem manuellem Aufwand bei einem neuen Cloud-Anbieter aufgebaut werden kann und welche Mitwirkungen des AG oder weiterer Auftragnehmer hierfür erforderlich sind.

Die Übergabestrategie muss so ausgestaltet sein, dass die in Kapitel 3.2.5.3 beschriebenen Exit-Leistungen ohne vermeidbare Unterbrechung der produktiven Nutzung durch den AG und die berechtigten Cloud-Nutzer durchgeführt werden können.

Der AN muss beschreiben, wie die Migration von Mandanten, Workloads und Trust Domains auf einen Nachfolgebetreiber oder eine andere Zielumgebung unterstützt wird.

Der AN muss dokumentieren, welche technischen, organisatorischen oder betrieblichen Abhängigkeiten gegenüber proprietären Diensten oder Komponenten des AN bestehen und welche Auswirkungen diese auf einen Betreiberwechsel haben können.

3.1.8.1.1 Datenmigration

Der AN muss beschreiben:

- welche Daten exportiert werden können,
- welche Konfigurationen exportiert werden können,
- welche Betriebsinformationen exportiert werden können,
- welche Exportmöglichkeiten unterstützt werden,
- welche Exportformate bereitgestellt werden.

Dies umfasst insbesondere:

- Infrastruktur, Konfiguration und Policy definierendem Code
- Betriebsdaten,
- Konfigurationen,
- Container- und Deployment-Artefakte,
- Infrastruktur- und Betriebsdokumentationen.

Der AN muss die Nutzung offener oder allgemein verbreiteter Schnittstellen, Formate und Verfahren dokumentieren, soweit diese für die Portabilität von Daten, Workloads und Konfigurationen relevant sind.

Der AN muss beschreiben, wie Trust-Domain-spezifische Konfigurationen, kryptographische Materialien, Schlüsselmanagementinformationen sowie sicherheitsrelevante Konfigurationen im Rahmen eines Betreiberwechsels übergeben oder migriert werden können, soweit regulatorische und sicherheitstechnische Anforderungen dies zulassen.

3.1.8.1.2 Risiken

Der AN muss alle aus seiner Sicht erkennbaren Risiken benennen, die eine vollständige, ordnungsgemäße und störungsfreie Übergabe beeinträchtigen könnten.

Für jedes identifizierte Risiko muss eine Bewertung hinsichtlich Eintrittswahrscheinlichkeit und Auswirkung erfolgen.

Der AN muss geeignete technische, organisatorische und prozessuale Gegenmaßnahmen beschreiben.

3.1.8.1.3 Kosten

Der AN muss die für die Durchführung der Exit- und Übergabeleistungen erforderlichen Aufwände und Kosten transparent darstellen.

Hierfür muss der AN entweder:

- Kosten bzw. Preise für die einzelnen Übergabeaktivitäten bereitstellen oder
- einen verbindlichen All-In-Preis für die vollständige Durchführung sämtlicher Exit- und Übergabeleistungen angeben.

Die Preisangaben müssen sämtliche zur vollständigen Übergabe erforderlichen Leistungen umfassen und die zugrunde gelegten Annahmen transparent ausweisen.

3.1.8.2 Übergabestrategie CI/CD Pipeline

Der AN muss für die CI/CD-Plattform eine Übergabestrategie erstellen, fortschreiben und dem AG zur Freigabe vorlegen.

Die Übergabestrategie muss beschreiben, wie die CI/CD-Plattform einschließlich der zugehörigen Repositories, Runner-Laufzeitumgebungen, Artefakt-Ablagen, Pipeline-Ausführungsumgebungen, Berechtigungsstrukturen, Betriebsdokumentationen und betriebsrelevanten Konfigurationen so an den AG oder einen vom AG benannten Dritten übergeben werden kann, dass ein geordneter, nachvollziehbarer und möglichst unterbrechungsarmer Weiterbetrieb oder eine geregelte Übernahme der Plattform ermöglicht wird.

Die Übergabestrategie muss insbesondere Festlegungen enthalten:

- zum Übergabegenstand und zur Abgrenzung der zu übergebenden Komponenten, Artefakte, Konfigurationen, Dokumentationen und Betriebsinformationen,
- zur technischen und organisatorischen Vorbereitung der Übergabe, einschließlich der Bereitstellung relevanter System-, Konfigurations- und Betriebsdokumentationen,
- zur Übergabe von Repository-Inhalten, Pipeline-Definitionen, Runner-Konfigurationen, Artefakt-Beständen, Protokolldaten und sonstigen für den Betrieb und die Nachvollziehbarkeit erforderlichen Informationen,
- zur Übergabe von Rollen-, Rechte- und Berechtigungsstrukturen sowie zur geregelten Übertragung oder Neuvergabe administrativer Zugänge,
- zur Sicherstellung der Nachvollziehbarkeit von Freigaben, Versionen, Artefakten, Protokollen und betriebsrelevanten Änderungen im Übergabezeitraum,
- zum Vorgehen für die Übernahme des Betriebs durch den AG oder einen vom AG benannten Dritten, einschließlich Einarbeitung, Wissensübergabe und Support während des Übergangs,
- zu Abhängigkeiten gegenüber der HCC-Cloud sowie zu den für eine geordnete Übergabe erforderlichen Schnittstellen und Abstimmungen,
- zum Umgang mit offenen Störungen, bekannten Einschränkungen, technischen Schulden und laufenden Changes zum Zeitpunkt der Übergabe.

Die Übergabestrategie muss ferner beschreiben, wie die Integrität, Vollständigkeit und Nutzbarkeit der zu übergebenden Artefakte und Informationen sichergestellt wird. Hierzu gehören insbesondere Regelungen zur Versionierung, zur Nachvollziehbarkeit des letzten gültigen Betriebsstands sowie zur Bereitstellung der für den weiteren Betrieb notwendigen Dokumentationen und Konfigurationen.

Soweit für die CI/CD-Plattform bereits Festlegungen in Umsetzungs-, Test-, Betriebs- oder Sicherheitskonzepten getroffen werden, muss die Übergabestrategie diese konsistent aufnehmen und für den Übergabefall zusammenführen.

Die Mitwirkung, Prüfung, Abstimmung oder Freigabe durch den AG entbinden den AN nicht von seiner Verantwortung für die inhaltliche Vollständigkeit, fachliche Eignung und konkrete Ausgestaltung der Übergabestrategie.

3.1.9 Arbeitspaket 8: Beratungs- und Unterstützungsleistungen

Dieses Arbeitspaket umfasst zusätzliche Beratungs- und Unterstützungsleistungen des Auftragnehmers (AN) im Kontext der Bereitstellung, des Betriebs, des Rollouts sowie der fachlichen und technischen Weiterentwicklung der HCC-Dienste, der HCC-Cloud und der CI/CD-Plattform, die nicht bereits Bestandteil der Arbeitspakete 1 bis 7 sind.

Die Leistungen dieses Arbeitspakets werden vom Auftraggeber (AG) bedarfsabhängig auf Grundlage der vertraglichen Regelungen (ohne Abrufverpflichtung) abgerufen und gemäß den im Preisblatt angebotenen Stundensätzen oder einem auf dieser Basis vom AN ange-

botenen Festpreis vergütet. Der Abruf der Leistungen aus Arbeitspaket 8 kann sowohl während der Projektphase als auch in der Betriebsphase erfolgen, ist jedoch nachrangig gegenüber vergleichbaren Leistungen, die bereits in den Arbeitspaketen 1 bis 7 enthalten sind. Eine Doppelabrechnung von Leistungen ist ausgeschlossen.

Im Rahmen dieses Arbeitspakets erbringt der AN Beratungs- und Unterstützungsleistungen durch fachlich und technisch qualifizierte Expertinnen und Experten für folgende Aufgaben:

- Unterstützungsleistungen bei der fachlichen und technischen Abstimmung zu Schnittstellen, Integrationsvoraussetzungen, Test- und Inbetriebnahme-Aktivitäten von auf der Cloud betriebenen Diensten sowie die Mitwirkung bei der Analyse und Eingrenzung von Fehlerursachen im Zusammenspiel zwischen HCC-Cloud, CI/CD-Plattform und HCC-Diensten sowie weiteren angebundenen Systemen.
- Vorbereitung, Durchführung und Nachbereitung von Integrations- und Interoperabilitätsveranstaltungen, insbesondere Connectathons, Piloten oder vergleichbare Test und Abstimmungsformate
- Erstellung und Durchführung von Qualitätssicherungsmaßnahmen für Integrationen, z.B. durch die Erarbeitung von Checklisten, Leitfäden, FAQ-Sammlungen, Best Practice Dokumenten sowie Beiträgen für Wissens- und Supportdatenbanken
- Unterstützung anderer Hersteller von Fachdiensten, Komponenten und Services der TI bei Durchstichs-, Integrations- und End-to-End-Tests im Zusammenspiel mit den vom AN entwickelten Komponenten und Diensten
- Unterstützung des Auftraggebers bei Migrations-, Übergabe- und Nachfolgeszenarien, insbesondere bei Tests der Übergabe- bzw. Migrationsstrategie im Hinblick auf einen Betreiberwechsel
- Vorbereitung, Durchführung und Nachbereitung von Informations- und Kommunikationsmaßnahmen des AG im Zusammenhang mit Einführungen, Erweiterungen oder Pilotierungen der vom AN entwickelten Komponenten und Dienste, z. B. gegenüber Marktteilnehmern oder in ausgewählten Modell- bzw. Pilotregionen
- Beratung des AG bei fachlichen und technischen Weiterentwicklungen, z. B. bei Performance-, Stabilitätsverbesserungen und im Zusammenhang mit der Einführung von TI 2.0 und Zero-Trust-Funktionalitäten im Kontext der vom AN entwickelten Komponenten und Diensten

Die im Rahmen dieses Arbeitspakets erbrachten Leistungen dienen der Stabilisierung, Qualitätssicherung und kontinuierlichen Weiterentwicklung der HCC-Cloud und der CI/CD-Plattform und stellen eine ergänzende, optional abrufbare Unterstützung des Auftraggebers dar.

Der AN muss den AG und die vom AG benannten Beteiligten während der Betriebsphase mit Beratungs- und Unterstützungsleistung unterstützen, soweit es für den stabilen und hochverfügbaren Betrieb der HCC-Cloud-Plattform sowie der CI/CD-Plattform erforderlich ist und die Leistung nicht bereits als eigenständige Leistung in anderen Arbeitspaketen beschrieben ist.

3.2 Betriebsphase

Die Betriebsphase umfasst die Bereitstellung, den Betrieb, die Überwachung, die Pflege, die Störungsbearbeitung, die Wiederherstellung, die Wartung, die Weiterentwicklung sowie die Unterstützung der Nutzung der HCC-Cloud als Managed-Cloud-Plattform für den AG und die durch den AG berechtigten Cloud-Nutzer.

Der AN muss die HCC-Cloud als mandantenfähige, hochverfügbare und sicher betriebene Cloud-Plattform bereitstellen. Die Verantwortung des AN erstreckt sich auf die bereitgestellte Cloud-Infrastruktur, die HCC-spezifischen Platforddienste, die Betriebsprozesse sowie die vereinbarten Service Levels.

Die Verantwortung für die fachliche Funktionalität und den fachlichen Betrieb der auf der HCC-Cloud betriebenen Anwendungen verbleibt beim jeweiligen Dienstanbieter.

Die Betriebsphase beginnt mit der Freigabe von MS6.

3.2.1 Anforderungen an den Dienst und Leistungsumfang

Der AN muss die beschriebenen Leistungen für den Betrieb der HCC-Cloud während der gesamten Vertragslaufzeit erbringen.

Der Leistungsumfang umfasst die Bereitstellung der HCC-Cloud als Managed Service sowie die hierfür erforderlichen Betriebs-, Support- und Managementleistungen.

Der AN muss die Leistungserbringung so ausgestalten, dass der AG sowie die berechtigten Cloud-Nutzer die HCC-Cloud entsprechend den Anforderungen dieser Leistungsbeschreibung nutzen können.

Der AN muss die hierfür erforderlichen Betriebsprozesse, Organisationsstrukturen und technischen Verfahren bereitstellen und während der Vertragslaufzeit aufrechterhalten.

Zur Beschreibung der Leistungserbringung und der Betriebsorganisation muss der AN die nachfolgend genannten Themen gegenüber dem AG dokumentieren und während der Vertragslaufzeit aktuell halten.

Die Nachweise können durch eigenständige Konzepte, Betriebsdokumentationen, Runbooks, Servicebeschreibungen, Architekturunterlagen oder sonstige Standarddokumentationen des AN erbracht werden.

Vorhandene Standarddokumentationen des AN können verwendet werden, sofern die geforderten Inhalte hierdurch vollständig abgedeckt werden. Eine projektspezifische Erstellung oder Anpassung von Dokumentationen wird nur insoweit gefordert, wie die erforderlichen Informationen nicht bereits in bestehenden Unterlagen des AN enthalten sind.

3.2.2 Serviceportfolio und Servicekatalog

Der AN muss einen Servicekatalog bereitstellen und während der Vertragslaufzeit aktuell halten.

Der Servicekatalog muss sämtliche für den AG sowie berechnigte Mandanten verfügbaren Cloud-, Plattform- und HCC-Services beschreiben.

Der Servicekatalog muss die verfügbaren Leistungen, Serviceeigenschaften, Service Levels und Nutzungsbedingungen transparent darstellen.

Hierbei können bestehende Servicebeschreibungen, Produktkataloge oder gleichwertige Standarddokumentationen des AN verwendet werden, die ggf. durch ein Erläuterungsdokument ergänzt werden.

3.2.2.1 Allgemeine Anforderungen

Der Servicekatalog muss mindestens folgende Informationen für jede bereitgestellte Leistung enthalten:

- eindeutige Bezeichnung der Services,
- Leistungsbeschreibung,
- Serviceklasse,
- Service Levels,
- Nutzungsbedingungen,
- technische Leistungsmerkmale,
- verfügbare Betriebsmodelle,
- unterstützte Deployment-Modelle,
- Preis und Abrechnungseinheiten und Abrechnungsmodell,
- Bereitstellungszeiten,
- Skalierungsgrenzen oder technische Limits sowie
- gegebenenfalls bestehende Abhängigkeiten zu anderen Services.

Der AN muss sicherstellen, dass die im Servicekatalog beschriebenen Leistungen während der Vertragslaufzeit nachvollziehbar versioniert und Änderungen dokumentiert werden.

Die Services müssen für Entwicklung und Betriebsaufgaben über das Internet nutzbar sein (broad network access nach [NIST SP 800-145]). Die Kommunikation zwischen Workloads und den in derselben Location bzw. Availability Zone genutzten Cloud-Services muss intern bzw. über private Netze erfolgen und darf nicht über das Internet geführt werden.

Der AN muss Metriken und Logs jedes Managed Service für den Export an ein System des Auftraggebers bereitstellen.

Der AN muss sicherheitsrelevante Zugriffe protokollieren, unabhängig davon, ob sie durch den HCC-Provider oder durch den Auftraggeber erfolgen. Die Protokolle müssen für den Auftraggeber exportierbar sein.

Der AN muss für jeden Service eine Mindestverfügbarkeit im Servicekatalog zusagen und deren Messverfahren beschreiben. Insbesondere für die Services Load Balancer, DNS, Object Storage und relationale Datenbank (Multi-AZ), Managed Kubernetes (Control Plane) muss die zugesagte Verfügbarkeit mindestens 99,95 % im Monat betragen.

Für virtuelle Maschinen muss der AN die Verteilung von Instanzen über Availability Zones und über getrennte physische Hosts innerhalb einer Availability Zone ermöglichen.

3.2.2.2 Umfang des Servicekatalogs

Der verpflichtende und optionale Umfang des Servicekatalogs wird in [gemLB_Anhang_SK] vorgegeben.

3.2.2.3 Bereitstellung und Skalierung

Der AN muss beschreiben, wie die im Servicekatalog enthaltenen Leistungen bereitgestellt und bedarfsgerecht erweitert und reduziert werden können.

Der AN muss darstellen:

- verfügbare Skalierungsmechanismen,
- technische Grenzen der Skalierung,
- Voraussetzungen für die Skalierung,
- Bereitstellungszeiten,
- Änderungsverfahren für bereitgestellte Kapazitäten sowie
- Auswirkungen auf die Service Levels.

Der AN muss Skalierungsgrenzen und technische Limits je Service dokumentieren. Die Auslastung gegenüber diesen Limits muss abfragbar sein, Warnungen vor deren Erreichen müssen konfigurierbar sein.

Der AN muss jeden Service vollständig über eine dokumentierte API bestellbar, bereitstellbar und verwaltbar machen.

Der AN muss einen Terraform- oder OpenTofu-Provider zur Verfügung stellen, sodass alle Services über Infrastructure as Code provisionierbar sind.

Der AN muss dem Auftraggeber ermöglichen, Quoten und Budgets je Projekt festzulegen, zu ändern und auf Antrag zu erhöhen. Die Auslastung gegenüber Quoten und Budgets muss abfragbar sein, Warnungen vor deren Erreichen müssen konfigurierbar sein.

Der AN muss zusätzlich ein Webfrontend zur Verfügung stellen, über welches der Auftraggeber sowie berechtigte Mandanten die angebotenen Services bestellen, bereitstellen, überwachen und verwalten können.

Über das Webfrontend müssen mindestens folgende Funktionen bereitgestellt werden:

- • Verwaltung der angebotenen Services
- • Verwalten von Verbrauchsmengen, Quoten und Budgets
- • Verwalten von Skalierungsgrenzen, technischen Limits und deren Auslastung
- • Konfiguration von Benachrichtigungen und Warnschwellen
- • Anzeige von Metriken, Logs und Audit-Protokollen

Der AN muss beschreiben, in welchem Umfang Kapazitäten kurzfristig erhöht oder reduziert werden können.

Der AN muss die für die einzelnen Services unterstützten Skalierungsraten, erforderlichen Vorlaufzeiten sowie etwaige technische oder organisatorische Einschränkungen darstellen.

Der AN muss beschreiben, welche Leistungen automatisiert skaliert werden können und für welche Leistungen eine manuelle Beauftragung oder Freigabe erforderlich ist.

Der AN muss darstellen, welche Kapazitätserweiterungen pro Umgebung (RU-DEV, RU, TU und PU) unterstützt werden.

Der AN muss beschreiben, wie Skalierungsvorgänge überwacht, dokumentiert und dem AG transparent gemacht werden.

Die Bereitstellung zusätzlicher Kapazitäten soll durch standardisierte Verfahren unterstützt werden.

Der AN muss weiterhin beschreiben, wie kurzfristige Laststeigerungen, unerwartete Nutzungsspitzen und dauerhaft erhöhte Kapazitätsbedarfe unterstützt werden.

Der AN muss bestehende technische, betriebliche, vertragliche oder regulatorische Einschränkungen der Skalierbarkeit transparent darstellen. Dies umfasst insbesondere die unterstützten Skalierungsgrenzen, die Voraussetzungen für Kapazitätserweiterungen sowie die hierfür erforderlichen Vorlaufzeiten.

3.2.2.4 Verbrauchsmodell

Der AN muss darstellen:

- welche Leistungen über Commitment-Modelle bereitgestellt werden können,
- welche Leistungen über Pay-as-you-Go-Modelle (PAYG) bezogen werden können,
- welche Verbrauchsgrößen der Abrechnung zugrunde liegen,
- wie zusätzliche Kapazitäten bereitgestellt werden,
- wie nicht mehr benötigte Kapazitäten reduziert werden können sowie
- welche technischen oder organisatorischen Randbedingungen hierbei gelten.

Der AN muss beschreiben, wie das Verhältnis zwischen reservierten und verbrauchsabhängigen Kapazitäten während der Vertragslaufzeit angepasst werden kann.

3.2.2.5 Verfügbarkeit der Leistungen

Die Services müssen die für die TI-Anwendungen, insb. die HCC-Dienste, erforderliche Zielverfügbarkeit von 99,99% im Monat ermöglichen. Hierbei ist zu berücksichtigen, dass TI-Anwendungen Load Balancer, DNS, Cache, Object Storage und relationale Datenbank, Managed Kubernetes und HSMs benötigen. Hierfür stellt der AN entsprechende Mechanismen und Availability Zones zur Verfügung. Der Ausfall einer Availability Zone darf die Funktion der Services und damit der HCC-Dienste in den übrigen Availability Zones nicht beeinträchtigen. Der AN muss beschreiben, wie mit einer geeigneten Konfiguration von Services die Zielverfügbarkeit erreicht wird (siehe auch Konzept K-09).

Der AN muss für jeden Service eine Mindestverfügbarkeit im Servicekatalog zusagen und deren Messverfahren beschreiben.

Der AN muss sicherstellen, dass die im Servicekatalog beschriebenen Leistungen mit den vereinbarten Service Levels bereitgestellt werden.

Für Leistungen, deren Standard-Service-Level zur Erreichung der geforderten Zielverfügbarkeit nicht ausreichen, muss der AN darstellen, durch welche technischen oder organisatorischen Maßnahmen die geforderte Verfügbarkeit erreicht werden kann.

Der AN muss insbesondere beschreiben:

- Redundanzmechanismen,
- Availability-Zone-Konzepte,
- Georedundanz,
- die indikativen Mengen-, Last- und Kapazitätsannahmen aus [gemSpec_Perf] ableiten und einfügen
- Failover-Verfahren sowie
- weitere Maßnahmen zur Erhöhung der Verfügbarkeit.

3.2.2.6 Kapazitäts- und Ressourcenreporting

Der AN muss regelmäßig Informationen zur Nutzung und Entwicklung bereitgestellter Ressourcen und Kapazitäten bereitstellen.

Die Informationen müssen insbesondere umfassen:

- Ressourcenauslastungen,
- Kapazitätsentwicklungen,
- Skalierungsereignisse,
- Verbrauchstrends,
- verfügbare Kapazitätsreserven,
- Forecasts zur Ressourcennutzung sowie
- wesentliche Abweichungen von Planwerten.

Der AN muss beschreiben, in welchen Intervallen diese Informationen bereitgestellt werden.

3.2.2.7 Verbrauchs-, Billing- und Kostentransparenz

Der AN muss beschreiben, wie die bereitgestellten Leistungen verbrauchsabhängig abgerechnet werden.

Der AN muss Verbrauchsmengen je Service und Projekt fortlaufend messen. Die Messwerte müssen mindestens tagesaktuell über API und Portal abrufbar sein. Das monatliche Reporting zur Rechnungsprüfung baut auf dieser Messung auf.

Der AN muss dem AG regelmäßig Informationen zur kommerziellen Steuerung der Leistungen bereitstellen.

Die bereitgestellten Informationen müssen mindestens beinhalten:

- genutzte Leistungen,
- Verbrauchsmengen,
- Kapazitätsauslastung,
- verursachte Kosten,
- Abrechnungszeiträume,
- historische Nutzungsentwicklungen sowie
- Zuordnungen zu Services, Mandanten oder Verbrauchsobjekten.

Der AN muss die Berichtszyklen, Datenformate und Bereitstellungsverfahren beschreiben.

Der AN muss dem AG die Nachvollziehbarkeit der in Anspruch genommenen Leistungen ermöglichen.

Hierfür müssen die bereitgestellten Abrechnungs-, Verbrauchs- und Nutzungsdaten den jeweiligen Mandanten, Services oder Verbrauchsobjekten eindeutig zuordenbar sein.

Der AG muss jederzeit lesenden Zugriff auf die für ihn relevanten Abrechnungs-, Nutzungs- und Verbrauchsdaten erhalten.

Der AN muss die für die Abrechnung relevanten Verbrauchs-, Leistungs- und Kapazitätsdaten in maschinenlesbarer Form bereitstellen.

Die Bereitstellung kann über:

- Self-Service-Portale,
- Dashboards,
- standardisierte Reports,
- Programmierschnittstellen (APIs) oder
- gleichwertige Verfahren

erfolgen.

Der AN muss beschreiben:

- mit welcher Aktualität Nutzungs- und Abrechnungsdaten bereitgestellt werden,
- welche historischen Daten für Auswertungs- und Nachweiszwecke verfügbar sind,
- welche Billing- und Kostendaten exportiert werden können sowie
- welche Schnittstellen hierfür zur Verfügung stehen.

3.2.2.8 Preis- und Abrechnungsmodell

Die Vergütung der Leistungen erfolgt auf Basis des vereinbarten Servicekatalogs.

Der Servicekatalog muss ein transparentes und nachvollziehbares Abrechnungsmodell auf Basis einer Kombination aus Commitment-/Reserved-Kapazitäten und verbrauchsabhängigen Leistungen (Pay-as-you-Go; PAYG) enthalten.

Hierbei können für vereinbarte Laufzeiten Kapazitäten oder Leistungen zu vorab definierten Konditionen reserviert werden. Zusätzlich muss die Möglichkeit bestehen, weitere Kapazitäten und Leistungen verbrauchsabhängig zu beziehen und wieder zu reduzieren.

Der AN muss für jede abrechnungsrelevante Leistung darstellen:

- die zugrunde liegende Abrechnungseinheit,
- die relevanten Verbrauchsgrößen,
- die Preisparameter,
- die Zuordnung zum Commitment- oder PAYG-Modell,
- die Voraussetzungen für die Nutzung reservierter Kapazitäten sowie
- die Bedingungen für die Bereitstellung zusätzlicher Kapazitäten.

Die Preisbestandteile müssen für den AG transparent, nachvollziehbar und prüfbar dargestellt werden.

Der AN muss zusätzlich einen Kosten- und Verbrauchskalkulator in einem offenen und bearbeitbaren Format (z. B. Webapplikation, Microsoft Excel) bereitstellen.

Der Kalkulator soll es dem AG ermöglichen, die Kosten der angebotenen Leistungen auf Basis unterschiedlicher Nutzungs- und Auslastungsszenarien nachvollziehbar zu berechnen.

Der Kalkulator muss insbesondere die Auswirkungen von:

- Commitment- bzw. Reserved-Kapazitäten,
- verbrauchsabhängigen Leistungen (PAYG),
- Kapazitätserweiterungen,
- Laststeigerungen,
- Änderungen von Laufzeiten,
- Skalierungsvorgängen sowie
- Änderungen der Nutzungsmengen

transparent darstellen.

Sämtliche Berechnungslogiken, Annahmen und Preisparameter müssen nachvollziehbar dokumentiert und durch den AG prüfbar sein.

3.2.2.9 Servicekatalogpflege

Der angebotene Servicekatalog unterliegt während der Vertragslaufzeit den vertraglichen Bedingungen und die angebotenen Services müssen aktuell gehalten werden.

Änderungen (Einschließlich Ergänzungen und Streichungen) im Servicekatalogs müssen grundsätzlich mittels einvernehmlicher Vertragsanpassung festgehalten werden.

Alle gegenwärtigen und zukünftigen vom Auftragnehmer angebotenen Services, die vom Auftragnehmer ausdrücklich den Regelungen dieses Vertrages unterworfen werden, können über eine Oberfläche des AN in technisch automatisierter Form in den Anwendungsbereich dieses Vertrages aufgenommen werden. Hierfür ist keine separate Ergänzungs- oder Änderungsvereinbarung erforderlich. Der Auftragnehmer informiert den Auftraggeber rückwirkend binnen eines Monats über die Aufnahme weiterer Services in Textform.

Der AN muss diesbezüglich folgende Punkte beschreiben:

- Änderungsverfahren,
- Versionierungsverfahren,
- Informationsverfahren,
- Vorlaufzeiten für Änderungen sowie
- Auswirkungen auf bestehende Leistungen.

3.2.3 Betrieb und IT-Service Management

Der AN muss ein IT-Service-Management-Konzept (ITSM-Konzept) bereitstellen und während der Vertragslaufzeit aktuell halten. Das ITSM-Konzept muss die Integration der HCC-Cloud in die Betriebsorganisation des AN sowie in eine Multi-Provider-Betriebsumgebung beschreiben.

Die im ITSM-Konzept beschriebenen Prozesse sollen sich an anerkannten Verfahren des IT-Service-Managements orientieren.

Der AN kann zur Erfüllung der Anforderungen bestehende ITSM-Prozesse, Supportmodelle, Service-Desk-Lösungen, Reportingverfahren und Standardwerkzeuge verwenden, sofern die geforderten Inhalte und Leistungen hierdurch vollständig erbracht werden.

Das ITSM-Konzept muss mindestens die folgenden Prozesse adressieren:

- Incident Management,
- Major Incident Management,
- Patch Management,
- Notfall- und Wiederanlaufmanagement,
- Problem Management,
- Change-Management,
- Release Management,
- Configuration Management,
- Knowledge Management,
- Deployment Management,
- Request Fulfillment,
- Capacity Management,
- Availability Management sowie
- Service Level Management.

Darüber hinaus muss der AN die Verfahren zur Validierung, Freigabe, Planung, Umsetzung und Nachverfolgung von Änderungen an Plattform-, Infrastruktur- und HCC-Komponenten beschreiben.

Für die beschriebenen Prozesse muss der AN insbesondere darstellen:

- Rollen und Verantwortlichkeiten,
- Verantwortungs- und Leistungsabgrenzungen zu Dritten,
- Leistungsübergabepunkte,
- Ticket- und Workflowintegration,
- Schnittstellen zu weiteren Dienstleistern,
- Eskalationsverfahren und Kommunikationswege,
- Servicezeiten,
- Reporting- und Nachweisverfahren sowie
- die zur Steuerung der Prozesse verwendeten Kennzahlen.

Der AN muss darstellen, wie die Zusammenarbeit mit dem AG sowie weiteren an der Leistungserbringung beteiligten Dienstleistern erfolgt und wie Informationen, Störungen, Änderungen und Eskalationen organisationsübergreifend ausgetauscht werden.

Das ITSM-Konzept muss die konkrete Umsetzung der genannten Prozesse einschließlich Rollen, Verantwortlichkeiten, Schnittstellen, Eskalationsverfahren und organisationsübergreifender Zusammenarbeit beschreiben.

3.2.3.1 Service Desk und Anwenderbetreuung

Der AN muss einen zentralen Service Desk als Single Point of Contact (SPoC) für den AG bereitstellen.

Der Service Desk muss die Annahme, Koordination und Nachverfolgung von Service Requests und Incidents ermöglichen.

Der Service Desk muss die Koordination der Bearbeitung innerhalb des Verantwortungsbereichs des AN sowie die Übergabe an beteiligte Dienstleister unterstützen.

Im ITSM-Konzept muss dargestellt werden, wie Service Desk, Supportorganisation, Kommunikationskanäle, Servicezeiten sowie Eskalationsverfahren umgesetzt werden.

Der AN muss die Servicezeiten, Kommunikationskanäle, Supportklassen und Eskalationsverfahren beschreiben.

Der AN muss darstellen:

- Erreichbarkeit des Service Desk,
- unterstützte Kommunikationskanäle,
- verfügbare Supportsprachen,
- Eskalationswege,
- Ansprechpartner und Rollen sowie
- Verfahren zur organisationsübergreifenden Koordination mit weiteren Dienstleistern.

Die Kommunikation mit dem AG muss in deutscher Sprache möglich sein.

3.2.3.2 Supportmodell

Der AN muss für die bereitgestellten Cloud- und Plattformdienste einen erweiterten Support bereitstellen, der den Anforderungen eines unternehmenskritischen Betriebs der HCC-Cloud entspricht.

Der Support muss mindestens folgende pauschal vergütete Leistungen umfassen:

- 24x7-Unterstützung für kritische Betriebsstörungen,
- definierte Reaktions- und Eskalationszeiten für alle Supportklassen,
- mehrstufige Eskalationsverfahren,
- Unterstützung bei Störungsanalyse und Fehlerbehebung,
- Unterstützung bei sicherheitsrelevanten Ereignissen und kritischen Schwachstellen, Unterstützung bei Major Incidents,
- Durchführung von Ursachenanalysen (Root Cause Analysis) für kritische Störungen, Unterstützung bei Betriebs- und Service Reviews.

Der Support muss mindestens folgende gesondert abzurufende Leistungen umfassen

- Unterstützung durch qualifizierte technische Ansprechpartner für Betriebs-, Infrastruktur-, Sicherheits- und Plattformthemen,
- Unterstützung bei geplanten Änderungen, Migrationen und Plattformweiterentwicklungen sowie
- Unterstützung bei Architektur-, Betriebs-, Performance- und Skalierungsfragen,

Der AN muss sicherstellen, dass bei kritischen Betriebsstörungen eine unverzügliche Eskalation an spezialisierte technische Experten des AN oder seiner Unterauftragnehmer möglich ist.

Im ITSM-Konzept muss dargestellt werden, wie die Supportorganisation aufgebaut ist und wie die Unterstützung bei Betriebsstörungen, Sicherheitsvorfällen, Major Incidents, Änderungen und Service Reviews erfolgt.

3.2.3.3 Notfall- und Wiederanlaufmanagement

Der AN muss im ITSM-Konzept zum Notfallmanagement, Business Continuity Management und Disaster Recovery mindestens folgende Themen beschreiben:

- Notfallorganisation,
- Rollen und Verantwortlichkeiten im Krisenfall,
- Eskalations- und Kommunikationsverfahren,
- Business Continuity Management,
- Disaster-Recovery-Verfahren,
- Wiederanlaufverfahren,
- Datenwiederherstellungsverfahren,
- Failover- und Fallback-Verfahren,
- Verfahren zur Wiederherstellung kritischer Plattformdienste sowie
- Verfahren zur Wiederherstellung des Regelbetriebs.

Der AN muss darstellen, wie die Betriebsfähigkeit der bereitgestellten Leistungen bei schwerwiegenden Störungen, Infrastruktur-Ausfällen, Standortausfällen oder vergleichbaren Notfallsituationen aufrechterhalten oder wiederhergestellt wird.

Der AN muss die Notfall- und Wiederanlaufverfahren regelmäßig testen und dokumentieren.

Der AN muss den AG über durchgeführte proaktiv Tests informieren und die Ergebnisse der durchgeführten Tests dem AG auf Anforderung zur Verfügung stellen.

3.2.3.4 Tooling und Schnittstellenintegration

Der AN muss im ITSM-Konzept auch beschreiben, wie bestehende ITSM-, Ticket-, Monitoring-, Reporting- und Governance-Systeme des AG sowie weiterer beteiligter Dienstleister zu den entsprechenden Systemen des AN integriert werden können.

Die Integration soll über standardisierte Schnittstellen, APIs oder gleichwertige marktübliche Verfahren erfolgen.

Der AN muss darstellen:

- verfügbare Integrationsschnittstellen,
- unterstützte Datenformate,
- Authentifizierungs- und Autorisierungsverfahren,
- Synchronisations- und Übergabeverfahren,
- Möglichkeiten zur Ticket- und Workflowintegration sowie
- Möglichkeiten zur Datenbereitstellung für Monitoring- und Reportingzwecke.

Die Anforderungen dürfen keine Nutzung eines bestimmten Produkts oder Herstellers voraussetzen.

Der AN muss Möglichkeiten zur automatisierten Integration von Betriebsprozessen bereitstellen. Hierzu gehören insbesondere die automatisierte Erstellung, Aktualisierung, Weiterleitung, Synchronisation und Schließung von Tickets auf Basis definierter Kategorien, Prioritäten, Ereignisse oder Statusänderungen. Die Lösung muss geeignet sein, organisationsübergreifende Prozesse zwischen dem AG, dem AN sowie weiteren beteiligten Auftragnehmern zu unterstützen.

3.2.3.5 Datenliefermodell

Der AN muss als Teil des ITSM-Konzeptes ein Datenliefermodell bereitstellen, das die für den Betrieb, die Steuerung sowie die Nachvollziehbarkeit der Leistungserbringung erforderlichen Informationen beschreibt.

Die Bereitstellung der Daten muss über standardisierte und automatisierbare Schnittstellen oder Exportverfahren erfolgen, welche eine technische Weiterverarbeitung und Auswertung der Daten durch den AG ermöglicht. Hierbei können bestehende Schnittstellen und Standardfunktionen des AN genutzt werden.

Das Datenliefermodell muss mindestens die Bereitstellung folgender Informationen ermöglichen:

- Incidents,
- Major Incidents,
- Problems,
- Changes,
- Releases,
- Service Requests,
- Konfigurations- und Inventardaten der bereitgestellten Services,
- Betriebskennzahlen,
- Kapazitäts- und Auslastungsdaten,
- Verfügbarkeitsdaten,
- Monitoring- und Observability-Daten (insbesondere Logs, Metriken und Traces),
- Nutzungsdaten,
- Abrechnungs- und Verbrauchsdaten,
- Service-Level-Kennzahlen,
- Wartungsereignisse sowie
- Eskalations- und Statusinformationen zu Betriebsstörungen.

Der AN muss beschreiben, in welcher Form (z. B. Bericht, Dashboard, API oder Datenexport), Granularität und Aktualität die jeweiligen Informationen bereitgestellt werden.

Die Datenbereitstellung muss den AG in die Lage versetzen, die Leistungserbringung, die Einhaltung der vereinbarten Service Levels, die Nutzung der bereitgestellten Cloud-Services sowie deren Betriebszustand nachvollziehen, überwachen und bewerten zu können.

Der AN muss zusätzlich die Berichtszyklen, Aktualisierungsfrequenzen, Aufbewahrungszeiträume sowie gegebenenfalls bestehende Einschränkungen hinsichtlich Verfügbarkeit oder Historisierung der bereitgestellten Informationen beschreiben.

Die Daten müssen über standardisierte Schnittstellen exportierbar sein. Die Bereitstellung kann ergänzend über Standardreports, Dashboards, Self-Service-Portale oder APIs erfolgen.

Für Monitoring- und Observability-Daten muss die Unterstützung offener Industriestandards, insbesondere OpenTelemetry (OTel) oder eines gleichwertigen Standards, gewährleistet sein.

Im ITSM-Konzept muss beschrieben werden, wie Betriebs-, Service- und Leistungsdaten bereitgestellt, ausgetauscht und für die organisationsübergreifende Zusammenarbeit genutzt werden.

3.2.4 Service Level und Verfügbarkeit

Der AN muss ein SLA-Konzept bereitstellen und während der Vertragslaufzeit aktuell halten. Das SLA-Konzept muss die für die bereitgestellten Cloud- und Plattformdienste geltenden Service Levels sowie die Verfahren zu deren Messung, Nachweisführung und Berichterstattung beschreiben.

Der AN kann hierbei bestehende Standard-SLA-Modelle, Standardreports und Standard-Messverfahren verwenden, sofern die geforderten Inhalte und Nachweise vollständig erbracht werden.

Zudem kann der AN hierbei auch auf bestehende Beschreibungen im Servicekatalog verweisen, soweit die hier geforderten Inhalte und Leistungen damit abgedeckt sind.

3.2.4.1 Service-Level-Kennzahlen

Der AN muss im SLA-Konzept die angebotenen Service Levels den bereitgestellten Services zuordnen und transparent beschreiben.

Für jeden Service müssen mindestens folgende Informationen definiert werden:

- Servicebeschreibung,
- Serviceklasse,
- Serviceverfügbarkeit,
- Servicezeiten,
- Reaktionszeiten,
- Wiederherstellungszeiten,
- Eskalationszeiten,
- Wartungsfenster sowie
- Reporting-Verfahren.

Für die CI/CD-Plattform gelten folgende Service Levels, jeweils bezogen auf den Kalendermonat:

- Servicezeit: 24/7 für die Auslösung von Bereitstellungen, Deployments und die Auslieferung von Hotfixes; Kernzeit Montag bis Freitag 09:00–17:00 Uhr für Deployments und Tests auf den Nicht-Produktionsumgebungen.
- Verfügbarkeit: mindestens 99,5 % bezogen auf die maßgebliche Servicezeit.
- Wiederanlaufzeit (RTO): höchstens 60 Minuten.

Der AN muss darstellen, für welche Leistungen Service Levels gelten und wie deren Einhaltung gemessen und nachgewiesen wird.

Soweit für einzelne Services relevant, muss der AN zusätzlich technische Leistungskennzahlen beschreiben. Hierzu gehören insbesondere:

- Verfügbarkeit,
- Antwortzeiten,
- Latenzen,
- Durchsatzwerte,
- Ressourcenbereitstellungszeiten,
- Skalierungszeiten sowie
- weitere für die Leistungserbringung relevante technische Kennzahlen.

Der AN muss ferner beschreiben, welche organisatorischen Service Levels gelten und wie deren Einhaltung gemessen wird. Hierzu gehören insbesondere:

- Reaktionszeiten,
- Bearbeitungs- bzw. Lösungszeiten,
- Eskalationszeiten,
- Informationspflichten sowie
- Kommunikationsfristen.

3.2.4.2 Mess- und Nachweisverfahren

Der AN muss im SLA-Konzept die Verfahren zur Messung, Nachweisführung und Berichterstattung für sämtliche vereinbarten Service Levels beschreiben.

Hierbei muss insbesondere dargestellt werden:

- die verwendeten Messpunkte,
- die verwendeten Messverfahren,
- die Berechnungsregeln,
- die Messzeiträume,
- die zugrundeliegenden Datenquellen,
- die Aggregations- und Auswertungsverfahren sowie
- die Verfahren zur Nachweisführung gegenüber dem AG.

Der AN muss nachvollziehbar darstellen, welche Messdaten zur Ermittlung von Verfügbarkeit, Reaktionszeiten, Wiederherstellungszeiten und weiteren Service Levels verwendet werden.

Die Messergebnisse müssen revisionssicher dokumentiert und dem AG auf Anforderung zur Verfügung gestellt werden können.

3.2.4.3 Verfügbarkeit und Betriebsstabilität

Der AN muss im SLA-Konzept beschreiben, durch welche technischen und organisatorischen Maßnahmen die vereinbarten Service Levels unterstützt werden.

Hierzu gehören insbesondere:

- Maßnahmen zur Sicherstellung der Verfügbarkeit,
- Redundanzmechanismen,
- Failover- und Wiederanlaufverfahren,
- Nutzung georedundanter Infrastrukturen, soweit dies zur Erreichung der vereinbarten Service Levels erforderlich ist,
- Nutzung mehrerer Availability Zones oder gleichwertiger Verfahren,
- Verfahren zur Kapazitätssteuerung und Skalierung sowie
- Maßnahmen zur Vermeidung von Single Points of Failure.

Der AN muss die Zielwerte für Verfügbarkeit sowie die hierzu erforderlichen technischen Voraussetzungen beschreiben.

Die HCC-Cloud dient als Betriebsplattform für hochverfügbare und versorgungskritische Anwendungen der Telematikinfrastruktur. Die durch den AN angebotenen Service Levels müssen geeignet sein, die Anforderungen solcher Anwendungen an Verfügbarkeit, Betriebsstabilität, Wiederherstellbarkeit und Leistungsfähigkeit zu unterstützen. Dabei gelten auch die Anforderungen und Verfügbarkeitsvorgaben aus Kapitel 3.2.2.5.

Geplante Wartungsarbeiten, Plattformänderungen und Infrastrukturaktualisierungen müssen ohne Unterbrechung des produktiven Dienstbetriebs durchführbar sein.

3.2.4.4 Redundanz und Nachweisführung

Der AN muss im SLA-Konzept die eingesetzten Redundanzmechanismen sowie deren Wirksamkeit beschreiben.

Hierzu gehören insbesondere:

- Infrastrukturredundanz,
- Service-Redundanz,
- Standortredundanz,
- Datenreplikation,
- Wiederanlaufverfahren,
- Failover-Verfahren sowie
- Disaster-Recovery-Verfahren.

Der AN muss darstellen, wie die Einhaltung der Redundanzanforderungen nachgewiesen wird.

Der AN muss die Ergebnisse entsprechender Prüfungen, Tests oder Validierungen dokumentieren und dem AG auf Anforderung zur Verfügung stellen.

3.2.4.5 Wartung

Der AN muss im SLA-Konzept Wartungsfenster sowie die hierfür geltenden Verfahren beschreiben.

Hierbei muss insbesondere dargestellt werden:

- Ankündigungsfristen,
- Informationswege,
- betroffene Leistungen,
- Auswirkungen auf vereinbarte Service Levels

Der AN muss sicherstellen, dass geplante Wartungsmaßnahmen transparent kommuniziert werden.

3.2.4.6 Reporting

Der AN muss im SLA-Konzept dem AG regelmäßig Reports zur Einhaltung der vereinbarten Service Levels bereitstellen.

Die Reports müssen mindestens folgende Informationen enthalten:

- Verfügbarkeiten,
- SLA-Erfüllung,
- SLA-Verletzungen,
- Incidents,
- Major Incidents,
- Wartungsereignisse,
- Kapazitätsentwicklungen,
- wesentliche Betriebsereignisse sowie
- Nachweise zur Einhaltung vereinbarter Service Levels.

Der AN muss die Berichtszyklen sowie die Aktualisierungsfrequenzen beschreiben.

Für die Bereitstellung können Standardreports, Dashboards, Self-Service-Portale oder Programmierschnittstellen (APIs) genutzt werden.

3.2.4.7 Umgang mit Schlechtleistung

Der AN muss im SLA-Konzept Verfahren für den Umgang mit der Nichteinhaltung vereinbarter Service Levels vorsehen.

Diese Verfahren müssen mindestens umfassen:

- Analyse der Ursachen,
- Dokumentation der Abweichungen,
- Maßnahmen zur Fehlerbehebung,
- Nachbesserungsmaßnahmen,
- Maßnahmen zur Vermeidung erneuter Verstöße sowie
- Eskalationsverfahren bei wiederholten oder schwerwiegenden SLA-Verletzungen.

Der AN muss darstellen, wie die Umsetzung und Wirksamkeit der eingeleiteten Maßnahmen nachgewiesen werden

3.2.4.8 Governance, Steuerung und Zusammenarbeit

Der AN muss ein Governance-Konzept bereitstellen und während der Vertragslaufzeit aktuell halten. Das Governance-Konzept muss die Zusammenarbeit zwischen dem AN, dem AG sowie weiteren durch den AG beauftragten Dienstleistern beschreiben.

Das Governance-Konzept muss insbesondere die organisatorischen Strukturen, Verantwortlichkeiten, Kommunikationswege sowie Steuerungs-, Eskalations- und Entscheidungsverfahren für die Leistungserbringung darstellen.

Der AN kann zur Erfüllung dieser Anforderungen bestehende Governance-Modelle, Standardprozesse und Standardverfahren verwenden, sofern die geforderten Inhalte und Leistungen hierdurch vollständig erbracht werden.

3.2.4.9 Rollen und Verantwortlichkeiten

Der AN muss im Governance-Konzept die für die Leistungserbringung relevanten Rollen und Verantwortlichkeiten beschreiben.

Dies umfasst insbesondere:

- Betriebsrollen,
- Eskalationsrollen,
- Ansprechpartner für fachliche, technische, organisatorische und kommerzielle Themen,
- Verantwortlichkeiten an Leistungs- und Prozessgrenzen,
- Verantwortlichkeiten gegenüber weiteren Dienstleistern sowie
- eine Verantwortungsmatrix (z. B. RACI oder ein gleichwertiges Modell).

Dabei muss nachvollziehbar dargestellt werden, welche Aufgaben durch den AN erbracht werden und welche Verantwortlichkeiten beim AG oder weiteren Dienstleistern verbleiben.

Der AN muss für betriebliche, technische, organisatorische und kommerzielle Themen jeweils benannte Ansprechpartner bereitstellen.

Für die Steuerung der Leistungserbringung muss der AN feste Ansprechpartner benennen. Hierzu gehören insbesondere:

- ein zentraler Service-Verantwortlicher,
- ein technischer Ansprechpartner für Architektur-, Betriebs- und Plattformthemen,
- ein Ansprechpartner für Eskalationen sowie
- ein Ansprechpartner für kommerzielle und vertragliche Fragestellungen.

Der AN muss beschreiben, welche Rollen dauerhaft benannt werden und mit welchen Reaktionszeiten diese erreichbar sind.

3.2.4.10 Gremien- und Steuerungsmodell

Der AN muss im Governance-Konzept die Verfahren zur Steuerung und Abstimmung der Leistungserbringung beschreiben.

Hierzu gehören insbesondere:

- regelmäßige Service Reviews,
- operative Betriebsabstimmungen,
- Eskalationsgremien oder vergleichbare Formate,
- Verfahren zur Behandlung wesentlicher Änderungen,
- Management Reviews sowie
- weitere für die Leistungserbringung erforderliche Steuerungsformate.

Der AN muss die für die Leistungserbringung erforderlichen Governance- und Steuerungsgremien beschreiben.

Hierbei sind mindestens darzustellen:

- Zweck und Aufgaben der jeweiligen Gremien,
- Teilnehmerkreise,
- Rollen und Verantwortlichkeiten,
- Entscheidungskompetenzen,
- Eskalationsbefugnisse,
- Sitzungsrhythmen,
- Dokumentationspflichten sowie
- Verfahren zur Nachverfolgung beschlossener Maßnahmen.

Der AN muss sicherstellen, dass qualifizierte technische und organisatorische Ansprechpartner an den vereinbarten Service Reviews, Management Reviews sowie Eskalationsverfahren teilnehmen können.

Der AN muss beschreiben, welche Rollen für die operative Steuerung, die technische Beratung und die Management-Eskalation vorgesehen sind.

Der AN kann hierfür bestehende Standardverfahren und Governance-Prozesse verwenden.

3.2.4.11 Leistungs- und Änderungsmanagement

Der AN muss im Governance-Konzept die Umsetzung des Verfahrens zur Beauftragung, Bewertung, Freigabe und Umsetzung von Leistungsänderungen beschreiben. Das im Governance-Konzept beschriebene Vorgehen muss auf den vertraglichen Vorgaben basieren und darf diesen nicht widersprechen (vgl. insbesondere „Anlage-12 der Vergabeunterlagen - IT Projektvertrag "TI-Flow - Cloud Services" (Los 2)").

Dies umfasst insbesondere:

- Änderungen des Leistungsumfangs,
- Änderungen von Service Levels,
- Änderungen von Serviceklassen,
- Änderungen von Kapazitäten oder Verbrauchsmengen,
- die Einführung neuer Services,
- die Außerbetriebnahme bestehender Services sowie
- wesentliche Änderungen von Betriebs- oder Supportleistungen.

Der AN muss darstellen,

- wie Änderungsanforderungen eingebracht werden,
- wie deren Auswirkungen bewertet werden,
- welche Freigaben erforderlich sind,
- wie Änderungen umgesetzt und dokumentiert werden sowie
- wie Auswirkungen auf Kosten, Termine, Risiken und Service Levels transparent gemacht werden.

3.2.4.12 Eskalations- und Konfliktmanagement

Der AN muss im Governance-Konzept Eskalationsverfahren für betriebliche, technische, organisatorische und vertragliche Sachverhalte beschreiben.

Hierzu gehören insbesondere:

- operative Eskalationen,
- Management-Eskalationen,
- Eskalationen bei SLA-Verletzungen,
- Eskalationen bei Sicherheitsvorfällen sowie
- Eskalationen mit Beteiligung weiterer Dienstleister.

Der AN muss sicherstellen, dass die hierfür erforderlichen Kommunikations- und Eskalationswege definiert und nachvollziehbar dokumentiert sind.

Darüber hinaus muss der AN Verfahren zur Konfliktlösung und Entscheidungsfindung bei:

- organisationsübergreifenden Betriebsstörungen,
- Verantwortungsunklarheiten,
- Leistungsabweichungen,
- Priorisierungskonflikten sowie
- Meinungsverschiedenheiten zwischen beteiligten Dienstleistern

beschreiben.

3.2.4.13 Zusammenarbeit in einer Multi-Provider-Betriebsumgebung

Der AN muss im Governance-Konzept darstellen, wie die Zusammenarbeit mit weiteren durch den AG beauftragten Dienstleistern, welche Anwendungen/Dienste auf der HCC-Cloud-Infrastruktur betreiben, erfolgt.

Dies umfasst insbesondere:

- Schnittstellenmanagement,
- Abstimmung betrieblicher Prozesse,
- Übergabe und Übernahme von Incidents,
- gemeinsame Fehler- und Ursachenanalysen,
- Abstimmung von Änderungen mit Auswirkungen auf andere Leistungserbringer,
- Informationsaustausch bei geplanten Wartungen und Betriebsmaßnahmen,
- gemeinsame Eskalationen,
- Zusammenarbeit bei kritischen Betriebsereignissen sowie
- Unterstützung der durch den AG vorgegebenen Multi-Provider-Governance.

Der AN muss darlegen, wie Leistungsgrenzen, Verantwortlichkeiten und Übergabepunkte zwischen den beteiligten Dienstleistern transparent und nachvollziehbar geregelt werden.

Der AN muss den Mandanten der auf der HCC-Cloud betriebenen Fachanwendungen sowie dem AG die für Betrieb, Fehleranalyse, Ursachenanalyse und gemeinsame Störungsbearbeitung erforderlichen Monitoring-, Telemetrie-, Logging- und Betriebsdaten bereitstellen.

Der AN muss dokumentieren, welche Monitoring- und Messpunkte entlang der Leistungserbringung vorhanden sind, welche Kennzahlen erhoben werden und welchen Komponenten diese jeweils zugeordnet sind.

Die bereitgestellten Informationen müssen eine nachvollziehbare Abgrenzung zwischen Ursachen innerhalb der HCC-Cloud und Ursachen innerhalb der betriebenen Fachanwendungen ermöglichen.

3.2.4.14 *Kontinuierliche Verbesserung und Innovation*

Der AN muss im Governance-Konzept Verfahren zur kontinuierlichen Verbesserung der Leistungserbringung beschreiben.

Hierzu gehören insbesondere:

- Identifikation von Optimierungspotenzialen,
- Analyse wiederkehrender Betriebsprobleme,
- Vorschläge zur Verbesserung von Verfügbarkeit, Sicherheit und Betriebsstabilität,
- Vorschläge zur Verbesserung von Performance und Skalierbarkeit,
- Empfehlungen zur Kosten- und Ressourceneffizienz,
- technologische Weiterentwicklungen der Plattform,
- Empfehlungen zur Standardisierung und Automatisierung sowie
- die regelmäßige Vorstellung relevanter Innovationen und Verbesserungsmöglichkeiten gegenüber dem AG.

Der AN muss beschreiben, wie Verbesserungsmaßnahmen bewertet, priorisiert, umgesetzt und nachverfolgt werden.

3.2.4.15 Reporting

Der AN muss im Governance-Konzept dem AG regelmäßig Informationen zur Steuerung und Bewertung der Leistungserbringung bereitstellen.

Das Reporting muss mindestens folgende Themen umfassen:

- Betriebs-Reporting,
- SLA-Reporting,
- Verfügbarkeits-Reporting,
- Kapazitäts- und Auslastungs-Reporting,
- Reporting zu wesentlichen Betriebsereignissen,
- Reporting zu kritischen Incidents und Problems,
- Reporting zu Eskalationen,
- Reporting zu Verbesserungsmaßnahmen sowie
- Managementberichte oder vergleichbare Zusammenfassungen.

Der AN muss die Berichtszyklen und Bereitstellungsverfahren beschreiben.

Der AN kann hierfür bestehende Standard-Reports, Dashboards, Service-Portale oder Reporting-Verfahren nutzen, sofern die geforderten Informationen vollständig bereitgestellt werden.

3.2.4.16 Bezug zu Support und Eskalation

Die Anforderungen an Supportleistungen, technische Expertenunterstützung, Major-Incident-Management, Reaktionszeiten, Eskalationsstufen sowie erweiterte Unterstützungsleistungen ergeben sich ergänzend aus Kapitel 3.2.3.

Der AN muss sicherstellen, dass die hierfür benannten Service-, Governance- und Technikverantwortlichen in die Support-, Incident-, Major-Incident-, Eskalations- und Kommunikationsprozesse eingebunden sind und ihre jeweiligen Aufgaben und Verantwortlichkeiten wahrnehmen.

Hierzu sind die erforderlichen Rollen, Kommunikationswege, Entscheidungsbefugnisse und Eskalationsverfahren zu definieren und organisatorisch zu verankern.

3.2.5 Transition, Transformation und Exit

Der AN muss sicherstellen, dass die durch ihn bereitgestellten Leistungen während der Vertragslaufzeit angepasst, erweitert, transformiert oder auf einen Nachfolgebetreiber übertragen werden können, ohne die vereinbarten Betriebsleistungen unangemessen zu beeinträchtigen.

Der AN muss den AG bei Transition-, Transformations- und Exit-Szenarien unterstützen und die hierfür erforderlichen organisatorischen, technischen und dokumentarischen Voraussetzungen schaffen.

Die Anforderungen dieses Kapitels sind durch die im Arbeitspaket 7 erstellte Übergabestrategie umzusetzen. Die Übergabestrategie ist während der Vertragslaufzeit fortzuschreiben und bei wesentlichen Änderungen der bereitgestellten Leistungen zu aktualisieren.

3.2.5.1 Transition

Unter Transition wird die Überführung neuer oder geänderter Leistungen in den Regelbetrieb verstanden.

Der AN muss Verfahren bereitstellen, die eine kontrollierte und nachvollziehbare Übernahme neuer Plattformdienste, neuer Mandanten, neuer Workloads sowie neuer Betriebsumgebungen ermöglichen.

Der AN muss hierbei insbesondere sicherstellen, dass:

- Betriebsverantwortlichkeiten eindeutig festgelegt sind,
- Betriebsdokumentationen vollständig vorliegen,
- Monitoring- und Alarmierungsfunktionen eingerichtet sind,
- Betriebsprozesse abgestimmt sind,
- notwendige Betriebsfreigaben vorliegen,
- erforderliche Betriebsprüfungen durchgeführt wurden.

3.2.5.2 Transformation

Unter Transformation wird die wesentliche Änderung von Architektur, Betriebsmodell, Plattformkomponenten oder Organisationsstrukturen verstanden.

Der AN muss Verfahren bereitstellen, die die Durchführung solcher Änderungen unter Aufrechterhaltung der vereinbarten Betriebsleistungen ermöglichen.

Hierzu muss der AN insbesondere beschreiben:

- Migrationsverfahren,
- Rollback-Verfahren,
- Test- und Freigabeverfahren,
- Kommunikationsverfahren,
- Risikominimierungsmaßnahmen,
- Parallelbetriebsverfahren,
- Verfahren zur Wahrung der Datenintegrität.

Wesentliche Transformationen müssen so geplant und durchgeführt werden, dass die Auswirkungen auf produktive Mandanten und Workloads minimiert werden.

3.2.5.3 Exit und Betreiberwechsel

Der AN muss den AG dabei unterstützen, die durch ihn bereitgestellten Leistungen nach Vertragsende oder bei vorzeitiger Vertragsbeendigung geordnet auf einen vom AG benannten Dritten zu übertragen. Der AN muss den AG während der gesamten Exit-Phase aktiv unterstützen.

Die Exit-Leistungen müssen insbesondere umfassen:

- Unterstützung der Migration zu einem anderen Cloud-Anbieter oder in eine andere Zielumgebung,
- Bereitstellung aller für die Übernahme der Leistungserbringung durch den neuen Anbieter relevanten Dokumentationen,
- Bereitstellung von Konfigurationen und Infrastruktur, Konfiguration und Policy definierendem Code, Rollen- und Berechtigungsinformationen sowie von Mandanten- und Trust-Domain-Konfigurationen als Referenzinformationen für die Einrichtung entsprechender Strukturen beim neuen Anbieter,
- Übertragung der Inhalte der CI/CD-Plattform

Der AN muss sicherstellen, dass alle Daten, Konfigurationen und betriebsrelevante Artefakte, welche für eine Überführung des Betriebes notwendig sind, in marktüblichen, standardisierten und maschinenlesbaren Formaten exportiert werden können. Für die Migration der von Anwendungen verschlüsselt persistierten Daten ist jede Anwendung selbst verantwortlich. Eine Exportmöglichkeit für HSM-geschützte und HCC-verwaltete Schlüssel ist nicht gefordert.

Der AN muss Verfahren zur Übergabe oder Löschung von Daten nach Abschluss der Migration bereitstellen und deren ordnungsgemäße Durchführung nachweisen können.

Der AN muss die Durchführung von Transition-, Transformations- und Exit-Maßnahmen dokumentieren.

Der erfolgreiche Abschluss einer Exit-Maßnahme ist durch ein gemeinsam abgestimmtes Übergabeprotokoll nachzuweisen.

3.2.6 Nachweis der erfolgreich durchgeführten Betriebs- und Schnittstellenprüfung

Die Betriebs- und Schnittstellenprüfung dient dem Nachweis der erfolgreichen Zusammenarbeit zwischen den Betriebsorganisationen von Auftraggeber und Auftragnehmer sowie der Funktionsfähigkeit der vereinbarten ITSM-Integration.

Zur Durchführung der Prüfung erstellt der AG praxisbezogene Testfälle und initiiert simulierte Betriebsprozesse. Hierbei sind insbesondere folgende Nachweise zu erbringen:

- erfolgreiche Übertragung von Incidents, Changes, Problems, Service Requests und Eskalationen zwischen den ITSM-Systemen von AG und AN,
- korrekte Synchronisation von Ticketstatus, Prioritäten, Kommentaren und Anhängen,
- Einhaltung der vereinbarten Kommunikationswege,
- Nachweis der Verfügbarkeit der benannten Ansprechpartner und Eskalationsinstanzen,
- nachvollziehbare Bearbeitung und Rückmeldung der Testfälle innerhalb der für die Prüfung vereinbarten Zeitvorgaben.

Die konkreten Testfälle werden durch den AG auf Basis der vereinbarten Betriebs-, Support- und Eskalationsprozesse festgelegt und dem AN vor Durchführung der Prüfung bereitgestellt.

Die Prüfung erfolgt gemeinsam mit dem AG. Sie gilt als erfolgreich abgeschlossen, wenn sämtliche Testfälle ohne kritische Fehler bearbeitet wurden und die vereinbarte ITSM-Integration die definierten Informationen vollständig, konsistent und nachvollziehbar zwischen den beteiligten Systemen austauscht.

3.2.7 Betrieb CI/CD-Plattform

Der Betriebsphase CI/CD-Plattform umfasst die Bereitstellung, den Betrieb, die Überwachung, die Wartung, die Pflege, die Störungsbearbeitung, die Wiederherstellung, die Weiterentwicklung und die Unterstützung der Nutzung der CI/CD-Plattform für die vorgesehenen Test-, Prüf-, Signatur-, Freigabe-, Promotion- und Deployment-Prozesse.

Die Umsetzung des Betriebs der CI/CD-Plattform muss auf Grundlage des Betriebshandbuchs CI/CD (Kapitel 3.1.4.16) und der Dokumentation CI/CD (Kapitel 3.1.4.17) erfolgen. Das Betriebshandbuch CI/CD und die Dokumentation CI/CD sind während der Betriebsphase fortzuschreiben und bei wesentlichen Änderungen der CI/CD-Plattform, der Betriebsprozesse, der Schnittstellen, der Verantwortlichkeiten oder der Support- und Eskalationswege zu aktualisieren und mit dem AG abzustimmen.

Der AN muss die CI/CD-Plattform so betreiben, dass die vorgesehenen Test-, Prüf-, Signatur-, Freigabe-, Promotion- und Deployment-Prozesse stabil, sicher, nachvollziehbar und für die berechtigten Nutzergruppen verfügbar durchgeführt werden können.

Betriebsumfang

Der Betrieb der CI/CD-Plattform muss insbesondere umfassen:

- den Betrieb und die Überwachung der Plattformkomponenten, Repositories, Artefakt-Ablagen, Registry-Komponenten, Pipeline-Orchestrierung und Runner-Ausführungsumgebungen,
- den Betrieb der Schnittstellen zur HCC-Cloud, insbesondere zur Übergabe freigegebener Artefakte, zur Nutzung definierter HCC-Schnittstellen, zur Verarbeitung von Laufzeit-, Versions- und Attestierungsinformationen sowie zur Nachvollziehbarkeit dieser Übergänge,
- die Bereitstellung und Pflege der technischen Voraussetzungen für Authentifizierung, Autorisierung, Rollen- und Berechtigungsverwaltung, Freigaben, Pipeline-Ausführung, Artefaktzugriffe und Auditierung,
- die Überwachung von Verfügbarkeiten, Kapazitäten, Auslastung, Fehlersituationen, Pipeline-Ausführungen, Runner-Ausführungsumgebungen, Artefakt-Ablagen, Registry-Komponenten und Schnittstellen,
- die Bearbeitung von Störungen, Fehlerbildern, Abbrüchen, Wiederanläufen, Recovery-Szenarien sowie sicherheitsrelevanten Updates, Patches und Hotfixes,
- die Durchführung und Dokumentation von Backup-, Restore-, Wiederanlauf- und Recovery-Verfahren für betriebsrelevante Plattformkomponenten, Konfigurationen, Repositories, Pipeline-Definitionen, Artefakte, OCI-Artefakte, Sicherheits- und Nachweisartefakte sowie Audit- und Protokolldaten,
- die Sicherstellung der Auditierbarkeit und Nachvollziehbarkeit des Plattformbetriebs, insbesondere hinsichtlich Änderungen an Pipeline-Definitionen, Pipeline-Templates, Berechtigungen, Freigaben, Artefakten, Runner-Konfigurationen und Schnittstellenkonfigurationen,
- die Bereitstellung von Betriebs-, Audit- und Nachweisinformationen für den AG,
- die Unterstützung der Betriebs-, Support-, Monitoring-, Logging-, Audit- und Eskalationsprozesse des AG und des AN.

Verantwortungsabgrenzung

Für die CI/CD-Plattform ist zwischen dem Betrieb der Plattform und der fachlichen Nutzung der Plattform zu unterscheiden.

Der AN ist verantwortlich für den sicheren, stabilen, verfügbaren und nachvollziehbaren Betrieb der CI/CD-Plattform. Dies umfasst insbesondere Betrieb, Wartung, Überwachung, Wiederherstellung, technische Pflege und technische Weiterentwicklung der Plattformkomponenten, Repositories, Artefakt-Ablagen, Registry-Funktionen, Schnittstellen, Berechtigungsfunktionen, Protokollierung, Auditierung und Betriebsprozesse.

Die fachliche Verantwortung für Pipeline-Definitionen, Testsuiten, Testfälle, Testdaten, Stage-Übergangslogiken, fachliche Prüfkriterien und Freigabeentscheidungen verbleibt beim AG, beim jeweiligen Fachdiensthersteller oder bei berechtigten Dritten, soweit diese Leistungsbeschreibung keine abweichende Verantwortung des AN ausdrücklich festlegt.

Support und Nutzungsunterstützung

Der AN muss den AG sowie berechnigte Nutzergruppen im Regelbetrieb bei der Nutzung der CI/CD-Plattform unterstützen. Dies umfasst insbesondere:

- Unterstützung bei Störungen der Plattformfunktionen und Schnittstellen,
- Unterstützung bei der Fehleranalyse im Zusammenhang mit Pipeline-Ausführungen, Runner-Ausführungsumgebungen, Artefakt-Ablagen, Registry-Komponenten und Schnittstellen zur HCC-Cloud,
- Unterstützung bei der Auswertung von Plattformereignissen, Pipeline-Läufen, Freigabeereignissen und Artefaktübergängen,
- Unterstützung bei geplanten Änderungen, Wartungen, Aktualisierungen und Weiterentwicklungen der CI/CD-Plattform.

Soweit für die CI/CD-Plattform bereits Festlegungen in Umsetzungskonzepten, Testkonzepten, Sicherheitskonzepten, Übergabestrategien oder sonstigen mitgeltenden Dokumenten getroffen werden, muss der Betrieb diese konsistent berücksichtigen.

Es gilt die Hinweispflicht des AN gem. Kapitel 2.2, sofern der AN Widersprüche in den Konzepten erkennt.

3.2.8 Begleitende Dokumentation

Der AN muss in der Betriebsphase die nachfolgenden Dokumentationen zur Prüfung beim AG einreichen. Ein Anpassungsbedarf entsteht immer dann, wenn für den Liefergegenstand relevante Objekte von wesentlichen Änderungen betroffen sind. Die Einreichung fortgeschriebener Dokumente muss innerhalb von 4 Wochen nach Umsetzung der jeweiligen Änderung erfolgen, sofern nichts Anderweitiges vereinbart wurde.

Die folgende Tabelle "Begleitende Dokumentationen der Betriebsphase" dient dem AN als allgemeine Orientierung, ist jedoch nicht abschließend. Es wird ausdrücklich darauf hingewiesen, dass darüber hinaus die in den Spezifikationen festgelegten Inhalte und Dokumente in vollem Umfang und in den dort definierten Häufigkeiten und Rhythmen zu erbringen sind. Bei Unklarheiten oder Widersprüchen haben die Vorgaben der Spezifikationen Vorrang.

Tabelle 4: Begleitende Dokumentationen der Betriebsphase

Dokumentation	Häufigkeit der Erstellung
Servicekatalog	Anlassbezogen
Governance-Konzept	Anlassbezogen bzw. mindestens einmal jährlich
SLA-Konzept	Anlassbezogen bzw. mindestens einmal jährlich
ITSM-Konzept	Anlassbezogen bzw. mindestens einmal jährlich

Betriebshandbuch CI/CD	Anlassbezogen bzw. mindestens einmal jährlich
Dokumentation CI/CD	Anlassbezogen bzw. mindestens einmal jährlich
Dokumentation HCC	Anlassbezogen
Übergabestrategie HCC Cloud	Anlassbezogen bzw. mindestens einmal jährlich
Sicherheitsgutachten Softwareentwicklungsprozesse	Alle 3 Jahre
Produktgutachten HCC	Alle 3 Jahre Anlassbezogen jährliche Delta-Gutachten
Sicherheitsgutachten HCC	Alle 3 Jahre Anlassbezogen Deltagutachten
Controls des TI Security Standards	siehe [gemTI_SEC_Standard]
Herstellererklärung sicherheitstechnische Eignung	Anlassbezogen
Herstellererklärung funktionale Eignung	Anlassbezogen
Zertifizierungen und Testate gemäß [gemSpec_HCC], Kapitel 9	Kontinuierliche Aufrechterhaltung des Zertifizierungsstatus

3.2.8.1 Sicherheitskonzept

Der AN muss dem AG das Sicherheitskonzept für HCC und dessen Betrieb mindestens mit den folgenden Inhalten und der Dokumentation seines Informationssicherheitsmanagementsystems (ISMS), welches im Rahmen des Sicherheitsgutachtens verwendet wird, zur Kenntnisnahme vorlegen:

- Inhalte gemäß [gemTI_SEC_Standard#6.2],
- Rollen- und Rechtekonzept,
- Als Anlage: Compliance Register und
- Als Anlage: Supply Chain und Third Party Risk Register.

Der AN muss das Sicherheitskonzept im Rahmen der Prozessprüfung sicherheitstechnische Eignung zur Güteprüfung vorlegen

3.2.8.2 Vorlage der Vereinbarung über die gemeinsame datenschutzrechtliche Verantwortung

Der AN legt dem AG die Vereinbarung über die gemeinsame datenschutzrechtliche Verantwortung gem. Art. 26 DSGVO mit dem Dienstbetreiber aus Los 1 zur Freigabe vor.

3.2.8.3 Security Monitoring Konzept

Die Telematikinfrastruktur ist eine kritische Infrastruktur, die der Verarbeitung von medizinischen personenbezogenen Daten in großem Umfang dient und unterliegt daher besonderen Anforderungen an die kontinuierliche Überwachung und sofortige Reaktion auf Aktivitäten, die zu Verletzungen der Sicherheitsvorkehrungen führen (können) oder auf potenzielle Angriffe hinweisen.

Gemäß [gemTI_SEC_Standard#6.6.8] muss der AN ein Security Monitoring betreiben und sich in der Projektphase mit dem Cyber Defense Center der gematik über die technische Umsetzung des Security Monitorings, die zu detektierende Ereignisse auf den jeweiligen Systemen und Diensten sowie zu den begleitenden organisatorischen Maßnahmen abstimmen. Der AN muss sein bereits in der Konzeptphase vorgelegtes Security Monitoring Konzept kontinuierlich fortschreiben, um es auf dem jeweils aktuellen Stand seiner Maßnahmen zu halten und dabei auch auf die Abstimmungsergebnisse mit dem AG anpassen. Der AN muss das Security Monitoring Konzept im Rahmen der Prozessprüfung sicherheitstechnische Eignung zur Güteprüfung vorlegen.

Für das Security Monitoring-Konzept gelten die Anforderungen aus [gemTI_SEC_Standard#6.6.8].

3.2.8.4 Notfallkonzept

Der AN muss dem AG das Notfallkonzept für HCC und dessen Betrieb, das sein Notfallmanagement nach [gemTI_SEC_Standard#6.15] . Der AN muss das Notfallkonzept im Rahmen der Prozessprüfung sicherheitstechnische Eignung zur Güteprüfung vorlegen.

3.3 Datenschutz und Informationssicherheit

Der AN muss in jedem Stadium seiner Leistungserbringung zwingend die Vorgaben des Datenschutzes und der Informationssicherheit umsetzen und gewährleisten.

Bei der Kommunikation zwischen den Vertragspartnern ist die Vertraulichkeit zu wahren. So ist bspw. die Kommunikation per E-Mail stets verschlüsselt durchzuführen.

Die Produktivumgebung (PU) ist informationstechnisch von allen anderen Umgebungen (RU DEV, TU und RU) zu trennen. Dies umfasst auch, dass in den Testumgebungen keine kryptographischen Identitäten bzw. Schlüssel der PU genutzt werden dürfen. Andersherum

dürfen keine Daten und kryptographischen Identitäten bzw. Schlüssel der Testumgebungen in der PU genutzt werden. Die Trennung der Umgebung muss über separate Trust Domains technisch durchgesetzt werden.

3.3.1 Datenschutz- und Informationssicherheitspflichten als Hersteller

Der AN muss die Anforderungen zur sicherheitstechnischen Eignung aus dem Produkttypsteckbrief [gemProdT_HCC_PTV] erfüllen.

3.3.2 Sicherheitsgutachten Softwareentwicklungsprozesse

Der AN muss für seine SW-Entwicklungsprozesse eine gesonderte Begutachtung durch eine unabhängige Instanz mittels eines Sicherheitsgutachtens und den Vorgaben aus [gemRL_PruefSichEig_DS] erstellen lassen und dem AG im Rahmen der Produktivfreigabe zur Prüfung übergeben. Das Sicherheitsgutachten muss die Anforderungen zur sicherheitstechnischen Eignung aus dem Produkttypsteckbrief [gemProdT_HCC_PTV] mit dem Prüfverfahren „Sicherheitsgutachten“ umfassen.

Der AG nimmt das Gutachten entgegen und prüft dessen Vollständigkeit in Bezug auf die geltende Anforderungslage, die Nachvollziehbarkeit der Prüfergebnisse und Bewertungen sowie die Angemessenheit der Prüfmethoden. Erst nach erfolgreicher Prüfung wird das Gutachten vom AG freigegeben.

Das Gutachten muss in Gänze alle drei Jahre wiederholt erstellt werden. Das neue Gutachten muss vom AN vor Ablauf der drei Jahre an den AG übergeben werden.

3.3.3 Produktgutachten HCC

Der AN muss für die Produktivfreigabe der HCC-Cloud ein Produktgutachten einreichen, das die Erfüllung der Anforderungen zur sicherheitstechnischen Eignung aus dem Produkttypsteckbrief [gemProdT_HCC_PTV] mit dem Prüfverfahren „Produktgutachten“ nachweist und den Vorgaben aus [gemRL_PruefSichEig_DS] entspricht.

Das Produktgutachten hat seinen Schwerpunkt in der tiefen technischen Prüfung der konkreten IT-Lösung und umfasst die Analyse von Quellcode sowie Penetrationstests auf eine Instanz in der Produktivumgebung.

Der AG nimmt das Gutachten entgegen und prüft dessen Vollständigkeit bzgl. der Anforderungslage, die Nachvollziehbarkeit der Prüfergebnisse und Bewertungen sowie die Angemessenheit der Prüfmethoden. Erst nach erfolgreicher Prüfung wird das Gutachten vom AG freigegeben.

Das Gutachten muss in Gänze alle drei Jahre wiederholt erstellt werden. Das neue Gutachten muss vom AN vor Ablauf der drei Jahre an den AG übergeben werden.

Zudem müssen Änderungen am Produkt jährlich in Form eines Delta-Gutachtens geprüft werden, wobei stets die gesammelten, über den Verlauf des jeweiligen Jahres umgesetzten Änderungen betrachtet werden. Entsprechend ist vom AN vor Ablauf eines Jahres ein Delta-Produktgutachten dem AG zu übergeben.

Unabhängig davon sind Änderungen immer dem AG zu kommunizieren. Der AG behält sich vor, bei größeren sicherheitskritischen Änderungen ein Delta-Gutachten noch vor dem Rollout der Änderung in der PU einzufordern.

3.3.4 Sicherheitsanalysen und Audits

Der AN muss gemäß [gemSpec_DS_Hersteller] # A_19163 zusichern, dass der AG oder ein von ihm zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt sind, Sicherheitsprüfungen (z.B. Whitebox oder Blackbox Pentest) seines Produktes HCC durchzuführen und im Rahmen einer Sicherheitsprüfung die konkrete Umsetzung der an das Produkt gestellten Anforderungen zu überprüfen. Der AN muss den AG hierbei unterstützen.

Der AN muss gemäß [gemSpec_DS_Hersteller] # A_19165 zusichern, dass der AG oder ein von ihm zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt sind, Audits durchzuführen. Im Rahmen eines Audits beim Hersteller werden die konkrete Umsetzung der an den AN als Hersteller gestellten Anforderungen überprüft und im Rahmen eines Audits während der üblichen Geschäftszeiten die Geschäftsräume des Herstellers betreten. Zudem müssen im Rahmen eines Audits alle für das Audit benötigten Informationen zur Verfügung gestellt und insbesondere die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte eingeräumt werden.

3.3.5 Datenschutz- und Informationssicherheitspflichten als Anbieter

Der AN muss die Anforderungen zur sicherheitstechnischen Eignung aus dem Anbieter-typsteckbrief [gemAnbT_HCC_ATV] erfüllen.

Der AN muss seine Betriebsleistung entsprechend [gemSpec_DS_Anbieter] # GS-A_5551-01 in Standorten in der EU bzw. dem EWR oder der Schweiz erbringen. Eine Verlagerung der Betriebsleistung in andere Rechenzentren darf nur nach vorheriger Zustimmung des AG erfolgen.

Für die Gewährleistung der betrieblichen Sicherheit muss der AN die Vorgaben aus [gemSpec_DS_Anbieter] und dem TI Security Standard [gemTI_SEC_Standard] fortwährend erfüllen und dies sowohl initial als auch periodisch während des Betriebs dem AG gegenüber nachweisen.

Entsprechend [gemTI_SEC_Standard] ist der Anbieter des TI-Flow-Fachdienstes aufgrund der Kritikalität des TI-Flow-Fachdienstes und der gesetzlichen Verantwortung des AG für den E-Rezept-Fachdienst dem Security Governance Level 1 zugeordnet. Der AN muss daher die Vorgaben aus [gemTI_SEC_Standard] für den Security Governance Level 1 erfüllen.

Die Integration des AN in die Security Governance Prozesse des AG erfolgt im Rahmen des Onboardings des AN durch die Prozessprüfung sicherheitstechnische Eignung.

3.3.5.1 TI Security Standard

Die gematik nimmt gemäß § 311 Nr. 1c SGB V sowie § 331 SGB V ihre gesetzliche Verantwortung für die Steuerung und Überwachung der Informationssicherheit und des Datenschutzes innerhalb der Telematikinfrastruktur wahr. Hierzu hat die gematik mit dem TI-Security-Standard [gemTI_SEC_Standard] verbindliche Vorgaben in Form von Sicherheitsanforderungen definiert, deren Einhaltung durch beauftragte Unternehmen sowie Anbieter und Hersteller von Komponenten und Diensten der Telematikinfrastruktur verpflichtend ist. Die Verpflichtung zur Umsetzung der Controls ergibt sich aus der Anforderung A_27098 der Spezifikation Datenschutz- und Sicherheitsanforderungen an Anbieter [gemSpec_DS_Anbieter].

Diese normativen Anforderungen und Mitwirkungspflichten dienen der gematik als Grundlage zur Überprüfung und Aufrechterhaltung des erforderlichen Sicherheitsniveaus innerhalb der Telematikinfrastruktur. Die Einhaltung und wirksame Umsetzung wird in allen Phasen der Zusammenarbeit – von Beauftragung, über Onboarding, laufender Betrieb und off-boarding - kontinuierlich durch die gematik überwacht.

3.3.5.2 Controls des TI Security Standards

Der AN muss sämtliche für den TI-Flow geltenden Anforderungen, Controls, Nachweis- und Mitwirkungspflichten aus [gemTI_SEC_Standard] des vorgesehenen Security Governance Levels vollständig und fristgerecht umzusetzen sowie deren Einhaltung gegenüber der gematik nachzuweisen.

3.3.5.3 Prozessprüfung sicherheitstechnische Eignung

Die initiale Überprüfung der Einhaltung der definierten Anforderungen erfolgt im Rahmen einer Prozessprüfung zur sicherheitstechnischen Eignung. Die Umsetzung der Anforderungen des TI-Security-Standards sowie die Mitwirkung an der Prozessprüfung zur sicherheitstechnischen Eignung sind wesentliche und verpflichtende Bestandteile der zu erbringenden Leistungen. Der Auftragnehmer hat dem AG sämtliche hierfür erforderlichen Nachweise, Dokumentationen, Konzepte und sonstigen Liefergegenstände (z.B. Sicherheitskonzept, Notfallkonzept, Security Monitoring Konzept) fristgerecht bereitzustellen die vom AG im Rahmen der Prozessprüfung geprüft und freigegeben werden. ah

Die erfolgreiche Durchführung der Prozessprüfung zur sicherheitstechnischen Eignung dient als Nachweis, dass die organisatorischen, technischen und betrieblichen Voraussetzungen für einen sicheren Betrieb des TI-Flow innerhalb der Telematikinfrastruktur erfüllt werden. Die hierfür erforderliche Umsetzung der Controls des TI-Security-Standards ist zwingende Voraussetzung für die Feststellung der sicherheitstechnischen Eignung.

3.3.6 Sicherheitsgutachten HCC

Der AN muss ein Sicherheitsgutachten einreichen, das die Erfüllung der Anforderungen zur sicherheitstechnischen Eignung aus dem Anbietertypsteckbrief für den Anbieter HCC [gemAnbT_HCC_ATV] mit dem Prüfverfahren „Sicherheitsgutachten“ nachweist und den Vorgaben aus [gemRL_PruefSichEig_DS] entspricht.

Das Sicherheitsgutachten hat seinen Fokus auf der sicheren Betriebsumgebung, dem sicheren Rechenzentrumsbetrieb sowie auf den Prozessen, die der Aufrechterhaltung des Datenschutzes und der Informationssicherheit dienen.

Der AG nimmt das Gutachten entgegen und prüft dessen Vollständigkeit bzgl. der Anforderungslage, die Nachvollziehbarkeit der Prüfergebnisse und Bewertungen sowie die Angemessenheit der Prüfmethoden.

Erst nach erfolgreicher Prüfung wird das Gutachten vom AG freigegeben.

Das Gutachten muss in Gänze alle drei Jahre wiederholt erstellt werden. Das neue Gutachten muss vom AN vor Ablauf der drei Jahre an den AG übergeben werden.

Zudem muss der AN dem AG bei größeren Änderungen an der Betriebsumgebung oder den Betriebsprozessen ein Delta-Gutachten gemäß [gemRL_PruefSichEig_DS] vorlegen.

3.3.7 IT-Security Management Meetings

Für die Zusammenarbeit von AG und AN hinsichtlich sicherheitsrelevanter Themen sind regelmäßige Security Management Meetings durchzuführen. Diese finden grundsätzlich monatlich sowie bei Bedarf als Videokonferenz statt. Gegenstand der Meetings sind insbesondere Cyber-Defence-Themen, darunter

- die Bewertung der aktuellen Bedrohungslage auf Basis von Cyber Threat Intelligence einschließlich Medienmonitoring,
- die Behandlung von Schwachstellen,
- die Auswertung von Schwachstellenscans des AG und des AN,
- Erkenntnisse aus dem Security Monitoring (bspw. kritische Alerts und besondere Use-Cases) beim AN sowie
- aktuelle Sicherheitsvorfälle.

Im Rahmen eines regelmäßigen Technik-Checks werden technische Schnittstellen, die Aktualisierung vorhandener Assets (und anderer Informationen), geplante Weiterentwicklungen sowie erforderliche Troubleshooting-Maßnahmen behandelt.

Darüber hinaus umfassen die Meetings Themen des Bereichs Security Governance & Management, mit besonderem Blick auf

- den Status vereinbarter Security-SLAs,
- Aspekte des Partner- und Projektmanagements, darunter organisatorische Schnittstellen sowie die Planung von Workshops und Veranstaltungen in Abstimmung mit dem AN sowie

- Aktivitäten im Zusammenhang mit der Planung, Durchführung und Nachbereitung von Audits.

Im Bereich des Business Continuity Managements (BCM) werden geplante sicherheitsrelevante Change Requests sowie die Vorbereitung, Durchführung und Auswertung von Notfallübungen behandelt.

Zudem werden Themen aus dem Bereich Security Engineering & Architecture besprochen, wie

- Sicherheitsanalysen,
- Penetrationstests,
- Gutachten und
- die Spezifikation sicherheitsrelevanter Eigenschaften.

Für vertragliche Change Requests (jenseits erforderlicher sicherheitsrelevanter Changes) ist ein weiteres Meeting von AG und An einzurichten, das regelmäßig sowie bei Bedarf als Videokonferenz stattfindet. Gegenstand dieses Meetings ist die Erlangung einer Übersicht über aktuelle Change Requests sowie die Abstimmung dafür notwendiger Freigaben. In diesem Zusammenhang ist auch ein Change Advisory Board einzurichten.

3.3.8 Sicherheitsanalysen und Audits

Der AN muss gemäß [gemSpec_DS_Anbieter#A_27099] zusichern, dass der AG oder ein von ihm zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt ist, Audits und Sicherheitsanalysen (z. B. Penetrationstests) nach vorheriger Ankündigung durchzuführen; der AN muss diese aktiv unterstützen.

4 Durchführung

4.1 Phasen, Meilensteine und Liefertermine im Überblick

Die Leistungserbringung des AN ist in folgende Phasen unterteilt:

- Projektphase
- Betriebsphase

Der Projektphase sind Meilensteine zugeordnet. Ein Meilenstein gilt als erreicht, wenn alle diesem Meilenstein gem. Kapitel 4.3 zugeordneten Liefergegenstände vom AN umgesetzt, vom AG gemäß der jeweils für den Liefergegenstand vorgesehenen Prüfungsart überprüft und durch den AG freigegeben wurden. Soweit der Abschluss der Meilensteine eine Mitwirkung des AG durch Kenntnisnahme, Güteprüfung, Freigaben oder Abnahme beinhaltet, ergibt sich deren Inhalt aus Kapitel 5.3.3.

Die Aktivitäten zur Erreichung der Meilensteine sind nicht sequenziell zu verstehen. Die zeitliche Abfolge der Meilensteine wird durch den AG nur insofern vorgegeben, wie diese Abhängigkeiten unabdingbar notwendig sind (bspw. Freigabe der Produkte vor Beginn des Produktivbetriebs mit Echtdaten). Einige Meilensteine müssen zu den in Kapitel 4.2 vorgegebenen Zielterminen erreicht werden.

Die Dokumenten-basierten Liefergegenstände müssen in einem vom AG bereitgestellten Repository (s. Kapitel 5.2) bereitgestellt werden. Die Bereitstellung der Entwicklungs- und Testartefakte erfolgt in einem vom AG vorgegebenen Repository, welches bei dem AG oder bei dem AN liegen kann.

Sofern der AN Lieferungen und Leistungen auf Grundlage nicht freigegebener Konzepte erbringt und diese deshalb überarbeitet oder neu erbracht werden müssen, bspw. durch die Erstellung eigener Dokumente, trägt der AN sämtliche dadurch entstehende Mehraufwände. Es erfolgt keine Vergütung durch den AG. Insbesondere berechtigt dies den AN nicht, vereinbarte Termine oder Fristen zur Leistungserbringung zu verschieben.

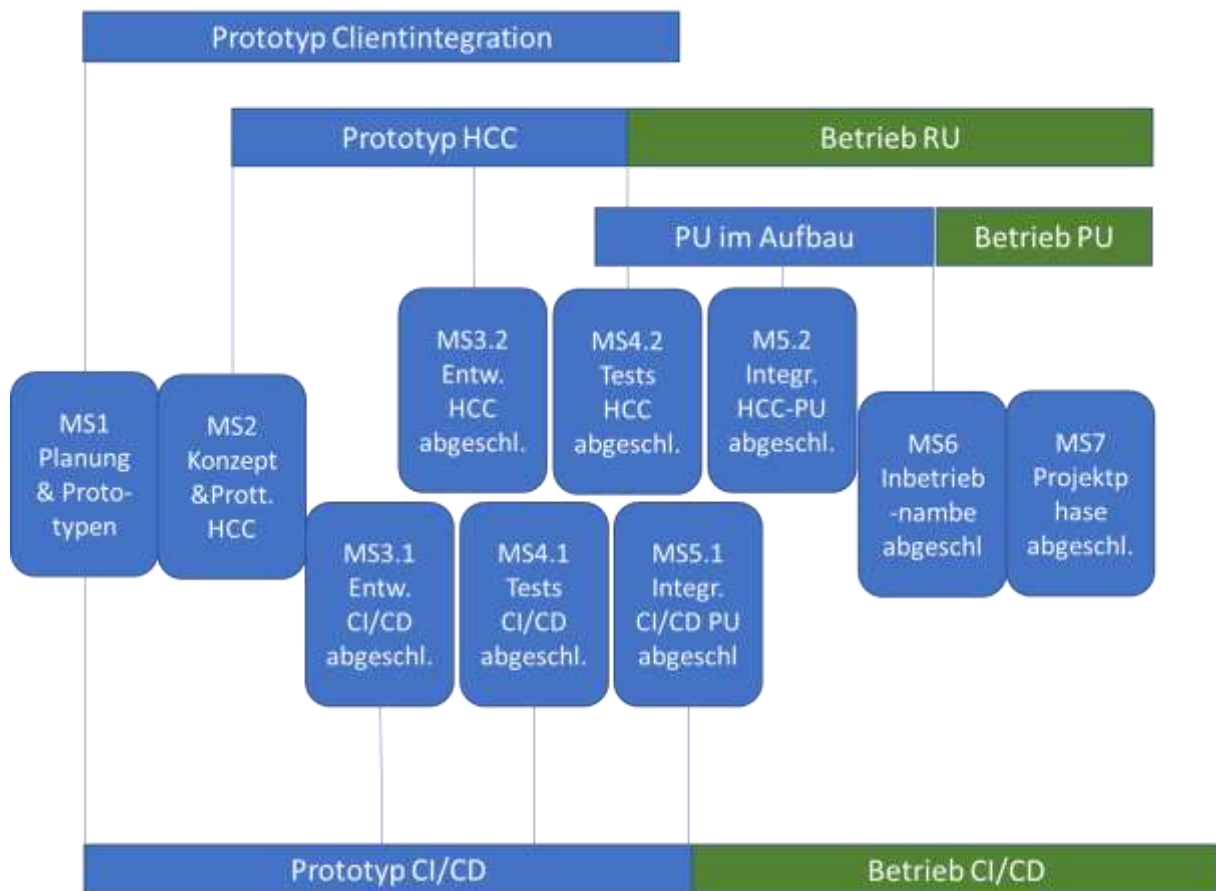


Abbildung 3: Phasen- und Meilensteinübersicht der Projektphase

4.2 Meilensteine mit verbindlichen Zielterminen

Der AN muss die nachfolgend aufgeführten Meilensteine spätestens zu den in Tabelle 5 angegebenen Zielterminen erreicht haben. Die übrigen Meilensteine können durch den AN eigenständig festgelegt werden und müssen im Projektplan eindeutig mit einem Zieltermin eingeplant werden.

Tabelle 5: Meilensteine mit Zielterminen

Bezeichnung	Zieltermin (spätestens)
MS1 Prototypen erstellt	15.07.2027
MS2 Planung und Konzeption abgeschlossen	10.09.2027
MS4.1 Herstellertests CI/CD-Plattform abgeschlossen	01.02.2028
MS4.2 Herstellertests HCC abgeschlossen	01.02.2028
MS6 Inbetriebnahme für die PU abgeschlossen	01.05.2028

4.3 Bereitstellung Liefergegenstände zu Meilensteinen

Der AN muss die Liefergegenstände als Kontrollpunktlieferung bzw. zur Kenntnisnahme oder Güteprüfung gem. Kapitel 5.3.3 dem AG bereitstellen. Die Bereitstellung muss zu den zuvor aufgeführten Meilensteinen gemäß der Tabelle 5 erfolgen.

Legende: KP: Kontrollpunkt / KN: Kenntnisnahme / GP: Güteprüfung

Tabelle 6: Übersicht der Liefergegenstände zu den Meilensteinen

LG.- Nr.	Liefergegenstand	Ref.	MS 1	MS 2	MS 3.1	MS 4.1	MS 5.1	MS 3.2	MS 4.2	MS 5.2	MS 6	MS 7
	Prototyp CI/CD	3.1.4.15	GP									
	Dokumentation Prototyp CI/CD-Plattform	3.1.4.17		GP								
	Prototyp Clientintegration	3.1.3.1	GP									
	Konzept zum Projektvorgehen	5.5.1	KP	GP								
	Projektplan	5.5.1	KP	GP								
	Umsetzungskonzept CI/CD	3.1.2.2	KP	GP								
	Umsetzungskonzept HCC	3.1.2.1	KP	GP								
	Schnittstellenbeschreibung HCC	3.1.2.1	KP	GP								
	Testkonzept CI/CD	3.1.2.3	KP	GP								
	Testkonzept HCC	3.1.2.3	KP	GP								
	CI/CD-Freigabeumgebung	3.1.4.15		GP								
	Prototyp HCC	3.1.3.2		GP								

LG.-Nr.	Liefergegenstand	Ref.	MS 1	MS 2	MS 3.1	MS 4.1	MS 5.1	MS 3.2	MS 4.2	MS 5.2	MS 6	MS 7
	Anbietererklärung zur funktionalen, betrieblichen und sicherheitstechnischen Eignung	3.1.3.7		KN								
	Servicekatalog	3.2.2	KP	GP								
	ITSM-Konzept	3.2.3	KP	GP								
	SLA-Konzept	3.2.4	KP	GP								
	Governance-Konzept	3.2.5	KP	GP								
	Betriebskonzept CI/CD	3.1.2.5	KP	GP								
	Sicherheitsgutachten SW-Entwicklungsprozesse	3.3.2				GP						
	Entwicklungsartefakte CI/CD-Plattform	3.1.2.2		KP	KP	KP	GP					
	Dokumentation CI/CD	3.1.4.17		KP	KP	KP	GP					
	Betriebshandbuch CI/CD	3.1.4.16			KP	KP	GP					
	Herstellererklärung zur funktionalen und sicherheitstechnischen Eignung	3.1.3.7						KN				
	Trust Domain für Test und Entwicklungstätigkeiten	3.1.2.1.1						KN				
	Trust Domain PU	3.1.2.1.1								KN		
	Nachweis der erfolgreichen Funktionsprüfung der Monitoring- und Alarmierungsmechanismen	3.1.7.4							GP			
	Nachweis der Datensicherung und Wiederherstellung	3.1.7.6							GP			
	Nachweis der Notfall- und Wiederanlauffähigkeit	3.1.7.7							GP			

LG.-Nr.	Liefergegenstand	Ref.	MS 1	MS 2	MS 3.1	MS 4.1	MS 5.1	MS 3.2	MS 4.2	MS 5.2	MS 6	MS 7
	HSM-Proxy	3.1.3.3		KP				KP	GP			
	Entwicklungsartefakte HCC	3.1.3.4		KP				KP	KP	GP		
	Dokumentation HCC	3.1.3.5		KP				KP	KP	GP		
	Referenz-Container	3.1.5.1		KP				KP	GP			
	Vorlage der Vereinbarung über die gemeinsame Verantwortung nach Art. 26 DSGVO	3.2.8.2									KN	
	Notfallkonzept	3.2.8.4									KN	
	Sicherheitskonzept	3.2.8.1									KN	
	Security Monitoring Konzept	3.2.8.3		KP							KN	
	Zertifizierungen und Testate gemäß [gemSpec_HCC]	gemSpec_HCC, Kapitel 9									KN	
	Prozessprüfung sicherheitstechnische Eignung	3.3.5.3									KN	
	Weitere Controls des TI Security Standards	3.3.5.2									KN	
	Produktgutachten HCC	3.3.3									GP	
	Sicherheitsgutachten HCC	3.3.6									GP	
	Betriebsbereitschaftsnachweis	3.1.7.8									GP	
	Übergabestrategie HCC-Cloud	3.1.8.1									KP	GP
	Übergabestrategie CI/CD-Plattform	3.1.8.2									KP	GP
	Projektabschlussbericht	5.5.1										GP

2026-0030 TI-Flow - Los 2

Anlage-02 Leistungsbeschreibung Los 2



4.4 MS1: Prototypen erstellt

- Freigabe des Prototypen CI/CD nach Kap 3.1.4.15
- Freigabe des Prototypen zur Clientintegration nach Kap 3.1.3.1

4.5 MS2: Planung und Konzeption abgeschlossen

- Erstellung eines Prototypen HCC nach Kap 3.1.3.2
- Finalisierung des Umsetzungskonzepts HCC mit den Erkenntnissen des Prototypen HCC.
- Finalisierung des Umsetzungskonzepts CI/CD
- Die TrustDomain für Test und Entwicklungstätigkeiten ist eingerichtet
- Gematik und LOS1 können zusätzlich zu den zu der Laufzeitumgebung aus MS1 RU- oder RU-DEV-Instanzen für Entwicklung und Integrationstests des TI-Flow-Dienstes abrufen.
- Der AN stellt eine CI/CD-Freigabeumgebung bereit, über die der AG neue Funktionen der CI/CD-Plattform testen kann.
- Erweiterungen der CI/CD-Plattform wurden auf der CI/CD-Freigabeumgebung bereitgestellt, vom AG getestet und erfolgreich in die CI/CD-Plattform integriert, so dass er Workloads in den Prototypen HCC deployen kann. Ab diesem Meilenstein werden regelmäßig iterative, funktionale Erweiterungen von CI/CD-Plattform und HCC vom AN mit der entsprechenden Release Notes bereitgestellt, die der AG oder Los1 in die CI/CD-Plattform und die HCC-Cloud übernehmen kann.
- Freigabe des aktualisierten Projektdurchführungskonzepts und Projektplans aus der Angebotsphase als Baseline für die Projektphase. Beide Liefergegenstände werden während der Projektphase fortgeschrieben

4.6 MS3.1: Entwicklung CI/CD-Plattform abgeschlossen

Der AN stellt die CI/CD-Plattform mit funktional vollständiger Umsetzung der Schnittstellen zu den Diensten der HCC-Vertrauensräume bereit, so dass gematik und Los1 Pipelines erstellen, Testläufe durchführen und Entwicklungsstände des TI-Flow-Fachdienstes in der HCC-Cloud deployen kann.

4.7 MS3.2: Entwicklung HCC abgeschlossen

Der AN stellt die vollständige HCC-Cloud bereit, , so dass die gematik und LOS1 RU oder RU-DEV Instanzen für Entwicklung und Integrationstests des TI-Flow-Dienstes abrufen kann. MS3.1: "Entwicklung CI/CD-Plattform abgeschlossen" ist Voraussetzung für diesen Meilenstein

4.8 MS4.1: Hersteller-Tests CI/CD-Plattform abgeschlossen

Der AN stellt die funktional vollständige und vollständig getestete Umsetzung seiner Entwicklung der CI/CD-Plattform bereit.

Der AN wird die erforderlichen Nachweise für die produktive Freigabe der CI/CD-Plattform erbringen und das Produkt als Referenz in RU/RU-DEV bereitstellen. Als Voraussetzung muss die Testphase EvT erfolgreich abgeschlossen sein.

4.9 MS4.2: Hersteller-Tests HCC abgeschlossen

Der AN stellt die funktional vollständige Umsetzung und vollständig getestete der HCC Funktionalität bereit.

Der AN wird die erforderlichen Nachweise für die produktive Freigabe des HCC-Services erbringen und das Produkt als Referenz in RU/RU-DEV bereitstellen. Als Voraussetzung muss die Testphase EvT erfolgreich abgeschlossen sein.

Diese Version bildet die Grundlage für die Tests des Auftraggebers und die sicherheitstechnische Begutachtung. Voraussetzung für die Freigabe dieses Meilensteins ist die Freigabe von MS4.1: "Hersteller-Tests CI/CD-Plattform abgeschlossen".

4.10 MS5.1: Integration CI/CD-Plattform mit der PU abgeschlossen

Der AN hat die Leistungen erbracht, die nach dem Umsetzungskonzept CI/CD von ihm für die Anbindung an die PU notwendig sind. Der AG führt daraufhin mit Unterstützung des AN die Konfiguration aus, so dass ein Deployment in die PU möglich wird.

4.11 MS5.2: Integration HCC auf PU abgeschlossen

Auftragnehmer und Auftraggeber haben den Vertrauensraum der PU initialisiert und die Ressourcen für den Betrieb des TI-Flow-Fachdienstes angelegt. Der Auftraggeber testet die Funktionalität der HCC-Cloud-Services unter Nutzung der Komponente ZETA-Guard und des Referenz-Containers. Voraussetzung für die Freigabe dieses Meilensteins ist die Freigabe von MS5.1: "Integration CI/CD-Plattform mit der PU abgeschlossen".

4.12 MS6: Inbetriebnahme für die PU abgeschlossen

Die Voraussetzungen für die produktive Nutzung der HCC-Cloud sind erreicht. Funktionalität und Interoperabilität der HCC-Cloud und der CI/CD-Plattform wurde hergestellt, durch den AN nachgewiesen und durch den AG überprüft. Die Sicherheitsnachweise Produktgutachten HCC und Sicherheitsgutachten HCC wurden dem AG vorgelegt und durch den AG freigegeben. Die operative Betriebsbereitschaft wurde erreicht und gemäß Kapitel 3.1.7 AP6 gegenüber dem AG nachgewiesen und von diesem freigegeben. Mit Freigabe des MS6 wird die Inbetriebnahme der HCC-Cloud abgeschlossen, die Produktivfreigabe erteilt und es beginnt die Betriebsphase und der Regelbetrieb. Der AG verarbeitet nun Change Request von Diensteanbietern zum Deployment von HCC-Diensten und zur Identitätsvergabe aus dem produktiven Vertrauensraum der Telematikinfrastruktur.

4.13 MS7: Projektphase abgeschlossen

Zum Projektabschluss führt der AN einen Lessons Learned Workshop mit dem AG durch und dokumentiert die Ergebnisse im Projektabschlussbericht (s. Kapitel 5.5.1).

Die Projektphase gilt als abgeschlossen, sobald alle Liefergegenstände und alle Meilensteine umgesetzt und freigegeben sowie sämtliche Leistungen der Projektphase erbracht worden sind. Bereits freigegebene Konzepte aus Kapitel 3.1.2, die im Laufe der Projektphase nach Freigabe angepasst worden sind, müssen erneut zur Freigabe vorgelegt werden. Die Erreichung des MS7 ist Voraussetzung für die vertragliche Gesamtabnahme des Gesamtsystems in der PU.

5 Übergreifende Vorgaben und Leistungen

5.1 Souveränitätsanforderungen

Zur Vermeidung kritischer technischer, rechtlicher und wirtschaftlicher Abhängigkeiten bei der Bereitstellung und dem Betrieb der Infrastruktur für den TI-Flow-Fachdienst muss der Auftragnehmer die nachstehend festgelegten Anforderungen an die digitale Souveränität während der gesamten Vertragslaufzeit einhalten.

Der Auftraggeber verfolgt dabei insbesondere die Ziele

- die selbstbestimmte Nutzung der Cloud-Infrastruktur für den TI-Flow-Fachdienst sicherzustellen,
- die Abhängigkeit von einzelnen Herstellern, Lieferanten, Staaten oder sonstigen Dritten zu minimieren,
- die Betriebsfähigkeit der Infrastruktur auch in Krisen-, Störungs- und Disconnect-Szenarien sicherzustellen,
- Schutz vor extraterritorialen Zugriffsrechten zu gewährleisten sowie
- Anbieter- und Technologiewechsel dauerhaft mit vertretbarem technischem und wirtschaftlichem Aufwand zu ermöglichen.

Bei den nachfolgenden Anforderungen handelt es sich um Ausführungsbedingungen gem. § 128 Abs. 2 GWB.

Ergänzend zu den nachfolgenden Anforderungen ist das vom Auftragnehmer mit Angebotsabgabe einzureichende Souveränitätskonzept verbindlicher Bestandteil des Vertrags. Die darin beschriebenen technischen, organisatorischen und rechtlichen Maßnahmen zur Gewährleistung der digitalen Souveränität sind während der gesamten Vertragslaufzeit einzuhalten.

Die nachfolgenden Anforderungen wurden unter Berücksichtigung der Grundsätze des BSI C3A und des Union Assurance Level 3 (UAL3) des von der EU-Kommission vorgeschlagenen Cloud and AI Development Act (CADA) entwickelt. Maßgeblich für die Leistungspflichten des Auftragnehmers sind ausschließlich die in dieser Leistungsbeschreibung ausdrücklich festgelegten Anforderungen.

5.1.1 Souveränitätskonzept

Der Auftragnehmer muss das mit Angebotsabgabe eingereichte Souveränitätskonzept während der Vertragslaufzeit aktuell halten und hat etwaig notwendig werdende Änderungen dem Auftraggeber unverzüglich anzuzeigen.

Das Souveränitätskonzept muss mindestens folgende Inhalte umfassen:

- Governance-, Eigentums- und Kontrollstrukturen,
- Darstellung bestehender Drittstaaten- und Jurisdiktionsrisiken,
- Maßnahmen zum Schutz vor extraterritorialen Zugriffen,
- Konzept zur Sicherstellung des EU-basierten Betriebs, der Betriebsautonomie sowie der Disconnect-Fähigkeit,
- Analyse kritischer technischer, organisatorischer und wirtschaftlicher Abhängigkeiten,
- Lieferketten- und Subunternehmerkonzept,

5.1.2 Strategische und rechtliche Souveränität

5.1.2.1 Eigentums- und Kontrollstrukturen

Folgende Souveränitätsanforderungen sind vom Auftragnehmer einzuhalten:

- Jurisdiktion: Der Auftragnehmer muss unter EU-Jurisdiktion operieren – mit Vertragssteuerung und Streitbeilegung unter EU-Recht.
- Hauptsitz: Der Auftragnehmer muss seinen eingetragenen Hauptsitz in der EU haben.
- Kontrolle: Der Auftragnehmer muss effektiv durch ein oder mehrere EU-Unternehmen kontrolliert werden. Der Auftragnehmer muss sicherstellen, dass die effektive Kontrolle für den Auftraggeber transparent ist. Als Kontrolle gilt insbesondere die Möglichkeit, unmittelbar oder mittelbar maßgeblichen Einfluss auf strategische Entscheidungen, Geschäftsführung oder die Ausübung von Gesellschafterrechten auszuüben.
- Informationspflicht: Der Auftragnehmer muss den Auftraggeber mindestens neunzig (90) Tage im Voraus über tatsächliche Änderungen informieren, die die Kontrolle über den Auftragnehmer betreffen und die die Einhaltung der vertraglichen Souveränitätsanforderungen oder der zugrunde gelegten C3A-Kriterien beeinträchtigen oder untergraben könnten – einschließlich wesentlicher Änderungen an Eigentümerschaft, Anteilsverhältnissen oder Governance-Beziehungen des Auftragnehmers.

Der Auftragnehmer hat zudem folgende Informationen vollständig offenzulegen und den Auftraggeber über etwaige Änderungen unverzüglich zu informieren:

- Konzernstruktur,
- Eigentümerstruktur,
- wirtschaftlich Berechtigte,
- Kontroll- und Weisungsrechte,
- sämtliche für die Leistungserbringung relevanten Mutter-, Schwester- und Tochtergesellschaften.

Darüber hinaus sind sämtliche für die Leistungserbringung relevanten Beteiligungs- und Kontrollverhältnisse offenzulegen, soweit diese Einfluss auf die digitale Souveränität oder die Leistungserbringung haben können.

5.1.2.2 Schutz vor Drittstaateneinflüssen

Folgende Souveränitätsanforderungen sind vom Auftragnehmer einzuhalten:

- **Risikobewertungspflicht:** Der Auftragnehmer muss mindestens einmal jährlich alle Nicht-EU-Gesetze identifizieren, die unmittelbar mit den bereitgestellten Cloud-Diensten zusammenhängen und grenzüberschreitende Auswirkungen auf die Verfügbarkeit von Cloud-Diensten sowie die Vertraulichkeit und Integrität auftraggeberbezogener Daten haben. Darüber hinaus muss er eine strukturierte Risikobewertung durchführen, um die aus diesen Gesetzen resultierenden Risiken zu bewerten.
- **Verfahrensdokumentationspflicht:** Der Auftragnehmer muss Verfahren dokumentieren, die eine unabhängige Überprüfung der Einhaltung der Souveränitätsanforderungen sowie der zugrunde gelegten C3A-Kriterien mittels eines Audits ermöglichen.
- **Testatspflicht:** Soweit für die vertragsgegenständlichen Leistungen ein Audit- und Testatverfahren nach dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geplanten C3A-Audit- und Testatverfahren oder einem dieses ersetzenden bzw. fortentwickelnden, inhaltlich vergleichbaren Verfahren verfügbar ist, hat der Auftragnehmer die hierfür erforderlichen Nachweise und Verfahrensdokumentationen vorzuhalten und für die vertragsgegenständlichen Leistungen ein entsprechendes gültiges Testat vorzulegen.

Der Auftragnehmer muss zudem darlegen:

- welchen Drittstaatenregelungen (Rechtsvorschriften oder behördliche Zugriffsbefugnisse von Staaten außerhalb der EU bzw. des EWR) er oder mit ihm verbundene Unternehmen unterliegen,
- welche Auswirkungen sich daraus auf die Leistungserbringung ergeben können,
- welche technischen, organisatorischen und rechtlichen Maßnahmen zur Verhinderung oder Abwehr extraterritorialer Zugriffe implementiert wurden.

Eine rein vertragliche Risikoanalyse genügt dabei nicht. Der Auftragnehmer hat nachweisbare technische und organisatorische Maßnahmen zum Schutz vor unberechtigten Datenzugriffen durch Drittstaaten nachzuweisen.

5.1.2.3 Änderungen der Souveränitätsarchitektur

Änderungen an Komponenten, Prozessen, Organisationsstrukturen oder Lieferkettenbestandteilen, welche Auswirkungen auf die digitale Souveränität der Leistung haben können, sind dem Auftraggeber unverzüglich schriftlich anzuzeigen.

Dies umfasst insbesondere Änderungen bezüglich:

- Eigentümer- oder Kontrollstrukturen,
- privilegierter Zugriffsmodelle,
- Rechenzentrumsstandorte,
- Schlüsselerwaltungs- und Kryptographiesysteme,
- IAM-Systeme,
- Netzwerk- und Sicherheitsarchitekturen,
- kritischer Plattformkomponenten,
- kritischer Unterauftragnehmer.

Soweit Änderungen unter die Anforderung "Informationspflicht" (vgl. Kapitel 5.1.2.1) fallen, erfolgt die Anzeige grundsätzlich mindestens neunzig (90) Tage vor deren Wirksamwerden.

Änderungen, die zu einer Unterschreitung des vertraglich geforderten Souveränitätsniveaus führen können, bedürfen, mit Ausnahme von Änderungen der Eigentümer- oder Kontrollstrukturen, der vorherigen Zustimmung des Auftraggebers. Änderungen von Eigentümer- oder Kontrollstrukturen, die zu einer Unterschreitung der Anforderungen gem. Kapitel 5.1.2.1 führen oder führen können, stellen eine wesentliche Änderung der Souveränitätsarchitektur dar und berechtigen den Auftraggeber zur erneuten Bewertung der Souveränitätsanforderungen sowie zur Ausübung vertraglich vorgesehener Rechte. Der Auftragnehmer hat bei Änderungen, die das zugesicherte Souveränitätsniveau prognostisch beeinträchtigen und denen der Auftraggeber nicht zustimmt, unverzüglich entsprechende Gegenmaßnahmen mit dem Auftraggeber abzustimmen und umzusetzen.

5.1.3 EU-basierter Betrieb der Cloud-Infrastruktur

Der Auftragnehmer verpflichtet sich, den vollständigen operativen Cloud-Betrieb und die Administration sämtlicher eingesetzter Plattform- und Infrastrukturkomponenten eigenständig innerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) zu gewährleisten.

Abhängigkeiten hinsichtlich Produktentwicklung, -pflege, Fehlerbehebung, Sicherheitsupdates oder Herstellersupport durch außerhalb der EU/des EWR ansässige Hersteller sind nur zulässig, soweit

- der ordnungsgemäße Betrieb der Cloud-Infrastruktur hierdurch nicht beeinträchtigt wird,
- keine unmittelbare betriebliche Abhängigkeit für den laufenden Betrieb besteht und
- die Betriebsfähigkeit im Falle eines Disconnects gemäß Kapitel 5.1.3.1 gewährleistet bleibt.

Der Auftragnehmer stellt sicher, dass sämtliche Betriebs-, Wartungs-, Support- und Administrationsleistungen ausschließlich durch Personen erbracht werden, die ihren Arbeitsort innerhalb der EU/des EWR haben und die organisatorisch einer Rechtseinheit innerhalb der EU/des EWR zugeordnet sind. Das umfasst insbesondere

- Incident-Management,
- Problem-Management,
- Change-Management,
- Sicherheitsüberwachung,
- Sicherheitsadministration,
- Patch- und Release-Management,
- Identitäts- und Berechtigungsmanagement,
- technische Eskalationsprozesse sowie
- privilegierte Administrationszugriffe.

Sämtliche Personen mit logischem oder physischem Zugang zu den für den Betrieb der Cloud-Plattform eingesetzten Infrastrukturen, sämtliche Personen mit privilegierten Administrationsrechten, sämtliche Personen mit Verantwortung für den Kundensupport sowie sämtliche Personen, die wesentliche Management-, Steuerungs- oder Entscheidungsbefugnisse hinsichtlich des Betriebs der vertragsgegenständlichen Cloud-Dienste besitzen, müssen ihren Arbeitsort innerhalb der EU oder des EWR haben und organisatorisch einer Rechtseinheit innerhalb der EU oder des EWR zugeordnet sein.

Eine Nutzung privilegierter Zugriffsrechte durch Personal außerhalb der EU/des EWR ist unzulässig.

Der Auftragnehmer hat organisatorische und technische Maßnahmen zu implementieren, die sicherstellen, dass ein administrativer Zugriff auf Systeme für den Betrieb der Cloud-Plattform ausschließlich über Zugangswege innerhalb der EU oder des EWR erfolgt. Ein administrativer Zugriff von Standorten außerhalb der EU oder des EWR ist technisch zu

unterbinden oder auf eng definierte und dokumentierte Ausnahmeszenarien mit zusätzlichen Autorisierungs- und Überwachungsmaßnahmen zu beschränken.

Der Auftragnehmer gewährleistet für den Betrieb der Cloud-Plattform redundante und voneinander unabhängige Konnektivität. Bei Ausfall eines Konnektivitätsanbieters sind geeignete alternative Verbindungen vorzuhalten, um die Einhaltung der vertraglich vereinbarten Betriebs- und Verfügbarkeitsanforderungen sicherzustellen. Mindestens einer der für den Betrieb wesentlichen Konnektivitätsanbieter muss seinen Sitz innerhalb der EU oder des EWR haben und auch im Disconnect-Fall für den Betrieb nutzbar bleiben.

5.1.3.1 Disconnect-Fähigkeit

Der Auftragnehmer hat im Souveränitätskonzept nachvollziehbar darzulegen, wie die Betriebsfähigkeit der Plattform im Falle einer dauerhaften Unterbrechung sämtlicher Verbindungen zu Organisationseinheiten, Dienstleistern oder Infrastrukturen außerhalb der EU aufrechterhalten wird.

Der Auftragnehmer gewährleistet, dass die bereitgestellte Cloud-Plattform im Falle eines solchen Disconnect innerhalb der EU ohne wesentliche Beeinträchtigung der vertraglich geschuldeten Betriebsfähigkeit weiterbetrieben werden kann. Hierfür dürfen keine für den Betrieb zwingend erforderlichen Leistungen, Infrastrukturkomponenten, Verwaltungsfunktionen oder Steuerungsmechanismen außerhalb der EU erforderlich sein.

Das umfasst insbesondere:

- zentrale Administrationsfunktionen,
- Authentifizierungs- und Autorisierungsdienste,
- Schlüssel- und Zertifikatsmanagement,
- Monitoring- und Sicherheitsfunktionen, einschließlich Security Operations Center (SOC)
- Lizenzierungs- und Aktivierungsmechanismen,
- Betriebs- und Wartungsprozesse.

Der Auftragnehmer muss sicherstellen, dass Security-Operations-Center-(SOC)-Fähigkeiten für die angebotenen Cloud-Dienste innerhalb der EU etabliert und betrieben werden. Im Falle eines Disconnects muss ein eigenständiges und gleichwertiges SOC innerhalb der EU verfügbar bleiben.

Alle Software-Updates und Betriebsdaten, die den Cloud-Dienst betreffen, müssen in einem gesicherten Netzwerkbereich empfangen, autorisiert und validiert werden, der vom Auftragnehmer verwaltet und kontrolliert wird. Updates müssen auf bekannte Schwachstellen geprüft werden, vollständige Dokumentation enthalten und auf Basis eines kontrollierten Change-Management-Prozesses eingespielt werden.

Die Disconnect-Fähigkeit setzt nicht voraus, dass während des Disconnect-Falls neue Softwarestände oder neue Produktversionen bereitgestellt werden können. Erforderlich ist, dass der Betrieb der Plattform mit dem zum Zeitpunkt des Disconnects vorhandenen Softwarestand aufrechterhalten werden kann.

5.1.4 Datensouveränität

5.1.4.1 Datenlokalisierung

Folgende Datenarten dürfen die EU nicht verlassen:

- Nutzdaten,
- Konfigurationsdaten,
- Backup-Daten,
- Metadaten mit Personenbezug oder Metadaten, aus denen Personenbezüge hergestellt werden könnten,
- Telemetriedaten,
- Audit- und Protokolldaten,
- Supportdaten.

Das gilt für Normalbetrieb, Wartungsbetrieb, Störungsbehebung und Notfallbetrieb.

Folgende Souveränitätsanforderungen sind zudem vom Auftragnehmer einzuhalten:

- Jeglicher Austausch von Cloud-Daten (Kundendaten, abgeleitete Daten, Kontodaten) zwischen dem Auftragnehmer und Dritten muss stets vom Auftragnehmer überwacht, kontrolliert und protokolliert werden. Der Auftragnehmer hat dafür einen dokumentierten Prozess zu etablieren (mindestens jährlich zu aktualisieren) und zu dokumentieren, welche Daten an welche Partei fließen. Diese Dokumentation muss dem Auftraggeber zugänglich gemacht werden. Das Austauschformat muss klar definiert und dokumentiert sein
- Der Auftragnehmer muss alle Datenaustausche zwischen ihm und Dritten dokumentieren, definieren und mittels eines Datenflussdiagramms visualisieren. Der Datenaustausch muss ausschließlich über bekannte Gateways erfolgen. Die Dokumentation muss Datenursprünge, -ziele, Transportprotokolle, Datentypen und Sicherheitsmechanismen eindeutig benennen und mindestens jährlich aktualisiert werden

Die vorstehenden Anforderungen zum Datenaustausch mit Dritten berechtigen nicht zur Verarbeitung, Speicherung oder Übermittlung der in dieser Ziffer genannten Daten außerhalb der EU.

5.1.4.2 Datenzugriff und Daten-Portabilität

Der Auftragnehmer gewährleistet dem Auftraggeber während der gesamten Vertragslaufzeit uneingeschränkten, unmittelbaren und diskriminierungsfreien Zugriff auf sämtliche dem Auftraggeber zuzuordnenden und im Rahmen der Leistungserbringung verarbeiteten Daten. Ausgenommen sind von der Workload verarbeitete Daten sowie durch ein HSM geschützte und durch HCC verwaltete Schlüssel. Für die von der Workload verschlüsselt gespeicherten Daten hat der Auftraggeber das Recht, eine sichere Migration zu einem anderen Anbieter zu veranlassen. Diese kann mittels Funktionalitäten der Workload über den HCC-Dienst erfolgen, aber auch auf anderen sicheren Wegen. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der sicheren Migration zu einem anderen Anbieter zu unterstützen.

Der Auftraggeber muss jederzeit in der Lage sein,

- Daten einzusehen,
- Daten zu exportieren,
- Daten in maschinenlesbaren Standardformaten bereitzustellen,
- Daten auf Drittsysteme zu übertragen,
- Daten vollständig zurückzuführen und
- Daten löschen zu lassen.

Zugriff, Export, Übertragung und technische Portabilität der Daten müssen innerhalb der EU vollständig gewährleistet sein, ohne dass hierfür Ressourcen, Dienste oder Systeme außerhalb der EU betrieblich erforderlich werden.

Proprietäre technische Hürden außerhalb von HCC, die einen Wechsel des Auftragnehmers oder der Plattform wesentlich erschweren, sind unzulässig.

5.1.4.3 Kryptographische Souveränität

Der Auftragnehmer muss für die bereitgestellte Cloud-Plattform mindestens bereitstellen:

- Verwaltung kryptographischer Schlüssel ausschließlich innerhalb der EU,
- technische Kontrolle der Schlüssel durch den Auftraggeber im Rahmen der Regelungen zum Umgang mit Schlüsseln von HCC.

Der Auftragnehmer darf keinen unbeaufsichtigten Zugriff auf kryptographische Schlüssel besitzen.

5.1.5 Lieferketten- und Infrastruktursouveränität

5.1.5.1 Dokumentation

Der Auftragnehmer verpflichtet sich, sämtliche für den Betrieb, die Administration, die Weiterentwicklung und die Migration der Cloud-Infrastruktur erforderlichen technischen und betrieblichen Dokumentationen (einschließlich etwaiger Quellcodes, soweit sie dem Auftragnehmer zur Verfügung stehen) während der gesamten Vertragslaufzeit innerhalb der EU verfügbar zu halten.

Das umfasst insbesondere:

- Systemdokumentationen,
- Architekturübersichten,
- Betriebshandbücher,
- Sicherheitskonzepte,
- Schnittstellenbeschreibungen,
- Datenmodelle,
- Migrations- und Exit-Dokumentationen.

Die Dokumentationen sind in deutscher oder englischer Sprache bereitzustellen und aktuell zu halten. Die Dokumentationen müssen so ausgestaltet sein, dass ein qualifizierter Dritter den Betrieb der bereitgestellten Cloud-Plattform übernehmen kann.

5.1.5.2 Transparenz der Lieferkette

Der Auftragnehmer hat sämtliche für die Leistungserbringung relevanten Unterauftragnehmer, Lieferanten und sonstige Dritte mit wesentlichem Einfluss auf Betrieb, Sicherheit oder Souveränität der Cloud-Plattform offenzulegen.

Das umfasst insbesondere:

- Infrastrukturprovider,
- Rechenzentrumsbetreiber,
- Netzbetreiber,
- Softwarelieferanten (für Komponenten der Trusted Computing Base, insbesondere HCC-Hosts und - Services),
- Sicherheitsdienstleister,
- Supportdienstleister.

Für jeden Unterauftragnehmer sind anzugeben

- Bezeichnung des Unternehmens,
- Art der erbrachten Leistung,
- Land des Leistungserbringungsortes,
- bestehende privilegierte oder administrative Zugriffsmöglichkeiten,
- Bedeutung der Leistung für den Betrieb der HCC-Plattform

Änderungen sind dem Auftraggeber vorab anzuzeigen und bedürfen für Leistungen, die qualitativ oder quantitativ für die HCC- und CI/CD-spezifischen Leistungsbestandteile wesentlich sind, der vorherigen Zustimmung des Auftraggebers. Wesentlich sind insbesondere Änderungen, die Auswirkungen auf die Betriebsfähigkeit, Informationssicherheit, Datenlokalisierung oder die Einhaltung der Souveränitätsanforderungen haben können.

5.1.5.3 Hardware

Der Auftragnehmer hat Transparenz über die Herkunft der für die Leistungserbringung eingesetzten kritischen Hardware-Komponenten und deren Lieferketten herzustellen.

Der Auftragnehmer hat geeignete Maßnahmen zum Management von Lieferkettenrisiken vorzuhalten und kritische Abhängigkeiten von einzelnen Herstellern, Staaten oder einzelnen Lieferketten im Souveränitätskonzept darzustellen.

Hardware- oder Infrastrukturkomponenten, deren Einsatz nach unionsrechtlichen, nationalen sicherheitsrechtlichen oder behördlichen Vorgaben ausgeschlossen ist, dürfen nicht verwendet werden.

5.1.5.4 Software-Lieferkette

Der Auftragnehmer hat auf aktuellem Stand vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zur Verfügung zu stellen:

- eine Software Bill of Materials (SBOM) (für Komponenten der Trusted Computing Base, insbesondere HCC-Hosts und - Services),
- Dokumentationen sicherheitskritischer Komponenten,
- Herkunftsnachweise sicherheitskritischer Softwarebestandteile,
- Nachweise über Schwachstellenmanagement-Prozesse.

5.1.6 Technologische Souveränität und Exit-Fähigkeit/ Vermeidung von Vendor Lock-in

Der Auftragnehmer hat nachzuweisen, dass Daten mit vertretbarem Aufwand auf alternative Plattformen migriert werden können, und er hat die Vorgaben zum Exit und Betreiberwechsel (vgl. Kapitel 3.2.5.3) einzuhalten.

Hierfür sind bereitzustellen:

- Exportfunktionen,
- Migrationswerkzeuge,
- Dokumentation der Plattformdienste,
- Dokumentation proprietärer Erweiterungen.

5.2 Beistellungen des Auftraggebers

Im Rahmen der Durchführung stellt der AG dem AN die für die termin- und leistungsgerechte Abwicklung der Beauftragung benötigten Beistellungen zur Verfügung.

Die insofern hier benannten Beistellungen des AG und von Dritten sind abschließend. Der AN bestätigt mit der verbindlichen Angebotsabgabe, dass er mit diesen Beistellungen und Mitwirkungen in der Lage ist, seine vertraglichen Verpflichtungen vollständig und vertragskonform zu erfüllen.

Stellt der AN fest, dass eine Beistellung nicht für den vertraglichen Verwendungszweck geeignet ist, so hat er dies unverzüglich dem AG mitzuteilen und entsprechende Abhilfemaßnahmen vorzuschlagen und mit dem AG abzustimmen.

Die im Folgenden genannten Beistellungen sind durch den AG zur Verfügung zu stellen.

- Zero Trust Access
 - Zero Trust (ZETA) ZETA Guard (OCI Images)
 - Dokumentation ZETA Guard (ZETA-Produkthandbuch)
- TI-Flow Policy über ZETA Artifact Registry
 - Referenzimplementierung ZETA-Client
 - OCI Images in der ZETA Artifact Registry
 - gematik Endpunkte für BDE, TI SIEM
 - ZETA-Testumgebung als OpenSource
- Bereitstellung notwendiger Zugänge und Berechtigungen zum Workspace für die Übergabe von Dokumentation im SharePoint
- Bereitstellung notwendiger Zugänge und Berechtigungen zu Repositories und Cloud Umgebungen für die Übergabe einiger Liefergegenstände (Owner ist gematik)
- Bereitstellung notwendiger Zugänge und Berechtigungen zur Zusammenarbeit zwischen AN und AG im gematik Jira und Confluence

5.3 Mitwirkung des Auftraggebers

Im Rahmen der Auftragsdurchführung durch den AN erbringt der AG die für die termin- und leistungsgerechte Abwicklung der Beauftragung benötigten Mitwirkungen (einschließlich Beistellung gem. Kapitel 5.2). Die im Folgenden genannten Mitwirkungen sind im Projektverlauf an den dafür vorgesehenen Meilensteinen durch den AG zu liefern. Die Mitwirkungen des AG werden im folgenden Abschnitt abschließend benannt.

Stellt der AN fest, dass eine Mitwirkung nicht für die Erfüllung der vertraglich geschuldeten Leistung ausreichend oder geeignet ist, so hat er dies unverzüglich dem AG mitzuteilen, entsprechende Abhilfemaßnahmen vorzuschlagen und mit dem AG abzustimmen.

5.3.1 Allgemeine Mitwirkungsleistungen des AG

- Bestimmung der fachlichen Ansprechpartner des AGs inkl. Kontaktdaten (Telefon, E-Mail) für den AN mit Start der Beauftragung
- Zeitnahe Benennung und Bereitstellung benötigter Mitarbeiter des AGs für Klärungen und Abstimmungen
- Benennung und Einbindung von Ansprechpartnern der beteiligten Unternehmen und Organisationen während der gesamten Projektphase inklusive der Interoperabilitätstests sowie der dafür benötigten Systeme
- Benennung von Ansprechpartner/Kontakte zu anderen Marktteilnehmern während der Durchführung der Pilotierung in den Modellregionen
- Durchführung von termingerechten Reviews und Freigaben der vom AN erstellten Dokumente, der Referenz-, Test- und Produktivumgebungen, der vom AN durchgeführten Tests in diesen Umgebungen sowie die Abnahme der implementierten Lösungen

5.3.2 Übergreifende Steuerungsmaßnahmen des AG

Der AG wird eine übergreifende Programmsteuerung zur Koordination aller Gewerke des Gesamtvorhabens TI-Flow sowie ggf. weitere übergreifende Steuerungsmeetings zu Technik, Test, Transition und Rollout etablieren.

Die übergreifende Programmsteuerung dient der Koordination, Abstimmung und Überwachung aller Leistungserbringenden, die zur Realisierung der Gesamtlösung erforderlich sind. Ziel ist die Sicherstellung eines abgestimmten Vorgehens aller beteiligten Auftragnehmer hinsichtlich Termine, Abhängigkeiten, Schnittstellen, Risiken, und Entscheidungen. Die Steuerung umfasst insbesondere regelmäßige Abstimmungs- und Statusrunden, die gemeinsame Bearbeitung von Risiken und Eskalationen sowie die Koordination aller fachlichen, technischen und organisatorischen Schnittstellen zur erfolgreichen Umsetzung der Gesamtlösung.

Die übergreifenden Steuerungsmeetings werden nach Bedarf und Projektsituation wöchentlich oder zweiwöchentlich durchgeführt.

5.3.3 Prüfmaßnahmen des AG

Im Verlaufe des Vorhabens und insbesondere zum Erreichen der Meilensteine (MS) muss der AN verschiedene Liefergegenstände (LG) bereitstellen, die dem AG in einem vom AG bereitgestellten Sharepoint-Workspace bzw. vom AG vorgegebenen Repository zur Verfügung (s. Kapitel 4.1) zu stellen sind und von diesem in unterschiedlichem Umfang geprüft und gegebenenfalls freigegeben werden.

Im Verhältnis AG und AN wird wie folgt unterschieden:

- Feedback zu Kontrollpunkten
- Kenntnisnahme von Liefergegenständen (Ergebnis: Freigabe)
- Güteprüfung von Liefergegenständen (Ergebnis: Freigabe)
- Freigabe von Meilensteinen
- Abnahme des Vertrags.

Für LG, die als Dokumente zu liefern sind (bspw. Umsetzungskonzept), behält sich der AG vor, Vorabversionen dieser Dokumente („Kontrollpunkte“ (KP) genannt) einzufordern. Diese Vorabversionen stellen den aktuellen Bearbeitungsstand des jeweiligen Dokumentes dar. Mit diesem Verfahren sollen Mängel bzw. Fehlinterpretationen frühzeitig erkannt sowie die vollständige fachlich inhaltliche Prüfung nach Fertigstellung der Dokumente erleichtert und beschleunigt werden. Die Anzahl weiterer zu liefernden Vorabversionen hängt einerseits vom Umfang und der Wichtigkeit des Liefergegenstandes ab und andererseits davon, inwieweit der AN Rückmeldungen des AG, während der Dokumenterstellung berücksichtigt und gewürdigt hat. Inhaltliche Abweichungen von der Kontrollpunktlieferung zur finalen Lieferung muss der AN frühzeitig mit dem AG abstimmen.

Bezüglich der Erstellung und Einreichung zum ersten Kontrollpunkt ist Folgendes vom AN zu beachten:

- Gliederung ist vollständig erstellt,
- Inhalte sind in Teilen erstellt, Umfang und Qualität muss der AN vor Lieferung mit dem AG abstimmen,
- Richtwert ist ein Fertigstellungsgrad von 50 % (die noch offenen Anteile sind zu benennen).

Für bestimmte LG wurden bereits Kontrollpunktlieferungen zu den LG der jeweiligen Meilensteine festgelegt (siehe Kapitel 4.3 mit entsprechender Hinweismeldung zu Kontrollpunkten). Ggf. weitere benötigte Kontrollpunkte bzw. die Zeitpunkte der jeweiligen KPLieferungen werden zwischen AG und AN zu Projektbeginn abgestimmt.

Für die Kenntnisnahme (KN) von Leistungen behält sich der AG eine Frist von 10 Arbeitstagen (AT) vor, um Nachbesserungen einzufordern. Die AT umfassen Montag bis Freitag ausgenommen bundeseinheitlicher und Berliner Feiertage.

Eine Güteprüfung wird vom AG innerhalb von 10 AT durchgeführt. Der AG wird dem AN das Ergebnis in einem Prüfprotokoll mitteilen. Sofern der LG Mängel enthält und damit eine Nachbesserung durch den AN erforderlich ist, sind die Mängel innerhalb von 4 AT nach Bekanntgabe der Mängel zu beheben und der LG dem AG erneut zur Prüfung vorzulegen. Der AG wird den LG innerhalb von 5 AT einer erneuten Prüfung unterziehen.

Sofern der LG keine freigabeverhindernden Mängel enthält, wird er vom Auftraggeber freigegeben.

5.4 Koordinierungsverantwortung des Auftragnehmers

Um eine fristgerechte, vollständige, performante und fehlerfreie Leistung sicherzustellen, wird der AN in der gesamten Projektphase und in der Betriebsphase eigenverantwortlich

- sich mit den aktuellen und zukünftigen Akteuren, die Schnittstellen zum Leistungsumfang des AN haben oder die für eine mangelfreie Erbringung der Leistungen des AN anzubinden sind, über die Herstellung der Funktionalität und die notwendigen Mitwirkungsleistungen organisatorisch abstimmen,
- die Verfügbarkeit von Beistellungen von Dritten und des AG durch Einforderung, Koordinierung, kontinuierliche Überwachung und Kontrolle sicherstellen,
- die Kompatibilität der eigenen Leistungen mit den Beistellungen Dritter und des AG vollumfänglich und nachweislich prüfen,
- im Rahmen von Störungsanalysen die Beistellungen Dritter und des AG prüfen und auf Fehlerfreiheit kontrollieren,
- etwaige im Rahmen der Beseitigung von Fehlern eigene und erforderliche Mitwirkungsleistungen Dritter und des AG einfordern, koordinieren, überwachen und kontrollieren,
- den AG über jegliches besondere Ereignis (z.B. Störung, Behinderung, neu auftretendes Risiko, dringende Architekturentscheidung) mit möglichen Auswirkungen auf die eigene fristgerechte Leistungserbringung oder den Projekterfolg insgesamt binnen zweier AT zu informieren und
- den AG regelmäßig, d.h. mind. wöchentlich über Status/ Projektfortschritt in schriftlicher Form und regelmäßigen Abstimmungsmeetings informieren.

Der AG wird eine übergreifende Programmsteuerung zur Koordination aller Gewerke des Gesamtvorhabens TI-Flow sowie ggf. weitere übergreifende Steuerungsmeetings zu Technik, Test, Transition und Rollout etablieren. Der AN muss mit geeigneten Vertretern seines Projektteams an diesen übergreifenden Programm- und Steuerungsrounds aktiv teilnehmen.

5.5 Projektmanagement

Die Vorgaben zum Projektmanagement im vorliegenden Kapitel finden während der gesamten Projektphase Anwendung. Die Projektphase gilt als abgeschlossen, sobald alle entsprechenden Liefergegenstände und Meilensteine erbracht bzw. umgesetzt und freigegeben worden sind (MS7). Die Vorgaben zur Betriebsphase ergeben sich aus Kapitel 3.2.

5.5.1 Anforderungen an das Projektmanagement

Das Projektmanagement des AN erfordert eine strukturierte, nachvollziehbare und effektive Planung und Steuerung während der Projektphase. Diese Anforderung ergibt sich insbesondere aus:

- der Komplexität und dem Umfang der Liefergegenstände
- der technischen Komplexität der Entwicklungs-, Integrations- und Testszenarien
- der erforderlichen Vernetzung des AN mit weiteren Auftragnehmern, Marktteilnehmern und dem Auftraggeber (AG)
- die Parallelisierung von Arbeitspaketen inklusive Kenntnisnahmen, Güteprüfungen und Abnahmen.

Daraus ergeben sich für den AN folgende übergreifende Anforderungen an das Projektmanagement:

- Der AN muss ein geeignetes Projektmanagement etablieren, das eine vertrags- und leistungsgerechte Durchführung des Projekts sicherstellt. Hierzu gehören insbesondere:
- eine nachvollziehbare Projektorganisation mit klar definierten Rollen, Verantwortlichkeiten und Zuständigkeiten,
- geeignete Entscheidungs- und Eskalationsverfahren,
- Verfahren zur Qualitätssicherung,
- Verfahren zum Umgang mit Änderungen,
- Verfahren zur Identifikation, Bewertung, Überwachung und Behandlung von Projektrisiken,
- geeignete Verfahren zur Steuerung und Überwachung des Projektfortschritts.
- Der AN ist für die Erstellung, Fortschreibung und Pflege des Projektplans verantwortlich. Der Projektplan muss die zur Leistungserbringung erforderlichen Aktivitäten, Abhängigkeiten, Ressourcen und Termine berücksichtigen.
- Der AN muss den AG in wöchentlichen Projektsteuerungsboards über den aktuellen Projektstand informieren, die Termine jeweils in Form schriftlicher Protokolle im Confluence-Bereich des AG festhalten. Das Template für die Agenda und das Protokoll dieses Regeltermins wird durch den AG zum Projektstart dem AN zur Verfügung gestellt
- Die Anforderungen an das Projektvorgehen und den Projektplan ergeben sich ergänzend aus den in Anlage 11 beschriebenen einzureichenden Konzepten. Die mit dem Angebot vorgelegten Konzepte sind nach Zuschlagserteilung während der Projektlaufzeit fortzuschreiben und aktuell zu halten.
- Sofern sich die Ansprechpartner beim AN zwischen Projekt- und Betriebsphase unterscheiden, muss der AN eine Übergabe zwischen den Beteiligten auf seiner Seite sowie den Ansprechpartnern beim AG durchführen.
- Relevante Änderungen der Projektplanung müssen durch den AG genehmigt werden.
- Der AN muss im Rahmen des Projektabschlusses eine strukturierte Erfassung der Projekterfahrungen im Rahmen eines „Lessons Learned“-Workshops mit dem AG durchführen. Er muss in einen Projektabschlussbericht die tatsächlich erreichte

Leistung des Projektes darstellen. In diesem Projektabschlussbericht beschreibt er neben der Ausgangssituation des Projekts und dem Projektverlauf insbesondere die Zielerreichung, Abweichungen zum ursprünglichen Projektauftrag, offene Punkte, Handlungsempfehlungen, Risiken bei Projektabschluss sowie Ergebnisse des Lessons Learned Workshops.

Die Leistungen können am Sitz des AN erbracht werden, auf Verlangen des AG auch vor Ort.

Als Sprache für den Austausch zwischen AN und AG ist Deutsch auf Sprachniveau C2 festgelegt.

5.5.2 Anforderungen an die agile Zusammenarbeit

Der AN muss die Projektdurchführung unter Anwendung geeigneter agiler Vorgehensweisen sicherstellen.

Die agile Zusammenarbeit muss eine enge, transparente und kontinuierliche Abstimmung zwischen AN und AG gewährleisten und insbesondere die frühzeitige Einbindung des AG in Planungs-, Umsetzungs- und Abstimmungsprozesse ermöglichen.

Hierzu gehören mindestens:

- die strukturierte Planung, Durchführung und Bewertung von Entwicklungszyklen,
- die transparente Verwaltung von Anforderungen, Aufgaben, Umsetzungsständen und offenen Punkten,
- regelmäßige Abstimmungen zwischen den fachlichen und technischen Projektbeteiligten von AN und AG,
- die kontinuierliche Einbindung des AG in Priorisierungs-, Review- und Abstimmungsprozesse,
- die transparente Kommunikation von Risiken, Abhängigkeiten, Hindernissen und Abweichungen,
- die Nachvollziehbarkeit des Projektfortschritts sowie des Bearbeitungsstands der vereinbarten Leistungen.

Für die agilen Prozesse des AN gilt:

- Der AG nimmt optional mit mindestens einem Teilnehmer an dem Sprint-Review und an dem Sprint-Planning-Meeting des AN teil. Der AG wird regulär nicht an den täglichen Regelterminen (z.B. Scrum Daily) teilnehmen.
- Der AG hat die Berechtigungen, auf Anfrage kurzfristig die Tickets im Sprint-Backlog und Product-Backlog und die Arbeitsstände einzusehen. Auf Wunsch kann der AG an projektrelevanten Meetings des AN teilnehmen.

Der AN muss die hierfür vorgesehenen Vorgehensweisen, Rollen, Kommunikations- und Abstimmungsmechanismen im Rahmen des mit dem Angebot vorzulegenden Konzepts zum Projektvorgehen darstellen.

Das mit dem Angebot eingereichte Konzept muss zu Projektbeginn in Abstimmung mit dem AG fortgeschrieben und konkretisiert werden und muss während der Projektlaufzeit aktuell gehalten werden.

5.5.3 Mitwirkung an übergreifenden Steuerungsmaßnahmen des AG

Der AN muss aktiv an der programmübergreifenden Steuerung der Gesamtmaßnahme (s. Kapitel 5.3.2) mitwirken. Die vom AN zu erbringenden Leistungen bilden gemeinsam mit den Leistungen weiterer AN eine fachlich und technisch zusammenhängende Gesamtlösung.

Der AN muss

- an regelmäßig stattfindenden Programm-, Abstimmungs-, Koordinierungs- und Steuerungsterminen teilnehmen,
- hierfür fachlich und organisatorisch qualifizierte Ansprechpartner mit ausreichender Entscheidungs- bzw. Auskunftsbefugnis benennen,
- erforderliche Informationen, Planungen, Abhängigkeiten, Risiken, Fortschrittsstände und Entscheidungsbedarfe transparent und rechtzeitig einbringen,
- mit anderen im Programm eingesetzten Auftragnehmern konstruktiv zusammenzuarbeiten und notwendige technische sowie organisatorische Schnittstellen abstimmen,
- bei der Erstellung und Fortschreibung programmübergreifender Planungen, Terminpläne, Risikobetrachtungen und Integrationskonzepte mitzuwirken sowie
- vereinbarte Maßnahmen und Ergebnisse aus den Steuerungsrounds fristgerecht umzusetzen.

5.5.4 Projektrollen- und Gremien

Für die Dauer der Projektphase muss der AN eine für die Art, die Komplexität und den Umfang der Beauftragung geeignete Projektorganisation bereitstellen. Der AN muss alle Mitglieder der Projektorganisation unter Angabe von Projektrolle, Verantwortung, Firmenanschrift, E-Mail-Adresse und Telefonnummer benennen. Ein Austausch ist nur nach Zustimmung des AG nach den Bestimmungen des abgeschlossenen Vertrages möglich. Der AN gewährleistet, dass die Ansprechpartner verbindliche Auskünfte/Entscheidungen innerhalb ihres Verantwortungsbereiches erteilen/treffen können oder jederzeit durch verbindliche Aussagen des Projektleiters unterstützt werden. Die Erreichbarkeit dieser Ansprechpartner für den geplanten Projektzeitraum ist durch den AN zu gewährleisten.

Die wesentlichen Projektrollen und -gremien der Projektphase sind in der Übersicht dargestellt:

- **Projektleitung AG (PL-AG):** kaufmännische, vertragliche und fachliche Projektleitung des AG
Die Projektleitung des AG (PL-AG) ist verantwortlich für die Überwachung des Projektfortschritts und dass die Ergebnisse des Projekts den Erwartungen des AG entsprechen. Sie ist für die Sicherstellung der Einhaltung des Vertrags seitens des AN zuständig und fungiert als Hauptansprechpartner für die Projektleitung

des AN (PL-AN). Sie steuert das Projektteam des AG und stellt sicher, dass die benötigten Beistellungen gem. der vereinbarten Planung geleistet werden.

- **Projektleitung AN (PL-AN):** kaufmännische, vertragliche und fachliche Projektleitung des AN in seiner Gesamtheit (mind. Projektleiter, Stellvertretender Projektleiter, Projekt-Management-Office)

Die Projektleitung des AN ist verantwortlich für die operative, vertragliche und kaufmännische Steuerung und Abwicklung des Projekts

Die Projektleitung ist der zentrale Ansprechpartner für den AG. Die Erreichbarkeit der Projektleitung bzw. der Vertretung ist für gesamte Projektphase durch den AN zu gewährleisten.

Der AN muss verantwortliche und entscheidungsbefugte Mitarbeiter als Projektleitung und Stellvertretung zur Verfügung stellen.

- **Product Owner AN (PO-AN):** Steuerung der Entwicklung der Software unter Anwendung von agilen Methoden

Der Product Owner mit dem Kernteam ist verantwortlich für die Zielerreichung des jeweiligen Sprints und arbeitet insbesondere am Sprint Backlog, an der Sprint-Planung und am Backlog Refinement und verantwortet die Entwicklung und Qualität der Software (insbesondere Design, Entwicklung und Testing) in der Projektphase und der Wartungsphase.

Die Funktion des Product Owners kann in Personalunion mit der Funktion des Projektleiters ausgeübt werden, wenn die Aufgaben und Verantwortlichkeiten beider Rollen durch eine Person vollumfänglich erfüllt werden können und ein Stellvertreter benannt wird, der bei Bedarf kurzfristig einsatzfähig ist.

- **Kernteam AG (KT-AG):** Experten aus den für die Umsetzung relevanten Themengebieten zur Unterstützung der Projektleitung
Das Kernteam des AG setzt sich zusammen aus fachlichen Experten für die Themengebiete Architektur, Sicherheit, Test, Betrieb und ggf. weiteren.
- **Kernteam AN (KT-AN):** Experten aus den für die Umsetzung relevanten Themengebieten zur Unterstützung der Projektleitung bei der Projektdurchführung
- **Projektsteuerungsboard (PSB):** Koordinations- und Abstimmungsgremium zur fachlichen, operativen, vertraglichen und kaufmännischen Steuerung des Projekts

Das Board dient der Integration der verschiedenen Arbeitsebenen auf Auftraggeber- und Auftragnehmer Seite.

Teilnehmer: PL-AG, PL-AN, PO-AN und bei Bedarf Mitarbeiter aus dem KT-AG sowie dem KT-AN

Frequenz und Dauer: wöchentlich, eine Stunde

Aufgabenstellungen:

- organisatorische Koordination und Abstimmung zu Liefergegenständen
- Anpassung und Fortschreibung der Projektplanung hinsichtlich Meilensteine und Testverfahren, Abgleich mit der Sprintplanung des AN und deren Inhalten und Reporting des Projektfortschritts im Vergleich zum Zeitplan und aktuelle Zeitplanung
- Abstimmung zu fachlichem Änderungsbedarf in Konzepten und Spezifikationen

- Abstimmung und Koordination zu Qualitätsmanagementmaßnahmen und Testverfahren
- Reporting zur Gesamtkostenschätzung und Einschätzung zur Kostenentwicklung (Forecast) für die Werkvertragsleistungen und Bedarfsleistungen
- Reporting und Abstimmung zu Risiken und möglichen Projekt-Hindernissen
- Berichterstattung an den Lenkungsausschuss
- Erstellung von Change Requests und Entscheidungsvorlagen zur Vorlage im Lenkungsausschuss
- **Lenkungsausschuss (LA):** übergreifendes Steuerungsgremium zur Überwachung der Erreichung der Projektziele und als Eskalationsinstanz
Das Gremium kann bei Bedarf durch den AG einberufen werden. Die Leitung und Moderation der Sitzung erfolgen durch den Projektleiter des AG.
Teilnehmer: Vertreter der Managementebene von Seiten AG und AN sowie PL-AG und PL-AN
Frequenz und Dauer: bei Bedarf, 1-2 Stunden
Aufgabenstellungen:
 - Überwachung der Erreichung der Projektziele
 - Entscheiden über Change Requests
 - Treffen von Eskalationsentscheidungen

Der Bedarf, der Umfang oder das Format der Besprechungen können während der Projektphase zwischen AN und AG abgestimmt und angepasst werden.

5.6 Qualitätsmanagement

Um die einwandfreie Qualität seiner Produkte und Dienstleistungen gewährleisten zu können, muss der AN über ein geeignetes Qualitätsmanagement bei Vertragsschluss verfügen, danach verfahren und dies umfassend dokumentieren sowie über die Vertragsdauer hinweg aufrechterhalten.

Der AN muss alle notwendigen Prozesse seines Qualitätsmanagementsystems auf den Vertragsgegenstand anwenden. Dies bedeutet, dass das Qualitätsmanagement des Unternehmens die für den jeweiligen Liefergegenstand geeigneten Qualitätsplanungs-, Qualitätslenkungs-, Qualitätssicherungs- und Qualitätsverbesserungstätigkeiten umfassen muss

5.7 Eskalationsmanagement

Tritt im Rahmen der Durchführung des Vertrages in der Projektphase ein Problem oder eine Meinungsverschiedenheit zwischen den Vertragsparteien auf und kann auf Ebene der Projektleitung keine einvernehmliche Einigung erzielt werden, die aber nach dem Vertrag erforderlich ist (Eskalationsfall), ist der AN zunächst verpflichtet, auf Verlangen des AG an einem Vor-Ort-Termin teilzunehmen. Kann auch dabei zwischen den Vertragsparteien keine Einigung erzielt werden, ist an den Lenkungsausschuss zu eskalieren. In der Betriebsphase ist das Eskalationsmanagement für die Betriebsprozesse in [gemRL_Betr_TI] geregelt.

5.8 Produktivfreigabe

Die Produktivfreigabe ist die Voraussetzung, um einen von dem AG beauftragten Dienst in die Telematikinfrastruktur produktiv einführen und nutzen zu können. Die Anforderungen hierfür sind in dieser Leistungsbeschreibung über Liefergegenstände abgebildet. Die Produktivfreigabe ersetzt die in den gematik-Spezifikationen verwendete Zulassung, sofern keine gesetzliche Zulassungspflicht besteht (vgl. Kapitel 1.6).

Die Produktivfreigabe entspricht inhaltlich der Zulassung der gematik [gemZul_übergrVerf] und verwendet deren Terminologie. Bei der Produktivfreigabe wird jedoch, anders als bei einer Zulassung, kein Verwaltungsakt erlassen (einschließlich dessen rechtlicher Wirkung) und auch die weiteren administrativen Tätigkeiten fallen nicht an.

Die Produktivfreigabe wird durch den AG erteilt, wenn alle funktionalen, betrieblichen und sicherheitstechnischen Nachweise gemäß Kapitel 3.1.7 sowie des Produkttyp- und Anbietersteckbriefes erbracht wurden. Sie wird durch den AG in der Projektphase über die Freigabe des MS6 und in der Betriebsphase über die betrieblichen Prozesse abgebildet.

Der AN muss die notwendigen Nachweise gemäß den Anforderungen aus Kapitel 3.1.7, den jeweils gültigen Produkt- [gemProdT_HCC_PTV] und den Anbietertypsteckbriefen [gem-AnbT_HCC_ATV] entsprechend den Meilensteinen (s. Kapitel 4.3) vorlegen, um die Produktivfreigabe erlangen zu können. Das gilt gleichermaßen für Folgefreigaben, zu denen der AN im Rahmen der betrieblichen Prozesse die notwendigen Nachweise erbringen muss.

6 Mitgeltende Dokumente

Die folgenden mitgeltenden Dokumente sind für die Auftragsdurchführung verbindlich einzuhalten.

Tabelle 7: Mitgeltende Dokumente

Referenz: Dokument	Ressource / Ort	Datum
gemLB_Anhang_SK	Anhang zur Leistungsbeschreibung mit Anforderungen an den zu erstellenden Servicekatalog Anlage-02 - TI-Flow Leistungsbeschreibung Los 1+2 - Anhang SK.pdf	14.10.2026
gem-ProdT_HCC_PTV	Produkttypsteckbrief HCC https://gemspec.gematik.de/docs/gemProdT/gem-ProdT_HCC/gemProdT_HCC_PTV_1.0.0-0_V1.0.0/	02.10.2026
gem-AnbT_HCC_ATV	Anbietertypsteckbrief HCC https://gemspec.gematik.de/docs/gemAnbT/gem-AnbT_HCC/gemAnbT_HCC_ATV_1.0.0-0_V1.0.0/	02.10.2026
gemSpec_HCC	Spezifikation Healthcare Confidential Computing (HCC), Version 1.0.0 https://gemspec.gematik.de/docs/gemSpec/gemSpec_HCC/gemSpec_HCC_V1.0.0/	02.10.2026
gemTI_SEC_Standard	TI Security Standard – Mitwirkungspflichten für Anbieter, Version 1.0.0 https://gemspec.gematik.de/docs/gemWeitere/gemTI_SEC_Standard/gemTI_SEC_Standard_V1.0.0/	26.05.2025
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter, Version 2.2.0 https://gemspec.gematik.de/docs/gemSpec/gemSpec_DS_Anbieter/gemSpec_DS_Anbieter_V2.2.0/	10.07.2026
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller, Version 1.7.0 https://gemspec.gematik.de/docs/gemSpec/gemSpec_DS_Hersteller/gemSpec_DS_Hersteller_V1.7.0/	27.05.2025

Referenz: Dokument	Ressource / Ort	Datum
gemKPT_Test	Testkonzept der TI Umfasst Anforderungen zum Testvorgehen für die TI-Produkttypen und deren Hersteller, Veröffentlichung der Fortschreibung für TI 2.0, Version 3.8.0 https://gemspec.gematik.de/docs/gemKPT/gemKPT_Test/gemKPT_Test_V3.8.0/	02.10.2026
C_12813_An- lage_CC	Anlage zur gemKPT_Test, Update der Testanforderungen für Auftragnehmer an Testsuiten, Version: 1.0.0_CC (in Kommentierung) https://gemspec.gematik.de/prereleases/Draft_Test_26_1/C_12813_Anlage_V1.0.0_CC/	25.09.2026
gemSpec_Perf	Spezifikation Performance und Mengengerüst TI-Plattform, Version 2.88.0 https://gemspec.gematik.de/docs/gemSpec/gemSpec_Perf/gemSpec_Perf_V2.88.0/	02.10.2026
gemRL_Betr_TI	Übergreifende Richtlinien zum Betrieb der TI, Version 2.23.0 https://gemspec.gematik.de/docs/gemRL/gemRL_Betr_TI/gemRL_Betr_TI_V2.23.0/	07.07.2026
gemRL_PruefSich- Eig_DS	Richtlinie zur Prüfung der Sicherheitseignung, Version 3.0.1 https://gemspec.gematik.de/docs/gemRL/gemRL_PruefSichEig_DS/gemRL_PruefSichEig_DS_V3.0.1/	29.07.2025
gemSpec_ZETA	gematik (09.07.2026): Spezifikation Zero Trust Access (ZETA) https://gemspec.gematik.de/prereleases/Draft_ZETA_26_2/gemSpec_ZETA_V2.0.0_CC/	09.07.2026
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.51.0 https://gemspec.gematik.de/docs/gemSpec/gemSpec_Krypt/gemSpec_Krypt_V2.51.0/	02.10.2026
gemSpec_PKI	Übergreifende Spezifikation PKI, Version 2.26.0 https://gemspec.gematik.de/docs/gemSpec/gemSpec_PKI/gemSpec_PKI_V2.26.0/	10.02.2026
BSI- Standortkriterien	BSI: Kriterien für die Standortwahl von Rechenzentren https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/RZ-Sicherheit/Standort-Kriterien_Rechenzentren.pdf?__blob=publicationFile&v=5	Dez.2024

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AG	Auftraggeber
AN	Auftragnehmer
CI/CD	Continuous Integration (kontinuierliche Integration) und Continuous Delivery bzw. Continuous Deployment (kontinuierliche Auslieferung oder Bereitstellung)
HCC	Healthcare Confidential Computing nach gemSpec_HCC
HCC-Cloud	Cloud Services, sowohl mit als auch ohne HCC Funktionalität
OCI	Open Container Initiative
OTel	OpenTelemetry
PAYG	Pay-as-you-Go-Modelle
PU	Produktionsumgebung
RU	Referenzumgebung
RU-DEV	Testreferenzumgebung
RTO	Recovery Time Objective / Wiederanlaufzeit
SCIM	System for Cross-domain Identity Management
SCS	Sovereign Cloud Stack
TDCAS	Trust Domain Configuration & Attestation Service
TU	Testumgebung

A2 – Glossar

Das Glossar wird als eigenständiges Dokument zur Verfügung gestellt.

Begriff	Erläuterung
Cloud Service Provider (CSP)	Ein Anbieter, der Cloud-Ressourcen (wie Netzwerke, Server, Speicher) bündelt, verwaltet und dem Nutzer mit minimaler Interaktion zur Verfügung stellt. (Nach NIST Special Publication 800-145 bzw. ISO/IEC 22123)
HCC Provider	Durch die gematik beauftragter Cloud Service Provider, der eine mandantenfähige Infrastruktur für den Betrieb von HCC-Diensten bereitstellt.

HCC-Cloud	Von der gematik beauftragte Infrastruktur nach den Vorgaben aus gemSpec_HCC für den Betrieb von HCC-Diensten
HCC-Dienst	Fachdienst oder anderer Dienst der TI. Der Dienst wird auf einer HCC-Infrastruktur betrieben, um schützenswerte Daten im Klartext zu verarbeiten.
HCC-Mandant	Kunde bzw. Mandant eines HCC-Providers, der mittels Konfiguration des durch den HCC-Provider bereitgestellten Mandantenkontextes die Dienste (eigene oder Dienste aus dem Portfolio des HCC-Providers oder von Dritten) definiert und parametrisiert, welche für ihn in der Infrastruktur des HCC-Providers laufen. HCC-Mandanten sind HCC-Dienstanbieter aus der Perspektive des HCC-Providers betrachtet.
Mandantenfähigkeit (engl. Multi-Tenancy)	Eigenschaft einer Software oder eines IT-Systems, mehrere Kunden oder Nutzergruppen auf derselben Infrastruktur zu bedienen, ohne dass dieser gegenseitige Einblick in ihre Daten haben.
Ausführungsumgebung (engl. Runtime Environment)	Gesamtheit aus Softwarekomponenten, Infrastruktur und Ressourcen, die notwendig ist, damit ein Computerprogramm oder ein IT-Service ausgeführt werden und ordnungsgemäß laufen kann.
Recovery Time Objective (RTO)	Die RTO-Variable bezeichnet die maximale Zeit, die benötigt wird, um ein System nach einer Störung wiederherzustellen. Das RTO ist ein wichtiger Faktor bei der Planung von Notfallwiederherstellungslösungen, da es definiert, wie schnell ein Unternehmen nach einer Störung wieder normal arbeiten kann.

A3 – Abbildungsverzeichnis

Abbildung 1: Staging und Stageübergänge beim HCC-Provider.....	33
Abbildung 2: Durch Referenz-Container abgedeckter Testumfang	55
Abbildung 3: Phasen- und Meilensteinübersicht der Projektphase	105

A4 - Tabellenverzeichnis

Tabelle 1: Bereitstellungsanforderungen der Umgebungen.....	30
Tabelle 2: Übersicht der geplanten Umgebungen	31
Tabelle 3: Fehlerursachen Abgrenzung	52
Tabelle 4: Begleitende Dokumentationen der Betriebsphase.....	96
Tabelle 5: Meilensteine mit Zielterminen	106

Tabelle 6: Übersicht der Liefergegenstände zu den Meilensteinen	107
Tabelle 7: Mitgeltende Dokumente.....	134

A5 – Referenzierte Dokumente

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
gemSpec_FD_eRp	gematik: Spezifikation E-Rezept-Fachdienst, Version 2.6.0 https://gemspec.gematik.de/docs/gemSpec/gemSpec_FD_eRp/gemSpec_FD_eRp_V2.6.0/
gemZul_übergrVerf	Übergeordnete Verfahrensbeschreibung für Zulassungs- und Bestätigungsverfahren https://fachportal.gematik.de/fileadmin/user_upload/gemZul_uebergrVerf_V2.12.0.pdf
gemSpec_FD_TI-Flow	Spezifikation: TI-Flow-Fachdienst, Version 1.0.0 https://gemspec.gematik.de/docs/gemSpec/gemSpec_FD_TI-Flow/gemSpec_FD_TI-Flow_V1.0.0/

Weitere Referenzierungen:

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
„Anlage-12 der Vergabeunterlagen - IT Projektvertrag "TI-Flow - Cloud Services" (Los 2)“	Zugrundeliegender IT-Projektvertrag „TI-Flow – Cloud Services“ Los 2 Anlage-12 der Vergabeunterlagen und vorrangig geltendes Vertragswerk für die gegenständliche Leistungserbringung
NIST SP 800-145	NIST Special Publication 800-145 https://csrc.nist.gov/pubs/sp/800/145/final