

Leistungsbeschreibung

Aufbau Apache Kafka-Plattform

Inhaltsverzeichnis

1. Einführung	5
1.1. Unternehmen (Auftraggeber)	5
1.2. Hintergrund und Ziele	5
1.3. Anwendungsfälle	6
1.4. Leistungsteile	6
1.5. Zeitlicher Überblick	7
2. Leistungsteil A – Aufbau der Plattform	8
2.1. Iterativer Aufbau der Plattform	8
2.1.1. Anforderungsmanagement	9
2.1.2. KRITIS-Relevanz	10
2.1.3. Aktualität der Kafka-Plattform	10
2.1.4. Systemtrennung und Migration	10
2.1.5. Verfügbarkeit & Ausfallsicherheit	10
2.1.6. Disaster Management	11
2.1.7. Kafka Tiered Storage und Diskless	11
2.1.8. Performance	11
2.1.9. Datenaufbewahrung	12
2.1.10. Skalierbarkeit	12
2.1.11. IT-Sicherheit	12
2.1.12. Container-Technologien	12
2.1.13. Stream Processing	13
2.1.14. Befähigung der Softwareentwickelnden	13
2.1.15. Developer Experience	13
2.1.16. Integration mit API Management	13
2.1.17. Lifecycle der Anwendungsentwicklung	14
2.1.18. Lineage & Anbindung an das Datenkatalogsystem der TK	14
2.1.19. Management Review	14
2.1.20. Fernzugriff	14
2.2. Enterprise Funktionen	14
2.2.1. Lieferung Enterprise-Funktionen	15
2.2.1.1. RBAC + ACL Security	15
2.2.1.2. Schema Registry	16
2.2.1.3. Topic Management & Quota-Steuerung	16
2.2.1.4. Graphische Oberfläche und Administrations-Konsole	17
2.2.1.5. Mirroring / Multi Region Replication	17

2.2.1.6.	Tiered Storage	18
2.2.1.7.	Diskless / Log Compaction Optimierung.....	18
2.2.1.8.	Streaming.....	18
2.2.2.	Installation der Enterprise-Funktionen	19
2.2.3.	Anpassung der Enterprise-Funktionen.....	19
2.3.	Kafka-Konnektoren	19
2.3.1.	Lieferung Kafka-Konnektoren.....	19
2.3.1.1.	Kafka-Konnektoren Umfang.....	20
2.3.2.	Installation der Konnektoren.....	21
2.3.3.	Anpassung der Konnektoren.....	21
2.4.	Production Readiness.....	22
2.4.1.	Einbindung in das IT-Servicemanagement der TK	22
2.4.2.	Mitbestimmung und Datenschutz.....	23
2.4.3.	Betriebsdokumentation und technische Lösungsskizze	23
2.4.4.	Support, Incidents und Anwenderdokumentation	24
2.4.5.	Systemadministration	25
2.4.6.	Systemüberwachung.....	26
2.4.7.	Performance Management.....	26
2.4.8.	Kontinuierliche Wartung	26
2.4.9.	Backup- und Wiederherstellungsdienste.....	27
2.4.10.	Kontinuitätstests.....	27
2.4.11.	Sicherheitsmanagement	27
2.4.12.	Software-Paketierung	28
2.4.13.	Fernzugriff.....	29
2.5.	Metriken	29
2.5.1.	Prozess-Metriken	29
2.5.2.	Health- und Zertifikats-Überprüfungen.....	30
2.5.3.	Logausgaben.....	30
2.5.4.	Alerts	30
2.5.5.	Prozess-Alerts	32
2.5.6.	Health-Alerts.....	32
2.5.7.	Zertifikats-Alerts	33
2.6.	Softwarepflege und Support	34
2.7.	Betrieb der Plattform in der Aufbauphase	34
3.	Leistungsteil B – Betrieb der Plattform nach Fertigstellung des Aufbaus (optional)	35
3.1.	Einbindung in das IT-Servicemanagement der TK.....	35
3.2.	Mitbestimmung und Datenschutz	35
3.3.	Betriebsdokumentation und technische Lösungsskizze.....	35

3.4.	Support und Anwenderdokumentation	36
3.5.	Unterstützung der Nutzung	36
3.6.	Systemadministration	36
3.7.	Systemüberwachung	36
3.8.	Performance Management	36
3.9.	Kontinuierliche Wartung	36
3.10.	Backup- und Wiederherstellungsdienste	36
3.11.	Kontinuitätstests	37
3.12.	Sicherheitsmanagement	37
3.13.	Incident-Management und Support	37
3.14.	Software-Paketierung	37
3.15.	Fernzugriff	37
4.	Aufgaben und Anforderungen an das vom AN eingesetzte Personal	38
4.1.	Aufgaben des eingesetzten Personals	38
4.1.1.	Aufgaben des Projektleiters	38
4.1.2.	Aufgaben des Kafka Senior Engineers (Aufbau der Kafka-Plattform)	39
4.1.3.	Aufgaben des Kafka Engineers (Betrieb der Plattform nach Fertigstellung des Aufbaus – optionale Leistung)	40
4.2.	Anforderungen an das vom AN eingesetzte Personal	41
4.2.1.	Projektleiter	41
4.2.2.	Kafka Senior Engineer	42
4.2.3.	Kafka Engineer	43

Hinweis:

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Auftragsbeschreibung die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

1. Einführung

1.1. Unternehmen (Auftraggeber)

Die Techniker Krankenkasse (TK) ist eine bundesweite Krankenkasse mit rund 9,7 Millionen Mitgliedern und insgesamt rund 12,4 Millionen Versicherten. Als gesetzliche Krankenversicherung ist die TK eine Körperschaft des öffentlichen Rechts mit Selbstverwaltung. Sie wird von einem hauptamtlichen Vorstand geführt. Circa 15.700 Mitarbeiterinnen und Mitarbeiter betreuen die Versicherten der TK bundesweit an ca. 250 Standorten und in der Unternehmenszentrale in Hamburg.

Die TK steht für eine qualitativ hochwertige und wirtschaftliche Versorgung, mit effizienten Strukturen und Prozessen, zum Vorteil ihrer Versicherten. Dabei berücksichtigt die TK gesellschaftliche Veränderungen ebenso wie Innovationen und technischen Fortschritt.

In ihrer Nachhaltigkeitsstrategie hat die TK sich die Ziele gesetzt, in ihrem eigenen Handeln und wesentlichen vor- und nachgelagerten Aktivitäten CO₂-neutral zu werden sowie Nachhaltigkeit in den Einkaufsprozess zu integrieren. Daher ist es der TK wichtig, auch bei der Gestaltung und Beschaffung ihrer digitalen Produkte und Leistungen ein Augenmerk auf Nachhaltigkeit und insbesondere ökologische Auswirkungen zu legen.

1.2. Hintergrund und Ziele

Die TK plant den Einsatz einer standardisierten Kafka-Plattform (im Folgenden auch nur „Plattform“ genannt) als einer oder mehrere Rechnerverbunde (Cluster) aus log-orientierten Event-Brokern auf Basis von Apache Kafka. Apache Kafka ist eine verteilte Plattform, die für die effiziente Verarbeitung von Echtzeitdatenströmen entwickelt wurde. Apache Kafka bietet eine robuste und skalierbare Lösung zur Verarbeitung großer Datenmengen. Daten werden in sogenannten "Topics" organisiert, welche eine chronologische Abbildung aller eingespeisten Ereignisse und Nachrichten darstellen. Topics können individuell konfiguriert und mit spezifischen Zugriffsregeln versehen werden.

Mit dieser Ausschreibung sollen folgende Leistungen beschafft werden:

- Unterstützung beim Aufbau der Plattform und Wissenstransfer.
- Enterprise-Funktionen und Kafka Konnektoren, inklusive Softwarepflege und Support,
- Unterstützung bei der Inbetriebnahme der Plattform
- Betrieb der Plattform während der Aufbauphase
- Ggf. Betrieb der Plattform nach Fertigstellung des Aufbaus (optional)

Die zu erbringenden Leistungen sollen sicherstellen, dass die Plattform höchsten Anforderungen an Skalierbarkeit, Sicherheit, Effizienz und Wirtschaftlichkeit genügen. Der Auftragnehmer (AN) übernimmt hierbei die zentrale Rolle, indem er Best Practices sowie innovative Ansätze einbringt, um einen leistungsfähigen, sicheren und effizienten Aufbau sowie Betrieb der Plattform zu gewährleisten.

Sämtliche Leistungen des AN werden auf Grundlage der EVB-IT Rahmenvereinbarung erbracht. Diese bildet die vertragliche Grundlage für sämtliche im Rahmen des Vorhabens und in der Leistungsbeschreibung beschriebenen Leistungen. Die Rahmenvereinbarung begründet selbst keinen unmittelbaren Anspruch. Alle Leistungen werden erst durch gesonderte Einzelaufträge (Abrufe) verbindlich beauftragt, siehe EVB-IT Rahmenvereinbarung. Die Einzelaufträge erfolgen mit Abrufformular der TK (Anlage L2).

1.3. Anwendungsfälle

In diesem Abschnitt werden die künftigen Anwendungsfälle für Apache Kafka bei der TK beschrieben. Der AN hat diese Anwendungsfälle bei der Konzeption und Aufbau einer passenden Plattform sowie eines passenden Betriebsmodells gemäß den technischen, organisatorischen und regulatorischen Rahmenbedingungen der TK zu berücksichtigen.

- Ein zentraler Anwendungsfall der Plattform ist die Kommunikation zwischen operativen Microservices. Durch die Entkopplung der Microservices wird eine flexible, skalierbare und fehlertolerante Architektur ermöglicht, die Daten in Echtzeit verarbeitet und bereitstellt. Dies erlaubt es den Microservices, effizient miteinander zu interagieren, ohne direkte Abhängigkeiten aufzubauen. Die Plattform dient somit als Grundlage für eine moderne, ereignisgesteuerte Microservice-Kommunikation, die sowohl die Entwicklungszeiten verkürzt als auch die Wartbarkeit verbessert.
- Die Plattform soll auch zur Datenversorgung von Microservices genutzt werden. Hierbei publiziert ein Quellsystem bei jeder Änderung an einem Geschäftsobjekt eine Nachricht, die den vollständigen Datensatz abbildet. Konsumenten können die zugehörigen Topics konsumieren und die Daten als Replik in ihrer Datenbank speichern bzw. aktualisieren und anschließend (lesend) nutzen. Da mindestens eine Nachricht pro Geschäftsobjekt auf dem Topic vorliegt, kann dieser Mechanismus auch zur Initial-Befüllung neuer Microservices dienen. Eine Langzeitspeicherung der Nachrichten ist hierzu notwendig.
- Die aufzubauende Plattform soll auch für die Versorgung dispositiver Systeme genutzt werden. Hierbei sind die Möglichkeiten des Kafka-Ökosystems (insbesondere Kafka Connect) zu berücksichtigen. Ein zentraler Anwendungsfall ist hierbei die Ablage von Business-Objekten in einem DWH/Data Lake, um diese für Berichtswesen und weiterführende Analysen bereitzustellen. Grundsätzlich wird angestrebt, durch die Plattform eine nahtlose Verbindung zwischen operativen und analytischen Prozessen zu schaffen, um datengetriebene Entscheidungsfindung und Innovation zu fördern.
- Ein weiterer Anwendungsfall der Plattform ist die Bereitstellung eines Kommunikationskanals, um für das zentrale IT-Cluster der TK "TKeasy" eine Möglichkeit zu schaffen, Audit-Ereignisse flexibel und skalierbar abzuschicken. In erster Linie dokumentieren die Audit-Ereignisse Anwender- und Systeminteraktionen in TKeasy, um bei Betrugsverdacht nachverfolgen zu können, welche Daten in TKeasy bewusst manipuliert worden sind. Der Kanal soll dabei zunächst der Zusammenführung der Audit-Ereignisse von den vielen TKeasy-Servern dienen und auch von den Microservices im TKeasy-Umfeld zu dem gleichen Zweck genutzt werden. Der Konsument der Ereignisse soll zunächst ein einfacher Dienst sein, der die Audit-Ereignisse dauerhaft persistiert und für konkrete Verdachtsverfolgungen vorhält. Perspektivisch wären auch andere Abnehmer denkbar, z.B. eine Echtzeit-Auswertung von Aufnahmezahlen oder Echtzeit-Betrugserkennung mit KI-Unterstützung. In diesem Kontext stellt die Nutzung von Plattform für den Transport von SIEM-Nachrichten einen weiteren perspektivischen Anwendungsfall dar, in dem das transportierte Datenvolumen signifikant wächst.

1.4. Leistungsteile

Diese Ausschreibung besteht aus zwei Leistungsteilen die in Abschnitten 2 und 3 detailliert erläutert werden:

- **Leistungsteil A (Abschnitt 2)** befasst sich mit dem Aufbau und Inbetriebnahme der Plattform. In diesem Teil erfolgen alle Vorbereitungen, die für den Betrieb der Plattform notwendig sind. Dies umfasst auch Arbeiten, die zur Erfüllung der Vorgaben des IT Service Managements der TK notwendig sind.
- Der optionale **Leistungsteil B (Abschnitt 4)** beinhaltet den tatsächlichen Betrieb der aufgebauten Plattform.

1.5. Zeitlicher Überblick

Die nachstehende Tabelle gibt einen groben zeitlichen Überblick über die Leistungsphasen innerhalb der Vertragslaufzeit. Die Regelungen zum Leistungsbeginn und dem Übergang von einer Leistungsphase in die nächste bzw. der Abbruch der weiteren Zusammenarbeit ist den entsprechenden Verträgen zu entnehmen.

Eine detaillierte Zeitplanung innerhalb einer bestimmten Phase stimmen die Vertragsparteien bei Bedarf in der Vertragsdurchführung ab. Diese wird nach Freigabe der TK verbindliche Grundlage für die weitere Leistungserbringung.

Phase	Aufgaben	Dauer
Initialer Aufbau – erste produktive Cluster im Betrieb	Zwei Cluster im Betrieb. Bereitstellung mindestens zweier Cluster für zwei Anwendungsfälle in jeweils drei Umgebungen. Monitoring, Schema-Registry, RBAC stehen in einem ersten Reifegrad bereit	ca. 2 Monate
Reifung und GitOps	IaC/GitOps werden eingeführt, weitere Enterprise-Funktionen kommen zum Einsatz. Erweitertes Monitoring und Auto-Scaling. Weitere Cluster werden aufgebaut auf Basis von Anwendungsfällen.	ca. 2 Monate
Erweiterte Features	Developer Experience wird verbessert. Weitere Enterprise Funktionen und Anwendungsfälle (z. B. Streaming, Backup, Tiered Storage, Diskless) werden bedarfsgerecht eingebaut.	ca. 2 Monate
Betrieb nach Fertigstellung des Aufbaus (optional)	Ausführung der betrieblichen Aufgaben (angelehnt an ITIL) nach Fertigstellung des Plattformaufbaus	42 Monate

2. Leistungsteil A – Aufbau der Plattform

Dieser Leistungsteil enthält die Anforderungen an den AN zur Erbringung der spezifischen Beratungs-, Konzeptions-, Umsetzungs- und Befähigungsleistungen, die für den Aufbau und die Inbetriebnahme Plattform notwendig sind.

2.1. Iterativer Aufbau der Plattform

Der AN erstellt für den Aufbau der Plattform ein Grobkonzept (Anlage A3). Auf Anforderung der TK ist der AN verpflichtet, sein Grobkonzept nach Vorgaben der TK anzupassen.

Der AN hat auf Grundlage seines Grobkonzeptes in Abstimmung mit der TK einen iterativen Entwicklungsprozess für den Aufbau der gewünschten Plattform zu definieren und umzusetzen. In diesem Prozess wird die Plattform inkrementell aufgebaut. Es werden dabei die Grundsätze der agilen Systementwicklung angewendet. Bei jedem Inkrement entsteht ein Feinkonzept (z.B. in Form einer Sprint-Planung) über die Plattform, welches im Anschluss validiert und vom AN umgesetzt wird. Dieses Feinkonzept wird im Sinne der agilen Vorgehensweise im Rahmen einer Iterationsplanung präsentiert und validiert. Nach jedem Inkrement entsteht sichtbarer Mehrwert für die TK. Die umgesetzten Inkremente sind zeitnah nach der Validierung vom AN in Zusammenarbeit mit der TK in Betrieb zu nehmen. Der AN übernimmt in dieser Phase auch den Betrieb dieser Inkremente (siehe Abschnitt 2.7). Über die Frequenz und Umfang (Anzahl Inkremente) der Inbetriebnahme entscheidet der AN in Rücksprache mit der TK. Bei Inbetriebnahme sind die Vorgaben unter Abschnitt 2.4 zu berücksichtigen.

Die Inkremente bauen aufeinander auf und ermöglichen eine kontinuierliche Verbesserung der Plattform. Jedes Inkrement wird vom AN in das Gesamtbild der Plattform integriert. Die Plattform entsteht als kohärentes System, in dem alle Teile sinnvoll zusammenwirken und gemeinsam einen stetigen Fortschritt in Richtung des Endziels ermöglichen.

Jedes Feinkonzept muss mindestens folgende Themen zum Gegenstand haben:

- Skizzierung der Arbeiten, die in der Iteration umgesetzt werden. Es ist ersichtlich, warum diese Arbeiten einpriorisiert wurden und welcher Mehrwert dabei entsteht.
- Skizzierung der geplanten Systemlandschaft in grafischer Form,

Bei jeder Iteration werden auch betriebliche Aspekte (s. auch Abschnitt 2.4) berücksichtigt wie:

- Darstellung der Integration und der Automation in die Systemlandschaft der TK,
- Benutzerverwaltung und Berechtigungen,
- Schwachstellen- und Patch-Management der Plattform,
- Beschreibung der Backup- und Recovery-Prozesse der Konfiguration der Plattform,
- Beschreibung der Zugriffshärtung auf die Plattform,
- Beschreibung der administrativen Tätigkeiten,
- geplanten Betriebsunterbrechungen,
- ungeplanten Betriebsunterbrechungen inklusive der Integration in das Alarming-System der TK,
- Support-Prozesse,
- Einbindung in die ITSM-Prozesse der TK,
- Reporting- und Logging-Funktionen der Plattform.

Die Leistung umfasst den Entwurf, den Aufbau und den Wissenstransfer einer zentralen Plattform für die IT der TK, als On-Premises-Lösung sowie den Betrieb der Plattform, während diese iterativ aufgebaut wird. Die Plattform umfasst einen bis mehrere Kafka-Cluster. Dabei ist der Wissenstransfer von essenzieller Bedeutung: Die TK muss in die Lage versetzt werden, den Betrieb, Wartung und Weiterentwicklung der aufgebauten Plattform zu übernehmen.

Es obliegt dem AN, die geeigneten technischen – insbesondere bzgl. der Dimensionierung der Plattform und Definition der passenden IT-Architektur – sowie organisatorischen (z. B. notwendiges Personal seitens der TK, Beschaffung spezieller Tools) Lösungen für die Umsetzung der zu erbringenden Leistungen zu benennen / aufzuzeigen. Der AN stimmt seine Lösungsvorschläge mit der TK ab und berücksichtigt dabei die Anwendungsfälle und Rahmenbedingungen der TK. Zu diesen Rahmenbedingungen zählen:

- Rechenzentren der TK,
- Verfügbare Hardware, Software, Netzwerk und Virtualisierung der TK,
- Geltende regulatorische Anforderungen im Kontext IT-Einkauf, Datenschutz und IT-Sicherheit sowie IT Service Management.

Beistellungen, die vonseiten der TK benötigt werden, sind vom AN transparent darzustellen und mit der TK abzustimmen.

2.1.1. Anforderungsmanagement

Die Plattform dient der Umsetzung der in Abschnitt 1.3 beschriebenen Anwendungsfälle. Darüber hinaus ist zu berücksichtigen, dass im Verlauf des Projekts weitere Anwendungsfälle entstehen können, die zum Zeitpunkt der Ausschreibung noch nicht identifiziert oder detailliert beschrieben sind. Die Anwendungsfälle werden von der zuständigen Fachabteilungen der TK mithilfe der aufzubauenden Plattform umgesetzt.

Der AN analysiert die Anwendungsfälle sowie die damit verbundenen funktionalen und nicht-funktionalen Anforderungen und beleuchtet dabei unter anderem folgende Aspekte:

- Funktionale Aspekte
 - Wie sind die Ereignisse strukturiert?
 - Ist die Reihenfolge der Ereignisverarbeitung wichtig?
 - Wie werden Ereignisse partitioniert?
 - Wie lange werden Ereignisse aufbewahrt?
 - Wie geschäftskritisch sind die gespeicherten Daten?
 - Werden sensitive Daten gespeichert?
 - Sind regulatorische Anforderungen zu beachten?
 - Sind die Ereignisse idempotent?
 - Ist eine Echtzeitverarbeitung mit Streams gefordert?
 - Müssen Ereignisse korreliert werden?
- Nicht-funktionale Aspekte
 - Welche Größe weisen die Ereignisse auf?
 - Welche Latenzen sind zugelassen?
 - Welcher Durchsatz wird erwartet?

Aus dieser Analyse identifiziert der AN die notwendigen Plattform-Komponenten, -Services und -Konfigurationen sowie Wissenstransferleistungen (z.B. Onboarding, Dokumentation, Beratung), die für die Realisierung der Anwendungsfälle durch die Fachabteilungen der TK notwendig sind.

Dabei entstehen Arbeitspakete (Epics, Stories, Unteraufgaben), die iterativ-inkrementell umgesetzt werden. Der AN stimmt die Einpriorisierung der Arbeitspakete in die Iterationsplanung mit der TK ab. Dies gilt auch für neu auftretende Anwendungsfälle während der Projektlaufzeit.

Der AN berät die TK in diesem Kontext dahingehend, ob sich die Plattform für den jeweiligen Anwendungsfall sinnvoll einsetzen lässt. Hierfür analysiert er die fachlichen Anwendungsfälle dahingehend, ob

eine Umsetzung mithilfe von Apache Kafka empfehlenswert ist. Durch seine Analyse muss der AN gegenüber der TK nachvollziehbar begründen, ob eine fachliche Anforderung mithilfe von Apache Kafka sinnvoll umgesetzt werden kann oder ob eine alternative Technologie die bessere Wahl darstellt.

2.1.2. KRITIS-Relevanz

Die anvisierte Plattform wird perspektivisch als kritische Infrastruktur (KRITIS) eingestuft, gemäß IT-Sicherheitsgesetz 2.0 und BSI-Verordnung. Die Plattform muss daher so aufgebaut sein, dass sie auf Anforderung der TK eine redundante Replikation, Multi-AZ-Deployment, kontinuierliches Monitoring sowie Meldepflichten bei Störungen umfasst, um die diesbezüglichen regulatorischen Anforderungen zu erfüllen und Produktionsbereitschaft zu gewährleisten.

2.1.3. Aktualität der Kafka-Plattform

Der AN baut die Plattform auf Basis der aktuellen Versionen der hierfür notwendigen Komponenten. Insbesondere bei der Kernkomponente Apache Kafka kommt mindestens die Version 4.2.0 zum Einsatz. Neue Versionen werden nach Rücksprache mit der TK zeitnah eingebaut.

Der AN beobachtet laufende Entwicklungen (z.B. neue KIPs, Kroxylicious) im Kafka-Ökosystem und macht die TK auf relevante Neuerungen aufmerksam, die Mehrwerte für die Plattform darstellen können. Nach Abstimmung mit der TK wird der Einbau der neuen Funktionen eingeplant und umgesetzt.

2.1.4. Systemtrennung und Migration

Der Aufbau der Plattform muss in verschiedenen Umgebungen erfolgen. Je nach Anwendungsfall kann die Anzahl dieser Umgebungen variieren. Es sind vom AN pro Cluster aber mindestens 3 Umgebungen, nämlich jeweils eine Entwicklungs-, eine Test- und Produktionsumgebung aufzubauen. Bei Bedarf der TK hat der AN weitere Test-Umgebungen aufzubauen.

Der AN stellt sicher, dass in jeder Umgebung die Prinzipien des Infrastructure-as-Code (IaC) und GitOps berücksichtigt werden. Die Infrastruktur in den Umgebungen werden mithilfe von IaC und GitOps sowie mit CI/CD (GitHub Actions) definiert, provisioniert und kontinuierlich gewartet. Infrastrukturelle Änderungen an der Plattform werden automatisiert von den Entwicklungs- über die Test- zu den Produktionsumgebungen propagiert.

IaC und GitOps sind auch bei der Konfiguration von Topics, Schemas, ACLs und sonstige Ressourcen zu berücksichtigen. Der AN definiert hierzu die notwendigen Abläufe (GitOps Pipelines, Pull Request Struktur) in Zusammenarbeit mit der TK. Es entstehen wohldefinierte GitOps-basierte Abläufe für Administratoren und Nutzer der Plattform.

Die TK hat derzeit einen Kafka-Test-Cluster in Betrieb. Ursprünglich wurde dieser Cluster für ein Proof of Concept genutzt. Erste Anwendungen der TK nutzen diesen Cluster sowohl für Test- als auch Produktionszwecke. Der AN migriert bei Bedarf und in Rücksprache mit der TK vorhandene Daten aus diesem Cluster in die neue Plattform.

2.1.5. Verfügbarkeit & Ausfallsicherheit

Die Plattform muss so aufgebaut werden, dass perspektivisch eine sehr hohe Verfügbarkeit erreicht werden kann. Daraus ergibt sich, dass die Plattform ab dem Zeitpunkt der Inbetriebnahme entsprechender Anwendungsfälle als kritisch angesehen wird und dass Incidents mit folgenden SLA-Zielen bearbeitet werden müssen (s. auch Abschnitt 2.4.4):

- Reaktionszeit maximal 1 Stunde
- Maximale Wiederanlaufzeit (RTO): 4 Stunden
- Maximaler Datenverlust (RPO): 10 Minuten
- Servicezeit 1: Montag bis Freitag von 08:00 bis 17:00 Uhr (Ausnahme bundeseinheitliche Feiertage und Hamburger Feiertage)
- Servicezeit 2: 24/7

Die entsprechende Ausfallsicherheit sowie die Lastverteilung sind zu gewährleisten. Das Konzept des Stretched Clusters ist hierbei zu berücksichtigen. Die TK verfügt über zwei Hauptrechenzentren und ein Nebenrechenzentrum (2,5 Rechenzentren), die zu diesem Zweck zum Einsatz kommen sollen.

Der Replikationsfaktor für alle Topics wird auf 3 gesetzt, um eine hohe Verfügbarkeit und Fehlertoleranz sicherzustellen. Die Plattform muss in der Lage sein, bei Ausfall von Brokern weiterhin Nachrichten zu verarbeiten, ohne die Leistung zu beeinträchtigen.

Die Plattform soll bei einer Erhöhung der Broker-Anzahl um mindestens 20 % automatisch ein Re-Balance der Partitionen auslösen, damit die Last gleichmäßig verteilt bleibt. Der Rebalance-Vorgang wird über ein bewährtes Open-Source-Tool (z. B. Kafka Cruise Control) oder ein Skript gesteuert.

2.1.6. Disaster Management

Sofern für bestimmte Bestandteile der Plattform und Anwendungsfälle Backups relevant sind, setzt der AN dedizierte Cluster nach Rücksprache mit der TK um.

2.1.7. Kafka Tiered Storage und Diskless

Um eine Langzeitspeicherung von Kafka-Nachrichten zu unterstützen, überprüft der AN die Anwendbarkeit von Kafka Tiered Storage sowie von einem Kafka Diskless Betrieb auf Basis der Anwendungsfälle der TK (s. auch Abschnitt 2.2.1.6 und 2.2.1.7).

2.1.8. Performance

Die Plattform weist perspektivisch eine sehr gute Performance auf. Folgende Anforderungen beschreiben einen Zielzustand, wenn die Plattform entsprechend gewachsen ist und alle unter Ziffer 1.3 genannten Anwendungsfälle der TK umgesetzt sind. Der AN erstellt auf Anforderung der TK einen klaren Skalierungs- und Architekturplan für die nachfolgend genannten Anforderungen, damit die TK diesen Zielzustand der Plattform perspektivisch erreichen kann:

- Durchsatz: Die Plattform ist in der Lage, bis zu 1.000.000 Nachrichten pro Sekunde zu verarbeiten.
- Es werden Nachrichten mit einer maximalen Größe von 1 MB pro Nachricht unterstützt.
- Latenz: Die End-to-End-Latenz für 95 % der Nachrichten liegt bei weniger als 100 Millisekunden. Es ist möglich, für spezifische Echtzeitanwendungsfälle mit einer entsprechenden Nachrichtengröße eine Latenz von weniger als 10 Millisekunden zu erreichen.
- Produzenten sind in der Lage, Nachrichten mit einer Batch-Größe von bis zu 1 MB pro Anforderung zu senden und eine Wartezeit (Linger) von bis zu 50 Millisekunden zu konfigurieren, um den Durchsatz zu optimieren.

- Konsumenten sind in der Lage, mit einer Latenz von weniger als 100 Millisekunden zu operieren, um einen Nachrichtenlag von maximal 10 Nachrichten zu erreichen.

2.1.9. Datenaufbewahrung

Die Plattform muss die unbegrenzte Speicherung von Nachrichten in bestimmten Topics unterstützen. Wechselwirkungen mit anderen Eigenschaften der Plattform werden hierbei berücksichtigt und aufgezeigt.

2.1.10. Skalierbarkeit

Die Plattform ist so aufzubauen, dass eine vertikale sowie horizontale Skalierung jederzeit und nahtlos ermöglicht werden. Für die Skalierung sind die bei der TK verfügbaren Virtualisierungsmechanismen zu verwenden, insbesondere die OpenShift Container Platform sowie bei Bedarf virtuelle Maschinen auf Basis von VMWare.

Die Plattform ist in der Lage, die Anzahl Broker dynamisch und ohne signifikante Leistungseinbußen hoch- und herunterzuskalieren. Genauso ist ein Scale-Up und -Down der Partitionen pro Topic möglich.

2.1.11. IT-Sicherheit

Die anvisierte Plattform weist einen hohen Schutzbedarf hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität auf. Der AN berücksichtigt diesen beim Aufbau der Plattform und setzt die Anforderungen gemäß Anlage „V3 Informationssicherheit“ um. Darüber hinaus setzt der AN folgende spezifische IT-Sicherheitsanforderungen um:

- Authentifizierung: Nur autorisierte Benutzer erhalten Zugriff auf die Plattform. Active Directory bzw. Entra ID ist einzusetzen. SSO ist zu implementieren. Bei Bedarf ist Keycloak einzusetzen.
- Autorisierung: Authentifizierte Benutzer dürfen nur die ihnen erlaubten Aktionen im System durchführen. Ein Autorisierungssystem wird mithilfe der bereits bestehenden TK-internen Rollenverwaltung aufgebaut, das die Berechtigungen der Benutzer definiert und durchsetzt. Die Autorisierungsfunktionen erlauben die Umsetzung feingranularer Berechtigungen auf Topic-Ebene.
- Verschlüsselung des Netzwerkverkehrs (in transit): Der AN implementiert Maßnahmen zur Verschlüsselung und Signierung des Netzwerkverkehrs, um die Integrität und Vertraulichkeit der übertragenen Daten zu gewährleisten.
- Field Level Encryption: Es ist möglich, auf Anforderung der TK bestimmte Felder in Nachrichten zu verschlüsseln, die hochsensible Daten erhalten (z.B. Personendaten). Client-Side Field Level Encryption (ggf. Kryptonite) kommt nach Möglichkeit zum Einsatz.
- Unterstützung für eine Vault-Integration (Secrets Management) zur dynamischen Bereitstellung von Secrets für Kafka-Komponenten

2.1.12. Container-Technologien

Die Plattform muss serverseitig mit Container-Technologien betrieben werden; Dabei ist OpenShift als Kubernetes-Plattform zu nutzen, wobei ausschließlich die von Red Hat offiziell freigegebenen Operators verwendet werden dürfen.

2.1.13. Stream Processing

Für Echtzeit- und ETL-Szenarien wird Stream-Processing mithilfe von ksqldb oder Apache Flink möglich sein. Persistente Queries sowie Materialized Views ermöglicht (s. auch 2.2.1.8).

2.1.14. Befähigung der Softwareentwickelnden

Bei Bedarf und auf Anforderung der TK befähigt der AN TK-Mitarbeitende, die Software entwickeln, die Plattform zu nutzen. Zur Befähigung gehören Maßnahmen wie Beratung, Coaching, Schulungen, Workshops, Pair Programming Sitzungen, Dokumentation, technische Leitplanken, Vermittlung von Best Practices. Ziel der Befähigung ist die Beschleunigung, Qualitätssicherung und Standardisierung der Softwareentwicklung auf Basis von Apache Kafka.

Der AN befähigt Softwareentwickelnde der TK insbesondere in folgenden Bereichen:

- Konfiguration und Implementierung von Consumer und Consumer-Gruppen
- Konfiguration und Implementierung von Producer
- Serialisierung und Deserialisierung
- Nutzung von Quotas
- Nutzung von Datenkompression
- Entwurf von Ereignissen und Schemas, Nutzung der Schema-Registry
- Nutzung von bewährten Kafka-Patterns und Vermeidung von Anti-Patterns
- Transaktionen mit Kafka
- Nutzung von Kafka Connect
- Nutzung von Kafka Streams

2.1.15. Developer Experience

Der AN berücksichtigt Self-Service und Developer Experience Aspekte. TK-Mitarbeitenden, die Anwendungen mithilfe der Plattform entwickeln, wird die Verwendung der Plattform durch Tooling, Automatisierung, Programmierung und ggf. Veredelung von Kafka-Funktionen erleichtert. Das Internal Developer Portal und sonstige Automatisierungsmechanismen (z.B. GitHub Actions, ArgoCD, OpenShift, Control-M) der TK sind nach Möglichkeit zu verwenden. Die kognitive Last wird für die Benutzer dabei reduziert, Standardisierung und Produktivität werden dabei erhöht.

2.1.16. Integration mit API Management

Der AN prüft die Möglichkeiten der Integration der Plattform mit dem API-Management-System der TK (aktuell Red Hat 3Scale. Das API-Management-System wird derzeit neu beschafft). Auf Anforderung der TK hat der AN diese Integration zu implementieren. Bei Bedarf hat der AN zudem die Anbindung an die API-Gateway und ggf. (falls die Komponente verfügbar ist) an das API-Schema-Repository auf Anforderung der TK zu implementieren.

2.1.17. Lifecycle der Anwendungsentwicklung

Die Zielarchitektur ist von lokalen Embedded Kafka Cluster oder Docker-Images für Softwareentwickler bis zu produktiven, hochverfügbaren (On-Premises) Clustern den Lifecycle der Anwendungsentwicklung ganzheitlich als zentrale Komponente zu unterstützen.

Ein hoher Automatisierungsgrad mittels CI/CD-Pipelines (GitHub Actions) und GitOps (GitHub, ArgoCD, OpenShift) ist umzusetzen. Der AN baut ein System auf, womit Änderungen systematisch durch die verfügbaren Umgebungen (s. Abschnitt 2.1.4) weitergeleitet werden, bevor sie in Betrieb genommen werden.

Bei Bedarf und nach Rücksprache mit der TK implementiert der AN auch Performance Tests der Plattform, um die Einhaltung der nicht-funktionalen Anforderungen kontinuierlich zu prüfen. Gängige Werkzeuge, Frameworks und Fault Injectors kommen dabei zum Einsatz.

2.1.18. Lineage & Anbindung an das Datenkatalogsystem der TK

Die TK nutzt das Datenkatalogsystem Synabi / D-QUANTUM. Auf Anforderung der TK implementiert der AN eine Integration zwischen der Kafka-Plattform und D-Quantum, so dass eine lückenlose Dokumentation von Topic-Änderungen, Partition- und Zugriffs-Metadaten (RBAC) erfolgen kann.

Die Integration hat die üblichen Kafka-Schnittstellen (Broker-API, Admin-Client, JMX, Connect-REST, ksqldb/Flink, Schema-Registry) sowie die Synabi-D-QUANTUM-REST-API und ggf. OpenTelemetry und OpenLineage zu nutzen, um eine konsistente, gesicherte und auditierbare Lineage-Dokumentation zu gewährleisten.

2.1.19. Management Review

Vierteljährlich oder auf besondere Anforderung der TK wird ein Management Review bei der TK vor Ort (Präsenz) in der Unternehmenszentrale der TK in Hamburg durchgeführt. Hieran nimmt bei Bedarf auf Anforderung der TK mindestens der Projektleiter des AN teil. Zudem unterstützt der AN auf Anforderung der TK auch bei der Erstellung von entsprechenden Berichten und Dokumentationen. Das Ziel dieser Reviews soll eine proaktive Betreuung fördern, Schwachstellen rechtzeitig aufzeigen sowie die Zusammenarbeit zwischen AN und TK fördern. Über die Notwendigkeit der Teilnahme und die in diesem Zusammenhang erforderlichen Unterstützungsleistungen stimmen sich die Parteien rechtzeitig vor dem Termin ab.

2.1.20. Fernzugriff

Der AN hat den Aufbau der Plattform grundsätzlich über einen Fernzugriff (remote) zu erbringen, sofern für einzelne Leistungsbestandteile in dieser LB nichts anderes geregelt ist. Die dafür notwendige Remote-Infrastruktur liegt bei der TK vor. Es kommen VPNs und JumpHosts zum Einsatz. Der Zugriff auf alle TK-Systeme erfolgt vorzugsweise über Benutzerkonten (Windows Accounts) und Endgeräte (z.B. Windows Notebooks), die von der TK an den AN bereitgestellt werden. Ein physischer Zugang zum Rechenzentrum der TK wird nur in Ausnahmefällen möglich sein.

2.2. Enterprise Funktionen

Der AN hat im Rahmen des Auftrags auf Abruf der TK, Enterprise-Funktionen für die Plattform zu liefern, anzupassen und zu installieren.

2.2.1. Lieferung Enterprise-Funktionen

Der AN hat auf Anforderung der TK die nachfolgend (Abschnitt 2.2.1.1 bis 2.2.1.8) aufgeführten Enterprise-Funktionen für die Plattform zu liefern, die aus einer marktüblichen Software, welche vom Hersteller bzw. der Community (im Fall von Open Source) aktiv weiterentwickelt wird, bestehen muss. Die Konkretisierung der Leistung (insbesondere die Konfiguration und ggf. erforderliche Implementierungsleistungen) erfolgt zu dem Zeitpunkt, an dem die Leistung benötigt wird.

Der AN hat die in diesem Abschnitt dargestellten Enterprise-Funktionen nach folgendem Schema auf Abruf zu liefern (s. auch Preisblatt Ziffer 2 Positionen 5 bis 9 sowie 10 bis 14):

1. Die Positionen 5 bis 9 unter Ziffer 2 im Preisblatt (Anlage A1) enthalten jeweils alle Enterprise-Funktionen gemäß den Abschnitten 2.2.1.1 bis 2.2.1.8. Es werden vom AN alle Enterprise-Funktionen zusammen als eine Position geliefert. Bei Abruf der Position ist die TK berechtigt alle darin enthaltenen kommerziellen Funktionen zu verwenden.
2. Die Positionen 5 bis 9 unter Ziffer 2 im Preisblatt (Anlage A1) gelten jeweils pro Kafka-Plattformknoten (Node), auf dem die Enterprise-Funktionen installiert und ausgeführt werden. Ruft die TK eine Position ab, so ist sie berechtigt, alle enthaltenen Enterprise-Funktionen auf einem Knoten zu verwenden.
3. Für jeden Kafka-Plattformknoten (Node), auf dem Enterprise-Funktionen installiert werden, wird zudem eine der nachfolgenden Kritikalitätsstufe abgerufen, welche die TK nach Bedarf festlegen kann:
 - a. Hoch: Eine 24x7- Erreichbarkeit für Support-Anfragen. Es ist eine unbegrenzte Anzahl an Support-Tickets pro Monat enthalten. Auf Support-Anfragen der höchsten Priorität wird innerhalb von 30 Minuten reagiert. Dringende Fehlerbehebungen und Sicherheitsupdates sowie Zugriff auf Wissensportale des Herstellers sind enthalten.
 - b. Mittel: Eine 24x7- Erreichbarkeit für Support-Anfragen. Es ist eine unbegrenzte Anzahl an Support-Tickets pro Monat enthalten. Auf Support-Anfragen der höchsten Priorität wird innerhalb von 60 Minuten reagiert. Dringende Fehlerbehebungen und Sicherheitsupdates sowie Zugriff auf Wissensportale des Herstellers sind enthalten.
 - c. Niedrig: Eine 24x7- Erreichbarkeit für Support-Anfragen. Es sind mindestens 6 Support-Tickets pro Monat enthalten. Auf Support-Anfragen der höchsten Priorität wird innerhalb von 90 Minuten reagiert. Regelmäßige (z. B. 1 x monatlich oder innerhalb einer definierten Frist) Fehlerbehebungen und Sicherheitsupdates sind enthalten.
4. Die Kafka-Plattformknoten (Nodes) werden in Rechnerverbunden (Clustern) gruppiert. Innerhalb eines Clusters gilt dieselbe Kritikalität für alle Kafka-Plattformknoten des Clusters.
5. Für jeden Kafka-Plattformknoten, der Enterprise-Streaming-Funktionen benötigt (siehe Abschnitt 2.2.1.8), wird vom AN ein Streaming-Add-on zusätzlich zu den Positionen 5 bis 9 unter Ziffer 2 im Preisblatt (Anlage A1) auf Bedarf und Abruf der TK geliefert.
6. Zur Klarstellung: Sofern eine Position auch solche Enterprise-Funktionen beinhalten, die über die in dieser Leistungsbeschreibung ausdrücklich genannten Leistungen hinausgehen, werden diese nicht gesondert vergütet, sondern sind in der jeweiligen Preisposition bereits enthalten.
7. Es ist möglich, dass eine in diesem Abschnitt geforderte Enterprise-Funktion auf Basis von Open-Source-Software realisiert wird. Es ist allerdings nur Open-Source-Software zugelassen, für die kommerzieller Support durch den AN oder einen Dritten gemäß obiger Kritikalitätsstufen zur Verfügung steht.

2.2.1.1. RBAC + ACL Security

Zweck	Zentrale, rollenbasierte Zugriffskontrolle (RBAC) und feingranulare Zugriffskontrolllisten (ACL) für Topics, Consumer Groups und Cluster Ressourcen.
--------------	--

Funktionsumfang	<ul style="list-style-type: none"> • Definition von Rollen (Admin, Producer, Consumer, Auditor). • Das Autorisierungsmodell folgt dem Default-Deny-Prinzip und stellt eine Standard-Konfliktauflösung für überlappende RBAC- und ACL-Richtlinien bereit. • Zuordnung von Rollen zu LDAP/AD-Nutzern oder Service Accounts. • Zugang zum Cluster über AD-basierte AuthN und AuthZ • ACL-Regeln auf Topic, Partition und Cluster Ebene (Read/Write/Describe). • ACL und RBAC unterstützen ressourcenbasierte Berechtigungen für Topics, Partitionen, Consumer Groups, TransactionalIds und Cluster-Ressourcen, einschließlich präfix- bzw. patternbasierter Regeln. • Echtzeitprüfung von Berechtigungen beim Produzieren und Konsumieren
Technische Schnittstellen	<ul style="list-style-type: none"> • REST-API für den standardisierten Zugriff auf das Rollen- und ACL-Management • Active Directory Bind (TLS gesichert). • (optional) JMX-MBeans zur Überwachung von AuthHits. / Erfüllung von KIP-220 • <code>org.apache.kafka.server.authorizer.Authorize</code>

2.2.1.2. Schema Registry

Zweck	<p>Zentraler, versionierter Speicher für Avro/Protobuf/JSON/AsyncAPI -Schemas; gewährleistet schemakompatible Datenflüsse.</p> <p>Der AN sorgt für die technische Infrastruktur und berät die TK über notwendige organisatorische Prozesse, sodass Produzenten und Konsumenten abgestimmt mit Daten-schemas sowie mit Schemaänderungen operieren können.</p>
Funktionsumfang	<ul style="list-style-type: none"> • Unterstützung konfigurierbarer Subject- und Naming-Strategien (z. B. Topic-, Record- oder kombinierte Strategien) zur Steuerung von Schema-Versionierung, Kompatibilitätsprüfung und Schema-Wiederverwendung. Unterstützung für Deterministische Schema-IDs (für Replikation und Multi-Cluster, Disaster Recovery) • Feingranulare Zugriffskontrolle (RBAC/ACL) für Schema-Operationen (Lesen, Registrieren, Löschen, Kompatibilität ändern). • Die Schema Registry ist hochverfügbar ausgelegt und kann ohne Single Point of Failure betrieben werden. • Registrierung, Versionierung und Abfrage von Schemas über REST / Kafka Topic. • Kompatibilitätsprüfungen (BACKWARD, FORWARD, FULL). • Gewährleistung der Unterstützung von Schema-Evolution durch robuste Validierungs- und Kompatibilitätsprüfungen, die einen nahtlosen Datenfluss selbst in Umgebungen mit hohem Datenaufkommen ermöglichen. • Möglichkeit zur Archivierung und Löschung veralteter Versionen.
Technische Schnittstellen	<ul style="list-style-type: none"> • REST-API (OpenAPI) für einen standardisierten Zugriff auf Schema-Metadaten • Schema-Registry-Integration für ksqldb und Apache Flink • KafkaProducerInterceptor (automatischer Schema Fetch). • SSO-Integration mit OAuth/OIDC.

2.2.1.3. Topic Management & Quota-Steuerung

Zweck	Zentralisierte Verwaltung von Topics, Partitions, Replication-Factor sowie Durchsatz und Speicher-Quotas.
--------------	---

Funktionsumfang	<ul style="list-style-type: none"> Die Erstellung, Änderung und Löschung von Topics ist automatisierbar (API/GitOps/IaC) Erstellung, Änderung und Löschung von Topics per API/CLI. Partitionserweiterungen sowie die Umverteilung von Partitionen erfolgen im laufenden Betrieb automatisiert und ohne Unterbrechung für Producer- und Consumer-Workloads. Dies schließt automatische Leader-Neuwahl, gleichmäßige Lastverteilung, konsistente Replikation und koordinierte Consumer-Group-Rebalancing-Mechanismen ein. Implementierung einer flexiblen automatisierten Naming Convention Prüfung, die anpassbar ist, um den spezifischen Anforderungen der TK gerecht zu werden. Festlegung von Producer/Consumer-Quotas (KB/s, Bytes/second). Retention Policy (Zeit / Größenbasiert) konfigurierbar.
Technische Schnittstellen	<ul style="list-style-type: none"> Kafka Admin Client (Java, Python). REST-Gateway.

2.2.1.4. Graphische Oberfläche und Administrations-Konsole

Zweck	Grafische Oberfläche zur Überwachung, Analyse und Steuerung der Kafka-Plattform.
Funktionsumfang	<ul style="list-style-type: none"> Live Dashboard (Broker Health, Lag Analyse, Throughput). Übersichtliche Darstellung von <ul style="list-style-type: none"> RBAC + ACL Topics, Partitionen, Replication-Factor und Quotas Schema Registry Unterstützung zur zentralen Ansicht und Steuerung (z.B. Topic-Erstellung, Quotas, Replication-Factor oder RBAC-Rollen) mehrerer Kafka-Cluster/Umgebungen inklusive der Mandantentrennung. Automatisierte Erzeugung von Alarmen- und Benachrichtigungs-Events (Grafana/Prometheus-Integration). Historische Metriken (bis 12 Monate). Rollenbasiertes UI-Zugriffs-Management (RBAC-Integration). Audit Log mittels OpenTelemetry aller Zugriffe auf die Konsole.
Technische Schnittstellen	<ul style="list-style-type: none"> REST API für externe Tool Integration. (optional) JMX Export für Metrics Collector / Erfüllung von KIP-220

2.2.1.5. Mirroring / Multi Region Replication

Zweck	Asynchrone, bidirektionale Replikation von Topics über mehrere Kafka Cluster (z. B. Produktion ↔ Backup).
--------------	---

Funktionsumfang	<ul style="list-style-type: none"> • Konfiguration von Replication Flows per Connect Connector. • Gewährleistung von hoher Konsistenz durch den Einsatz von Fehlerbehandlung, die auch bei Netzwerkunterbrechungen eine hohe Datenintegrität sicherstellt. • Split-Brain-/Loop-Prevention bei bidirektionaler Replikation • Automatisches Failover und Wiederherstellung. • Erfüllung von KIP-965 und KIP-382 zur Unterstützung von Mirroring / Multi Region Replication • Verschlüsselung (TLS) und Authentifizierung (SASL) über die Replication Links.
Technische Schnittstellen	<ul style="list-style-type: none"> • Kafka Connect-API (REST). • Konfigurationsdateien (JSON/YAML).

2.2.1.6. Tiered Storage

Zweck	Grundfunktionalität für das Offloading alter Log Segmente in On-Prem Object Stores, um lokale Speicherkapazität zu schonen.
Funktionsumfang	<ul style="list-style-type: none"> • Automatisches Verschieben von Logs ab definiertem Retention Alter oder Segment Größe. • Unterstützung von S3-kompatiblen Object Stores, idealerweise von ECS • Realisierung einer transparenten Lese-/Schreibmethode durch den Einsatz standardisierter Schnittstellen, die eine reibungslose Zusammenarbeit zwischen verschiedenen Clients unabhängig von ihren spezifischen Implementierungen ermöglicht. • Second-Level Autoscaling • Multi-AZ ohne Cross-AZ Traffic • Unterstützung für KIP-405
Technische Schnittstellen	<ul style="list-style-type: none"> • TLS-gesicherte Verbindung zum Object Store.

2.2.1.7. Diskless / Log Compaction Optimierung

Zweck	Grundfunktionalität zur Reduktion von Festplatten-I/O und Speicherverbrauch durch Log Compaction sowie diskless Cache Techniken für passende Anwendungsfälle.
Funktionsumfang	<ul style="list-style-type: none"> • Diskless Broker Architecture • Aktivierbare log-compaction-Policy pro Topic. • Diskless-Cache (Memory-Mapped Files) für Hot-Data-Segment-Zugriffe. • Monitoring-Metriken für Compaction-Rate und Cache-Hit-Ratio • S3-Native Compaction, die direkt im Object Store statt auf Broker-Disks ausgeführt wird
Technische Schnittstellen	<ul style="list-style-type: none"> • (optional) JMX-MBeans für Compaction-Statistiken.

2.2.1.8. Streaming

Zweck	Hochverfügbare, sichere und regelkonforme Streaming-Pipelines
Funktionsumfang	<ul style="list-style-type: none"> • Stream Katalog

	<ul style="list-style-type: none"> • Data Contracts inklusive dem entsprechenden Lebenszyklus (Definition, Versionierung, Impact-Analyse) und nahtlose Integration mit der Schema Registry • Zentrale Governance-Engine: Rollen- und Rechte-Policies, Auditing und Änderungs-Log. • Automatisierte, regelbasierte Skalierung und Load-Balancing, die Broker-Instanzen dynamisch hoch- bzw. runterskaliert. • Feldverschlüsselung (CSFLE)
Technische Schnittstellen	<ul style="list-style-type: none"> • REST-APIs

2.2.2. Installation der Enterprise-Funktionen

Der AN hat die von ihm gelieferten Enterprise-Funktionen in den drei Rechenzentren der TK in Hamburg zu installieren.

2.2.3. Anpassung der Enterprise-Funktionen

Der AN hat bei Bedarf und Abruf der TK die von ihm gelieferten Enterprise-Funktionen in Abstimmung mit der TK anzupassen, beispielweise durch Programmierung oder Konfiguration.

2.3. Kafka-Konnektoren

Der AN hat im Rahmen des Auftrags auf Abruf der TK Kafka Konnektoren nach den Vorgaben der Kafka Connect Architektur für die Plattform zu liefern, anzupassen und zu installieren.

2.3.1. Lieferung Kafka-Konnektoren

Der AN hat der TK auf Abruf die nachfolgend aufgeführten Kafka-Konnektoren für die Plattform zu liefern, die aus einer marktüblichen Software, welche vom Hersteller bzw. der Community (im Fall von Open Source) aktiv weiterentwickelt wird, bestehen muss.

Der AN hat die in diesem Abschnitt dargestellten Kafka-Konnektoren nach folgendem Schema auf Abruf zu liefern, sofern diese kostenpflichtig sind (s. auch Preisblatt Ziffer 2 Positionen 15 bis 23):

- a) Kommerzielle-Konnektoren werden in Paketen angeboten. Ein Paket beinhaltet fünf Arten von Konnektoren.
- b) Spezielle Konnektoren (Premium), die besondere Anforderungen erfüllen (z. B. Integration mit bestimmten Systemen, Unterstützung proprietärer Technologien) werden einzeln angeboten.
- c) Für jeden Konnektor (kommerziell oder Premium) wird zudem eine der nachfolgenden Kritikalitätsstufe abgerufen, welche die TK nach Bedarf festlegen kann:
 - (1) Hoch: Eine 24x7- Erreichbarkeit für Support-Anfragen. Es ist eine unbegrenzte Anzahl an Support-Tickets pro Monat enthalten. Auf Support-Anfragen der höchsten Priorität wird innerhalb von 30 Minuten reagiert. Dringende Fehlerbehebungen und Sicherheitsupdates sowie Zugriff auf Wissensportale des Herstellers sind enthalten.
 - (2) Mittel: Eine 24x7- Erreichbarkeit für Support-Anfragen. Es ist eine unbegrenzte Anzahl an Support-Tickets pro Monat enthalten. Auf Support-Anfragen der höchsten Priorität wird innerhalb von 60 Minuten reagiert. Dringende Fehlerbehebungen und Sicherheitsupdates sowie Zugriff auf Wissensportale des Herstellers sind enthalten.
 - (3) Niedrig: Eine 24x7- Erreichbarkeit für Support-Anfragen. Es sind mindestens 6 Support-Tickets pro Monat enthalten. Auf Support-Anfragen der höchsten Priorität wird innerhalb von 90 Minuten reagiert.

- ten reagiert. Regelmäßige (z. B. 1 x monatlich oder innerhalb einer definierten Frist) Fehlerbehebungen und Sicherheitsupdates sind enthalten.
- d) Konnektoren werden in Rechnerverbunden (Clustern) betrieben. Innerhalb eines Clusters gilt dieselbe Kritikalität für alle Knoten des Clusters.

2.3.1.1. Kafka-Konnektoren Umfang

Nachfolgend werden Datenquellen und -senken sowie Transformationsfunktionen dargestellt, die in der TK relevant sind und auf Anforderung der TK abgerufen werden.

1. **Datenquelle für Oracle-Datenbanken:** Ermöglicht das Abrufen von Daten aus einer Oracle-Datenbank und das Senden an Kafka.
2. **Datenziel für Oracle-Datenbanken:** Ermöglicht das Schreiben von Daten aus Kafka in eine Oracle-Datenbank.
3. **Datenquelle für PostgreSQL-Datenbanken:** Ermöglicht das Abrufen von Daten aus einer PostgreSQL-Datenbank und das Senden an Kafka.
4. **Datenziel für PostgreSQL-Datenbanken:** Ermöglicht das Schreiben von Daten aus Kafka in eine PostgreSQL-Datenbank.
5. **Datenquelle für Microsoft SQL Server:** Ermöglicht das Abrufen von Daten aus einem Microsoft SQL Server und das Senden an Kafka.
6. **Datenziel für Microsoft SQL Server:** Ermöglicht das Schreiben von Daten aus Kafka in einen Microsoft SQL Server.
7. **Datenquelle für MySQL-Datenbanken:** Ermöglicht das Abrufen von Daten aus einer MySQL-Datenbank und das Senden an Kafka.
8. **Datenziel für MySQL-Datenbanken:** Ermöglicht das Schreiben von Daten aus Kafka in eine MySQL-Datenbank.
9. **Datenquelle für Change Data Capture (CDC) von Oracle:** Ermöglicht das Abrufen von Änderungen aus einer Oracle-Datenbank und das Senden an Kafka.
10. **Datenquelle für Redis:** Ermöglicht das Abrufen von Daten aus einem Redis-Datenspeicher und das Senden an Kafka.
11. **Datenquelle für Neo4j:** Ermöglicht das Abrufen von Daten aus einer Neo4j-Datenbank und das Senden an Kafka.
12. **Datenquelle für MongoDB:** Ermöglicht das Abrufen von Daten aus einer MongoDB-Datenbank und das Senden an Kafka.
13. **JDBC-Datenquelle/-ziel:** Ermöglicht die Verbindung zu verschiedenen relationalen Datenbanken über JDBC, um Daten zu lesen und zu schreiben und diese an Kafka zu senden.
14. **Datenquelle/-ziel für InfluxDB:** Ermöglicht das Abrufen und Schreiben von Zeitreihendaten in eine InfluxDB und das Senden an Kafka.
15. **Datenquelle/-ziel für Amazon S3:** Ermöglicht das Abrufen von Daten aus und das Schreiben von Daten in Amazon S3 und das Senden an Kafka.

16. **Datenquelle/-ziel für ActiveMQ:** Ermöglicht das Abrufen und Schreiben von Nachrichten zu und von einem ActiveMQ-Message Broker und das Senden an Kafka.
17. **Datenquelle/-ziel für RabbitMQ:** Ermöglicht das Abrufen und Schreiben von Nachrichten zu und von einem RabbitMQ-Message Broker und das Senden an Kafka.
18. **Datenquelle/-ziel für JMS (Java Message Service):** Ermöglicht die Interaktion mit JMS-kompatiblen Messaging-Systemen und das Senden an Kafka.
19. **Datenquelle/-ziel für HTTP:** Ermöglicht das Abrufen von Daten von HTTP-Endpoints und das Senden von Daten an HTTP-Endpoints sowie an Kafka.
20. **Datenquelle für Jira:** Ermöglicht das Abrufen von Daten aus Jira und das Senden an Kafka.
21. **Datenquelle für GitHub:** Ermöglicht das Abrufen von Daten aus GitHub und das Senden an Kafka.
22. **Datenquelle für SAP HANA:** Ermöglicht das Abrufen von Daten aus einer SAP HANA-Datenbank und das Senden an Kafka.
23. **Datenquelle für Celonis EMS:** Ermöglicht das Abrufen von Daten aus Celonis EMS und das Senden an Kafka.
24. **Datenkonverter für Avro:** Ermöglicht die Konvertierung von Daten in das Avro-Format für den Datenaustausch mit Kafka.
25. **Transformationsfunktionen (SMT):** Bietet Funktionen zur Transformation von Daten während der Übertragung zwischen Systemen und Kafka. Die Funktionen gehen über den Umfang vom Open Source Kafka Connect hinaus.

2.3.2. Installation der Konnektoren

Der AN hat die von ihm gelieferten Konnektoren in den drei Rechenzentren der TK in Hamburg zu installieren.

2.3.3. Anpassung der Konnektoren

Der AN hat bei Bedarf und Abruf der TK die von ihm gelieferten Konnektoren in Abstimmung mit der TK anzupassen, beispielsweise durch Programmierung oder Konfiguration.

2.4. Production Readiness

Dieser Abschnitt beschreibt alle administrativen, prozessualen und planerischen Arbeiten, die der AN vorbereitend auf die Inbetriebnahme der Plattform gemäß den Vorgaben zur IT Production Readiness (Produktionsbereitschaft) der TK durchzuführen hat.

Mitarbeiter der TK werden den AN bei der Erfüllung dieser Aufgaben unterstützen. Diese Unterstützung ist integraler Bestandteil des Leistungsprozesses und wird in den nachfolgenden Absätzen nicht gesondert erwähnt.

2.4.1. Einbindung in das IT-Servicemanagement der TK

Der AN integriert die Plattform in das bestehende IT-Servicemanagement-System der TK, welches sich an ITIL orientiert. Der AN dokumentiert alle relevanten Informationen, die für das IT-Servicemanagement erforderlich sind, und stellt sicher, dass diese Informationen jederzeit aktuell und zugänglich sind.

Insbesondere umfasst die Dokumentation:

- **Verantwortlichkeiten:** Geschäftsprozess-Verantwortlicher (Kunde) und Service-Owner (IT-Business und IT-Infrastrukturservice) sind bestimmt; Rollen (IT-Produkt/Service-Owner) werden durch das IT-Demandmanagement oder das IT-Management besetzt.
- **Service-Katalog:** Der Service/Produkt-Datensatz wird im Service-Katalog angelegt.
- **Service-Beschreibung:** Vollständige Leistungs- und Funktionsbeschreibung des IT-Services, Freigabe durch den Service-Owner und Eintragung in den Service-Katalog.
- **Rücksprachen mit Gremien:**
 - Service Catalogue Management – Koordination Service-Katalog.
 - IT-Service-Transition – Information und Aufnahme in die Transition-Liste.
 - Mitbestimmung – Prüfen der Mitbestimmungspflicht.
 - Informationssicherheit – Schutzbedarfsfeststellung.
 - Datenschutz – Verfahrensbeschreibung bzw. Datenschutzfolgeabschätzung.
- **KRITIS-Prüfung & RTO:** Fortlaufende Bewertung der KRITIS-Relevanz und Festlegung des Recovery Time Objective (RTO) im Service-Katalog.
- **Datenschutz:** Erstellung einer Datenschutz-Folgeabschätzung oder eines Eintrags im Verfahrensverzeichnis.
- **Technische Lösungsskizze (TL):** Erstellung und Freigabe der TL im Architektur-Board; Aktualisierung bei Änderungen.
- **Knowledge Management:** Einbindung des Knowledge Managements der TK, Einreichung der zugehörigen Checkliste.
- **Schwachstellen und Sicherheits-Check:** Durchführung einer Schwachstellen-Überprüfung durch das SOC bzw. der Informationssicherheit der TK; Dokumentation von Ergebnissen.
- **Betriebsdokumentation:** Erstellung von Betriebshandbuch (BHB), Advices, Alarm und Serviceklassendefinitionen in Abstimmung mit IT Operating.
- **Recovery & Resumption Plan (RRP):** Erstellung und Freigabe des RRP, Durchführung eines Walk-Through-Tests.
- **Kontinuitätstests:** Durchführung und Protokollierung von Kontinuitätstests, Versand an ITSCM.

- **Observability / Monitoring:** Definition einer Monitoring-Strategie (Logs, Metriken, Traces) und Anbindung an das zentrale TK-Monitoring; bei KRITIS-Services mindestens ein Service Health Check.
- **IT-Sicherheitsmonitoring:** Prüfung und ggf. Einrichtung einer Anbindung an das I-Sicherheitsmonitoring (SOC/VSOC).
- **Informationssicherheit:** Umsetzung von Maßnahmen aus der Schutzbedarfsfeststellung; ggf. Einholung einer Ausnahmegenehmigung über das ISM-Board.
- **Zugangsdaten:** Verwaltung und Dokumentation administrativer Logins, insbesondere Notfall-User.
- **Systemdesign & TL-Umsetzung:** Sicherstellung, dass das Systemdesign gemäß der TL umgesetzt ist; ggf. Aktualisierung der TL.
- **Systemtrennung:** Getrennte Entwicklungs-, Test- und Produktionsumgebungen; Dokumentation im Betriebshandbuch und ggf. Staging-Konzept.
- **Anbindung an ITSM-Tool (SMAX):** Prüfung der Notwendigkeit einer SMAX-Anbindung; Erstellung bzw. Anpassung von Ticket bzw. Change-Vorlagen bei Bedarf.
- **Konfigurationsanalyse:** Analyse zur Erkennung von Fehlkonfigurationen und Dokumentation der Ergebnisse.
- **Change-Management für Inbetriebnahme:** Erstellung des Inbetriebnahme-Changes im SMAX, Verknüpfung mit dem Service-Katalog (CMS) und Freigabe durch den Service-Owner.

Auf einige der vorgenannten Punkte wird in den folgenden Abschnitten gesondert eingegangen.

Die Einzelheiten werden nach Vertragsschluss zwischen dem AN und der TK abgestimmt.

2.4.2. Mitbestimmung und Datenschutz

Der AN unterstützt die TK bei der Durchführung der Mitbestimmung durch den zuständigen Personalrat der TK sowie bei der Erstellung einer Verfahrensbeschreibung oder einer Datenschutzfolgeabschätzung. Dies dient dem Schutz der Privatsphäre und Persönlichkeitsrecht der Mitarbeiter oder Versicherten.

2.4.3. Betriebsdokumentation und technische Lösungsskizze

Der AN erstellt ein Betriebshandbuch für die Plattform. Folgende Liste enthält die typischen Elemente nach Vorgaben der TK, die Gegenstand des Betriebshandbuchs sein müssen:

- Glossar
- Konfiguration
- Schnittstellen zu anderen Systemen / Externe Schnittstellen
- Sicherheit
- Benutzerverwaltung und Berechtigungen
- Systemhärtung
- Schwachstellen-Management
- Kryptographie
- Virenschutz

- Aufnahme und Unterbrechung des Betriebs
- Laufender Betrieb
- Datensicherung
- Backup
- Restore
- Überwachung
- Alarmierung
- Reporting
- Logging
- Systemautomation
- Einbindung in ITSM-Prozesse
- Patchmanagement

Zusammen mit dem jeweils begleitenden IT-Architekten der TK erstellt der AN eine technische Lösungsskizze auf Basis der Feinkonzepte (s. Abschnitt 2.1). Diese wird im Architekturboard der TK vorgestellt. Die Lösungsskizze bietet einen Überblick über die beteiligten Hard- und Softwarekomponenten, die Datenhaltung, die Skalierbarkeit, die Integration in die IT-Landschaft der TK, die IT-Sicherheit, die Systemvoraussetzungen und die Rahmenbedingungen für den geplanten Betrieb.

2.4.4. Support, Incidents und Anwenderdokumentation

Für den Betrieb der Plattform definiert und implementiert der AN standardisierte IT-Supportprozesse, die eine effiziente Bearbeitung von Anfragen und Störungen gewährleisten. Auf Anforderung der TK erstellt der AN ein Service-Level-Agreement (SLA) für folgende Verfügbarkeitsanforderungen:

- Reaktionszeit maximal 1 Stunde
- Maximale Wiederanlaufzeit (RTO): 4 Stunden
- Maximaler Datenverlust (RPO): 10 Minuten
- Servicezeit 1: Montag bis Freitag von 08:00 bis 17:00 Uhr (Ausnahme bundeseinheitliche Feiertage und Hamburger Feiertage)
- Servicezeit 2: 24/7

Hinweis zu den Servicezeiten: Der Betrieb der Plattform findet grundsätzlich in der Zeit Montag bis Freitag von 08:00 bis 17:00 Uhr statt. Nach aktueller Schätzung der TK und wenn Anwendungsfälle mit hoher Kritikalität umgesetzt sind, wird ab 2027 ggf. ein 24x7 Betrieb der Plattform erforderlich.

Die durchgängig erreichbare Betriebsabteilung der TK muss vom AN in die Lage versetzt werden, (einfache) Wartungsvorgänge an der Plattform selbst durchzuführen. Hierfür erstellt der AN ein entsprechendes Betriebshandbuch gemäß Vorlage der TK (s. Abschnitt 2.4.3) inklusive geeigneter Playbooks und stellt diese der TK zur Verfügung.

Alle Support- und Incidentfälle müssen im Service Management der TK (SMA von OpenText) dokumentiert werden. Hierzu erstellt der AN entsprechende Ticketvorlagen für SMA und stimmt die Ticket-Workflows mit den TK-Experten ab. Der AN entwickelt ein kontinuierliches Verbesserungssystem, das

auf Nutzerfeedback basiert und die Qualität der Supportleistungen regelmäßig evaluiert. Der AN stellt sicher, dass alle Mitarbeiter im Supportbereich entsprechend den Vorgaben in dieser Leistungsbeschreibung qualifiziert sind und über die notwendigen Ressourcen verfügen, um eine die geforderten Servicezeiten und SLA einzuhalten.

Für den Betrieb der Plattform richtet der AN richtet bei der TK einen Service Desk ein, der für die effiziente Bearbeitung von Vorfällen verantwortlich ist und als zentrale Anlaufstelle für Benutzeranfragen dient. Hierbei sind die Rahmenbedingungen der TK zu berücksichtigen (MS-Teams für die Kommunikation, SMAX für das Incident Management).

Der AN definiert Incident-Kategorisierungen und -Priorisierungen, um sicherzustellen, dass Vorfälle angemessen und zeitnah behandelt werden. Für kritische Vorfälle implementiert er Eskalationsprozesse, die eine schnelle Reaktion und Unterstützung durch höhere Support Level Instanzen gewährleisten. Alle Vorfälle werden im SMAX-Ticketsystem der TK dokumentiert und nachverfolgt, um Transparenz zu schaffen und die Bearbeitungshistorie nachvollziehbar zu machen.

Der AN entwickelt bzw. definiert eine geeignete Eskalationsstruktur mit unterschiedlichen Support Levels gemäß folgenden Vorgaben:

- Servicezeit 1 (Montag bis Freitag von 08:00 bis 17:00 Uhr)
 - o 1st und 2nd Level Support übernimmt der AN
 - o 3rd Level Support bei Bedarf durch den Hersteller der Softwarekomponenten
- Servicezeit 2 (24/7) - sofern notwendig
 - o 1st Level Support durch die Operating-Rufbereitschaft der TK. Betriebshandbücher und Playbooks stehen zur Verfügung, die das Operating bei der Handhabung einfacher Incidents anwenden kann
 - o 2nd Level Support durch die Bereitschaft des AN für die Bearbeitung komplexer Incidents. Es gelten die obigen Verfügbarkeitsanforderungen.
 - o 3rd Level Support bei Bedarf durch den Hersteller der Softwarekomponenten
 - o Handover an die Betriebsunterstützung beim Übergang zu den Bürozeiten

2.4.5. Systemadministration

Der AN implementiert Prozesse für das Benutzer- und Rollenmanagement, das die Zuweisung von Rechten und Zugängen zur Plattform regelt und Sicherheitsanforderungen erfüllt (s. auch Abschnitt 2.1.11).

Er definiert Prozesse für die Durchführung der Systemkonfiguration und -anpassung, um die IT-Infrastruktur der Plattform optimal an die spezifischen Anwendungsfälle der TK anzupassen.

Der AN organisiert ein zuverlässiges Patch- und Update-Management, das alle Systeme regelmäßig auf den neuesten Stand bringt und Sicherheitslücken proaktiv schließt.

Der AN organisiert, dass alle Systemänderungen und -konfigurationen gemäß IT Change Management der TK dokumentiert werden können, um eine nachvollziehbare Historie zu gewährleisten und Compliance-Vorgaben der TK zu erfüllen. Dies beinhaltet auf Anforderung der TK auch die Einreichung, Vorstellung und Abstimmung von Changes im Change Advisory Board der TK.

2.4.6. Systemüberwachung

Die Systemressourcen müssen kontinuierlich überwacht werden, um die Leistung der Plattform durchgehend sicherzustellen.

Der AN erstellt Monitoring-Definitionen zusammen mit der Monitoring-Abteilung der TK. Abhängig von Art und Kritikalität werden Logs, Metriken und Traces in das zentrale TK-Monitoring (Grafana) eingebunden. Sofern Observability-Funktionen verfügbar sind, sind diese zu nutzen. OpenTelemetry ist dabei als Standard nach Möglichkeit zu verwenden. Die Einrichtung von mindestens einem Servicehealth-Check ist ab dem Zeitpunkt der Umsetzung kritischer Anwendungsfälle verpflichtend.

Der AN setzt Überwachungsmetriken gemäß KIP-220 und Abschnitt 2.5 um, um relevante Leistungsindikatoren effektiv zu erfassen und auszuwerten. Zudem etabliert er ein Alarm- und Benachrichtigungssystem, das eine zeitnahe Reaktion auf kritische Ereignisse ermöglicht. Die Alarmdefinitionen werden mit dem Operating der TK abgestimmt und entsprechende Operating Advices werden erstellt.

Der AN implementiert Abläufe zur Protokollierung und Analyse von Systemereignissen, um Muster zu erkennen und potenzielle Probleme frühzeitig zu identifizieren. Außerdem plant der AN regelmäßige Überprüfungen und Anpassungen der Überwachungsrichtlinien durch, um sicherzustellen, dass diese stets den aktuellen Anforderungen und Bedrohungen entsprechen.

2.4.7. Performance Management

Der AN implementiert Kapazitätsplanungs- und -managementprozesse, um sicherzustellen, dass die Cluster-Ressourcen den aktuellen und zukünftigen Anforderungen entsprechen.

Der AN plant Abläufe zur Identifikation von Engpässen in der Systemleistung und entwickelt Maßnahmen zur Performance-Optimierung, um die Effizienz der Plattform zu steigern.

2.4.8. Kontinuierliche Wartung

Der AN plant für die Durchführung geordneter Wartungsfenster gemäß Vorgaben der TK, um sicherzustellen, dass alle Systeme regelmäßig gewartet werden, ohne den Betrieb erheblich zu stören (insbesondere ohne Downtimes).

Er setzt einen Service Transition Prozess für die Überführung von Änderungen in die Produktion gemäß IT Service Management der TK um. Dabei werden folgende Aspekte berücksichtigt:

- Verständnis für Risiken (Risikoanalysen) schaffen.
- Wissens- und Informationsbereitstellung.
- Kommunikation und Abstimmung mit Stakeholdern.
- Einhaltung von rechtlichen, vertraglichen, behördlichen und TK spezifischen Anforderungen

Regelmäßige Systemüberprüfungen sind vom AN zu planen, um den Zustand der Systeme zu evaluieren und potenzielle Probleme frühzeitig zu identifizieren. Zudem hat der AN auch die Dokumentation aller Wartungsaktivitäten und -ergebnisse gemäß IT Service Management der TK für den späteren Betrieb der Plattform zu planen.

Der AN implementiert Feedback-Mechanismen für die Plattform auf Basis der in der TK verfügbaren Mittel (z.B. Teams-Kanäle, Sharepoint-Räume, Confluence-Seiten, JIRA-Tickets) für die Stakeholder der

TK, um Verbesserungspotenziale zu identifizieren und die Wartungsprozesse kontinuierlich zu optimieren. Zudem integriert er Best Practices und Standards in seine Arbeitsabläufe, um die Qualität und Effizienz der Wartungsaktivitäten nachhaltig zu steigern.

2.4.9. Backup- und Wiederherstellungsdienste

Sofern relevant (s. Abschnitt 2.1.6) plant der AN für die Durchführung regelmäßiger Backups, darunter vollständige, inkrementelle und differentielle Backups, um sicherzustellen, dass alle wichtigen Daten zeitnah gesichert werden. Darüber hinaus werden Abläufe etabliert, so die Wiederherstellungsverfahren und -prozesse regelmäßig überprüft werden, um sicherzustellen, dass die Daten im Notfall schnell und zuverlässig wiederhergestellt werden können.

Der AN erstellt ein Recovery & Resumption Plan, um eine klare und nachvollziehbare Vorgehensweise zu gewährleisten. Der AN stellt zudem sicher, dass alle Aktivitäten in Übereinstimmung mit den in der TK geltenden Datenschutzanforderungen durchgeführt werden, um rechtliche Risiken zu minimieren und die Sicherheit sensibler Daten zu garantieren.

2.4.10. Kontinuitätstests

Auf Anforderung der TK organisiert der AN für die Durchführung von Kontinuitätstests und für die Protokollierung der Testergebnisse. Diese bespricht der AN mit dem IT-Service Continuity Management der TK.

Hierbei

- erstellt der AN einen Plan für Kontinuitätstests mit Zieldefinition, Szenarien, Rollen und Ansprechpartner,
- baut der AN eine passende Testumgebung auf und
- bereitet somit die spätere Durchführung vor.

2.4.11. Sicherheitsmanagement

Der AN plant für die Durchführung von Risikoanalysen und Bedrohungseinschätzungen, um potenzielle Sicherheitsrisiken und Schwachstellen der Kafka-Plattform zu identifizieren. Er implementiert Sicherheitsrichtlinien und -standards, gemäß Informationssicherheits-Management-System sowie Informationssicherheitsrichtlinien der TK. Diese orientieren sich an einschlägigen Vorgaben des BSI und den entsprechenden ISO/IEC-Standards.

Es werden Prozesse etabliert, so dass die Sicherheit kontinuierlich überwacht wird, unter anderem durch CVE-Scanning, um aktuelle Bedrohungen zu erkennen und proaktiv darauf zu reagieren. Der AN entwickelt Incident Response-Pläne für Sicherheitsvorfälle, um im Falle eines Vorfalls schnell und effektiv handeln zu können. Diese Pläne gewährleisten eine strukturierte Reaktion auf Sicherheitsvorfälle und minimieren potenzielle Schäden für die TK.

Im Rahmen des Projektes und auf Anforderung der TK ist vom AN ein Kafka-spezifisches Sicherheitskonzept und ggf. Arbeitsanweisungen gemäß Anlage „V3 Informationssicherheit“ zu erstellen. Die regelmäßige Aktualisierung des Sicherheitskonzeptes und ggf. Arbeitsanweisungen sind vom AN zu planen. Der AN aktualisiert auf Anforderung der TK die Schutzbedarfsfeststellung für die Plattform. Ziel ist es, den aktuellen Schutzbedarf der von der Plattform verarbeiteten Informationen hinsichtlich der Aspekte Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu ermitteln.

Eine Anbindung an das SIEM der TK (aktuell IBM QRadar) hat nach Abstimmung mit dem Security Operations Center (SOC) der TK zu erfolgen.

2.4.12. Software-Paketierung

Falls Client-Software für die Nutzung der Plattform benötigt wird, erstellt der AN mithilfe der entsprechenden Abteilung der TK die hierfür notwendigen Softwarepakete, die für die Verteilung der Software an die Nutzer verwendet werden und plant für deren regelmäßige Aktualisierung. Nach Möglichkeit werden Automatismen etabliert, die wichtige notwendige Änderungen an der paketierte Client-Software automatisch erkennen.

2.4.13. Fernzugriff

Der AN hat die Leistungen zur Inbetriebnahme der Plattform grundsätzlich über einen Fernzugriff (remote) zu erbringen, sofern für einzelne Leistungsbestandteile in dieser LB nichts anderes geregelt ist. Für die Einzelheiten des Fernzugriffs wird auf Abschnitt 2.1.19 verwiesen.

2.5. Metriken

Der AN setzt mindestens die nachfolgend aufgeführten Datenpunkte auf Basis des Monitoring-Systems der TK (Grafana, Prometheus) und nach Rücksprache mit der TK um. Die Datenpunkte werden für jeden durch den AN aufgebauten Apache Kafka-Cluster mindestens einmal pro Minute erhoben und mindestens für 28 Tage rückwirkend historisiert und analysierbar vorgehalten werden.

Einige der Metriken werden direkt von Apache Kafka, im Rahmen von KIP-220 bzw. von Enterprise-Funktionen (s. Abschnitt 2.2) mitgeliefert. Es ist davon auszugehen, dass bestimmte Metriken (z. B. Zertifikats-Überprüfungen) Implementierungsarbeiten durch den AN voraussetzen. Diese stimmt der AN vor der Umsetzung mit der TK ab.

Die Darstellung beruht auf angenommenen API-Endpunkten, Metriken-Namen und Beschreibungen, die auf den bereitgestellten Informationen und bestehenden Wissen basieren. Tatsächliche Metriken und Endpunkte können je nach verwendeter Version und spezifischem Monitoring-Setup variieren.

2.5.1. Prozess-Metriken

Das vom AN aufgebaute Monitoring muss Metriken erheben und zur Verfügung stellen, welche separat Auskunft über den aktuellen Prozessstatus bzgl. der Software-Komponenten der Kafka-Broker geben. Der Prozessstatus kann je nach gewählter Betriebskonfiguration über eine „systemd“-Unit, einen Linux-Cluster, einen OCI-kompatiblen Container, den Status eines Pods innerhalb einer OpenShift-Plattform erhoben werden, oder über einen vergleichbaren Mechanismus erhoben werden. Prozess-Metriken sollen außerdem den aktuell durch den Prozess in Anspruch genommene CPU-Zeit sowie Arbeitsspeicher enthalten; insofern hier prozessabhängige Limits bestehen (beispielsweise cgroups, OCI-Container-Limits, Pod-Limits) sollen diese ebenfalls als Metrik abgebildet werden.

Beschreibung/Gruppe	Metriken
Server Metrics	kafka_server_**
Controller Metrics	kafka_controller_**
Consumer Metrics	kafka_consumer_**
Producer Metrics	kafka_producer_**
LDAP Metrics	kafka_metadata_ldapgroupmanager_value oder vergleichbar
Auth Store Metrics	kafka_metadata_kafkaauthstore_value oder vergleichbar
Kafka Connect Server Metrics	kafka_connect_**
Schema Registry Metrics	Registry-spezifisch
REST Proxy Metrics	kafka_rest_**

2.5.2. Health- und Zertifikats-Überprüfungen

Zusätzlich müssen die folgenden Ports der Plattform in regelmäßigen Abständen, mindestens einmal pro Minute, durch einen geeigneten Test (z.B. http-GET, TCP-Verbindungsaufbau) auf Funktionalität überprüft werden.

Sofern vorhanden, muss auf die durch die/den Hersteller der Software bereitgestellten Schnittstellen, z.B. Health- oder Ready-Endpoints, zurückgegriffen werden. Das Ergebnis über den Erfolg der Nutzung dieser Schnittstellen ist in jeweils einer eigenen Metrik abgebildet werden.

Sofern der Datenverkehr des jeweiligen Ports durch Transport Layer Security (TLS/SSL) verschlüsselt bzw. authentifiziert ist, muss automatisiert ebenfalls die verbleibende Gültigkeitsdauer der Zertifikate als Metrik abgebildet werden, um bei Zertifikatsablauf entsprechend handlungsfähig zu sein.

Sollte in der individuellen Konfiguration vom Standard-Port abgewichen werden, oder zusätzliche Ports mit vergleichbarer Funktionalität konfiguriert werden, so gelten die Anforderungen an die Health- und Zertifikats-Überprüfungen analog für diese Ports.

Beschreibung/Gruppe	Protokoll
Kafka Interbroker Listener	TLS
Kafka External Listener	TLS
Server REST API; Metadata Cluster (MDS)	HTTPS
Kafka Connect	HTTPS
ksqlDB / Flink	HTTPS
Schema Registry	HTTPS
REST Proxy	HTTPS
Administrationskonsole	HTTPS

2.5.3. Logausgaben

Logausgaben unter Einhaltung der regulatorischen Anforderungen, welche während der Laufzeit durch die Komponenten der Anwendung entweder über die Standard-/Fehlerausgabe oder in Dateien geschrieben werden, müssen über ein entsprechendes, durch die TK unterstütztes, Monitoring-System von jeder durch die TK betriebenen Apache Kafka-Instanz kontinuierlich erhoben und mindestens für 28 Tage rückwirkend historisiert und durchsuchbar vorgehalten werden.

2.5.4. Alerts

Mindestens die nachfolgend aufgeführten Alerts müssen über ein entsprechendes, durch die TK unterstütztes, Monitoring-System von jeder durch den AN betriebenen Kafka-Instanzen auf Basis der entsprechenden Metriken bei Bedarf ausgelöst, und an das Ticketsystem der TK gemeldet werden. Die notwendigen Voraussetzungen und weitere Systeme (z.B. SMTP-Server), um die Alerts im AN Ticketsystem zu melden, liegen in der Verantwortung der TK.

Beschreibung	Expression	Dauer/ Wert	Severity
BrokersDown	count(kafka_server_replican nager_value{name="LeaderCoun t"}) < 2	1m	Critical

Beschreibung	Expression	Dauer/ Wert	Severity
UnhealthyBrokerShut-downs	sum(kafka_controller_controller_channelmanager_count{name="UnhealthyBrokerControlledShutdown"}) > 0	1m	Warn
ActiveController-CountCritical	sum(kafka_controller_kafkacontroller_value{name="ActiveControllerCount"}) != 1	20s	Critical
RequestHandleIdle	avg(kafka_server_kafkarequesthandlerpool_count{name="RequestHandlerAvgIdlePercent"}) < 0.4	3m	Warn
UncleanLeaderElections-PerSecOverZero	kafka_controller_controllers_stats_count{name="UncleanLeaderElectionsPerSec"} > 0	30s	Warn
UncleanLeaderElections-PerSecOverZero Critical	kafka_controller_controllers_stats_count{name="UncleanLeaderElectionsPerSec"} > 0	1m	Critical
UnderReplicatedPartitions	sum(kafka_server_replicamanager_value{name="UnderReplicatedPartitions"}) > 0	30s	Warn
UnderReplicatedPartitionsCritical	sum(kafka_server_replicamanager_value{name="UnderReplicatedPartitions"}) > 0	60s	Critical
IsrShrinksPerSec (reduction of in-sync replicas per second)	kafka.server:type=ReplicaManager,name=IsrShrinksPerSec	0	Critical
UnderMinIsrPartition-Count	kafka_server_replicamanager_value{name="UnderMinIsrPartitionCount"} > 0	30s	Critical
RequestHandlerAvgIdle-Percent	kafka_server_kafkarequesthandlerpool_oneminuterate{name="RequestHandlerAvgIdlePercent"} < 0.4	30s	Warn
RequestHandlerAvgIdle-PercentCritical	kafka_server_kafkarequesthandlerpool_oneminuterate{name="RequestHandlerAvgIdlePercent"} < 0.4	3m	Critical
NetworkProcessorAvgIdlePercent	kafka_network_socketserver_value{name="NetworkProcessorAvgIdlePercent"} < 0.4	30s	Warn
NetworkProcessorAvgIdlePercentCritical	kafka_network_socketserver_value{name="NetworkProcessorAvgIdlePercent"} < 0.4	3m	Critical
OfflinePartitions	kafka_controller_kafkacontroller_value{name="OfflinePartitionsCount"} > 0	5m	Warn
AvgRequestLatency	avg(kafka_consumer_consumer_coordinator_metrics_commit_latency_avg) > 10	30s	Warn

Beschreibung	Expression	Dauer/ Wert	Severity
AvgRequestLatencyCritical	avg(kafka_consumer_consumer_coordinator_metrics_commit_latency_avg) > 10	60s	Critical
FailedStartSecondsAgo	sum(kafka_metadata_ldap_roupmanager_value{name="failure-start-seconds-ago"}) > 0 oder vergleichbar	1m	Warn
WriterFailedStartSecondsAgo	sum(kafka_metadata_kafka_authstore_value{name="writer-failure-start-secondsago"}) > 0 oder vergleichbar	1m	Warn
ReaderFailedStartSecondsAgo	sum(kafka_metadata_kafka_authstore_value{name="reader-failure-start-secondsago"}) > 0 oder vergleichbar	1m	Warn
RemoteFailedStartSecondsAgo	sum(kafka_metadata_kafka_authstore_value{name="remote-failure-start-secondsago"}) > 0 oder vergleichbar	1m	Warn
ActiveWriterCountOver1	count(kafka_metadata_kafkaauthstore_value{name="active-writer-count"}) > 0) != 1 oder vergleichbar	1m	Warn
MetadataStatus	count(kafka_metadata_kafkaauthstore_value{name="metadata-status"} == FAILED) > 0 oder vergleichbar	1m	Warn
KafkaProducerThrottleTimeAvg	(kafka_producer_producer_metrics_produce_throttle_time_avg >= 0) > 0	5m	Warn
KafkaConsumerFetchThrottleTimeAvg	(kafka_consumer_consumer_fetch_manager_metrics_fetch_throttle_time_avg >= 0) > 0	5m	Warn

2.5.5. Prozess-Alerts

Beschreibung	Ereignis	Group	Dauer	Severity
Prozessstatus nicht gestartet	Der Prozess wird gegenwärtig nicht ausgeführt	Prozess	1m	Warn
Prozessstatus dauerhaft nicht gestartet	Der Prozess wird gegenwärtig nicht ausgeführt	Prozess	5m	Critical

2.5.6. Health-Alerts

Die referenzierten Ports beziehen sich auf die Standard-Ports gemäß der Metriken; sollte in der individuellen Konfiguration hiervon abgewichen werden, oder zusätzliche Ports mit vergleichbarer Funktionalität konfiguriert werden, so gelten die Anforderungen an die Alerts analog.

Beschreibung	Ereignis	Dauer	Severity
Kafka Interbroker Listener	TLS-Health Check nicht erfolgreich absolviert	1m	Warn
Kafka External Listener	TLS-Health Check nicht erfolgreich absolviert	1m	Warn
Kafka Server REST API; Metadata Cluster (MDS)	HTTPS-Health Check nicht erfolgreich absolviert	1m	Warn
Kafka Connect	HTTPS-Health Check nicht erfolgreich absolviert	1m	Warn
ksqlDB / Flink	HTTPS-Health Check nicht erfolgreich absolviert	1m	Warn
Schema Registry	HTTPS-Health Check nicht erfolgreich absolviert	1m	Warn
REST Proxy	HTTPS-Health Check nicht erfolgreich absolviert	1m	Warn
Administrationskonsole	HTTPS-Health Check nicht erfolgreich absolviert	1m	Warn

2.5.7. Zertifikats-Alerts

Die referenzierten Ports beziehen sich auf die Standard-Ports gemäß der Metriken; sollte in der individuellen Konfiguration hiervon abgewichen werden, oder zusätzliche Ports mit vergleichbarer Funktionalität konfiguriert werden, so gelten die Anforderungen an die Alerts analog.

Beschreibung	Ereignis	Dauer	Severity
Kafka Interbroker Listener	Zertifikatsgültigkeit läuft in unter 35 Tagen ab dem aktuellen Zeitpunkt aus	0m	Warn
Kafka External Listener	Zertifikatsgültigkeit läuft in unter 35 Tagen ab dem aktuellen Zeitpunkt aus	0m	Warn
Kafka Server REST API; Metadata Cluster (MDS)	Zertifikatsgültigkeit läuft in unter 35 Tagen ab dem aktuellen Zeitpunkt aus	0m	Warn
Kafka Connect	Zertifikatsgültigkeit läuft in unter 35 Tagen ab dem aktuellen Zeitpunkt aus	0m	Warn
ksqlDB / Flink	Zertifikatsgültigkeit läuft in unter 35 Tagen ab dem aktuellen Zeitpunkt aus	0m	Warn
Schema Registry	Zertifikatsgültigkeit läuft in unter 35 Tagen ab dem aktuellen Zeitpunkt aus	0m	Warn
REST Proxy	Zertifikatsgültigkeit läuft in unter 35 Tagen ab dem aktuellen Zeitpunkt aus	0m	Warn
Administrationskonsole	Zertifikatsgültigkeit läuft in unter 35 Tagen ab dem aktuellen Zeitpunkt aus	0m	Warn
Kafka Interbroker Listener	Zertifikatsgültigkeit läuft in unter 21 Tagen ab dem aktuellen Zeitpunkt aus	0m	Critical
Kafka External Listener	Zertifikatsgültigkeit läuft in unter 21 Tagen ab dem aktuellen Zeitpunkt aus	0m	Critical
Kafka Server REST API; Metadata Cluster (MDS)	Zertifikatsgültigkeit läuft in unter 21 Tagen ab dem aktuellen Zeitpunkt aus	0m	Critical
Kafka Connect	Zertifikatsgültigkeit läuft in unter 21 Tagen ab dem aktuellen Zeitpunkt aus	0m	Critical
ksqlDB	Zertifikatsgültigkeit läuft in unter 21 Tagen ab dem aktuellen Zeitpunkt aus	0m	Critical

Beschreibung	Ereignis	Dauer	Severity
Schema Registry	Zertifikatsgültigkeit läuft in unter 21 Tagen ab dem aktuellen Zeitpunkt aus	0m	Critical
REST Proxy	Zertifikatsgültigkeit läuft in unter 21 Tagen ab dem aktuellen Zeitpunkt aus	0m	Critical
Administrationskonsole	Zertifikatsgültigkeit läuft in unter 21 Tagen ab dem aktuellen Zeitpunkt aus	0m	Critical

2.6. Softwarepflege und Support

Der AN hat dafür zu sorgen, dass die Software durch die/den Hersteller gepflegt wird. Die Softwarepflege umfasst insbesondere folgende Support-Levels (s. auch 2.2 und 2.3), die von der TK bedarfsorientiert abgerufen werden und folgende Leistungen beinhaltet:

- Hoch:** Eine 24x7- Erreichbarkeit für Support-Anfragen. Es ist eine unbegrenzte Anzahl an Support-Tickets pro Monat enthalten. Auf Support-Anfragen der höchsten Priorität wird innerhalb von 30 Minuten reagiert. Dringende Fehlerbehebungen und Sicherheitsupdates sowie Zugriff auf Wissensportale des Herstellers sind enthalten.
- Mittel:** Eine 24x7- Erreichbarkeit für Support-Anfragen. Es ist eine unbegrenzte Anzahl an Support-Tickets pro Monat enthalten. Auf Support-Anfragen der höchsten Priorität wird innerhalb von 60 Minuten reagiert. Dringende Fehlerbehebungen und Sicherheitsupdates sowie Zugriff auf Wissensportale des Herstellers sind enthalten.
- Niedrig:** Eine 24x7- Erreichbarkeit für Support-Anfragen. Es sind mindestens 6 Support-Tickets pro Monat enthalten. Auf Support-Anfragen der höchsten Priorität wird innerhalb von 90 Minuten reagiert. Regelmäßige (z.B. 1 x monatlich oder innerhalb einer definierten Frist) Fehlerbehebungen und Sicherheitsupdates sind enthalten.

2.7. Betrieb der Plattform in der Aufbauphase

In den ersten 6 Monaten (nach aktueller Schätzung) des Projektes ist es geplant, die Plattform iterativ aufzubauen (siehe Abschnitt 2.1). In dieser Phase entstehen Inkremente der Plattform, die in Betrieb genommen werden. Der AN übernimmt in dieser Phase auch den Betrieb dieser Inkremente gemäß den Abschnitten 2.4 und 3.

Der Betrieb der Plattform während des Aufbaus hat – entgegen den Angaben im Abschnitt 3 – in dieser Phase durch Kafka Senior Engineer zu erfolgen, welche die Mindestanforderungen an Qualifikation und Erfahrung nach Abschnitt 4.2.2 erfüllen.

3. Leistungsteil B – Betrieb der Plattform nach Fertigstellung des Aufbaus (optional)

Nachdem die notwendigen Schritte zur Production Readiness (Abschnitt 2.4) der Plattform abgeschlossen wurden, folgt die Ausführung dieser Maßnahmen im eigentlichen Betrieb der Plattform. In diesem Abschnitt werden die in Abschnitt 2.4 geplanten Arbeiten durchgeführt. Jeder Ausführungsschritt steht dabei in direkter Verbindung zu seinem entsprechenden Planungsschritt aus Abschnitt 2.4) und bildet dessen praktische Umsetzung ab.

Hinweis:

- Während des Plattformaufbaus ist dieser Leistungsteil verpflichtend (siehe Abschnitt 2.7)
- Nach Abschluss des Plattformaufbaus stellt der weitere Betrieb der Plattform eine optionale Leistung des AN dar und erfolgt nur auf gesonderte Beauftragung der TK

Auf Abruf der TK hat der AN die Plattform für die TK zu betreiben. Der Abruf dieser Leistung kann zu jedem Zeitpunkt der Vertragslaufzeit erfolgen, d.h. auch bereits während des laufenden Aufbaus der Plattform und sobald Inkremente der Plattform fertiggestellt werden und in Betrieb genommen werden können (s. auch Abschnitt 2.1).

Der Betrieb der Plattform hat nach Fertigstellung des Plattformaufbaus durch Kafka-Engineers zu erfolgen, welche die Mindestanforderungen an Qualifikation und Erfahrung nach Abschnitt 4.2.3 erfüllen.

Im Rahmen des Betriebs der Plattform, sind vom AN folgende Leistungen zu erbringen:

3.1. Einbindung in das IT-Servicemanagement der TK

Der AN stellt sicher, dass alle Informationen und Dokumente gemäß Abschnitt 2.4.1 für das IT-Servicemanagement der TK aktuell sind.

3.2. Mitbestimmung und Datenschutz

Eine Umsetzung von Änderungen an der Plattform dürfen vom AN erst nach Zustimmung der TK vorgenommen werden. Sofern zur Umsetzung dieser Änderungen TK-interne Abstimmungsprozesse notwendig werden (z. B. mit dem Personalrat, IT-Sicherheit oder Datenschutz), hat der AN die TK hierbei zu unterstützen (siehe Abschnitt 2.4.2). Falls die Änderungen einen Einfluss auf die Privatsphäre und das Persönlichkeitsrecht der Mitarbeiter oder Versicherten darstellen, ist eine erneute Abstimmung mit der Mitbestimmung und dem Datenschutz erforderlich. Dabei werden die relevanten Dokumente (Servicebeschreibung, Verfahrensbeschreibung, Datenschutzfolgeabschätzung) aktualisiert.

3.3. Betriebsdokumentation und technische Lösungsskizze

Änderungen an der Plattform werden vom AN in die Betriebsdokumentation (siehe Abschnitt 2.4.4) aufgenommen und beschrieben.

Eine erneute Vorstellung der technischen Lösungsskizze beim Architekturboard der TK ist erforderlich, sobald sich die Änderungen auf die Systemarchitektur, die zugrundeliegenden Architekturentscheidungen, die nicht-funktionalen Anforderungen der Plattform oder auf die zu erwartenden Kosten auswirken. In diesem Fall hat der AN die TK auf deren Anforderung zu unterstützen und bei der Umsetzung der aus Sicht des Architekturboards der TK erforderlichen Anpassungen an der technischen Lösungsskizze mitzuwirken.

3.4. Support und Anwenderdokumentation

Der AN bearbeitet alle Supportfälle, die im Zusammenhang mit dem Betrieb der Plattform auftreten. Auf Anforderung der TK hat der AN auch das Nutzerfeedback gemäß Abschnitt 2.4.4 zu bearbeiten.

3.5. Unterstützung der Nutzung

Gemäß Ziffer 2.1.1 und 2.1.14 unterstützt der AN auf Anforderung der TK auch das Onboarding neuer Anwendungen auf die Plattform sowie bei Problemen in bereits bestehenden Kafka-basierten Anwendungen.

3.6. Systemadministration

Der AN führt die Prozesse zur Systemadministration gemäß Abschnitt 2.4.5 aus. Die Plattform wird vom AN kontinuierlich gewartet. Notwendige Patches und Updates werden vom AN zeitnah getestet und nach Abstimmung mit der TK installiert. Die IT-Change-Prozesse der TK werden bei jeder Änderung berücksichtigt.

3.7. Systemüberwachung

Der AN überwacht die Plattform mithilfe des aufgebauten Monitorings und reagiert entsprechend auf Systemereignisse und Alerts gemäß Abschnitt 2.4.6. Außerdem werden vom AN regelmäßige (mindestens 1xMonat) Überprüfungen und Anpassungen der Überwachungsrichtlinien durchgeführt, um sicherzustellen, dass diese stets den aktuellen Anforderungen und Bedrohungen entsprechen.

3.8. Performance Management

Der AN führt eine umfassende Leistungsüberwachung und -analyse durch, die Reaktionszeiten und Durchsatz der IT-Systeme gemäß Abschnitt 2.4.7 erfasst und bewertet. Auf Anforderung der TK werden Reviews und Reports bereitgestellt.

3.9. Kontinuierliche Wartung

Gemäß Abschnitt 2.4.8 implementiert der AN Wartungsfenster gemäß Vorgaben der TK durch, um sicherzustellen, dass alle Systeme regelmäßig gewartet werden, ohne den Betrieb erheblich zu stören.

Er setzt eine Service Transition gemäß IT Service Management der TK um, um die Verfügbarkeit und Skalierbarkeit der Kafka-Plattform kontinuierlich zu verbessern.

Auf Anforderung der TK sind Systemüberprüfungen durchzuführen, um den Zustand der Systeme zu evaluieren und potenzielle Probleme frühzeitig zu identifizieren. Alle Wartungsaktivitäten und -ergebnisse werden gemäß IT Service Management der TK dokumentiert.

Der AN nutzt die implementierten Feedback-Mechanismen, um Verbesserungspotenziale zu identifizieren und die Wartungsprozesse kontinuierlich zu optimieren.

3.10. Backup- und Wiederherstellungsdienste

Gemäß Abschnitt 2.4.9 und sofern relevant (s. Abschnitt 2.1.6) führt der AN regelmäßige Backups, darunter vollständige, inkrementelle und differentielle Backups. Darüber hinaus werden die implementierten Wiederherstellungsverfahren und -prozesse (Recovery & Resumption Plan) regelmäßig überprüft, um sicherzustellen, dass die Daten im Notfall schnell und zuverlässig wiederhergestellt werden können.

3.11. Kontinuitätstests

Gemäß Abschnitt 2.4.10 und auf Anforderung der TK (zum Beispiel bei größeren infrastrukturellen Änderungen in den TK-Rechenzentren wie Netzwerkänderungen oder bei Änderung der Backup-Systeme) führt der AN Kontinuitätstests im laufenden Betrieb durch.

3.12. Sicherheitsmanagement

Gemäß Abschnitt 2.4.11 führt der AN Risikoanalysen und Bedrohungseinschätzungen fortlaufend durch, um potenzielle Sicherheitsrisiken und Schwachstellen der Plattform zu identifizieren.

Es werden die relevanten Prozesse aus Abschnitt 2.4.11 ausgeführt, so dass die Sicherheit kontinuierlich überwacht wird, unter anderem durch CVE-Scanning, um aktuelle Bedrohungen zu erkennen und proaktiv darauf zu reagieren. Im Falle von Sicherheitsvorfällen werden die relevanten Incident Response-Pläne angewendet.

Der AN aktualisiert regelmäßig das definierte Kafka-spezifisches Sicherheitskonzept. Des Weiteren nutzt er die implementierte Anbindung an das SIEM der TK (aktuelle IBM QRadar), um sicherheitsrelevante Erkenntnisse und Maßnahmen abzuleiten.

3.13. Incident-Management und Support

Gemäß Abschnitt 2.4.4 nutzt der AN den eingerichteten Service Desk sowie die Eskalationsprozesse und bearbeitet alle eingehenden Anfragen.

Zudem führt der AN regelmäßige Analysen von Vorfällen durch, um Trends und Ursachen zu identifizieren und somit kontinuierliche Verbesserungen im Incident Management zu ermöglichen.

3.14. Software-Paketierung

Gemäß Abschnitt 2.4.12 aktualisiert der AN regelmäßig die implementierten Software-Pakete, insbesondere wenn wichtige Änderungen (z.B. Security Patches) bei den genutzten Paketen vorliegen.

3.15. Fernzugriff

Der AN hat den Betrieb der Plattform grundsätzlich über einen Fernzugriff zu erbringen, sofern für einzelne Leistungsbestandteile in dieser LB nichts anderes geregelt ist. Für die Einzelheiten des Fernzugriffs wird auf Abschnitt 2.1.20 verwiesen.

4. Aufgaben und Anforderungen an das vom AN eingesetzte Personal

Auf Abruf der TK hat der AN zur Leistungserbringung folgende Rollen parallel einzusetzen:

- Im Rahmen des Leistungsteil A (Aufbau der Plattform)
 - einen Projektleiter
 - bis zu zwei Kafka Senior Engineers
- Im Rahmen des optionalen Leistungsteil B (Betrieb der Plattform)
 - bis zu drei Kafka Engineers.

Achtung: Ab dem Zeitpunkt eines 24x7 Betriebs der Kafka Plattform (s. auch Abschnitt 2.4.4) kann sich Anzahl der vom AN parallel einzusetzenden Kafka Engineers auf bis zu 5 Personen erhöhen.

Der geschätzte Umfang an Personentage, der auf die einzelnen Profile über die Vertragslaufzeit entfällt, ergibt sich aus dem Preisblatt (Anlage A1).

Nachfolgend werden die Aufgaben und Anforderungen an das vom AN eingesetzte Personal beschrieben:

4.1. Aufgaben des eingesetzten Personals

Die Aufgaben der eingesetzten Mitarbeiter:innen werden in diesem Abschnitt erläutert. Bei der folgenden Auflistung der Aufgaben besteht kein Anspruch auf Vollständigkeit. Alle weiteren Details der Aufgabenstellung ergeben sich aus dem jeweiligen Abruf.

4.1.1. Aufgaben des Projektleiters

1. Gesamtsteuerung des Projekts des Aufbaus und der Inbetriebnahme der Plattform
 - a. Verantwortung für Zielerreichung (Scope, Zeit, Budget, Qualität).
 - b. Transparente Steuerung über Fortschritt, Risiken und Entscheidungen gegenüber Auftraggeber und Gremien.
2. Struktur und Governance aufsetzen
 - a. Projektstruktur definieren (Plan, Meilensteine, Abhängigkeiten).
 - b. Definition von Rollen, Verantwortlichkeiten und Entscheidungswegen.
 - c. Etablierung effizienter Kommunikations- und Abstimmungsformate nach den Prinzipien der agilen Softwareentwicklung
3. Anforderungs- und Stakeholdermanagement
 - a. Konsolidierung und Priorisierung fachlicher und technischer Anforderungen.
 - b. Aktives Stakeholdermanagement (inkl. IT, Fachbereiche, IT-Sicherheit, IT Service Management, Datenschutz, Mitbestimmung).
 - c. Steuerung von Scope-Änderungen
4. Steuerung der technischen Umsetzung
 - a. Koordination aller beteiligten Teams (AN/TK).

- b. Sicherstellen, dass die Plattform die Anforderungen erfüllt:
 - c. Sicherheit und Compliance
 - d. Performance und Skalierbarkeit
 - e. Betriebsfähigkeit (Monitoring, Support, SLAs)
 - f. Fokus auf ein tragfähiges Betriebsmodell
5. Risikomanagement
- a. Frühe Identifikation kritischer Risiken (z. B. Know-how-Abhängigkeit, Architekturentscheidungen, Betriebsreife).
 - b. Priorisierung und aktive Steuerung von Gegenmaßnahmen.
6. Inbetriebnahme
- a. Verantwortung für eine stabile Inbetriebnahme (inkl. Teststrategie, Cutover, Fallback).
 - b. Sicherstellung eines funktionierenden Betriebs- und Supportmodells.
 - c. Gesteuerte Übergabe in den Regelbetrieb.
 - d. Steuerung des Zusammenspiels zwischen iterativem Aufbau und Betrieb
 - e. Übernahme administrativer, organisatorischer Aufgaben oder Aufgaben im Bereich der Dokumentation im Rahmen der Inbetriebnahme
7. Wissenstransfer
- a. Sicherstellen, dass Know-how in der TK aufgebaut wird.
 - b. Etablierung nachhaltiger Strukturen (Dokumentation, Enablement, ggf. Community/Plattform-Governance).
8. Abschluss und Lernen
- a. Transparenter Projektabschluss (Ergebnisse, Abweichungen).
 - b. Sicherstellung, dass Lessons Learned tatsächlich nutzbar gemacht werden.

4.1.2. Aufgaben des Kafka Senior Engineers (Aufbau der Kafka-Plattform)

1. Architektur und Plattformdesign
- a. Verantwortung für Zielarchitektur (Cluster-Setup, KRaft, Multi-Cluster, Deployment-Modell).
 - b. Definition zentraler Designprinzipien:
 - i. Topic- und Partitionsstrategie
 - ii. Replikation, Verfügbarkeit, Skalierung
 - iii. Umgang mit Schemas und Datenverträgen
2. Technische Umsetzung der Plattform
- a. Aufbau und Konfiguration der Kafka-Plattform (Cluster, zentrale Komponenten).
 - b. Definition und Umsetzung von Standards:
 - i. Security (TLS, AuthN/AuthZ, ACL-Modell)
 - ii. Konfigurationen und Defaults

- c. Automatisierung des Setups (IaC, standardisierte Deployments).
 - d. Sicherstellung der Developer Experience für die Nutzer (Softwareentwickler) der Plattform
3. Integration und Enablement
- a. Technische Leitplanken für die Nutzung von Kafka:
 - i. Referenzarchitekturen und Best Practices
 - ii. Integrationen (z. B. Connect)
 - b. Unterstützung bei der Umsetzung von Anwendungsfällen
4. Observability und Betriebsfähigkeit sicherstellen
- a. Aufbau von Monitoring, Logging und Alerting auf Plattformebene.
 - b. Definition von Betriebsmetriken
 - c. Validierung der Plattform durch Tests
5. Governance und Sicherheit
- a. Definition verbindlicher Regeln:
 - i. Naming, Retention, ACLs
 - ii. Umgang mit sensiblen Daten
 - b. Sicherstellen, dass die Plattform revisions- und compliancefähig ist.
6. Wissenstransfer und Übergabe
- a. Befähigung der TK für den Betrieb der Plattform:
 - i. Dokumentation der Plattform und Betriebsprozesse
 - ii. Coaching
 - iii. Geordnete Übergabe an den Betrieb inkl. klarer Verantwortlichkeiten.
7. Go-Live-Unterstützung und Betrieb der Plattform-Inkrementen, die während des iterativen Plattformaufbaus entstehen
- a. Technische Verantwortung in Go-Live und Hypercare.
 - b. Schnelle Analyse und Stabilisierung bei Problemen.
 - c. Betriebliche Unterstützung während des Plattformaufbaus gemäß Aufgabendefinition in Abschnitt 4.1.3 (s. auch 2.7)

4.1.3. Aufgaben des Kafka Engineers (Betrieb der Plattform nach Fertigstellung des Aufbaus – optionale Leistung)

Der Kafka Engineer ist für die Betrieb der bereits aufgebauten Plattform zuständig und hat in diesem Zusammenhang folgende Aufgaben zu erbringen. Diese Aufgaben werden erbracht, nach vollständigem Abschluss des Plattformaufbaus.

1. Betrieb und Stabilität der Plattform
- a. Sicherstellung des laufenden Betriebs der Kafka-Cluster.
 - b. Überwachung zentraler Metriken:

- c. Support- und Incident-Handling und nachhaltige Fehlerbehebung.
- 2. Monitoring und kontinuierliche Verbesserung
 - a. Pflege und Weiterentwicklung von Monitoring und Alerting.
 - b. Analyse von Engpässen und Performanceproblemen.
 - c. Umsetzung von Tuning-Maßnahmen im laufenden Betrieb.
- 3. Plattform-Administration
 - a. Verwaltung von Topics, ACLs und Konfigurationen gemäß Governance.
 - b. Durchführung von Changes (Deployments, Upgrades, Skalierung).
 - c. Sicherstellung von Backups, Recovery und Failover-Fähigkeit.
- 4. Unterstützung der Nutzung (Use Cases)
 - a. Onboarding neuer Anwendungen auf die Plattform.
 - b. Unterstützung bei Problemen in Producer/Consumer-Integrationen.
 - c. Sicherstellen der Einhaltung von Standards (keine Wildwuchs-Nutzung).
- 5. Security und Compliance im Betrieb
 - a. Operative Umsetzung von Security-Vorgaben (Zugriffe, Zertifikate etc.).
 - b. Unterstützung bei Audits und Nachweisen.
- 6. Betriebsprozesse und Dokumentation
 - a. Arbeiten nach definierten Prozessen (Incident, Problem, Change).
 - b. Pflege betriebsrelevanter Dokumentation und Runbooks.

4.2. Anforderungen an das vom AN eingesetzte Personal

Der AN hat für die Leistungserbringung ausschließlich fachlich geeignetes und qualifiziertes Personal einzusetzen. Die eingesetzten Mitarbeiter:innen müssen über die für die jeweilige Arbeiten erforderliche berufliche Qualifikation, praktische Erfahrung sowie ausreichende Sprachkenntnisse verfügen und dabei die folgenden Mindestanforderungen – sowie die im jeweiligen Mitarbeiterprofil zugesagten Zusatzqualifikationen – erfüllen:

4.2.1. Projektleiter

Der vom AN eingesetzte Projektleiter muss mindestens über folgende Qualifikation und praktische Erfahrung sowie Sprachkenntnisse verfügen:

- Erfahrung in der Projektleitung
 - 3 Jahre praktische Erfahrung in der Leitung von IT-Projekten mit Infrastruktur bzw. Plattformbezug.
 - Praktische Erfahrung in der Steuerung interdisziplinärer Teams (Mischung aus Mitarbeitern eines Auftraggebers und eines Auftragnehmers), die Apache Kafka Plattformen aufgebaut haben.

- Erfahrung in der Leitung von Kafka-Projekten
 - Praktische Erfahrung in der Leitung von Projekten im Bereich des Aufbaus einer Apache Kafka Plattform, erworben durch die Leitung von mindestens 2 abgeschlossenen Projekten in den letzten 3 Jahren (vor Ablauf der Angebotsfrist).
 - Praktische Erfahrung in der Identifikation, Abwägung und Priorisierung von ereignisgesteuerten Anwendungsfällen.
 - Praktische Erfahrung in der Erhebung funktionaler Anforderungen für Kafka Topics
- Methodische Kompetenz (agile und hybride Projektabwicklung)
 - Praktische Erfahrung in der Arbeit in agilen Projektteams.
 - Fundierte Kenntnisse in der Anwendung agiler Methoden (z. B. Scrum, Kanban).
- Kommunikative und organisatorische Fähigkeiten
 - Ausgeprägte Fähigkeit zur verständlichen Aufbereitung und Darstellung technischer Sachverhalte für unterschiedliche Zielgruppen (Management, Fachbereiche, IT).
 - Praktische Erfahrung in der Moderation von Workshops sowie in der Steuerung von Abstimmungs- und Entscheidungsprozessen.
 - Gute Kommunikationsfähigkeiten.
 - Selbständige Sprachverwendung der deutschen Sprache in Wort und Schrift, entsprechend dem Sprachniveau B2 des Gemeinsamen Europäischen Referenzrahmens für Sprachen (GER).

4.2.2. Kafka Senior Engineer

Die vom AN eingesetzten Kafka Senior Engineers müssen mindestens über folgende Qualifikation und praktische Erfahrung sowie Sprachkenntnisse verfügen:

- Ausbildung und Grundqualifikation
 - Abgeschlossenes Hochschulstudium der (Wirtschafts-)Informatik oder eines vergleichbaren Studiengangs mit eindeutigem IT-Schwerpunkt (z. B. Medieninformatik, technische Informatik, Software Engineering) oder mindestens 5 Jahre einschlägige Berufserfahrung im IT-Umfeld (z. B. in Softwareentwicklung, IT-Architektur, Systembetrieb oder vergleichbaren Tätigkeiten mit überwiegendem IT-Bezug).
- Erfahrung im Aufbau und Betrieb von Kafka-Plattformen
 - Mindestens 1 Jahr (kumulativ) praktische Erfahrung in der IT-Architekturarbeit im Kontext Apache Kafka, insbesondere in der Erstellung von Architekturskizzen, in der Anwendung Kafka-spezifischer Architekturtaktiken sowie in der Abwägung architektonischer Trade-Offs und nicht-funktionaler Eigenschaften, erworben in den letzten 3 Jahren (vor Ablauf der Angebotsfrist).
 - Praktische Erfahrung in der Identifikation, Abwägung und Priorisierung von ereignisgesteuerten Anwendungsfällen.
 - Praktische Erfahrung in der Erhebung funktionaler Anforderungen für Kafka Topics.
 - Mindestens 3 Jahre (kumulativ) praktische Erfahrung im Aufbau und Betrieb komplexer on-prem Kafka-Plattformen mit den Charakteristiken, die im Abschnitt 2 beschrieben werden, erworben in den letzten 5 Jahren (vor Ablauf der Angebotsfrist).

- Vertiefte technische Kenntnisse im Bereich Apache Kafka und der unterliegenden Infrastruktur (insbesondere GitHub Actions, ArgoCD, Kubernetes/OpenShift) sowie in den entsprechenden Enterprise Funktionen und Konnektoren gemäß Abschnitten 2.2 und 2.3, erworben durch die Umsetzung von mindestens 2 abgeschlossenen Projekten in den letzten 3 Jahren (vor Ablauf der Angebotsfrist).
- Kommunikative und organisatorische Fähigkeiten
 - Praktische Erfahrung in Projekten mit agilen Vorgehensmodellen (z. B. Scrum, Kanban).
 - Gute Kommunikationsfähigkeiten.
 - Selbständige Sprachverwendung der deutschen Sprache, entsprechend dem Sprachniveau B2 des Gemeinsamen Europäischen Referenzrahmens für Sprachen (GER).

4.2.3. Kafka Engineer

Die vom AN eingesetzten Kafka Engineers müssen mindestens über folgende Qualifikation und praktische Erfahrung sowie Sprachkenntnisse verfügen:

- Berufserfahrung im Betrieb von Kafka-Plattformen
 - Mindestens 1 Jahr (kumulativ) praktische Erfahrung im Betrieb komplexer on-prem Kafka-Plattformen mit den Charakteristiken, die im Abschnitt 2 beschrieben werden, erworben in den letzten 3 Jahren (vor Ablauf der Angebotsfrist).
 - Vertiefte technische Kenntnisse im Bereich Support, Troubleshooting und Patching von Kafka-Plattformen auch auf Basis von GitHub Actions, ArgoCD, Kubernetes/OpenShift sowie von den entsprechenden Enterprise Funktionen und Konnektoren gemäß Abschnitten 2.2 und 2.3.
 - Erfahrungen in der Handhabung von Support-Fällen mit Softwareherstellern.
 - Praktische Erfahrung im Umgang mit Monitoring- und Logging-Systemen.
- Kommunikative und organisatorische Fähigkeiten
 - Gute Kommunikationsfähigkeiten.
 - Hohe Serviceorientierung.
 - Strukturiertes Vorgehen in Störungssituationen.
 - Selbständige Sprachverwendung der deutschen Sprache, entsprechend dem Sprachniveau B2 des Gemeinsamen Europäischen Referenzrahmens für Sprachen (GER).

Anlage:

- Vorgaben aus IT-Sicht (Anlage L1)
- Abrufformular (Anlage L2)