

Qualitätsanforderungen & Service Level Agreement (SLA)

Multi Product Owner System

Dateiname:	Qualitätsanforderungen
Zuletzt geändert am:	04.05.2026 12:21
Version:	0,9

VDV eTicket Service GmbH & Co. KG

Im Mediapark 8a, 50670 Köln
Steuer-Nr. 215/5770/0172
Ust-IdNr. DE 241694352
Handelsregister: Amtsgericht Köln,
RA 21866, Sitz Köln

Konto: Sparkasse KölnBonn
BLZ 370 501 98
Kto.-Nr. 163302953
Swift-BIC: COLSDE 33
IBAN: DE36 3705 0198 0163 3029 53

Komplementärin: VDV eTicket
Verwaltungsgesellschaft mbH
Geschäftsführer der Komplementärin:
Nils Zeino-Mahmalat
Martin Schmitz

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkung
0.1	René Schmid (VDV-ETS)	29.12.2025	Ersterstellung
0.2	Wilk Hoffmann, Dr. Fabian Ohler, Can Apak	03.04.2026	Review
0.9	Sebastian Krammer (VDV-ETS)	04.05.2026	Bekanntmachung

Inhaltsverzeichnis

Versionsverwaltung.....	2
Tabellenverzeichnis	5
1 Qualitätsanforderungen.....	5
1.1 Anforderungen an die Informationssicherheit	6
1.1.1 Klassifizierung von Informationen.....	6
1.1.2 Personal	7
1.2 Eingesetzte Protokolle	7
1.2.1 Physische und Umweltsicherheit	8
1.2.2 Betriebs- und Kommunikationsmanagement.....	9
1.3 Anwendungsspezifische Sicherheitsanforderungen	10
1.3.1 Produktionsumgebung.....	11
1.3.2 Staging-Umgebung.....	11
1.4 Wartbarkeit	12
1.4.1 Anforderungen an Third-Party-Software	13
1.4.2 Testing	13
1.5 Abnahme	15
1.5.1 Definition der Abnahme.....	15
1.5.2 Abnahmeanforderungen	15
1.5.3 Abnahmetests	16
1.5.4 Abnahmekriterien	16
1.5.5 Abnahmezeitraum	17
1.5.6 Abnahmeverweigerung.....	17
1.5.7 Schlussbestimmungen.....	17
1.6 Version Management	17
1.7 Change- und Release-Management.....	18

1.8	Administrator Management	18
1.9	Nutzerfreundlichkeit.....	19
1.10	Adressierbarkeit.....	20
1.11	Monitoring.....	20
1.12	Logging.....	21
1.12.1	Allgemeines.....	21
1.12.2	Umfang.....	21
1.12.3	Struktur und Inhalte.....	22
1.12.4	Log-Level	22
1.12.5	Speicherung, Sicherheit & Compliance	22
1.12.6	Aufbewahrung	22
1.12.7	Monitoring und Integration.....	22
2	Service Level Agreements.....	23
2.1	Support	23
2.2	Störungen & Fehler	24
2.2.1	Benachrichtigung.....	26
2.3	Performance.....	27
2.3.1	Produktions-System	28
2.3.2	Staging-System	29
2.4	Skalierbarkeit.....	29
2.4.1	Transaktionsvolumen.....	30
2.5	Verfügbarkeit.....	30
2.5.1	Verfügbarkeit des Produktions-Systems.....	30
2.5.2	Verfügbarkeit des Staging-Systems.....	31
2.6	Wartung.....	32
2.6.1	Produktions-System	33

2.6.2	Staging-System	34
2.6.3	Reaktions- und Entstörungs-Zeit.....	34
2.6.4	Eskalations-Management	35
3	Zusätzliche funktionale Anforderungen	37
3.1	Archivierung / Löschkonzept.....	37
3.1.1	Löschung gemäß DSGVO.....	37
3.1.2	Vorbedingungen	37
3.2	Sicherung und Wiederherstellung.....	39
3.3	Export	40
4	Mitgeltende Dokumente	40

Tabellenverzeichnis

Tabelle 1: Performance Produktionssystem	29
Tabelle 2: Verfügbarkeiten für Produktivsysteme.....	31
Tabelle 3 Verfügbarkeiten für Staging-Systeme.....	31
Tabelle 4 Störungsklassen Staging.....	34
Tabelle 5: Störungsklassen Produktion.....	35
Tabelle 6: Störung und Eskalation.....	36

1 Qualitätsanforderungen

Dieses Dokument beschreibt die Leistungen, Verfügbarkeiten und Verpflichtungen zwischen dem Auftragnehmer der IT-Systeme (nachfolgend „Auftragnehmer“) und dem Auftraggeber (nachfolgend „VDV-ETS“). Ziel ist es, die Qualität der bereitgestellten Systeme und IT-Dienste zu gewährleisten. Zu den Leistungen zählen Themen zu Software, Tests, Abnahmekriterien, Sicherheitsanforderungen, sowie die vereinbarten Service-Levels für Themen wie Verfügbarkeit und Wiederherstellung von Services.

1.1 Anforderungen an die Informationssicherheit

Der Auftragnehmer ist verpflichtet ein Informationssicherheitskonzept (ISK) zur Umsetzung der Anforderungen an die Informationssicherheit gemäß der im Folgenden aufgeführten Normen und Standards vorzulegen. Dieses Konzept enthält eine detaillierte Beschreibung der geplanten Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme, die verarbeitet werden. Der Auftragnehmer muss sich an die Vorgaben von ISO 27001, BSI-Standard 200-1, BSI-Standard 200-2, BSI-Standard 200-3, BSI-Standard 200-4 und gesetzlichen Vorgaben halten. Das Konzept muss im Rahmen des Umsetzungsprojekts fertiggestellt und durch den Auftraggeber abgenommen sein.

Der VDV-ETS behält sich das Recht vor, das Konzept zu prüfen und gegebenenfalls Ergänzungen oder Änderungen vorzugeben, um sicherzustellen, dass die Umsetzung den vertraglichen Vereinbarungen, den geltenden Best Practices sowie den Sicherheitsstandards entspricht. Beide Parteien einigen sich auf einen finalen Umsetzungsplan, der verbindlich für den Schutz der Informationen und Systeme ist.

1.1.1 Klassifizierung von Informationen

Alle Informationen müssen entsprechend ihrer Vertraulichkeit, Integrität und Verfügbarkeit klassifiziert werden. Sensible Daten sind angemessen zu schützen, um unbefugten Zugriff, Verlust oder Manipulation zu verhindern. Die Klassifizierung der Informationen wird durch den Auftraggeber vorgenommen. Dabei gelten folgende Kategorien:

- Öffentlich: Informationen, die frei zugänglich sind und deren Offenlegung keine negativen Folgen hat.
- Intern: Informationen, die nur für den internen Gebrauch bestimmt sind, aber bei unbefugtem Zugriff keinen erheblichen Schaden anrichten würden.
- Vertraulich: Geschäftskritische oder sensible Informationen, deren unbefugter Zugriff dem Unternehmen erheblichen Schaden zufügen könnte, wie z.B. Kundeninformationen, Verträge oder Finanzdaten.
- Hochsensibel: Informationen, deren unbefugter Zugriff, Verlust oder Änderung schwerwiegende rechtliche oder finanzielle Konsequenzen haben könnte. Beispiele sind personenbezogene Daten, geistiges Eigentum oder strategische Unternehmenspläne.

Für jede Klassifizierungsstufe müssen spezifische Sicherheitsmaßnahmen implementiert werden, darunter Verschlüsselung, Zugriffsbeschränkungen und Protokollierung. Die Klassifizierung muss regelmäßig, z.B. jährlich überprüft und aktualisiert werden, um der sich ändernden Informationslandschaft gerecht zu werden. Der genaue Rhythmus der Aktualisierung wird im Projekt festgelegt.

1.1.2 Personal

Sämtliches Personal, das Zugang zu sensiblen Informationen hat, muss regelmäßig Schulungen zur Informationssicherheit absolvieren. Sicherheitsüberprüfungen und Zugangskontrollen sind entsprechend den Rollen und Verantwortlichkeiten des Personals durchzuführen. Der Nachweis über durchgeführte Schulungen und/oder Kontrollen muss dem Auftraggeber auf Anfrage zur Verfügung gestellt werden.

Diese Schulungen sind regelmäßig durchzuführen, um sicherzustellen, dass das Personal über aktuelle Bedrohungen und Sicherheitsprotokolle informiert ist.

Zugriff auf vertrauliche oder hochsensible Informationen darf nur entsprechend autorisiertem Personal gewährt werden. Rollenbasierte Zugriffskontrollen (RBAC) müssen implementiert werden, um sicherzustellen, dass der Zugriff auf sensible Informationen strikt auf das benötigte Minimum beschränkt bleibt (Prinzip der geringsten Privilegien).

Im Fall von Austritten oder Änderungen in den Verantwortlichkeiten von Mitarbeitern müssen alle Zugangsdaten und Berechtigungen unverzüglich aktualisiert oder entzogen werden, um unbefugten Zugriff zu verhindern.

1.2 Eingesetzte Protokolle

Im Rahmen dieses Dokuments wird festgelegt, dass die vom Auftragnehmer verwendeten Protokolle zur Kommunikation, Datenübertragung und Sicherheit durch den Auftragnehmer definiert werden. Diese Protokolle müssen den geltenden Sicherheits- und Leistungsanforderungen entsprechen und den aktuellen Standards in der IT-Sicherheit und Netzwerkkommunikation folgen.

Der Auftragnehmer erstellt eine detaillierte Dokumentation der geplanten Protokolle, die in den verschiedenen Bereichen des Systems eingesetzt werden, einschließlich Netzwerk-, Sicherheits-, Datenübertragungs-, E-Mail-, Anwendungs- und Datenbankprotokollen. Diese Protokollauswahl muss gewährleisten, dass die Anforderungen an Vertraulichkeit,

Integrität und Verfügbarkeit der Daten erfüllt werden und die Performance des Systems nicht beeinträchtigt wird. Die verwendeten Protokolle schließen alle bereits durch das Lastenheft_MPS und referenzierten Spezifikationen, vorgegebenen Protokolle mit ein.

Der VDV-ETS behält sich das Recht vor, die vom Auftragnehmer definierten Protokolle zu prüfen. Der Auftragnehmer legt der VDV-ETS den Vorschlag zur Freigabe vor. Der VDV-ETS prüft die Auswahl und stellt sicher, dass die Protokolle den Sicherheits- und Leistungsanforderungen des Unternehmens entsprechen

Änderungen an den verwendeten Protokollen müssen ebenfalls vom Auftragnehmer rechtzeitig vorgeschlagen und der VDV-ETS zur erneuten Prüfung und Freigabe vorgelegt werden.

1.2.1 Physische und Umweltsicherheit

Die genutzten Rechenzentren müssen nach ISO27001 und ISO9001 zertifiziert sein.

Die physische Sicherheit der IT-Infrastrukturen muss durch eine Kombination aus Zugangskontrollen, Überwachung und Schutzmechanismen gewährleistet werden. Alle sensiblen IT-Systeme, wie Server, Netzwerkausrüstung und Speichermedien, müssen in gesicherten Räumlichkeiten untergebracht sein, die nur für autorisiertes Personal zugänglich sind.

Die Bereiche, in denen die Systeme betrieben werden, müssen durch Sicherheitszonen geschützt werden. Diese müssen entsprechend gekennzeichnet sein und dürfen nur auf kontrollierte Weise und an definierten Punkten betreten werden. Ein physischer Zugang zu diesen sicherheitsbeschränkten Bereichen darf an keinem anderen Punkt möglich sein.

Ressourcen, die für die Systeme relevant sind, müssen innerhalb von Sicherheitszonen platziert und geschützt werden, um das Risiko von Umweltgefahren, Katastrophen und unbefugtem Zugriff zu verringern, insbesondere durch den Schutz von:

- Geräten vor Stromausfällen und Ausfällen anderer Dienste (z. B. Wasserversorgung, Klimaanlage, Kommunikation)
- Stromversorgung für Informationssysteme und Telekommunikationsleitungen, die Daten transportieren vor Beschädigung und Abhörung schützen

- Geräten, die kryptografische Schlüssel verwenden und sensible Daten in Sicherheitszonen verschlüsseln, gegen die Überwachung ihrer elektromagnetischen Strahlung während des Gebrauchs.

Der Zugang zu diesen sicherheitsbeschränkten Bereichen darf nur über eine Zugangskontrolle erfolgen, deren Sicherheit den zu schützenden Informationswerten angemessen ist. Es muss sichergestellt werden, dass nur autorisierte Personen Zugang erhalten (z. B. durch Schlösser mit Chipkartenverifikation oder durch kontrollierte Schlüsselvergabe oder durch Kontrollen durch Sicherheitspersonal). Die Ausübung von Zugriffsrechten muss ebenfalls protokolliert werden.

Alle Zutrittsbereiche müssen durch Überwachung (Video, Sicherheitskräfte) und Bewegungssensoren geschützt sein.

1.2.2 Betriebs- und Kommunikationsmanagement

Um die Sicherheit und Integrität der IT-Systeme sowie der darauf laufenden Prozesse zu gewährleisten, müssen klare Richtlinien und Verfahren für das Betriebs- und Kommunikationsmanagement implementiert werden.

Zu den wichtigsten Maßnahmen gehören:

- Softwaresicherheit: Software-Patches, die zur Erhaltung oder Erhöhung der Systemsicherheit notwendig sind, müssen regelmäßig und zeitnah nach Bekanntwerden einer Sicherheitslücke auf den Systemen eingespielt werden.
- Netzwerksicherheit: Alle Netzwerkverbindungen, sowohl intern als auch extern, müssen durch Firewalls, Intrusion Detection Systems (IDS), und Intrusion Prevention Systems (IPS) geschützt werden, um unbefugte Zugriffe oder Angriffe zu verhindern. Jährliche Penetrationstests und Sicherheitsüberprüfungen sind durchzuführen, um potenzielle Schwachstellen zu identifizieren und zu beheben. Diese können durch interne Fachabteilungen oder in Absprache mit dem Auftraggeber durch externe Partner durchgeführt werden.
- Datenverschlüsselung: Jede Datenübertragung, insbesondere über unsichere Netzwerke (z.B. das Internet), muss durch geeignete Verschlüsselungsverfahren wie TLS (Transport Layer Security) oder VPN (Virtual Private Network) gesichert werden. Daten im Ruhezustand, in der Datenbank nach der Übertragung oder

ausgelagert (z.B. in Backups), müssen dementsprechend durch geeignete Verschlüsselungsverfahren geschützt werden.

- Authentifizierung und Autorisierung: Der Zugriff auf Systeme und Kommunikationskanäle muss durch starke Authentifizierungsmechanismen, wie Zwei-Faktor-Authentifizierung (2FA) oder Public Key Infrastructure (PKI), gesichert sein. Nur autorisierte Benutzer dürfen auf die Systeme zugreifen, und alle Zugriffe müssen protokolliert werden.
- Protokollierung und Überwachung: Alle Kommunikations- und Betriebsaktivitäten müssen protokolliert werden, um eine lückenlose Überwachung zu gewährleisten. Logs müssen regelmäßig durch den Auftragnehmer überprüft und auf Anomalien untersucht werden, um Sicherheitsvorfälle frühzeitig zu erkennen.
- Redundanz und Fehlertoleranz: Kommunikationsinfrastrukturen müssen redundant ausgelegt sein, um bei Ausfällen alternative Kommunikationswege zur Verfügung zu stellen. Dies stellt sicher, dass betriebliche Abläufe bei einem Ausfall weiterhin aufrechterhalten werden können.

Zugriffsverwaltung: Der Zugriff auf Betriebs- und Kommunikationsressourcen muss auf die jeweils autorisierten Nutzer beschränkt werden. Dies erfolgt über rollenbasierte Zugriffskontrollen (Role-Based Access Control, RBAC), um sicherzustellen, dass jeder Nutzer nur die für ihn notwendigen Berechtigungen erhält.

1.3 Anwendungsspezifische Sicherheitsanforderungen

Im Rahmen dieses Dokuments wird festgelegt, dass die anwendungsspezifischen Sicherheitsanforderungen vom Auftragnehmer definiert werden. Diese Anforderungen umfassen alle sicherheitsrelevanten Maßnahmen, die speziell für die Anwendung erforderlich sind, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme zu gewährleisten.

Der Auftragnehmer erstellt eine umfassende Dokumentation der anwendungsspezifischen Sicherheitsmaßnahmen. Diese Dokumentation umfasst sowohl technische als auch organisatorische Maßnahmen, die den besonderen Anforderungen der Anwendung gerecht werden. Dazu gehören unter anderem spezifische Zugriffs- und Berechtigungskonzepte, Verschlüsselungsverfahren, Sicherheitsmechanismen für Produktions- und Staging-Umgebungen sowie Maßnahmen zur Sicherung der Datenintegrität.

Der VDV-ETS hat das Recht und die Pflicht, die vorgeschlagenen Sicherheitsanforderungen zu prüfen. Ziel der Prüfung ist es, sicherzustellen, dass die Anforderungen den internen Richtlinien und den gesetzlichen Vorgaben entsprechen.

1.3.1 Produktionsumgebung

Die Produktionsumgebung muss isoliert und getrennt von anderen Umgebungen, wie Test- oder Entwicklungsumgebungen, betrieben werden, um die Integrität und Sicherheit der laufenden Systeme zu gewährleisten. In dieser Umgebung laufen geschäftskritische Anwendungen und Prozesse, die kontinuierlich verfügbar und stabil sein müssen.

Wichtige Anforderungen an die Produktionsumgebung:

- **Zugriffsrestriktionen:** Nur autorisiertes und qualifiziertes Personal darf auf die Produktionsumgebung zugreifen. Änderungen an dieser Umgebung müssen nach einem gemeinsam definierten Change-Management Prozess erfolgen, um ungewollte Unterbrechungen oder Fehler zu verhindern.
- **Datensicherheit:** Die Daten in der Produktionsumgebung müssen vor unbefugtem Zugriff, Verlust oder Manipulation geschützt werden. Regelmäßige Backups sind erforderlich, um im Falle eines Systemausfalls eine schnelle Wiederherstellung zu ermöglichen. Mehr dazu wird in *Sicherung* und in Kapitel 3.2 definiert.
- **Monitoring und Überwachung:** Um einen stabilen Betrieb sicherzustellen, muss die Produktionsumgebung durch Monitoring-Systeme kontinuierlich überwacht werden, die Leistungskennzahlen (z.B. CPU-Auslastung, Speicherverbrauch und Erreichbarkeit) sowie sicherheitsrelevante Ereignisse protokollieren. Der Auftragnehmer muss dabei den Auftraggeber gemäß Kapitel 2.6.4 Eskalations-Management über Ereignisse informieren.

Hochverfügbarkeit: Um Ausfallzeiten zu minimieren, sind Mechanismen zur Erhöhung der Verfügbarkeit wie Load Balancing und Failover-Lösungen zu implementieren. Geplante Wartungsarbeiten müssen so organisiert werden, dass sie den Produktionsbetrieb nicht beeinträchtigen.

1.3.2 Staging-Umgebung

Die Staging-Umgebung ist eine prä-produktive Umgebung, in der neue Funktionen, Änderungen oder Updates getestet werden, bevor sie in die Produktionsumgebung

übertragen werden. Sie dient als Spiegelbild der Produktionsumgebung und ermöglicht es, reale Bedingungen zu simulieren.

Anforderungen an die Staging-Umgebung:

- Ähnlichkeit zur Produktionsumgebung: Die Staging-Umgebung muss möglichst identisch zur Produktionsumgebung eingerichtet sein, um realistische Tests zu ermöglichen. Dies umfasst die Konfiguration von Servern, Netzwerken und Datenbanken.
- Isolierung: Die Staging-Umgebung muss strikt von der Produktionsumgebung getrennt sein, um sicherzustellen, dass Tests keine unbeabsichtigten Auswirkungen auf produktive Systeme haben.
- Testdurchführung: In der Staging-Umgebung werden alle Änderungen, neue Funktionen und Patches unter realistischen Bedingungen getestet. Hier müssen sowohl Funktionalität als auch Sicherheit überprüft werden, bevor eine Freigabe für die Produktionsumgebung erfolgt.
- Rollback-Optionen: Sollte ein Test fehlschlagen, muss es möglich sein, die Staging-Umgebung schnell wieder in den Ursprungszustand zurückzusetzen, um Folgefehler zu vermeiden.

Datenmanagement: Testdaten in der Staging-Umgebung müssen anonymisiert oder anderweitig geschützt sein, um die Sicherheit sensibler Informationen zu gewährleisten.

Live-Daten dürfen nicht in der Staging-Umgebung verwendet werden, um Datenschutzrisiken zu minimieren.

1.4 Wartbarkeit

Die Systeme müssen so gestaltet und dokumentiert sein, dass sie einfach zu warten sind. Dies beinhaltet klare und nachvollziehbare Strukturen in der Softwarearchitektur, um zukünftige Anpassungen, Bugfixes oder Erweiterungen effizient durchführen zu können. Wartungsfreundliche Systeme zeichnen sich durch eine modulare Architektur aus, in der Komponenten unabhängig voneinander aktualisiert oder ersetzt werden können, ohne dass das gesamte System beeinträchtigt wird. Eine umfassende technische Dokumentation aller Komponenten, Schnittstellen und Konfigurationen muss stets aktuell gehalten werden, um das Verständnis und die Wartung zu erleichtern. Darüber hinaus müssen regelmäßige

Überprüfungen und Tests durchgeführt werden, um die Wartbarkeit und die Leistung des Systems zu gewährleisten.

Darüber hinaus muss der Code gut strukturiert, dokumentiert und testbar sein. Es gelten branchenübliche Codierungsstandards (wie Clean Code).

1.4.1 Anforderungen an Third-Party-Software

1.4.1.1 Qualitätskriterien

Alle Third-Party-Bibliotheken müssen die folgenden Kriterien erfüllen:

- **Aktive Wartung:** Die Bibliothek wird aktiv entwickelt und gewartet (z. B. durch regelmäßige Updates oder eine aktive Community).
- **Dokumentation:** Die Bibliothek verfügt über eine vollständige und klare Dokumentation.
- **Testabdeckung:** Die Bibliothek muss nachweislich gut getestet sein (z. B. Unit-Tests, Community-Erfahrungsberichte).
- **Sicherheitsstatus:** Es dürfen keine bekannten, ungepatchten Sicherheitslücken bestehen.

1.4.1.2 Lizenzbedingungen

Die Lizenzbedingungen der Bibliothek müssen prüfbar und mit den Projektanforderungen kompatibel sein. Besonders problematische Lizenzen (z. B. GPL in proprietärer Software) dürfen nicht verwendet werden.

1.4.2 Testing

Die Systeme und deren Software sind während der Erstellung und im laufenden Betrieb innerhalb des Change-Managements zu testen. Diese Tests teilen sich in drei Testarten auf, welche im Folgenden beschrieben sind.

Für die Software ist ein umfangreiches Testkonzept, gemäß der gängigen Regeln der Technik, zu erstellen, bestehend aus:

- Testspezifikation in einem Testfallkatalog
- Testdurchführungsreports für Unit-, Regressions- und Integrationstests sowie Last- und Penetrationstests.

- Für das Graphical-User-Interface (GUI) sind spezifische Tests innerhalb des Testfallkatalogs zu definieren.

Hinweis: der Testfallkatalog wird vom Anbieter mit Unterstützung durch VDV-ETS während der Projektlaufzeit erstellt und enthält die Beschreibung von manuellen und/oder automatisierten Tests zur Prüfung der Funktionsfähigkeit der Software.

1.4.2.1 Unit-Tests

Ein Unit Test ist eine Softwaretesttechnik, bei der einzelne, isolierte Komponenten oder Einheiten einer Anwendung – typischerweise Funktionen oder Methoden – getestet werden, um sicherzustellen, dass sie korrekt arbeiten. Das Ziel eines Unit Tests ist es, die kleinste testbare Einheit des Programms auf Fehler zu überprüfen, oft unabhängig von anderen Komponenten des Systems.

Dabei müssen mehr als 70% der Codebasis durch Unit-Tests abgedeckt sein, um eine entsprechende Software-Qualität nachzuweisen.

1.4.2.2 Integration-Tests

Ein Integrationstest ist eine Testtechnik in der Softwareentwicklung, bei der mehrere Komponenten oder Module eines Systems gemeinsam getestet werden, um sicherzustellen, dass sie korrekt miteinander interagieren und zusammenarbeiten. Im Gegensatz zum Unit Test, der nur einzelne Einheiten (z. B. Funktionen oder Methoden) isoliert prüft, fokussiert sich der Integrationstest auf das Zusammenspiel zwischen mehreren Komponenten. Der Auftragnehmer ist verpflichtet die einzelnen Systemkomponenten im Falle von Änderungen, im Rahmen des Change-Managements, einem Integrationstest zu unterziehen, um das Zusammenwirken der Systemkomponenten zu gewährleisten. Dieser Integrationstest wird in der Staging-Umgebung (siehe 2.3.2) durchgeführt, um die Funktionsfähigkeit produktionsnah zu überprüfen.

1.4.2.3 Regression-Testing

Ein Regressionstest ist eine Art von Softwaretest, der durchgeführt wird, um sicherzustellen, dass neue Änderungen am Code (wie Bugfixes, neue Features oder Refactoring) keine unbeabsichtigten negativen Auswirkungen auf bereits funktionierende Teile des Systems haben. Das Ziel eines Regressionstests ist es, sicherzustellen, dass die bestehende Funktionalität der Software nach einer Änderung weiterhin korrekt

funktioniert. Alle Anpassungen an den Systemen durch Weiterentwicklung, Wartung oder Fehlerbehebung müssen vor der Bereitstellung auf der produktiven Systemumgebung, in einem Regressionstests überprüft werden.

Die Regressionstests müssen vor dem Release jeder Änderung am System im Rahmen des Change-Managements durchgeführt werden. Auf Basis der Testergebnisse gibt VDV-ETS die Änderung für den Rollout in der Produktionsumgebung frei.

1.4.2.4 Penetrations-Tests

Penetrationstests sind kontrollierte Sicherheitsüberprüfungen, bei die Tester versuchen, in ein IT-System, eine Anwendung oder ein Netzwerk einzudringen. Das Ziel eines Penetrationstests ist es, Sicherheitslücken aufzudecken, bevor böswillige Angreifer diese ausnutzen können.

Es handelt sich dabei um eine praxisnahe Simulation realer Cyberangriffe, die dazu dient, Schwachstellen in Sicherheitsmechanismen zu identifizieren und ihre potenziellen Auswirkungen zu bewerten.

Im Rahmen des Betriebs- und Kommunikationsmanagements ist der Auftragnehmer verpflichtet, zur Sicherstellung der Netzwerksicherheit regelmäßige Penetrationstests durchzuführen. (Siehe Kapitel 1.2.2) Die VDV-ETS behält sich vor diese durch unabhängige Dritte durchführen zu lassen.s

1.5 Abnahme

1.5.1 Definition der Abnahme

Die Abnahme der Software erfolgt durch den Auftraggeber, sobald der Auftragnehmer die Bereitstellung zur Abnahme (BzA) erklärt. Die schlussendliche Abnahme erfolgt nach erfolgreicher Durchführung sämtlicher Tests aus dem gemeinsam definierten Testfallkatalog, die die Erfüllung der definierten Anforderungen bestätigen. Die Abnahme ist Voraussetzung für die finale Übergabe der Software und die Durchführung der Restzahlung. Die genauen Fristen und der Zahlungsplan sind Teil des Vertrags.

1.5.2 Abnahmeanforderungen

Die Software gilt als abnahmebereit, wenn:

- Alle definierten funktionalen und nicht-funktionalen Anforderungen umgesetzt und getestet wurden.
- Die Software fehlerfrei läuft.
- Alle definierten grafische Benutzeroberflächen (GUIs) sind wie abgestimmt, vollständig und freigegeben umgesetzt.
- Alle Dokumentationen (Benutzerhandbuch, technische Dokumentation) vollständig und verständlich vorliegen.
- Ein Abnahmetestplan erstellt wurde, der alle relevanten Tests und Prüfkriterien beinhaltet. Der Abnahmetestplan basiert auf dem, durch den Auftragnehmer in Abstimmung mit dem Auftraggeber, definierten Testfallkatalog.

1.5.3 Abnahmetests

Die Abnahme erfolgt durch die Durchführung eines Abnahmetests, der folgende Phasen umfasst:

1. **Testspezifikation:** Basis des Abnahmetests bildet der gemäß Kapitel 1.4.2 definierte Testfallkatalog.
2. **Testdurchführung:** Der Auftraggeber führt in Absprache mit dem Auftragnehmer die Tests durch. Diese beinhalten alle Tests zur Überprüfung der Funktionalität, Performance und Sicherheit.
3. **Fehlerbehebung:** Falls während der Tests Fehler auftreten, sind diese vom Auftragnehmer zu beheben, und die betroffenen Tests sind erneut durchzuführen.
4. **Abnahmeprotokoll:** Nach Abschluss der Tests erstellt der Auftraggeber ein Abnahmeprotokoll, in dem die Ergebnisse dokumentiert werden. Dieses Protokoll wird von beiden Parteien unterzeichnet.

1.5.4 Abnahmekriterien

Die Software gilt als abgenommen, wenn:

- Alle im Testkonzept definierten Kriterien erfüllt sind.
- Alle grafischen Benutzeroberflächen (GUI) sind, wie durch den Auftragnehmer freigegeben, umgesetzt.
- Alle zur Abnahme zu behebende Fehler behoben wurden und die Software stabil und funktionsfähig läuft.

1.5.5 Abnahmezeitraum

Die Abnahme erfolgt spätestens 10 Werktage nach der Durchführung des Abnahmetests, es sei denn, es wurden vorher noch offene Punkte festgestellt, die eine erneute Prüfung erfordern. Nach erfolgter Teilabnahme der Umsetzungsphase 2 schließt eine, im Lastenheft definierte, 3-monatige Probephase im Produktivbetrieb an. Nach erfolgreichem Abschluss der Probephase erfolgt die finale Abnahme des Gesamtsystems. Die zugehörigen Zahlungsziele werden im Zahlungsplan im Vertrag definiert.

1.5.6 Abnahmeverweigerung

Der Auftraggeber kann die Abnahme verweigern, wenn:

- Wesentliche Anforderungen nicht erfüllt sind oder gravierende Fehler bestehen, die die Nutzung der Software unzumutbar machen.
- Der Abnahmetest nicht erfolgreich abgeschlossen werden konnte und die Fehlerbehebung nach dem vereinbarten Zeitraum noch nicht erfolgt ist.

1.5.7 Schlussbestimmungen

Mit der Abnahme der Software bestätigt der Auftraggeber, dass die Software die vereinbarten Anforderungen erfüllt und die Projektdokumentation abgeschlossen ist. Eventuelle zusätzliche Funktionen oder Änderungen, die nach der Abnahme verlangt werden, werden in einem Change-Management-Prozess behandelt.

1.6 Version Management

Für alle Softwarekomponenten und Dokumentationen muss eine zuverlässige Versionsverwaltung vorhanden sein. Dies stellt sicher, dass alle Änderungen nachvollziehbar sind und bei Bedarf auf frühere Versionen zurückgegriffen werden kann. Versionierungssysteme ermöglichen eine lückenlose Nachverfolgung von Änderungen, die Angabe der Verantwortlichen sowie die Dokumentation von durchgeführten Tests und Freigaben. Es muss klar definiert sein, welche Versionen als stabil gelten und für den Einsatz in der Produktionsumgebung freigegeben sind. Jeder Release-Prozess muss durch Versionskennzeichnungen unterstützt werden, die eindeutige Referenzen zu Änderungen, Verbesserungen oder Bugfixes enthalten. Dabei sollten die Prinzipien von Semantic Versioning befolgt werden.

1.7 Change- und Release-Management

Jede Änderung am System muss über ein formales Änderungsmanagement (Change-Management) gesteuert werden. Dieses umfasst die Planung, Genehmigung, Implementierung und Bewertung von Änderungen. Änderungen dürfen nur nach erfolgreichem Testen und einer detaillierten Bewertung der potenziellen Auswirkungen auf die Produktion ausgerollt werden.

Release Management ist der Prozess, der sicherstellt, dass alle neuen Versionen oder Updates eines Systems reibungslos und kontrolliert in die Produktionsumgebung eingeführt werden. Es muss eine klare Trennung zwischen Entwicklungs-, Test- und Produktionsphasen geben, und die Freigabeprozesse müssen dokumentiert und durch den Auftraggeber genehmigt werden, bevor sie in Kraft treten.

Nach ITIL wird beschrieben, dass Änderungen nur nach einer sorgfältigen Bewertung der potenziellen Risiken und Auswirkungen durchgeführt werden dürfen. Der Prozess beginnt mit der Erstellung eines Change Requests (RFC – Request for Change), der alle Details der geplanten Änderung, einschließlich der Ziele, Risiken, betroffenen Systeme und der beteiligten Parteien, enthält. Dieser Request wird anschließend durch ein Change Advisory Board (CAB) geprüft, das die Relevanz und das Risiko der Änderung bewertet und eine Entscheidung über die Genehmigung oder Ablehnung trifft. Die Zusammensetzung des CAB wird im Projekt definiert. Diese Funktion kann auch im Rahmen von Service-Meetings zwischen dem Auftragnehmer und Auftraggeber erfolgen.

Laut ITIL müssen Releases in einer kontrollierten Umgebung, bspw. in Staging- oder Testumgebungen, überprüft werden, bevor sie im Produktionssystem implementiert werden. Auch das Rollback-Verfahren, falls ein Release Probleme verursacht, muss im Vorfeld durch den Auftragnehmer definiert werden.

1.8 Administrator Management

Administrative Zugriffsrechte für den reibungslosen Betrieb des Systems müssen strikt kontrolliert und auf autorisiertes Personal beschränkt sein. Es ist notwendig, dass die Administratorenrollen klar definiert und ihre Berechtigungen auf das notwendige Minimum beschränkt sind. Zugriffe auf administrative Konten müssen regelmäßig überprüft und protokolliert werden, um sicherzustellen, dass nur autorisierte Handlungen durchgeführt werden. Multi-Faktor-Authentifizierung (MFA) und strenge Passwortrichtlinien müssen

angewendet werden, um das Risiko unbefugter Zugriffe zu minimieren.

Administratorrechte dürfen nur nach einem klaren Genehmigungsverfahren vergeben werden, und diese Rechte müssen regelmäßig überprüft werden, um sicherzustellen, dass sie weiterhin erforderlich sind.

VDV-ETS sieht die Verwendung der für das eTicket Security Hub (ESH) bestehende Single-Sign-On-Verfahren vor, um den Zugriff und auch die Rechte- und Rollen der jeweiligen Benutzer zu regeln. Der Auftragnehmer muss daher den administrativen Zugriff auf die Anwendung über das SSO-Verfahren umsetzen.

1.9 Nutzerfreundlichkeit

Das System muss so gestaltet sein, dass es den Benutzern ermöglicht, ihre Aufgaben effektiv und effizient durchzuführen, ohne unnötige Komplexität.

Dies umfasst eine intuitive Benutzeroberfläche, klare Anweisungen und eine konsistente Navigation, die den Nutzern hilft, sich schnell zurechtzufinden. Fehler- und Erfolgsmeldungen müssen klar und verständlich sein, damit die Benutzer wissen, ob ihre Aktionen erfolgreich waren oder welche Schritte unternommen werden müssen, um Probleme zu beheben. Zudem müssen Hilfsfunktionen oder Dokumentationen leicht zugänglich sein, damit Benutzer bei Bedarf auf Anleitungen zugreifen können. Die Benutzeroberfläche muss auch Barrierefreiheit berücksichtigen, um allen Nutzern einen gleichberechtigten Zugang zu gewährleisten. Es müssen also entsprechende Kontraste und Schriftgrößen verwendet werden, eine Vorlesefunktion ist nicht gesondert zu entwickeln.

Geeignete Qualitätskriterien für die Benutzerfreundlichkeit (Ergonomie) der Administrator-Oberfläche sind in der EN ISO 9241 Teil 110 "Grundsätze der Dialoggestaltung" definiert. Dementsprechend muss das Design der Benutzeroberflächen die folgenden Kriterien berücksichtigen:

1. **Angemessenheit der Aufgaben** – Geeignete Funktionalität, Minimierung unnötiger Interaktionen.
2. **Selbstbeschreibbarkeit** – Verständlichkeit durch Hilfestellungen / Feedback.
3. **Kontrollierbarkeit** – Kontrolle des Dialogs durch den Benutzer.
4. **Erwartungskonformität** – Konsistenz, Anpassung an das Benutzer-Modell.
5. **Fehlertoleranz** – Nicht erkannte Fehler hindern den Benutzer nicht daran, seine Ziele zu erreichen, erkannte Fehler lassen sich leicht korrigieren.

6. **Individualisierung** – Anpassungsfähigkeit an individuelle Benutzer und Arbeitssituationen.
7. **Erleichterung des Lernens** – Benutzerführung, Minimierung der Lernzeit. Integration des Benutzerhandbuchs als Online-Hilfe in der Oberfläche.

Für die Darstellung auf mobilen Geräten muss ein entsprechendes responsive Design für alle gängigen iOS, Android und Windows Phone Geräte erstellt werden.

1.10 Adressierbarkeit

Die Adressierbarkeit bezieht sich auf die Fähigkeit des Systems, Dienste, Komponenten oder Ressourcen eindeutig und zuverlässig zu identifizieren und zu adressieren. Dies stellt sicher, dass alle Anfragen und Zugriffe auf die richtigen Ziele geleitet werden. Eine klare und strukturierte Adressierung ist entscheidend für die Interoperabilität und Skalierbarkeit des Systems, insbesondere in verteilten Umgebungen. Jede Ressource oder Komponente muss über eine eindeutige Kennung oder URL verfügen, die sicherstellt, dass keine Konflikte auftreten und alle Elemente des Systems leicht aufgerufen und genutzt werden können.

1.11 Monitoring

Das System muss kontinuierlich überwacht werden, um Leistung, Sicherheit und Verfügbarkeit zu gewährleisten. Diese Überwachung erfolgt durch spezialisierte Monitoring-Tools, die automatisch Anomalien, Performance-Engpässe oder sicherheitsrelevante Vorfälle erkennen.

Sobald das Monitoring-System Auffälligkeiten feststellt, ist der Betreiber verpflichtet, unverzüglich eine Benachrichtigung an die zuständigen Stellen zu senden. Diese Benachrichtigung muss klar und präzise formuliert sein und die Art des Vorfalls sowie dessen Schweregrad beschreiben. Potenzielle Ereignisse, die eine Benachrichtigung auslösen, umfassen:

- Leistungseinbrüche: Wenn das System eine festgelegte Schwelle überschreitet, z.B. bei CPU-Auslastung, Speicherverbrauch oder Netzwerklatenz.
- Sicherheitsvorfälle: Jeder unautorisierte Zugriffsversuch oder eine potenzielle Sicherheitslücke, wie z.B. unerwartete Änderungen an Daten oder Konfigurationsdateien.

- Systemausfälle: Unerwartete Ausfälle oder Unterbrechungen der Verfügbarkeit, die die Nutzung des Systems einschränken.
- Fehlgeschlagene Prozesse: Wiederholte oder kritische Fehler bei der Ausführung von Anwendungen oder Diensten.
- Nichterreichbarkeit von Systemkomponenten

Der Betreiber muss sicherstellen, dass die Benachrichtigungen zeitnah erfolgen, um die zuständigen Teams in die Lage zu versetzen, schnell zu reagieren. Außerdem müssen die Monitoring-Protokolle regelmäßig ausgewertet werden, um präventive Maßnahmen ergreifen zu können und zukünftige Vorfälle zu minimieren.

1.12 Logging

Das Logging dient der Nachvollziehbarkeit von Systemabläufen, der Fehleranalyse, der Sicherheitsüberwachung sowie der Erfüllung regulatorischer Anforderungen.

1.12.1 Allgemeines

Das System muss alle relevanten Ereignisse automatisiert und kontinuierlich protokollieren.

Die Protokollierung darf die Systemperformance nicht wesentlich beeinträchtigen und muss skalierbar sein.

1.12.2 Umfang

Mindestens folgende Ereignisse sind zu erfassen:

- Systemereignisse (Start/Stop, Konfigurationsänderungen)
- Benutzeraktivitäten (Anmeldungen, Berechtigungsänderungen)
- Sicherheitsrelevante Ereignisse (Zugriffsversuche, Fehlermeldungen)
- Anwendungs- und Fehlerereignisse

1.12.3 Struktur und Inhalte

Logs müssen strukturiert, maschinenlesbar und archivierbar sein. Der Auftragnehmer hat dafür ein geeignetes Dateiformat, auch durch Nutzung eines Logging-Frameworks, auszuwählen. Jeder Eintrag muss mindestens Zeitstempel, Log-Level, Quelle und Beschreibung enthalten.

1.12.4 Log-Level

Es müssen mehrere Log-Level (z. B. DEBUG, INFO, WARN, ERROR) unterstützt werden.

Die Konfiguration des Log-Level muss zur Laufzeit durch die Systemadministratoren möglich sein.

1.12.5 Speicherung, Sicherheit & Compliance

Logs müssen revisionssicher gespeichert und vor unbefugtem Zugriff geschützt werden.

Personenbezogene, personenbeziehbare oder sensible Daten (z.B. Kennwörter) dürfen nicht im Klartext protokolliert werden. Die Verarbeitung der Informationen muss immer DSGVO-konform erfolgen.

Zugriff auf Logs muss auf die Systemadministratoren beschränkt sein.

1.12.6 Aufbewahrung

Die Aufbewahrungsdauer muss konfigurierbar sein und regulatorische Anforderungen erfüllen.

Die Archivierung und Löschung der Logdateien erfolgen im Rahmen der in Kapitel 3.1 definierten Mechanismen.

1.12.7 Monitoring und Integration

Logs müssen in das Systemmonitoring- und Analysewerkzeuge integrierbar bzw. durch solche auswertbar sein. Kritische Ereignisse müssen Alarme auslösen können.

2 Service Level Agreements

In den nachfolgenden Kapiteln werden Service Levels für den Betrieb der beauftragten Systeme vereinbart. Dazu gehören der Support, Fehlerbehandlung und Fehlerklassen, die Performance, die Systemverfügbarkeiten und die Wartung der Systeme.

2.1 Support

Ein effektiver Support ist unerlässlich, um auftretende Probleme schnell zu beheben und die Anwender des Systems bestmöglich zu unterstützen. Dabei geht es nicht nur um die Behebung von Störungen, sondern auch um die Unterstützung bei der Nutzung und Verwaltung des Systems.

Der Auftragnehmer muss die folgenden zwei Arten von Unterstützung für die Staging- und Produktionssysteme bereitstellen. „Benutzer“ in diesem Zusammenhang sind Mitarbeiter von VDV-ETS oder seiner Mitgliedsunternehmen, die die Systeme nutzen, oder technisches Personal eines von VDV-ETS autorisierten Lieferanten.

1. Fehler- und Störungsmeldungen sowie Anfragen werden mit dem Standard-Incident-Management-Tool von VDV-ETS erfasst und verfolgt. Die verbale und schriftliche Kommunikation muss mindestens auf Deutsch oder Englisch unterstützt werden.
2. Der Auftragnehmer stellt eine Support-Telefonnummer und E-Mail-Adresse für technisches Personal zur Verfügung, die während der Hauptbetriebszeit (Montag bis Freitag jeweils von 06:00 bis 22:00 Ortszeit (Deutschland), ausgenommen bundeseinheitliche Feiertage) beantwortet werden. Die verbale und schriftliche Kommunikation muss auf Deutsch oder Englisch unterstützt werden.

Folgendes wird darüber hinaus für den Support definiert:

- Mehrstufiger Support: Der Support wird in verschiedene Eskalationsstufen unterteilt, um sicherzustellen, dass Probleme gemäß Ihrer jeweiligen Kritikalität und Lösbarkeit schnell gelöst oder an spezialisierte Teams weitergeleitet werden können.
- Reaktions- und Entstörungszeiten: Es sind klare Reaktionszeiten für den Start der Bearbeitung von Anfragen und Entstörungszeiten für die Behebung von Störungen festgelegt, je nach Schweregrad des Problems. (siehe Kapitel 2.6.3).

- Kommunikationskanäle: Der Support ist über verschiedene Kanäle wie E-Mail, Telefon und das JIRA-Ticket-System der VDV-ETS erreichbar. Alle Supportanfragen werden dokumentiert, um eine lückenlose Nachverfolgung und Analyse von wiederkehrenden Problemen zu ermöglichen.

Der Auftragnehmer wird die VDV-ETS und dessen Vertragspartner über das ETS-Kundenportal „Jira Service Desk“ durch die in dieser Vereinbarung beschriebenen Leistungen unterstützen.

Die maßgebliche Internet-Adresse des ETS-Kundenportals lautet:

<https://eticket-deutschland.atlassian.net/servicedesk/customer/portals>

Das ETS-Kundenportal steht der VDV-ETS und dessen Vertragspartnern zur Einreichung von Meldungen zur Verfügung. Die Anlage neuer Benutzer (Mitarbeiter des Kunden, Mitarbeiter von Auftragnehmer oder Vertragspartner der VDV-ETS) im Jira Service Desk liegt in der Verantwortung der VDV-ETS.

Über das ETS-Kundenportal können der VDV-ETS und seine Vertragspartner Fehlfunktionen der Software und Beratungsfragen über ein entsprechendes Formular berichten. Dadurch wird ein Support-Ticket erzeugt. Die Kontaktaufnahme erfolgt ausschließlich über das ETS-Kundenportal. Der Auftragnehmer verpflichtet sich, den Support für die definierte Reaktionszeit sowie die Verfügbarkeit sicherzustellen.

2.2 Störungen & Fehler

Bei Störungen oder Fehlern handelt es sich um unerwartet eintretende Ereignisse, bei denen die festgelegte Funktionalität beeinträchtigt oder nicht mehr möglich ist.

Im Rahmen dieses Service Level Agreements (SLA) wird festgelegt, dass der Auftragnehmer ein vollständiges und nachvollziehbares Betriebshandbuch für das bereitgestellte IT-System zu erstellen und dem Auftraggeber zu übergeben hat. Das Betriebshandbuch muss alle für den sicheren, stabilen und effizienten Betrieb erforderlichen Informationen enthalten und sich an anerkannten Standards und Best Practices orientieren.

Insbesondere sind folgende Inhalte abzudecken:

- Systemübersicht und Architektur

- Installations- und Konfigurationsanleitungen
- Betriebsprozesse (inkl. Start, Stopp, Monitoring, Backup und Recovery)
- Benutzer- und Berechtigungskonzepte
- Wartungs- und Updateverfahren
- Störungsbehebung (Incident- und Problem-Management)
- Sicherheitsmaßnahmen und Notfallverfahren

Das Betriebshandbuch ist in strukturierter, verständlicher und revisionsfähiger Form bereitzustellen und während der gesamten Vertragslaufzeit aktuell zu halten.

Die Erstellung hat sich insbesondere an folgenden Normen und Standards zu orientieren:

- ISO/IEC 20000 (IT-Service-Management)
- ISO/IEC 27001 (Informationssicherheitsmanagement)
- ITIL (Best Practices für IT-Service-Management)

Sofern einschlägig, sind zusätzlich projektspezifische oder organisationsinterne Vorgaben des Auftraggebers zu berücksichtigen.

Das System muss Mechanismen zur effektiven Fehlerbehandlung bereitstellen, um eine schnelle und sichere Wiederherstellung nach Störungen zu ermöglichen. Störungen, die während des Betriebs auftreten, müssen protokolliert und dem zuständigen Support-Team gemeldet werden. Es ist notwendig, dass das System Fehlermeldungen verständlich und detailliert ausgibt, damit Benutzer und Administratoren die Störung schnell erkennen und beheben können.

Die Störungsbehandlung muss folgende Schritte umfassen:

- Erkennung: Das System muss in der Lage sein, Fehler automatisch zu erkennen und die Ursache zu identifizieren.
- Benachrichtigung: Nach der Fehlererkennung muss das System automatisierte Benachrichtigungen an die zuständigen Stellen senden.
- Fehlerprotokollierung: Jeder Fehler muss umfassend protokolliert werden, einschließlich des Zeitpunkts, der betroffenen Komponenten und einer Beschreibung des Fehlers.

- Wiederherstellung: Das System muss automatisierte Mechanismen zur Wiederherstellung nach bestimmten Fehlern bieten, um die Auswirkungen auf die Benutzer und den Betrieb zu minimieren.

2.2.1 Benachrichtigung

Im Falle einer Störung oder eines Fehlers muss das System eine sofortige Benachrichtigung an die zuständigen Support- und IT-Teams senden, um eine schnelle Behebung zu ermöglichen. Die Benachrichtigung muss detaillierte Informationen enthalten, damit die Art und Dringlichkeit des Fehlers schnell bewertet werden können.

Zusätzlich muss der Auftragnehmer die VDV-ETS unmittelbar über alle relevanten Fehler informieren, insbesondere wenn sie Auswirkungen auf die Verfügbarkeit oder Funktionalität der Dienstleistungen haben. Diese Benachrichtigung dient dazu, den VDV-ETS zeitnah über den Zustand des Systems zu informieren und gegebenenfalls Maßnahmen auf seiner Seite zu koordinieren.

Zur Meldung von Störungen und Ausfällen, verwendet die VDV-ETS ein JIRA-System der Firma Atlassian, in welchem für jede Störung oder jeden Ausfall ein entsprechendes Ticket zu eröffnen ist. Die Eröffnung kann dabei auch automatisiert durch die Nutzung vorhandener Schnittstellen erfolgen. Die genaue Definition des Prozesses erfolgt im Rahmen des Umsetzungsprojekts.

2.2.1.1 Inhalt der Benachrichtigung

Für eine qualifizierte Störungsmeldung sind folgende Meldungsinhalte erforderlich:

- Name des Meldenden und Kontaktdaten (Telefon, E-Mail)
- Name des fachlichen Ansprechpartners und Kontaktdaten (Telefon, E-Mail)
- Name und Kontaktdaten für Rückmeldungen (Telefon, E-Mail)
- Ausführliche Problem-, Fehler-, oder Störungsbeschreibung:
 - Bei welcher Aktion ist das Problem aufgetreten?
 - Betrifft das Problem einen spezifischen Mandanten?
 - Wenn ja, Angabe der Mandantenkennung (Org-ID)
 - In welcher Umgebung ist das Problem aufgetreten?
 - Staging-Umgebung (Level-2)
 - Produktions-Umgebung (Level-3)

Zeitpunkt an dem das Problem bemerkt wurde (Datum und Uhrzeit (MEZ=UTC+1))

2.2.1.2 Fehler Klassifizierung

Fehler müssen je nach ihrem Schweregrad und ihren Auswirkungen auf den Betrieb des Systems klassifiziert werden. Diese Klassifizierung ermöglicht es, Prioritäten bei der Fehlerbehebung zu setzen.

Die Klassifizierungen umfassen:

- Störungsklasse 1 (Niedrig): Der Fehler hat nur geringe Auswirkungen auf das System oder die Benutzerfreundlichkeit und verursacht keine unmittelbaren Betriebsstörungen. Eine Behebung kann im Rahmen eines regulären Updates erfolgen
- Störungsklasse 2 (Unwesentlich): Der Fehler betrifft einige nicht-kritische Funktionen oder verursacht geringe Beeinträchtigungen. Der Fehler muss in einem angemessenen Zeitrahmen behoben werden, um langfristige Auswirkungen zu vermeiden.
- Störungsklasse 3 (Schwerwiegend): Wichtige Funktionen sind betroffen, aber das System bleibt weiterhin nutzbar, wenn auch mit Einschränkungen. Eine schnelle Lösung wird benötigt, jedoch ist der Betrieb teilweise noch möglich.
- Störungsklasse 4 (Kritisch): Der Fehler führt zu einem vollständigen Systemausfall oder einer schwerwiegenden Beeinträchtigung der Kernfunktionen. Sofortiges Handeln ist erforderlich, da der Betrieb stark beeinträchtigt ist.

2.3 Performance

Die Performance des Systems ist ein wesentlicher Bestandteil dieses Service Level Agreements (SLA) und hat direkten Einfluss auf die Nutzererfahrung sowie die Effizienz der bereitgestellten Dienste. Eine hohe Performance sorgt dafür, dass alle Systeme und Anwendungen schnell und zuverlässig arbeiten, selbst bei erhöhter Belastung. Die Leistung des Systems umfasst mehrere Aspekte, die in diesem SLA geregelt sind, um eine stabile und leistungsfähige IT-Umgebung sicherzustellen.

2.3.1 Produktions-System

- Das Produktionssystem muss so konzipiert sein, dass es eine hohe Verfügbarkeit und Reaktionsgeschwindigkeit bietet. Die Verarbeitung von Transaktionen, Prüfungen und Auswertungen muss auch bei paralleler Nutzung durch mehrere Mandanten performant erfolgen. Lastspitzen einzelner Mandanten dürfen andere Mandanten nicht beeinträchtigen.

Die folgenden Kriterien müssen berücksichtigt werden:

- Reaktionszeiten: Die Reaktionszeiten für Benutzeranfragen und Transaktionen dürfen bestimmte, festgelegte Grenzen nicht überschreiten. Die Reaktionszeit des Systems muss im Normalbetrieb unter 300 Millisekunden liegen. Dies bezieht sich auf die Zeit, die das System benötigt, um auf eine Benutzereingabe oder einen Anwendungsaufwurf zu reagieren. Hiervon ausgenommen sind komplexe Datenexporte, welche aufgrund der Datenmenge mehr Zeit benötigen.
- Antwortzeit: Die Antwortzeit ist die Zeit, die zwischen der Benutzerinteraktion (z. B. Klick, Eingabe oder Scrollen) und der Anzeige einer Antwort (z. B. eine Änderung auf der Benutzeroberfläche) vergeht. Eine Antwortzeit darf jedoch nicht länger als 1 Sekunde sein. Im Rahmen der Projektarbeit werden Benutzeraktionen und Anzeige der Antworten konkretisiert. Sollten Abweichungen während der Implementierungsphase von dem Auftragnehmer angemerkt werden, müssen die Abweichungen analysiert und mögliche Lösungen abgestimmt werden.
- Erwartete Benutzerzahlen: Das System muss die folgenden zu erwartenden Benutzerzahlen zulassen und unterstützen. Die Angabe ist jeweils für die ersten drei Jahre des Betriebs (Staging und Production) antizipiert:
 - 2027: 150 Benutzer (25 Mandanten + VDV-ETS Administratoren)
 - 2028: 175 Benutzer (30 Mandanten + VDV-ETS Administratoren)
 - 2029: 225 Benutzer (40 Mandanten + VDV-ETS Administratoren)
- Durchsatz: Das System muss in der Lage sein, mindestens 50 gleichzeitige Benutzer oder Transaktionen ohne merkliche Leistungseinbußen zu verarbeiten. Der Durchsatz gibt an, wie viele Nachrichten das System in einem bestimmten Zeitraum verarbeiten kann.
- Ressourcennutzung: Die Nutzung von CPU, Speicher und Netzwerkressourcen muss effizient sein. Überwachungssysteme müssen kontinuierlich die Ressourcennutzung

analysieren, um Engpässe frühzeitig zu identifizieren und gegebenenfalls zu beseitigen.

- Lasttests: Last- und Stresstests müssen durch den Auftragnehmer durchgeführt werden, um die Leistungsgrenzen des Systems zu ermitteln und sicherzustellen, dass es auch unter hohen Belastungen stabil bleibt. Eine jährliche Wiederholung der Lasttests muss durchgeführt werden.

Tabelle 1: Performance Produktionssystem

System	Reaktionszeit	Antwortzeit	Transaktionen pro Sekunde (TPS)
MPS je Mandant	300 Millisekunden	1 Sekunde	10

2.3.2 Staging-System

Das Staging-System ist die Testumgebung, in der neue Funktionen und Updates durch den Auftragnehmer, vor der Bereitstellung im Produktionssystem, validiert werden. Die Leistungsanforderungen an das Staging-System müssen ebenfalls hoch sein, um realistische Tests durchführen zu können.

- Übereinstimmung mit Produktionsanforderungen: Das Staging-System muss in Bezug auf Leistung und Ressourcen ähnlich wie das Produktionssystem konfiguriert sein, um realistische Testergebnisse zu erzielen.
- Testen von Performance: In der Staging-Umgebung müssen umfassende Tests zur Performance durchgeführt werden, einschließlich Last- und Stresstests, um sicherzustellen, dass neue Funktionen oder Updates die Leistung nicht beeinträchtigen.
- Analyse der Testergebnisse: Nach den Tests müssen die Ergebnisse sorgfältig analysiert werden, um Optimierungspotenziale zu identifizieren und sicherzustellen, dass das System vor der Einführung im Produktionsbetrieb optimal funktioniert.

2.4 Skalierbarkeit

Das System muss von Anfang an so konzipiert sein, dass sie problemlos skalierbar sind, um den steigenden Anforderungen gerecht zu werden. Skalierbarkeit ist sowohl für die Hardware- als auch für die Softwarearchitektur von Bedeutung.

Das System muss für den Betrieb von mindestens 15 bis 50 Mandanten ausgelegt sein, ohne dass sich Anzahl oder Aktivität einzelner Mandanten negativ auf die Performance anderer Mandanten auswirken.

2.4.1 Transaktionsvolumen

Das System muss ein monatliches Nachrichtenvolumen von 30 Millionen Nachrichten, mit ca. 1 Millionen Nachrichten pro Tag, verarbeiten können. VDV-ETS rechnet mit Lastspitzen im Zeitraum von 22:00 – 4:00Uhr, da in diesem Zeitraum nächtliche Prozesse bei den Unternehmen zur Datenentsorgung laufen.

Der Auftragnehmer muss die Skalierung der Ressourcen je Mandant im Produktivbetrieb sicherstellen. Dies ist notwendig, da die Lastspitzen und das Nachrichtenvolumen der einzelnen Mandate stark variieren können. Zum Beispiel haben Verbünde ohne Check-In/Check-Out deutlich weniger Kontroll-/Erfassungstransaktionen als Verbünde mit diesen Systemen. Auch die Größe des Verbundes hat maßgeblichen Einfluss auf die Datenmenge des zugehörigen Mandanten.

2.5 Verfügbarkeit

Eine hohe Verfügbarkeit stellt sicher, dass die Anwendungen und Dienste kontinuierlich und ohne größere Ausfallzeiten genutzt werden können. Im Rahmen dieses SLA sind klare Verfügbarkeitsanforderungen definiert, die regelmäßige Wartungen, unvorhergesehene Ausfälle und Datenwiederherstellung abdecken.

2.5.1 Verfügbarkeit des Produktions-Systems

Die Verfügbarkeit des Produktiven Systems ist ein kritischer Faktor für den reibungslosen Betrieb und die Nutzerzufriedenheit. Eine hohe Verfügbarkeit stellt sicher, dass die Anwendungen und Dienste kontinuierlich und ohne größere Ausfallzeiten genutzt werden können.

Das System soll 24/7 betrieben werden. Während der Hauptbetriebszeit (Montag bis Freitag jeweils von 06:00 bis 22:00 Ortszeit (Deutschland), ausgenommen bundeseinheitliche Feiertage) muss eine Verfügbarkeit von mindestens gemäß Tabelle 2 gewährleistet werden.

Tabelle 2: Verfügbarkeiten für Produktivsysteme

System	Verfügbarkeit pro Monat während der Hauptbetriebszeit	Ausfallzeit pro Monat während der Hauptbetriebszeit
MPS	99,0 %	3,2 Stunden

Maximale Ausfallzeiten für zwei aufeinanderfolgende Monate dürfen nicht zusammenhängend auftreten.

Die Verfügbarkeitsüberwachung muss in Abständen von 10 Minuten erfolgen. Geplante und abgestimmte Wartungsfenster werden bei der Berechnung der Verfügbarkeit nicht auf die Ausfallzeit angerechnet.

2.5.2 Verfügbarkeit des Staging-Systems

Das Staging-System dient der Vorbereitung und dem Testen von Änderungen vor deren Einsatz im Produktionssystem.

Das System soll 24/7 betrieben werden. Während der Hauptbetriebszeit (Montag bis Freitag jeweils von 06:00 bis 22:00 Ortszeit (Deutschland), ausgenommen bundeseinheitliche Feiertage) muss eine Verfügbarkeit von mindestens gemäß Tabelle 3 gewährleistet werden.

Tabelle 3 Verfügbarkeiten für Staging-Systeme

System	Verfügbarkeit pro Monat während der Hauptbetriebszeit	Ausfallzeit pro Monat während der Hauptbetriebszeit
MPS	93,33%	22 Stunden

Maximale Ausfallzeiten für zwei aufeinanderfolgende Monate dürfen nicht zusammenhängend auftreten.

Die Verfügbarkeitsüberwachung muss in Abständen von 10 Minuten erfolgen. Wartungsfenster werden bei der Berechnung der Verfügbarkeit nicht auf die Ausfallzeit angerechnet.

2.6 Wartung

Die Wartung der Systeme und Anwendungen ist ein wesentlicher Bestandteil dieses Service Level Agreements (SLA) und dient dazu, die Stabilität, Sicherheit und Verfügbarkeit der IT-Infrastruktur langfristig zu gewährleisten. Regelmäßige Wartungen sind erforderlich, um Sicherheitsupdates, Patches, Hardware-Optimierungen und Software-Verbesserungen zu implementieren und somit potenzielle Risiken zu minimieren.

Die Wartungen werden vom Auftragnehmer geplant und in regelmäßigen Intervallen durchgeführt. Dabei werden alle erforderlichen Maßnahmen getroffen, um sicherzustellen, dass die Systeme auch nach der Wartung stabil und zuverlässig arbeiten. Notwendige Software-Updates, Sicherheits-Patches sowie Systemoptimierungen werden innerhalb der festgelegten Wartungsfenster durchgeführt.

Der VDV-ETS wird rechtzeitig, mindestens 10 Werktage vor einer geplanten Wartung, schriftlich über den Umfang, den Zeitpunkt und die voraussichtliche Dauer der Wartungsarbeiten informiert. Diese Vorankündigung ermöglicht der VDV-ETS entsprechende Vorbereitungen zu treffen, insbesondere bei Wartungen, die zu vorübergehenden Einschränkungen oder Ausfällen des Systems führen könnten.

Wartungsarbeiten werden nach Möglichkeit außerhalb der Hauptbetriebszeiten durchgeführt, um die Auswirkungen auf den laufenden Betrieb so gering wie möglich zu halten. Typischerweise werden dafür Wartungsfenster in den späten Abendstunden oder am Wochenende vorgesehen. Die genaue Festlegung des Wartungsfensters erfolgt in Abstimmung zwischen VDV-ETS und Auftragnehmer, um den Geschäftsbetrieb möglichst wenig zu beeinträchtigen. In Ausnahmefällen, wie bei sicherheitskritischen Vorfällen oder dringenden Störungsbehebungen, können Notfallwartungen notwendig sein. Der VDV-ETS wird in solchen Fällen so früh wie möglich informiert, wobei die Vorankündigungsfrist in dringenden Fällen entfallen kann, um den Schutz und die Stabilität des Systems nicht zu gefährden.

Nach jeder Wartung erhält der VDV-ETS eine detaillierte Dokumentation der durchgeführten Maßnahmen. Diese umfasst Informationen zu den durchgeführten Arbeiten, etwaige aufgetretene Probleme, die angewandten Lösungen und eine Einschätzung der Systemperformance nach der Wartung.

Der Auftragnehmer legt ein Wartungskonzept der VDV-ETS zur Prüfung, welche die vorangegangenen Punkte berücksichtigt, vor. Der VDV-ETS überprüft, ob die im Konzept beschriebenen Maßnahmen und Prozesse den Anforderungen und Erwartungen entsprechen und den Geschäftsbetrieb nicht unverhältnismäßig beeinträchtigen. Nach erfolgter Prüfung und Genehmigung durch den VDV-ETS tritt das Konzept in Kraft und bildet die Grundlage für die regelmäßige Wartung der Systeme. Änderungen oder Ergänzungen des Konzepts werden ebenfalls durch den Auftragnehmer vorgeschlagen und durch den VDV-ETS geprüft und freigegeben.

Generell erfolgen Änderungen an den Systemen in einem Mehrstufigen Prozess. Änderungen an den Systemen werden immer zuerst auf dem Staging-System erprobt, über einen im Vertrag definierten Zeitraum. Erfolgt diese Erprobungs-/Testphase erfolgreich, so kann die Änderung in Abstimmung mit dem Auftraggeber auf das Produktions-System eingespielt werden.

2.6.1 Produktions-System

Die Wartung des Produktionssystems muss so geplant und durchgeführt werden, dass Ausfallzeiten auf ein Minimum reduziert werden und die Betriebsbereitschaft des Systems sichergestellt bleibt. Dazu gehören:

- Geplante Wartungsfenster: Alle notwendigen Wartungsarbeiten müssen in vorab festgelegten und kommunizierten Zeitfenstern durchgeführt werden, vorzugsweise außerhalb der Hauptnutzungszeiten. Nutzer und relevante Ansprechpartner müssen im Voraus über geplante Arbeiten informiert werden, um eventuelle Auswirkungen auf den Betrieb zu minimieren.
- Regelmäßige Sicherheitsupdates: Um Sicherheitslücken zu schließen und die Verfügbarkeit zu gewährleisten, müssen regelmäßig Updates und Patches installiert werden. Diese Arbeiten müssen nach Möglichkeit ohne Ausfallzeiten erfolgen, z. B. durch den Einsatz von Hotfixes oder redundanten Systemen.
- Performance-Optimierung: Periodische Wartungsmaßnahmen müssen genutzt werden, um die Systemleistung zu optimieren. Dies umfasst die Analyse und Behebung von Engpässen in der Hardware- oder Softwareinfrastruktur.

2.6.2 Staging-System

Das Staging-System erfordert ebenfalls regelmäßige Wartungsmaßnahmen, um eine zuverlässige Testumgebung zu gewährleisten. Hierbei ist besonders auf die Erhaltung der Integrität der Testdaten und der Umgebung selbst zu achten.

- Synchronisierung mit dem Produktionssystem: Wartungsarbeiten am Staging-System müssen idealerweise in enger Abstimmung mit den Wartungszyklen des Produktionssystems erfolgen, um eine möglichst ähnliche Umgebung zu schaffen. Dabei ist sicherzustellen, dass Systemkonfigurationen und Versionen so weit wie möglich übereinstimmen.
- Regelmäßige Updates und Tests: Das Staging-System muss regelmäßig mit neuen Updates, Patches und Konfigurationsänderungen aktualisiert werden, um vorab die Auswirkungen dieser Änderungen auf das Produktionssystem zu testen. Dies umfasst auch die Durchführung von Sicherheits- und Performance-Tests.
- Datenaktualisierung: Um realistische Testszenarien zu gewährleisten, muss die Testumgebung regelmäßig mit repräsentativen Beispieldaten befüllt werden, ohne dabei Datenschutz- oder Compliance-Vorgaben zu verletzen.

2.6.3 Reaktions- und Entstörungs-Zeit

Die Reaktionszeit bezeichnet den Zeitraum vom Eingehen einer Störungsmeldung (Störungseingang) im Support bis zur Aufnahme der Bearbeitung der Störung durch den zuständigen Mitarbeiter und darf nicht länger als zwei Stunden dauern. Tritt eine Störung außerhalb der Hauptbetriebszeit (Montag bis Freitag jeweils von 06:00 bis 22:00 Ortszeit (Deutschland), ausgenommen bundeseinheitliche Feiertage) auf, gilt der Beginn der nächsten Hauptbetriebszeit als Zeitpunkt des Störungseingangs.

Die Entstörungszeit bemisst den Zeitraum ab Störungseingang bis zur Behebung der Störung.

Die folgende Tabellen definiert den Entstörungszeitraum, basierend auf den definierten Störungsklassen und der betroffenen Umgebung.

Tabelle 4 Störungsklassen Staging

Störungsklasse	Entstörungszeitraum
Störungsklasse 1 (Niedrig)	Störungseingang + 640 Hauptbetriebszeitstunden

Störungsklasse 2 (Unwesentlich)	Störungseingang + 320 Hauptbetriebszeitstunden
Störungsklasse 3 (Schwerwiegend)	Störungseingang + 160 Hauptbetriebszeitstunden
Störungsklasse 4 (Kritisch)	Störungseingang + 80 Hauptbetriebszeitstunden

Tabelle 5: Störungsklassen Produktion

Störungsklasse	Entstörungszeitraum
Störungsklasse 1 (Niedrig)	Störungseingang + 320 Hauptbetriebszeitstunden
Störungsklasse 2 (Unwesentlich)	Störungseingang + 120 Hauptbetriebszeitstunden
Störungsklasse 3 (Schwerwiegend)	Störungseingang + 48 Hauptbetriebszeitstunden
Störungsklasse 4 (Kritisch)	Störungseingang + 6 Hauptbetriebszeitstunden

2.6.4 Eskalations-Management

Eine Eskalation tritt ein, wenn die vereinbarten Leistungen und Qualitäten dieses Service Level Agreements im Falle der Erledigung eines Auftrages nicht erfüllt werden. Eine Eskalation beginnt grundsätzlich mit der Stufe 1 und tritt sofort bei einer Unterschreitung der zugesagten Qualität bzw. Überschreitung der zugesagten Lieferzeiten in Kraft.

Die Stufe 2 erfolgt nur, wenn die Stufe 1 durchlaufen wurde und steht zur Verfügung, wenn der festgestellte Qualitätsmangel nach Beginn der Stufe 1 nicht innerhalb von 24 Stunden beseitigt wurde.

Die Stufe 3 erfolgt dementsprechend nur, wenn die Stufe 2 durchlaufen wurde und steht zur Verfügung, wenn der festgestellte Qualitätsmangel nach Beginn der Stufe 2 nicht innerhalb von 24 Stunden beseitigt wurde.

Die Stufe 4 erfolgt nur, wenn die Stufe 3 durchlaufen wurde und steht zur Verfügung, wenn der festgestellte Qualitätsmangel nach Beginn der Stufe 3 nicht innerhalb von 24 Stunden beseitigt wird.

Für den Betrieb der Systeme ist eine Anlage „Ansprechpartner“ gemäß der folgenden Tabelle 7 „Störung und Eskalation“ zu diesem SLA-Dokument in Abstimmung zwischen VDV-ETS und dem Auftragnehmer zu erstellen und zu pflegen.

Im Eskalationsfall sind die in Anlage “Ansprechpartner” aufgeführten Eskalationsinstanzen anzurufen.

Tabelle 6: Störung und Eskalation

Stufen	Entstörungsdauer	Ansprechpartner	Ansprechpartner ETS
Eskalationsstufe 1	Reaktionszeit + Lösungszeit		
Eskalationsstufe 2	Plus 24 Stunden		
Eskalationsstufe 3	Plus 24 Stunden		
Eskalationsstufe 4	Plus 24 Stunden		

3 Zusätzliche funktionale Anforderungen

3.1 Archivierung / Löschkonzept

Das primäre Ziel dieses Löschkonzept ist es, den Speicherbedarf für Daten aus den Nachrichten in der Datenbank und den Registern des MPS zu minimieren. Durch das vollständige Löschen oder Archivieren nicht mehr benötigter Daten kann die Datenbankleistung verbessert und der benötigte Speicherbedarf reduziert werden. Es muss sichergestellt werden, dass alle Daten korrekt behandelt werden, insbesondere wenn spezifische Aufbewahrungsfristen für Daten bestehen.

3.1.1 Löschung gemäß DSGVO

Das System muss neben dem Archivierungskonzept geeignete Mechanismen zur Löschung von DSGVO relevanten Daten umsetzen. Genauer müssen personenbezogene Daten auf Anfrage hin gelöscht werden können. Zu beachten ist dabei die Kopplung an die Benutzerverwaltung des eTicket Security Hub (ESH) und das angeschlossene SSO-System.

3.1.2 Vorbedingungen

Bei der Archivierung bzw. Löschung der Daten ist zu berücksichtigen, dass bestimmte Daten auch nach Ablauf einer konfigurierten Frist nicht gelöscht werden dürfen. Im Folgenden werden Ausnahmen beschrieben, welche bei der Löschung und Archivierung berücksichtigt werden müssen.

3.1.2.1 Berechtigungsausgaben

Berechtigungen sind wertschaffend und sind daher, unabhängig vom konfigurierten Wert, mindestens 10 Jahre ab Gültigkeitsende durch das System vorzuhalten.

3.1.2.2 Fehlerhafte Daten

Daten, welche einen fehlerhaften Status aufweisen, sollen aus Gründen der Nachvollziehbarkeit und zur weiteren Analyse abweichend behandelt werden. Für diese Daten muss eine abweichende Vorhaltdauer der Transaktionsdaten durch die Super-Administratoren konfiguriert werden können.

3.1.2.3 Daten in Analyse

Befinden sich Daten in einer bestehenden Analyse (z.B. in einem Klärfall), welche noch nicht abgeschlossen ist, so dürfen diese Daten nicht von der Löschroutine erfasst werden. Eine Analyse gilt als abgeschlossen, sobald der zugehörige Klärfall VDV-ETS als gelöst quittiert wurde.

3.1.2.4 Konfiguration

Über die Systemparameter des MPS lässt sich durch die Super-Administratoren konfigurieren, nach wie vielen Tagen bestimmte Daten gelöscht oder archiviert werden. Die Konfiguration lässt sich je Nachrichtentyp (siehe Lastenheft_MPS_VO.9 [1], Kapitel 4.7.2.1) vornehmen.

3.1.2.5 Vorgehen

Zum Löschen oder Archivieren der Daten wird ein Job eingerichtet und dementsprechend im Joblogbuch (Lastenheft_MPS_VO.9[1], Kapitel 4.8.1) protokolliert. Der Job löscht/archiviert in einem konfigurierbaren Abstand in Tagen die Daten. Bei Ausführung des Jobs werden neben den konfigurierten Parametern für die einzelnen Typen die Vorbedingungen berücksichtigt.

3.1.2.6 Randbedingungen

Jeder Lösch-/Archivierungsvorgang wird zusätzlich in einem Archivierungslogbuch protokolliert. Die Protokollierung umfasst die folgenden Daten: Konfigurationsdaten der Jobparameter, Durchführungszeitpunkt, Dauer, Anzahl gelöschter Daten je Nachrichtentyp.

3.1.2.7 Statistische Daten

Das System stellt sicher, dass auch nach dem Löschen/archivieren von Daten weiterhin Analysen bzw. statistische Auswertungen zu der Anzahl von Erfassungs- und Ausgabenachweisen durchgeführt werden können. Aus diesem Grund wird durch einen täglichen Job die Anzahl der eingegangenen Daten pro Tag je CCP bzw. SO dokumentiert. Anhand dieser Daten lassen sich langfristige Aussagen über die Anzahl der durchgeführten Kontrollen sowie über die Entwicklung ausgegebener Berechtigungen tätigen, ohne dass sämtliche Daten vorgehalten werden müssen.

3.2 Sicherung und Wiederherstellung

Eine effiziente Sicherungs- und Wiederherstellungsstrategie ist von zentraler Bedeutung, um den Schutz von Daten und die Kontinuität des Betriebs sicherzustellen. Das System muss in der Lage sein, automatisierte Datensicherungen in regelmäßigen Abständen durchzuführen, um sicherzustellen, dass im Falle eines Ausfalls eine Wiederherstellung möglich ist.

Für das MPS, welches deutschlandweit genutzt wird, ist eine Point-In-Time-Lösung zur Datensicherung und Wiederherstellung zu nutzen. Diese Methode bietet entscheidende Vorteile gegenüber einer reinen täglichen Snapshot-Sicherung. Die Sicherung & Wiederherstellung der Daten muss dabei je Mandant möglich sein.

Eine Point-In-Time-Recovery-Lösung ermöglicht die Wiederherstellung der Datenbank zu einem beliebigen Zeitpunkt innerhalb des letzten Sicherungsintervalls. Dies minimiert den potenziellen Datenverlust auf wenige Sekunden oder Minuten, während bei einer täglichen Snapshot-Sicherung alle Transaktionen, die seit dem letzten Snapshot erfolgt sind, verloren gingen. Da das MPS kontinuierlich Daten verarbeitet, würde die Vorgehensweise „Snapshot nur einmal pro Tag“, erhebliche Lücken hinterlassen und könnte zu einem vollständigen Verlust aller Daten eines Tages führen.

Zusätzlich gewährleistet die Point-In-Time-Recovery-Lösung eine hohe Konsistenz der Transaktionsdaten, indem alle abgeschlossenen Transaktionen bis zum letzten Moment des Systemausfalls wiederhergestellt werden können. Snapshots hingegen sichern die Daten nur zu festgelegten Zeitpunkten und bieten keine Möglichkeit, inkonsistente oder unvollständige Transaktionen in der Datenbank zu rekonstruieren, was das Risiko von Inkonsistenzen erheblich erhöht. Ein weiterer Vorteil der Point-In-Time-Lösung ist die Flexibilität: Die Datenbank kann auf jeden beliebigen Zeitpunkt in der Vergangenheit zurückgesetzt werden, was besonders hilfreich ist, wenn versehentliche oder fehlerhafte Transaktionen rückgängig gemacht werden müssen.

Schließlich erhöht die Point-In-Time-Recovery mit WAL-Logging die Verfügbarkeit des Systems und beschleunigt die Wiederherstellung, da die Datenbank nicht vollständig aus einem Snapshot wiederhergestellt werden muss. Stattdessen werden die relevanten Transaktionen seit dem letzten Snapshot zügig eingespielt, was den Ausfall verkürzt und die Datenintegrität sicherstellt. Insgesamt bietet die Point-In-Time-Lösung damit eine

höhere Datensicherheit und Verfügbarkeit, was für ein zentrales Transaktionssystem von entscheidender Bedeutung ist.

Zusätzlich ist es erforderlich, automatisierte Benachrichtigungen zu implementieren, die das Support-Team und den VDV-ETS im Falle eines Sicherheitsausfalls informieren. So können sofortige Maßnahmen ergriffen werden, um das Problem zu beheben und den Verlust von Daten zu verhindern.

3.3 Export

Der Datenexport ist besonders wichtig für Analysen, die Sicherung von Geschäftsdaten oder die Integration mit anderen Systemen. Das System muss daher die Möglichkeit bieten, Daten in verschiedenen gängigen Formaten zu exportieren, darunter CSV, XML, JSON und Excel. Diese Formate erleichtern die Verarbeitung der exportierten Daten in anderen Anwendungen und ermöglichen eine einfache Weiterverarbeitung und Analyse.

Der Export von Daten muss jedoch stets durch geeignete Sicherheitsmaßnahmen geschützt werden. Dies umfasst sowohl den Schutz vor unautorisierten Zugriffen als auch die Authentifizierung der Nutzer, die den Export durchführen. In sensiblen Fällen muss zudem eine Verschlüsselung der exportierten Daten vorgesehen sein, um deren Sicherheit zu gewährleisten.

Für die Handhabung größerer Datenmengen muss das System Massenexporte unterstützen, die in einem angemessenen Zeitrahmen durchgeführt werden können. Dies ist vor allem dann von Bedeutung, wenn Daten archiviert oder in ein anderes System überführt werden müssen. Um die Nachvollziehbarkeit und Sicherheit der Exporte zu gewährleisten, müssen alle Exporte im System protokolliert werden. So ist jederzeit ersichtlich, welche Daten von wem und wann exportiert wurden.

4 Mitgeltende Dokumente

[1] Lastenheft_MPS_V0.9