

Lastenheft

Multi Product Owner System (MPS)

Dateiname:	Lastenheft_MPS_V0.9
Zuletzt geändert am:	04.05.2026 12:18
Version:	0.9
Ersteller:	Sebastian Krammer, Wilk Hoffmann, René Schmid, Dr. Fabian Ohler, Can Apak, David Brinkmann
Abnahme am:	04.05.2026

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkung
0.1	Sebastian Krammer, Wilk Hoffmann, René Schmid, Dr. Fabian Ohler, Can Apak, David Brinkmann	30.12.2025	Ersterstellung
0.9	Sebastian Krammer	04.05.2026	Bekanntmachung

Inhaltsverzeichnis

Versionsverwaltung.....	2
Abbildungsverzeichnis	7
1 Einleitung	9
1.1 Projektbeschreibung	9
1.2 Auftraggeber	10
1.3 (((etiCORE Rollenmodell.....	10
1.4 Übersicht Systemkontext.....	11
1.4.1 Multi Product Owner System (MPS).....	11
1.4.2 Weitere System (außerhalb des Projektrahmens)	12
2 Organisation	14
2.1 Projektentwicklung.....	14
2.1.1 Projektleiter	14
2.1.2 Kommunikation und Berichtswesen.....	15
2.1.3 Projektmeetings	15
2.1.4 Änderungen.....	16
2.1.5 Projektplan.....	16
2.2 Workshops zur Ausarbeitung grafischer Oberflächen.....	17
2.2.1 Mockup-Erstellung	17
2.2.2 Workshop-Durchführung	17
2.2.3 Überarbeitung und Freigabe	18
2.3 Mitwirkung des Auftraggebers	18
2.4 Abnahme	18
3 Dokumentation	19
3.1 Pflichtenheft.....	20
3.2 Nutzerhandbuch.....	20
3.3 Administrationshandbuch.....	21

3.4	Betriebshandbuch	21
3.5	Softwaredokumentation	21
3.6	Form, Aktualität und Bereitstellung	22
4	Funktionale Anforderungen	22
4.1	Deployment Variant	23
4.1.1	Ordered Action Management	23
4.1.2	Payment Methods	23
4.1.3	In/Out	24
4.2	Grundfunktionalitäten	24
4.2.1	Dashboard	24
4.2.2	Optional: Dashboard Konfiguration	28
4.2.3	Super Admin Dashboard	31
4.2.4	Fachliches Monitoring	35
4.2.5	Meldungen / Anwendungsfälle Operatoren	36
4.2.6	ION-Monitoring	45
4.3	Stammdaten	47
4.3.1	Ansicht	48
4.3.2	Erfassung und Pflege	48
4.3.3	Trennung der Mandanten	48
4.3.4	Organisationsverwaltung	49
4.3.5	EFM-Produktverwaltung	50
4.3.6	Zusätzliche Anforderungen für den nationalen Mandaten	51
4.4	Zugriff	52
4.4.1	SSO	52
4.4.2	Benutzerrechte und Benutzerrollen	52
4.4.3	Benutzer- und Mandantenverwaltung	54
4.5	Aktionsmanagement	55
4.5.1	Oberfläche: Konfiguration	55

4.5.2	Oberfläche: Aktionslistenabruf	55
4.5.3	Oberfläche: Order Inventory.....	56
4.6	Sperrwesen.....	56
4.6.1	HLS-Produktkonfiguration.....	56
4.6.2	Abholen von Hotlists.....	58
4.6.3	Bestand an Hotlist-Einträgen (Hotlist-Inventory).....	59
4.6.4	Übertragung der Hotlist-Informationen in die Bestände.....	60
4.6.5	Hotlisting-Demands (Sperranforderungen).....	61
4.6.6	Hotlisting Demand Revocations (Sperraufhebungsanforderungen).....	63
4.6.7	Auswerten der Reports über abgeholte Hotlisten	64
4.7	Register und Bestände	65
4.7.1	Allgemein	65
4.7.2	ION-Nachrichtenregister (ION-Message Registry)	66
4.7.3	Register für Applikationsstatus (Application Status Registry).....	81
4.7.4	Meldungsregister für Berechtigungen (Entitlement Notification Registry).....	83
4.7.5	Ausgaberegister (Issuance Registry).....	88
4.7.6	Register für Ausgabeabbruch von Berechtigungen.....	90
4.7.7	Kontrolldatenregister (Inspection Registry).....	91
4.7.8	Nutzungsregister (Recording Registry).....	93
4.7.9	Product Owner Token.....	95
4.7.10	Zustandsbehaftete Bestände	96
4.8	Logbücher.....	109
4.8.1	Joblogbuch.....	109
4.8.2	Änderungslogbuch.....	109
4.9	Nationaler Mandant.....	110
4.9.1	Funktionsprüfung	110
4.9.2	Regionale Filterbarkeit von Aktionslisten im nationalen Mandanten.....	113
4.9.3	MPS – Zentrale	113

4.9.4	Optional: Zugriff des nationalen Mandanten auf regionale POs für das D-TICKET ..	114
4.9.5	Optional: Integration von D-Tickets im UIC-FCB Format	115
4.10	Zusatzinformationen zu spezifizierten Warnungen und Fehlern.....	115
4.10.1	Events in Nachrichten aus dem ION-Nachrichtenregister	116
4.10.2	Warnungen in den verschiedenen Entitlement-Notification-Registern.....	117
4.10.3	Events beim Monitoring.....	117
4.10.4	Warnungen im Bestand	117
4.10.5	Abruf der Event-Information und Lösungsvorschlag	117
4.11	Negativnachweise	118
4.11.1	Senden der Meldungen an das MPS	118
4.11.2	Entgegennahme der Meldungen.....	119
4.11.3	Weiterleiten der Meldungen.....	119
4.11.4	Register für Negativnachweise.....	119
4.11.5	Monitoring-Prüfungen.....	120
4.12	Applikations-Monitoring	122
4.12.1	Voraussetzungen	122
4.12.2	Monitoring-Prüfungen.....	122
4.12.3	Handhabung verlorener Medien.....	123
4.13	Auskunft über Berechtigungen / Defekte Medien	123
4.14	Mandantenübergreifende Produktanerkennung	124
4.15	Online-ALISE.....	125
4.16	JIRA Integration	125
4.17	ION An-/Abmeldung	126
4.18	Sperrlisten für Dritte.....	126
4.19	Optional: Anbindung von Online-Ticketspeichern.....	127
5	Grafische Oberflächen.....	128
5.1	Allgemeine Gestaltungsprinzipien.....	128
5.2	Sprache	128

5.3	Typografie.....	128
5.4	Farben und visuelle Gestaltung	129
5.5	Navigation und Seitenstruktur	129
5.6	Interaktionselemente.....	129
5.7	Tabellen und Listen.....	129
5.8	Hinweise, Meldungen und Statusanzeigen	130
5.9	Avatare und benutzerbezogene Darstellungen	130
5.10	Referenz.....	130
6	Schnittstellen.....	130
7	Datenmodelle.....	131
7.1	Übersicht	132
7.2	Benötigte Stammdaten.....	133
7.2.1	Organisationsverwaltung	133
7.2.2	Produktverwaltung	133
7.3	Register	134
7.4	Bestände (Inventories)	135
8	Mandantenfähigkeit.....	136
8.1	Begriffsdefinition Mandant	136
8.2	Grundanforderungen an die Mandantenfähigkeit	136
9	Mitgeltende Dokumente.....	137

Abbildungsverzeichnis

Abbildung 1: Statusübergänge einer empfangenen synchronen Anfrage	68
Abbildung 2: Statusübergänge einer gesendeten synchronen Rückmeldung.....	69
Abbildung 3: Statusübergänge einer gesendeten asynchronen Anfrage.....	69
Abbildung 4: Statusübergänge einer empfangenen asynchronen Rückmeldung.....	70
Abbildung 5: Statusübergänge der asynchronen Anfrage nach Verarbeitung und Zuordnung der Rückmeldung.....	71

Abbildung 6: Statusübergänge einer gesendeten synchronen Anfrage	71
Abbildung 7: Zuordnung einer synchronen Rückmeldung.....	72
Abbildung 8: Statusübergänge einer empfangenen asynchronen Anfrage.....	72
Abbildung 9: Statusübergänge einer gesendeten asynchronen Rückmeldung.....	73
Abbildung 10: Meldungen für Applikationen	81
Abbildung 11: Mögliche eingehende Notifications für Berechtigungen.....	85
Abbildung 12: Mögliche eingehende Notifications für statische Berechtigungen	86
Abbildung 13: Mögliche Zustände von Berechtigungen im Bestand.....	99
Abbildung 14: Mögliche Zustände einer Applikation im Bestand.....	104
Abbildung 15: Mögliche Zustände eines SAMs im Bestand.....	107
Abbildung 16: Datenmodell für Register, Bestände und HLS Konfiguration	132
Abbildung 17: Stammdaten Organisationen und Produkte.....	133
Abbildung 18: Register im MPS.....	134
Abbildung 19: Bestände für Berechtigungen, Applikationen, SAMs und Hotlist-Einträgen	135

1 Einleitung

1.1 Projektbeschreibung

Das vorliegende Lastenheft beschreibt die Anforderungen an die Entwicklung und Bereitstellung eines mandantenfähigen Product Owner-Systems (PO-System) genannt Multi Product Owner System (MPS), im Kontext des elektronischen Fahrgeldmanagements (EFM) nach dem bundesweit etablierten Standard ((etiCORE. Ziel des Projektes ist die Realisierung einer zentralen Plattform, die die fachlichen und technischen Aufgaben des Produktverantwortlichen für mehrere voneinander unabhängige Verkehrsverbünde bzw. Tarifgemeinschaften unterstützt.

In der aktuellen Systemlandschaft betreiben Produktverantwortliche in der Regel jeweils eigene PO-Systeme. Mit der Umstellung bestehender EFM-Systeme von der bisherigen VDV-Kernapplikation auf den Standard ((etiCORE ergibt sich die Notwendigkeit, diese Systeme anzupassen oder durch neue Lösungen zu ersetzen. Vor diesem Hintergrund wurde seitens mehrerer Marktteilnehmer der Bedarf nach einer zentral bereitgestellten, mandantenfähigen Lösung geäußert, die von unterschiedlichen Produktverantwortlichen als PO-System genutzt werden kann.

Darüber hinaus besteht ein interner Bedarf der VDV ETS an einem PO-System zur Ausübung einiger Aufgaben eines Produktverantwortlichen im Zusammenhang mit bundesweiten Produkten wie dem Deutschlandticket. Vor diesem Hintergrund wurde die Entscheidung getroffen, ein mandantenfähiges PO-System als Branchenlösung zu entwickeln, das sowohl für interne Zwecke als auch durch externe Kunden eingesetzt werden kann.

Die Organisation und der Betrieb interoperabler EFM-Systeme basieren auf dem ((etiCORE Standard, der die Verantwortlichkeiten der beteiligten Akteure sowie deren Zusammenarbeit definiert. Ein Verkehrsverbund bzw. eine Tarifgemeinschaft nimmt hierbei die Rolle des Product Owner ein. Diese Rolle wird technisch durch ein PO-System unterstützt, das als Hintergrundsystemkomponente innerhalb des ((eTicket Deutschland fungiert. Das MPS dient als solches PO-System und setzt dabei unter anderem die Use Cases eines PO-Systems nach ((etiCORE Spezifikation [4] um.

Das zu realisierende PO-System ist als mandantenfähige Plattform konzipiert, auf der mehrere Product Owner-Mandanten parallel und voneinander unabhängig betrieben werden können. Jeder Mandant repräsentiert dabei einen eigenständigen Product Owner (in der

Regel ein Verkehrsverbund bzw. Verkehrsunternehmen) mit eigener fachlicher Verantwortung mit eigenen Transaktions- und Auswertungsdaten.

Zentrale Aufgabe des PO-Systems ist es, die Nachrichten der Teilnehmer entgegenzunehmen, zu verwalten und im Rahmen des Sicherheits- und Konsistenzmanagements zu prüfen. Hierzu zählt insbesondere die Sicherstellung der Vollständigkeit, Integrität und Nachvollziehbarkeit der ausgetauschten Daten.

Gegenstand dieses Lastenheftes ist die Beschreibung der funktionalen und nicht-funktionalen Anforderungen an das PO-System. Dazu zählen unter anderem die mandantenbezogene Konfiguration, die Verarbeitung und Analyse von Nachrichten und die Integration in die bestehende Systemlandschaft. Die konkreten Anforderungen sind in den folgenden Kapiteln strukturiert und detailliert beschrieben. Anforderungen an den Plattformbetrieb befinden sich in einem separaten Dokument Qualitätsanforderungen 9.

Dieses Lastenheft dient als verbindliche Grundlage für die Planung, Umsetzung und Abnahme des MPS und bildet die Basis für die weitere Projektumsetzung.

1.2 Auftraggeber

Initiator des Projekts ist die Geschäftsführung der VDV ETS auf Anforderung aus der Teilnehmerschaft des ((eTicket Deutschland. Die Ausschreibung des Systems findet auf Basis von Geschäftsbesorgungsverträgen statt, die mit den späteren Mandanten des MPS geschlossen worden sind. Die VDV ETS handelt in dieser Ausschreibung demnach im Auftrag der Vertragspartner und stimmt dieses Dokument mit den Vertragsparteien vor Beginn des Teilnahmewettbewerbs ab.

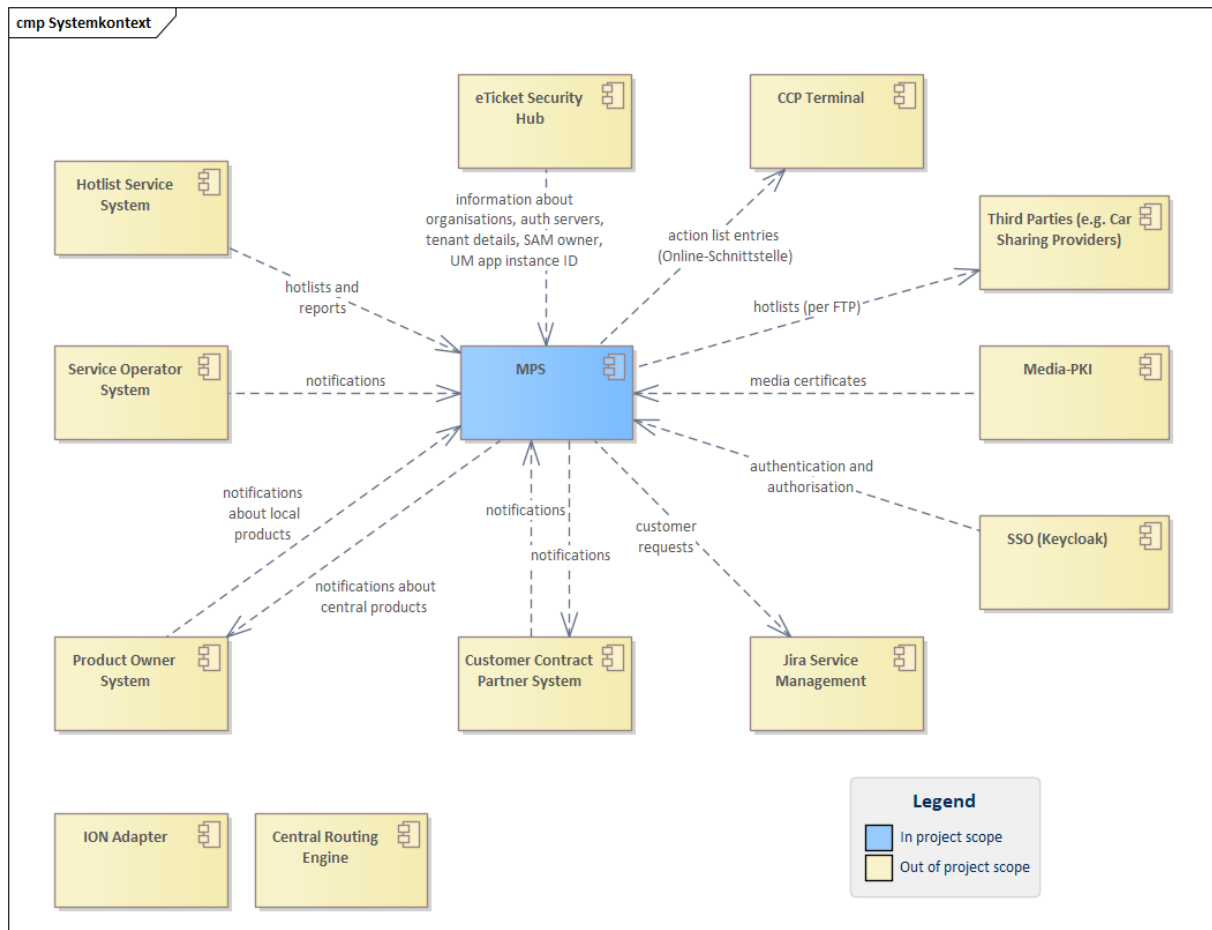
1.3 ((etiCORE Rollenmodell

Die in diesem Lastenheft verwendeten ((etiCORE Rollenbezeichnungen, insbesondere der Product Owner (PO), beziehen sich auf das im Standard ((etiCORE definierte Rollenmodell (siehe [3] oder [Role Model](#)). Jeder PO betreibt bzw. lässt entsprechende Systemkomponenten betreiben, insbesondere das PO-System.

Die im System verwendeten technischen Rollen (Super-Administrator, Administrator, Nutzer) sind unabhängig von den fachlichen Rollen gemäß etiCORE-Spezifikation (z. B. Product Owner, Customer Contract Partner, Service Operator). Diese fachlichen Rollen und deren Beziehungen sind beschrieben und sind nicht Bestandteil des Benutzerrechte- und Benutzernrollenmodells.

1.4 Übersicht Systemkontext

Dieser Abschnitt stellt die Systeme vor, die an den Geschäftsprozessen beteiligt sind, die das zu entwickelnde System unterstützen muss. Dazu gehören sowohl das System im Projektrahmen (das entwickelt werden soll) als auch die Systeme im Projektkontext (mit denen Interaktionen erforderlich sind).



1.4.1 Multi Product Owner System (MPS)

Das Multi Product Owner System (MPS) ist ein System zur Unterstützung der *Product Owner* Rolle im Kontext des elektronischen Fahrgastmanagements nach ((etiCORE-Standard. Es richtet sich sowohl an Verbünde, die als *Product Owner* für eigene Tarife auftreten, als auch an interne Nutzer, die das System zur technischen Wahrnehmung der *Product Owner* Rolle für das Deutschland-Ticket betreiben.

Das MPS ist als *Product Owner*-System gemäß der ((etiCORE-Spezifikation ausgelegt. Die zentrale Aufgabe des MPS ist das fachliche Monitoring zur Betrugsprävention. Hierzu führt

das System ein automatisiertes, regelbasiertes Monitoring produktbezogener Daten durch. Erkannte Auffälligkeiten werden als Meldungen zur weiteren fachlichen Bearbeitung bereitgestellt.

Darüber hinaus ermöglicht das MPS den Zugriff auf alle relevanten fachlichen Informationen aus Sicht eines *Product Owners*. Dazu zählen insbesondere Informationen zu ausgegebenen Fahrberechtigungen und Tickets, deren Status, Interaktionen mit angebundenen Drittsystemen sowie Nachweise über Kontrollen und Prüfungen.

Neben den Monitoring-Funktionen stellt das MPS Funktionen zur operativen Umsetzung fachlicher Maßnahmen bereit. Dazu gehören die Weiterleitung relevanter Informationen an beteiligte *Customer Contract Partner* und *Service Operator* sowie die Bereitstellung von Aktionsaufträgen, beispielsweise zur Entsperrung oder Neuausgabe von Fahrberechtigungen, für (*executing*) *Customer Contract Partner* bzw. deren ausführende Systeme.

1.4.2 Weitere System (außerhalb des Projektrahmens)

Dieser Abschnitt stellt die Systeme vor, die außerhalb des Projektrahmens liegen, aber innerhalb des Systemkontexts.

1.4.2.1 Customer Contract Partner System

Siehe Customer Contract Partner Reference System Specification “etiCORE SPEC-CCP-RS_v3.0.0-rc.6 en” [7].

1.4.2.2 Service Operator System

Siehe Service Operator Reference System Specification “etiCORE SPEC-SO-RS_v3.0.0-rc.6 en” [8].

1.4.2.3 Product Owner System

Siehe Product Owner Reference System Specification “etiCORE SPEC-PO-RS_v3.0.0-rc.6 en” [4].

1.4.2.4 eTicket Security Hub

Siehe ((eTicket Security Hub Specification “etiCORE SPEC-ESH_v3.0.0-rc.6 en” [9].

1.4.2.5 Hotlist Service System

Siehe Hotlist Service System Specification “etiCORE SPEC-Hotlist_v3.0.0-rc.6 en” [5].

1.4.2.6 SSO (Keycloak)

Das Single-Sign-On-System (SSO) bietet Benutzerauthentifizierung und Autorisierung für Systeme von VDV ETS im Zusammenhang mit ((eTicket Deutschland. Zu seinen Benutzern zählen ETS-Mitarbeiter sowie Personen aus dem Bereich des öffentlichen Nahverkehrs. Das Single Sign-On-System authentifiziert seine Benutzer anhand mehrerer Faktoren, wenn dies für die Geschäftsprozesse erforderlich ist. Zu diesem Zweck ermöglicht es seinen Benutzern, ihre Faktoren zu verwalten. Aktuell wird hierfür Keycloak eingesetzt.

1.4.2.7 Third Parties (e.g. Car Sharing Providers)

Third Parties sind Vertragspartner einzelner MPS-Mandanten, die nicht über einen Teilnahmevertrag an ((eTicket Deutschland verfügen. Dies können beispielsweise Carsharing Anbieter sein.

1.4.2.8 CCP Terminal

Siehe Customer Contract Partner Reference Terminal Specification “etiCORE SPEC-CCP-RT_v3.0.0-rc.6 en” [6].

1.4.2.9 Jira Service Management

Atlassian Jira Service Management, ein Helpdesk Ticket System.

1.4.2.10 Media PKI

2GSI PKI für card verifiable certificates. Siehe auch ((etiCORE Media PKI Specification “etiCORE SPEC-Media-PKI_V1.0.0” [11].

1.4.2.11 ION Adapter

Der ION-Adapter erleichtert die Anbindung an das Interoperable Network (ION, siehe ION-Specification “etiCORE SPEC-ION_v3.0.0-rc.6 en” [2]).

1.4.2.12 Central Routing Engine

Siehe Central Routing Engine Specification “etiCORE SPEC-CRE_v3.0.0-rc.6 en” [10].

2 Organisation

2.1 Projektabwicklung

Ziel der Projektabwicklung ist eine transparente, strukturierte und effiziente Zusammenarbeit zwischen Auftraggeber und Auftragnehmer zur erfolgreichen Umsetzung des beschriebenen IT-Systems.

Die konkrete Projektmethodik wird nicht vorgegeben. Unabhängig vom gewählten Vorgehen sind eine enge Abstimmung, eine frühzeitige Kommunikation von Risiken sowie eine nachvollziehbare Dokumentation sicherzustellen.

2.1.1 Projektleiter

Auftraggeber und Auftragnehmer benennen jeweils einen verantwortlichen Projektleiter sowie entsprechende Stellvertreter. Diese fungieren als zentrale Ansprechpartner und sind für die Koordination, Steuerung und Kommunikation innerhalb des Projekts verantwortlich.

Ist ein Projektleiter auf absehbar unangemessen lange Zeit verhindert oder scheidet es aus dem Unternehmen der jeweiligen Partei aus, ist rechtzeitig eine Ersatzperson zu benennen

2.1.1.1 Projektleiter Auftraggeber

Der Projektleiter auf Seiten des Auftraggebers ist verantwortlich für:

- die fachliche Steuerung des Projekts,
- die Abstimmung und Priorisierung fachlicher Anforderungen,
- die Bereitstellung fachlicher Informationen und Entscheidungen,
- die Abnahme von Projektergebnissen gemäß den vereinbarten Abnahmekriterien,
- die Eskalation von Problemen innerhalb der Organisation des Auftraggebers.

2.1.1.2 Projektleiter Auftragnehmer

Der Projektleiter auf Seiten des Auftragnehmers ist verantwortlich für:

- die operative Planung und Steuerung der Projektumsetzung,
- die Koordination der eingesetzten Projektressourcen,
- die termingerechte Erbringung der vereinbarten Leistungen,
- die regelmäßige Berichterstattung über den Projektfortschritt,
- das frühzeitige Anzeigen von Risiken, Verzögerungen oder Abweichungen.

Der vom Auftragnehmer bestimmte Projektleiter ist Ansprechpartner für die Kommunikation zwischen Auftraggeber und Auftragnehmer. Die direkte Kommunikation mit Entwicklern und Unterauftragnehmern pflegt der Auftraggeber nur in von ihm gebilligten Ausnahmefällen und unter Information des Projektleiters des Auftragnehmers.

2.1.2 Kommunikation und Berichtswesen

Der Auftragnehmer ist verpflichtet, den Auftraggeber mindestens alle 14 Tage über den aktuellen Stand des Projekts zu informieren. Die Berichterstattung hat strukturiert und nachvollziehbar zu erfolgen und umfasst insbesondere:

- den Umsetzungsstand der vereinbarten Leistungen,
- erreichte und anstehende Meilensteine,
- offene Punkte und identifizierte Risiken,
- Abweichungen von Planung, Aufwand oder Zeitplan.

Die Berichte sind in geeigneter Form zu dokumentieren und dem Auftraggeber zur Verfügung zu stellen.

Bei absehbaren oder eingetretenen Verzögerungen, wesentlichen Risiken oder sonstigen kritischen Abweichungen ist der Projektleiter des Auftraggebers unverzüglich zu informieren. Der Auftragnehmer hat in diesem Fall geeignete Maßnahmen zur Problemlösung und zur Minimierung der Auswirkungen vorzuschlagen.

Der Auftraggeber erhält jederzeit eine angemessene Transparenz über den Projektstand und die erarbeiteten Ergebnisse.

2.1.3 Projektmeetings

Zur Steuerung des Projekts wird mindestens alle 14 Tage ein Projektmeeting, wahlweise in Präsenz oder Online-Terminen, zwischen Auftraggeber und Auftragnehmer durchgeführt. Teilnehmerkreis und Form der Meetings werden zu Projektbeginn gemeinsam festgelegt. An den Projektgesprächen nehmen mindestens die jeweiligen Projektleiter des Auftraggebers und des Auftragnehmers teil.

Projektmeetings dienen insbesondere:

- der Abstimmung über den Projektfortschritt,
- der Klärung offener Punkte,
- der Identifikation und Bewertung von Risiken,
- der Abstimmung der nächsten Arbeitsschritte.

Der Auftragnehmer legt Entwürfe der Ergebnisprotokolle möglichst schnell, spätestens aber sieben Tage nach dem entsprechenden Projektgespräch vor. Protokolle werden im jeweils nächsten Projektgespräch, eventuell nach Korrektur, genehmigt.

Der Auftraggeber kann darüber hinaus jederzeit nach billigem Ermessen mit angemessener Frist Projektbesprechungen einberufen und bei Bedarf weitere Gesprächsteilnehmer zu den Projektbesprechungen einladen.

2.1.4 Änderungen

Änderungen an Anforderungen, Umfang, Prioritäten oder Zusammenarbeit sind zwischen Auftraggeber und Auftragnehmer abzustimmen und nachvollziehbar zu dokumentieren.

2.1.5 Projektplan

Es sind folgende Meilensteine bei Auftragsvergabe bis 07.08.2026 zu berücksichtigen

- Bis 30.09.2026 Erstellung Pflichtenheft
- Bis 01.10.2027 Bereitstellung zur Abnahme MVP in der Staging Umgebung
- Ab 15.11.2027 Pilotbetrieb MVP
- Ab 01.01.2028 Start Produktivbetrieb MVP
- Bis 15.03.2028 Bereitstellung zur Abnahme Phase 2 in der Staging Umgebung
- Ab 01.05.2028 Produktivbetrieb Phase 2
- Bis 01.08.2028 Finale Abnahme nach 3-monatiger Probephase im Produktivbetrieb

Die Entwicklung soll in zwei Tranchen (MVP und Phase 2) erfolgen. Ziel ist es den Anwendern möglichst früh den Zugang zu einem brauchbaren System zu ermöglichen. Die Zuordnung der einzelnen Anforderungen zu den jeweiligen Phasen befindet sich in [20] Anlage_2_Erklärung_über_technische_und_funktionale_Eigenschaften.

Der Pilotbetrieb muss Anwendertests und das Testen von Interaktionen mit Drittsystemen wie SO und CCP Systemen ermöglichen.

Der Auftragnehmer hat zu Projektbeginn einen detaillierten Projektplan zu erstellen und dem Auftraggeber zur Abstimmung vorzulegen. Die konkrete Ausgestaltung des Projektplans bleibt dem Auftragnehmer überlassen und richtet sich nach dem gewählten Vorgehensmodell.

Der Projektplan sowie die definierten Meilensteine sind zwischen Auftraggeber und Auftragnehmer abzustimmen und fortlaufend zu pflegen. Änderungen am Projektplan oder

an den Meilensteinen sind nur einvernehmlich erlaubt, transparent darzustellen und zu dokumentieren.

Der Auftragnehmer berichtet im Rahmen des regelmäßigen Berichtswesens über den Status der Meilensteine sowie über Abweichungen von der Planung.

2.2 Workshops zur Ausarbeitung grafischer Oberflächen

Sämtliche grafischen Oberflächen des Systems sind vor Beginn der Entwicklung durch den Auftraggeber freizugeben. Zu diesem Zweck führt der Auftragnehmer gemeinsam mit den zukünftigen Anwendern Workshops durch, in denen Benutzerführung und Gestaltung aller Oberflächen erarbeitet und abgestimmt werden.

2.2.1 Mockup-Erstellung

Der Auftragnehmer erstellt für sämtliche grafischen Oberflächen des Systems Mockups. Die Erstellung erfolgt in zwei Stufen:

Stufe 1 – Low-Fidelity: Strukturelle Darstellung der Oberflächen als Wireframes inkl. Anordnung von Bedienelementen, Navigationsstruktur und konditionaler Benutzerführung.

Stufe 2 – High-Fidelity: Ausgearbeitete, realitätsnahe Darstellung inkl. finaler Beschriftung von Buttons und Steuerelementen, visueller Gestaltung sowie vollständiger Abbildung aller Zustände und Verzweigungen der Benutzerführung.

Die Mockups bilden die verbindliche Grundlage für die Entwicklung. Eine Entwicklung von Oberflächen ohne vorherige schriftliche Freigabe durch den Auftraggeber ist nicht zulässig.

2.2.2 Workshop-Durchführung

Der Auftragnehmer plant und moderiert die Workshops. Für jeden Workshop gelten folgende Anforderungen:

Agenda, Zeitplan und Ziele sind den Teilnehmern mindestens 3 Werktage vor dem Workshop schriftlich mitzuteilen. Im Workshop präsentiert der Auftragnehmer die Mockups und stellt sicher, dass die anwesenden Anwender Kommentare und Optimierungsvorschläge einbringen können. Der Auftragnehmer erstellt zu jedem Workshop ein Protokoll und übermittelt dieses spätestens 5 Werktage nach dem

Workshop an den Auftraggeber. Das Protokoll enthält mindestens: alle getroffenen Entscheidungen sowie deren Begründungen, dokumentierte Anmerkungen der Anwender und vereinbarte nächste Schritte.

2.2.3 Überarbeitung und Freigabe

Nach jedem Workshop überarbeitet der Auftragnehmer die Mockups entsprechend der dokumentierten Anmerkungen. Der Freigabeprozess läuft wie folgt:

1. Der Auftragnehmer reicht die überarbeiteten Mockups beim Auftraggeber zur Prüfung ein.
2. Der Auftraggeber prüft die Mockups, ggf. unter Einbeziehung der Anwender, und erteilt entweder die Freigabe oder gibt konkrete Änderungsanforderungen zurück.
3. Schritt 1 und 2 werden wiederholt, bis die Freigabe erteilt wird.

Die Freigabe erfolgt schriftlich. In der Regel wird von maximal zwei Überarbeitungsrounds pro Oberfläche ausgegangen.

2.3 Mitwirkung des Auftraggebers

Der Auftraggeber unterstützt den Auftragnehmer bei der Durchführung des Projekts insbesondere durch:

- die zeitnahe Beantwortung fachlicher Fragen,
- die Bereitstellung notwendiger fachlicher Informationen,
- die Benennung fachlicher Ansprechpartner,
- die Mitwirkung bei Abstimmungen, Workshops und Reviews.

Der Auftraggeber stellt sicher, dass erforderliche Entscheidungen, Rückmeldungen und Zusatzen innerhalb angemessener Fristen erfolgen. Verzögerungen, die durch fehlende oder verspätete Mitwirkung des Auftraggebers entstehen, sind dem Auftragnehmer nicht anzulasten.

2.4 Abnahme

Der Auftragnehmer erbringt die vereinbarten Leistungen gemäß den Anforderungen dieses Lastenhefts.

Die Abnahme der Leistungen erfolgt durch den Auftraggeber auf Basis der vereinbarten Anforderungen sowie der jeweils definierten Abnahmekriterien. Die Abnahme kann sich

sowohl auf einzelne Liefergegenstände als auch auf Projektphasen oder Meilensteine beziehen.

Die im Projekt vorgesehenen Meilensteine und zugehörigen Liefergegenstände werden zu Projektbeginn oder im weiteren Projektverlauf einvernehmlich konkretisiert und dokumentiert.

Der Auftragnehmer hat dem Auftraggeber alle zur Abnahme erforderlichen Unterlagen, Nachweise und Ergebnisse zur Verfügung zu stellen.

Der Auftragnehmer hat vor der Abnahme des Systems durch den Auftraggeber eigenverantwortlich die Funktionalität der gelieferten Software anhand der im Pflichtenheft beschriebenen Funktionstests zu überprüfen und das Ergebnis dem Auftraggeber vor der Abnahme des Systems schriftlich vorzulegen.

Nach Bereitstellung eines abnahmefähigen Liefergegenstands prüft der Auftraggeber diesen innerhalb eines angemessenen Zeitraums. Das Ergebnis der Abnahmeprüfung ist zu dokumentieren.

Werden im Rahmen der Abnahme Mängel festgestellt, sind diese vom Auftragnehmer innerhalb einer angemessenen Frist zu beheben. Nach erfolgreicher Mängelbeseitigung erfolgt eine erneute Abnahmeprüfung.

Eine (Teil-)Abnahme gilt erst als erfolgt, wenn sie ausdrücklich durch den Auftraggeber erklärt oder dokumentiert wurde. Eine stillschweigende Abnahme ist ausgeschlossen.

Die weiteren Details zur Abnahme sind in den Qualitätsanforderungen "MPS_Qualitätsanforderungen_VO.9.pdf" [1] definiert.

3 Dokumentation

Der Auftragnehmer ist verpflichtet, eine vollständige, verständliche und zielgruppengerechte Dokumentation der entwickelten Software bereitzustellen.

Die Softwaredokumentation dient der Unterstützung der Nutzer, Administratoren und des Betriebs sowie der Sicherstellung eines nachhaltigen, sicheren und wartbaren Systembetriebs.

Die Dokumentation ist in einer Form zu erstellen, die auch für fachfremde Dritte nachvollziehbar ist, und ist spätestens zur Abnahme des Systems bereitzustellen.

3.1 Pflichtenheft

Der Auftragnehmer erstellt eigenverantwortlich in Abstimmung mit den Auftraggebern ein Pflichtenheft, in dem Funktionen, Schnittstellen, Voraussetzungen für den Betrieb und die Einführung im Detail beschrieben sind.

Die Erstellung des Pflichtenheftes ist in die Phasen Dokumentenerstellung und Dokumentenreview einzuteilen.

Neben dem funktionalen Teil beschreibt das Pflichtenheft mindestens:

- Die Softwarearchitektur
- Das Datenmodells
- Eingesetzte Technologien
- Den Betrieb
- Testfälle für die Durchführung der diversen Systemtests im Rahmen des Freigabe- und Abnahmeprozesses
- Freigabeprozesse und den Freigabeformularen
- Einen Detailprojektplan für den weiteren Projektverlauf

3.2 Nutzerhandbuch

Der Auftragnehmer stellt eine Nutzerdokumentation in deutscher Sprache zur Verfügung, die sich an die fachlichen Endnutzer des Systems richtet.

Die Nutzerdokumentation beschreibt insbesondere:

- Zweck und grundlegende Funktionsweise des Systems,
- die Bedienung der Benutzeroberfläche,
- typische Anwendungsfälle und Abläufe,
- Eingaben, Ausgaben und deren Bedeutung,
- Hinweise zu Fehlern und deren Behebung aus Nutzersicht.

Die Nutzerdokumentation ist verständlich, strukturiert und praxisnah zu gestalten. Das Nutzerhandbuch kann in Teilen oder gänzlich über Infotexte und Hilfen innerhalb der Software abgebildet werden.

3.3 Administrationshandbuch

Der Auftragnehmer stellt eine Administrationsdokumentation in deutscher Sprache für Administratoren und Super-Administratoren bereit.

Die Administrationsdokumentation beschreibt insbesondere:

- Benutzer-, Rollen- und Rechteverwaltung,
- Mandantenverwaltung (sofern relevant),
- Mandantenspezifische Konfiguration,
- typische administrative Abläufe und Wartungstätigkeiten.

Die Administrationsdokumentation muss eine eigenständige Verwaltung und Konfiguration des Systems durch den Auftraggeber ermöglichen.

Die Dokumentation für Super-Administratoren muss den fachlichen Betrieb der Software beschreiben und ermöglichen.

3.4 Betriebshandbuch

Der Auftragnehmer stellt eine Betriebsdokumentation in Form eines Betriebshandbuchs in deutscher Sprache bereit. Das Betriebshandbuch richtet sich an den technischen Betrieb und beschreibt insbesondere:

- Systemarchitektur und Komponenten,
- Voraussetzungen für Installation und Betrieb,
- Deployment-, Update- und Rollback-Prozesse,
- Backup- und Restore-Verfahren,
- Monitoring, Logging und Fehleranalyse,
- Anforderungen an Verfügbarkeit, Sicherheit und Performance,
- Inbetriebnahme bzw. Außerbetriebnahme,
- Vorgehen bei Störungen und Notfällen.

Das Betriebshandbuch muss auch Dritten einen sicheren und stabilen Betrieb des Systems ermöglichen.

3.5 Softwaredokumentation

Der Auftragnehmer stellt eine vollständige, strukturierte und verständliche Dokumentation der Softwarelösung bereit. Diese muss alle für das Verständnis, die Konfiguration und die

Weiterentwicklung der Lösung erforderlichen Informationen enthalten und sowohl fachliche als auch technische Zielgruppen adressieren.

Die Dokumentation umfasst insbesondere:

- Beschreibung der Systemarchitektur, Komponenten und zentralen Designprinzipien
- Darstellung der Datenmodelle und Datenflüsse
- Vollständige Beschreibung aller relevanten Schnittstellen (inkl. Formate, Protokolle und Nutzung)
- Übersicht über Konfigurationsmöglichkeiten und Systemparameter
- Beschreibung der fachlichen Funktionen und Abläufe
- Technische Grundlagen der Lösung (z. B. eingesetzte Technologien, Frameworks, Abhängigkeiten)
- Hinweise zur strukturierten Weiterentwicklung (z. B. Build- und Entwicklungsprozesse)

Abschließend gilt:

Die Dokumentation muss so gestaltet sein, dass Dritte sich ohne zusätzliche Erläuterungen in die Lösung einarbeiten können.

3.6 Form, Aktualität und Bereitstellung

Jegliche Dokumentation ist in geeigneter elektronischer Form bereitzustellen und aktuell zu halten.

Änderungen an der Software, die Auswirkungen auf Bedienung, Administration oder Betrieb haben, sind in der Dokumentation nachvollziehbar zu berücksichtigen.

Form, Struktur und Ablageort der Softwaredokumentation sind zwischen Auftraggeber und Auftragnehmer abzustimmen.

4 Funktionale Anforderungen

Die nachfolgenden Kapitel beschreiben die funktionalen Anforderungen, die das ausgeschriebene System umsetzen muss. Die mit „Optional:“ in der Überschrift gekennzeichneten Kapitel, sind durch den Bieter zu bepreisen. Die mögliche Umsetzung dieser Optionen wird erst zur Projektlaufzeit entschieden und eingeplant.

4.1 Deployment Variant

In Anlehnung an die Ausbaustufen der VDV-KA, hat man sog. *Deployment Variants* in ((etiCORE definiert, welche die Anwendungsfälle über mehrere Rollen und Systeme hinweg in Themenbereiche zusammenfasst. Die *Functionality Bundles* nehmen diese Bündelung auf Basis einer speziellen Funktionalität hin vor.

Das MPS basiert im Kern auf der Spezifikation des ((etiCORE Standards für die Rolle des Product Owners. Das System muss alle Anwendungsfälle der *Deployment Variant D-Ticket full* vollständig umsetzen. Dieses Lastenheft verwendet den, zum Zeitpunkt der Erstellung aktuellen, Releasekandidaten des ((etiCORE Modells, siehe Customer Contract Partner Reference System Specification “etiCORE SPEC-CCP-RS_v3.0.0-rc.6 en” [12]. Das System setzt alle verpflichtenden Anwendungsfälle der *Deployment Variant* in der Ausprägung der *D-Ticket full - PO* (siehe im Modell: <https://modell.eticket-deutschland.de/3.0.0-rc.6/EA/EARoot/EA2/EA2/EA4/EA1/EA1164.html>) vollständig konform um.

Dieses Dokument enthält Verweise auf die jeweils gültige Spezifikation.

4.1.1 Ordered Action Management

Neben den verpflichtenden Anwendungsfällen der *Deployment Variant D-Ticket full*, setzt das System die Anwendungsfälle des *Ordered Action Management Bundle PO-System* aus der Referenzspezifikation Product Owner Reference System Specification “etiCORE SPEC-PO-RS_v3.0.0-rc.6 en”[4] vollständig um.

4.1.2 Payment Methods

Das System muss die Anwendungsfälle der folgenden *Functionality Bundles* aus der Referenzspezifikation Product Owner Reference System Specification “etiCORE SPEC-PO-RS_v3.0.0-rc.6 en”[4] umsetzen:

- *Account-Based Payment Basic Bundle PO-System*
- *Stored-Value Payment Basic Bundle PO-System*
- *Sale Electronic Ticket via Account-Based Payment Bundle PO-System*
- *Sale Electronic Ticket via Stored-Value Payment Bundle PO-System*

4.1.3 In/Out

Das System muss die Anwendungsfälle des *Functionality Bundles: IN-OUT Bundle PO-System* aus der Referenzspezifikation Product Owner Reference System Specification “etiCORE SPEC-PO-RS_v3.0.0-rc.6 en”[4] umsetzen.

4.2 Grundfunktionalitäten

4.2.1 Dashboard

4.2.1.1 Zielsetzung und Zweck

Das Dashboard ist die Startseite der Web-Applikation und stellt eine zentrale Übersicht über die wesentlichen Kennzahlen im PO-System bereit. Es dient der operativen Überwachung des Systems sowie der schnellen Identifikation von Auffälligkeiten und Handlungsbedarfen.

Das Dashboard unterstützt die Nutzer bei der Analyse der Integration mit Drittsystemen wie CRE, CCP- und SO-Systemen und zeigt die wesentlichen Ergebnisse des Monitorings für eine effiziente Abarbeitung von Vorfällen. Es ermöglicht den direkten Einstieg in weiterführende Fachansichten des Systems für eine detailliertere Analyse.

4.2.1.2 Allgemeine Anforderungen

Das Dashboard muss nach erfolgreicher Anmeldung als erste Ansicht der Web-Applikation angezeigt werden.

Die Darstellung der Inhalte erfolgt in mehreren klar abgegrenzten Kacheln.

Alle wesentlichen Informationen müssen ohne Wechsel der Seite erfassbar sein.

Die angezeigten Daten müssen automatisch und nahe Echtzeit aktualisiert werden.

Die Aktualisierung erfolgt ohne manuelle Aktion des Nutzers.

Das Dashboard ist als reine Übersichts- und Navigationsoberfläche auszugestalten. Fachliche Bearbeitungen erfolgen ausschließlich in den jeweiligen Detailansichten der Applikation.

Alle im Dashboard dargestellten Kennzahlen, Diagramme und Listen müssen interaktiv ausgeführt sein.

Durch Auswahl einer Kachel oder eines dargestellten Wertes muss eine direkte Navigation in die jeweils zugehörige Fachansicht erfolgen.

Die Zielansicht muss dabei automatisch mit passenden Filterkriterien vorbelegt werden, sodass ausschließlich die dem ausgewählten Dashboard-Inhalt entsprechenden Datensätze angezeigt werden.

Das Dashboard muss eine zusammenfassende Übersicht über Monitoring, Statuslisten, Meldungen und Anbindung an das ION bereitstellen.

Die Darstellung erfolgt aggregiert und dient der schnellen Einschätzung des Systemzustands.

Farb- und Symbolik müssen konsistent und fachlich verständlich eingesetzt werden.

4.2.1.3 ION-Nachrichten

Das Dashboard muss ein Diagramm zur Darstellung des zeitlichen Verlaufs von ION-Nachrichten bereitstellen. Die Kennzahlen sind als aggregierte Werte darzustellen.

Die Ansicht muss dabei auf bestimmte Zeiträume einzuschränken sein. Folgende Zeiträume müssen mindestens auswählbar sein:

- Jahr
- Monat
- Woche

Zu unterscheiden sind die Typen von ION-Nachrichten wie beschrieben in Abschnitt 4.7.2.2.

Das Dashboard muss ION-Nachrichten im ausgewählten Zeitraum anzeigen. Die Darstellung muss nach ION-Nachrichten nach Typ differenziert getrennt oder eindeutig unterscheidbar abbilden.

Die Übersicht muss nach Senderichtung wie definiert in Abschnitt 4.7.2.1 filterbar sein.

4.2.1.4 ION-Nachrichten mit Bearbeitungsbedarf

Das Dashboard muss eine Übersicht über aktuell zu bearbeitende Meldungen im Rahmen des ION-Monitorings wie beschrieben in 4.2.5 anzeigen.

Die Meldungen müssen nach Typ zusammengefasst dargestellt werden. Meldungen beziehen sich auf die Prüfungen des ION-Monitorings, die eine Auffälligkeit einer solche Prüfung signalisieren.

Die Übersicht muss mindestens folgende Sortiermöglichkeiten bieten:

- EventIdentifier (wie z.B. Fehlercode)
- Kommunikationspartner
- Senderichtung

Bei Auswahl einer Meldungskategorie muss eine Navigation in die Meldungsansicht mit entsprechenden Filtern erfolgen.

Bei Auswahl einer einzelnen Meldung soll eine Ansicht der Meldung erfolgen.

4.2.1.5 Monitoring Meldungen mit Bearbeitungsbedarf

Das Dashboard muss eine Übersicht über aktuell zu bearbeitende Meldungen im Rahmen der Klärfälle wie beschrieben in 4.2.5 anzeigen.

Die Meldungen müssen nach Typ zusammengefasst dargestellt werden. Meldungen beziehen sich auf die Art der Klärfälle.

Bei Auswahl einer Meldungskategorie muss eine Navigation in die Meldungsansicht mit entsprechenden Filtern erfolgen.

Bei Auswahl einer einzelnen Meldung soll eine Ansicht der Meldung erfolgen.

4.2.1.6 Listenstatus

Das Dashboard muss eine Statusübersicht der Sperr- und Aktionslisten bereitstellen. Diese Übersicht zeigt anhand eines Listenstatus, wann die entsprechenden Listen zuletzt aktualisiert wurden.

Die Statusübersicht zeigt jeweils für Sperr- und Aktionslisten die Anzahl der Organisationen mit jeweiligem Listenstatus.

Das Dashboard des nationalen Mandanten (siehe Abschnitt 4.9) zeigt den Listenstatus aller berechtigten Organisationen an.

4.2.1.6.1 Sperrlistenstatus

Sperrlisten werden von Customer Contract Partnern und Service Operatoren beim Hotlist Service (HLS) abgefragt und benutzt, um Berechtigungen zu sperren.

Hinweis: Welche Organisationen für den Sperrlistenstatus relevant sind wird über Produktakzeptanz wie beschrieben in 4.6.14.5.1 konfiguriert. Die Informationen über den Abholungsstatus der Listen muss das MPS beim HLS Service abfragen.

Der Listenstatus ist zeigt an, wann Listen zuletzt abgerufen wurden. Der Status ist in folgende Kategorien einzuordnen:

- „Aktuell“ bei Abruf des letzten Zyklus
- „Verzögert“ bei Abruf des vorletzten Zyklus
- „Nicht abgeholt“ sonst.

Die Statusanzeige muss aggregiert erfolgen und Abweichungen vom Sollzustand klar hervorheben.

Bei Auswahl einer Statuskategorie erfolgt die Navigation in eine Detailansicht mit entsprechender Filterung.

4.2.1.6.2 Aktionslistenstatus

Aktionslisten werden (executing) Customer Contract Partnern beim Product Owner System abgefragt und zum Anpassen von Berechtigungen benötigt.

Hinweis: Welche Organisationen für den Aktionslistenstatus relevant sind wird über das Aktionsmanagement wie beschrieben in 4.5.1 konfiguriert.

Der Listenstatus ist zeigt an, wann Listen zuletzt abgerufen wurden. Der Status ist in folgende Kategorien einzuordnen:

- „Aktuell“ bei Abruf innerhalb der letzten 24 Stunden
- „Verzögert“ bei Abruf innerhalb der letzten 48 Stunden
- „Nicht abgeholt“ bei Überschreitung von 48 Stunden

Die oben aufgeführten Zeiträume müssen pro Mandanten konfigurierbar sein.

Die Statusanzeige muss aggregiert erfolgen und Abweichungen vom Sollzustand klar hervorheben.

Bei Auswahl einer Statuskategorie erfolgt die Navigation in eine Detailansicht mit entsprechender Filterung.

4.2.1.7 Kontrolldaten

Das Dashboard muss eine Statusübersicht über Kontrolldaten wie beschrieben in 4.7.7 bereitstellen. Diese Übersicht zeigt die Anzahl an Kontrolldaten im zeitlichen Verlauf aufgeteilt nach Typ. Es wird mindestens zwischen Kontrollnachweisen und Negativnachweisen (siehe [15] CR-405 „((etiCORE: Weiterleiten von Negativnachweisen“)) unterschieden.

Die Ansicht muss dabei auf bestimmte Zeiträume einzuschränken sein. Folgende Zeiträume müssen mindestens auswählbar sein:

- Jahr
- Monat
- Woche

Zusätzlich muss die Ansicht nach OrgID und Tag filterbar sein.

4.2.1.8 Aggregierte Übersicht weiterer Register und Datenbestände

Das Dashboard muss eine aggregierte Übersicht über die Inhalte folgender Register bereitstellen:

- Bestand an Berechtigungen wie beschrieben in Abschnitt 4.7.10.1
- Nutzungsregister wie beschrieben in Abschnitt 4.7.8
- Job-Protokoll wie beschrieben in Abschnitt 4.8.1

Die Übersicht dient der schnellen Einschätzung des Datenbestands und des Systemzustands.

Bei Auswahl eines Registers oder Datenbestandes muss eine Navigation in die jeweilige Detailansicht erfolgen.

Die Detaillierung der Ansicht (Daten, Zeiträume und Aggregation) erfolgt im Rahmen des Pflichtenheftes.

4.2.2 Optional: Dashboard Konfiguration

Das Dashboard dient der übersichtlichen und individuellen Darstellung relevanter Informationen aus dem System. Ziel ist es, Nutzern eine flexible Möglichkeit zu bieten, für ihre jeweiligen Aufgaben relevante Daten und Kennzahlen aus dem System zusammenzustellen und visuell aufzubereiten. Neben dem Standardisierten Dashboard – beschrieben in Abschnitt 4.2.1 – soll es Nutzern optional möglich sein, das Dashboard zu konfigurieren.

4.2.2.1 Allgemeine Anforderungen

Das System muss jedem Nutzer genau ein individuelles Dashboard zur Verfügung stellen.

Das Dashboard muss aus mehreren voneinander unabhängigen Kacheln bestehen.

Jede Kachel muss eine klar abgegrenzte Information oder Auswertung darstellen.

Änderungen an der Dashboard-Konfiguration eines Nutzers dürfen keine Auswirkungen auf Dashboards anderer Nutzer haben.

Das System muss ein vorkonfiguriertes Standard-Dashboard wie beschrieben in 4.2.1 bereitstellen.

Das Standard-Dashboard muss dem Nutzer als Ausgangspunkt für die individuelle Konfiguration dienen.

Vorkonfigurierte Kacheln müssen vom Nutzer entfernt, angepasst oder neu angeordnet werden können.

Das System muss dem Nutzer ermöglichen, das Standard-Dashboard jederzeit wiederherzustellen.

4.2.2.2 Benutzerdefinierte Kacheln

4.2.2.2.1 Erstellung eigener Kacheln

Das System muss Nutzern ermöglichen, eigene Kacheln zu erstellen.

Die Konfiguration des Dashboards und der Kacheln muss über eine grafische, Benutzeroberfläche erfolgen. Eine manuelle Bearbeitung von Konfigurationsartefakten (z. B. Textdateien oder Skripten) darf nicht erforderlich sein.

Bei der Erstellung einer Kachel muss der Nutzer einen Datentyp auswählen können.

Es müssen grundsätzlich alle im System verfügbaren Datenbestände auswählbar sein, sofern der Nutzer über die entsprechenden Berechtigungen verfügt.

Die Erstellung einer Kachel muss schrittweise erfolgen (Datenauswahl, Filterung, Aggregation, Visualisierung).

Das System muss Eingaben validieren und den Nutzer bei fehlerhaften oder unvollständigen Konfigurationen informieren.

4.2.2.2.2 Filterung

Das System muss die Filterung der ausgewählten Daten ermöglichen.

Filter müssen auf Attributen des gewählten Datentyps basieren können (z. B. Zeitraum, Status, Kategorie).

Es müssen mehrere Filter gleichzeitig konfigurierbar sein.

4.2.2.2.3 Aggregation

Das System muss die Aggregation der gefilterten Daten ermöglichen.

Die Aggregation muss auf auswählbaren Attributen des Datentyps erfolgen können.

Das System muss mindestens folgende Aggregationsarten für sämtliche Visualisierungen unterstützen:

- Anzahl
- Summe
- Durchschnitt
- Minimum
- Maximum

Nicht syntaktisch sinnvolle Kombinationen aus Datentyp, Aggregation und Visualisierung müssen vom System unterbunden werden (z.B. Maximum bei nicht-numerischen Werten)

4.2.2.2.4 Visualisierung

Das System muss die visualisierte Darstellung der aggregierten Daten innerhalb einer Kachel ermöglichen.

Für jede Kachel muss eine Visualisierungsart ausgewählt werden können.

Das System muss mindestens folgende Standarddiagramme unterstützen:

- Balkendiagramm
- Kreisdiagramm
- Zeitlicher Verlauf (z. B. Liniendiagramm)

Die Auswahl der Diagrammtypen muss abhängig vom zugrunde liegenden Datentyp und der Aggregation sinnvoll eingeschränkt werden (z. B. zeitlicher Verlauf nur bei vorhandener Zeitdimension).

4.2.2.2.5 Layout und Anordnung

Das System muss es Nutzern ermöglichen, Kacheln frei auf dem Dashboard anzuordnen.

Kacheln müssen in ihrer Größe veränderbar sein, sofern dies die jeweilige Visualisierung unterstützt.

Änderungen an Anordnung und Größe müssen unmittelbar wirksam werden.

4.2.2.3 Dashboard-Vorlagen

Dashboard-Vorlagen dienen der Wiederverwendung bewährter Dashboard-Konfigurationen innerhalb eines Mandanten und reduzieren den Konfigurationsaufwand für andere Nutzer.

Das System muss es allen Nutzern ermöglichen, ihr eigenes Dashboard als Vorlage zu speichern und anderen Nutzern bzw. Nutzergruppen (z.B. allen Nutzern des eigenen Mandanten) zur Verfügung zu stellen.

Das System muss Nutzern ermöglichen, eine vorhandene Dashboard-Vorlage als Basis für ihr eigenes Dashboard zu übernehmen.

Beim Übernehmen einer Vorlage muss eine Kopie der Dashboard-Konfiguration erstellt werden.

Änderungen am Dashboard eines Nutzers dürfen keine Auswirkungen auf die zugrunde liegende Vorlage oder auf Dashboards anderer Nutzer haben.

4.2.2.4 Persistenz

Das System muss die individuelle Dashboard-Konfiguration eines Nutzers dauerhaft speichern und anwenden.

Das System muss konsistent mit Kacheln umgehen, deren zugrunde liegende Datenquellen nicht mehr verfügbar sind (z. B. Hinweis oder Deaktivierung der Kachel).

4.2.3 Super Admin Dashboard

Das Super Admin Dashboard dient der fachlichen Überwachung und dem operativen Betrieb des Gesamtsystems durch Nutzer mit der Rolle Super Admin.

Das Dashboard ist ausschließlich für Nutzer der Rolle Super Admin zugänglich.

Es stellt eine zentrale Übersicht über fachlich relevante Systemereignisse und -zustände bereit und unterstützt Super Admins bei der Analyse, Bewertung und Nachverfolgung von Auffälligkeiten im laufenden Betrieb.

Alle im Dashboard dargestellten Kennzahlen, Diagramme und Listen müssen interaktiv ausgeführt sein.

Durch Auswahl einer Kachel oder eines dargestellten Wertes muss eine direkte Navigation in die jeweils zugehörige Fachansicht erfolgen.

Die Zielansicht muss dabei automatisch mit passenden Filterkriterien vorbelegt werden, sodass ausschließlich die dem ausgewählten Dashboard-Inhalt entsprechenden Datensätze angezeigt werden.

4.2.3.1 Allgemein

Das Dashboard zeigt alle Informationen aggregiert über das gesamte System in einer übersichtlichen Dashboard Struktur.

Die angezeigten Daten müssen automatisch und nahe Echtzeit aktualisiert werden.

Die Aktualisierung erfolgt ohne manuelle Aktion des Nutzers.

Die dargestellten Daten müssen zeitlich auswertbar sein. Zeitliche Verläufe sollen primär in geeigneten Diagrammformen (z. B. Linien- oder Balkendiagramme) visualisiert werden.

Farb- und Symbolik müssen konsistent und fachlich verständlich eingesetzt werden.

Alle Visualisierungen müssen eine klare fachliche Interpretation ermöglichen (z. B. Trends, Auffälligkeiten, Peaks).

Die dargestellten Daten sind nur zur Analyse. Eine direkte fachliche Bearbeitung im Dashboard ist nicht vorgesehen.

4.2.3.2 SLAs und Performance

Das Dashboard muss eine Übersicht über ausgewählte fachliche Performance- und SLA-Kennzahlen bereitstellen. Die Darstellung erfolgt aggregiert über das Gesamtsystem.

Das System muss die durchschnittliche Antwortzeit im zeitlichen Verlauf darstellen. Die Darstellung muss je Stunde aggregiert erfolgen und sich auf die letzten 24 Stunden beziehen.

Das System muss die maximale Antwortzeit im zeitlichen Verlauf darstellen. Die Darstellung muss je Stunde aggregiert erfolgen und sich auf die letzten 24 Stunden beziehen.

Das System muss das Transaktionsvolumen im zeitlichen Verlauf darstellen. Hierbei muss die Anzahl der verarbeiteten Transaktionen je Stunde aggregiert und für die letzten 24 Stunden visualisiert werden.

Das System muss die Verfügbarkeit des Gesamtsystems als prozentualen Kennwert darstellen. Die Berechnung muss sich auf den letzten abgeschlossenen Kalendermonat beziehen.

Die Darstellung der Kennzahlen muss in geeigneter Form erfolgen, sodass zeitliche Entwicklungen, Trends und Auffälligkeiten für den Nutzer eindeutig erkennbar sind.

Ziel ist die Ermöglichung einer schnellen fachlichen Bewertung der Systemperformance sowie der Einhaltung definierter Service Level Agreements im Zeitverlauf.

4.2.3.3 ION-Nachrichten

Das Super Admin Dashboard muss eine Übersicht über alle im System verarbeiteten ION-Nachrichten im zeitlichen Verlauf bereitstellen. Die Kennzahlen sind als aggregierte Werte darzustellen.

Das Dashboard muss ein Diagramm zur Darstellung des zeitlichen Verlaufs von ION-Nachrichten bereitstellen. Die Kennzahlen sind als aggregierte Werte darzustellen.

Die Ansicht muss dabei auf bestimmte Zeiträume einzuschränken sein. Folgende Zeiträume müssen mindestens auswählbar sein:

- Jahr
- Monat
- Woche

Zu unterscheiden sind die Typen von ION-Nachrichten wie beschrieben in Abschnitt 4.7.2.2.

Das Dashboard muss ION-Nachrichten im ausgewählten Zeitraum anzeigen. Die Darstellung muss nach ION-Nachrichten nach Typ differenziert getrennt oder eindeutig unterscheidbar abbilden.

Die Übersicht muss nach Senderichtung wie definiert in Abschnitt 4.7.2.1 filterbar sein.

4.2.3.4 Listenstatus

Das Super Admin Dashboard muss eine Statusübersicht der Sperr- und Aktionslisten bereitstellen. Diese Übersicht zeigt anhand eines Listenstatus, wann die entsprechenden Listen zuletzt aktualisiert wurden.

Die Statusübersicht zeigt jeweils für Sperr- und Aktionslisten die Anzahl der Organisationen mit jeweiligem Listenstatus.

4.2.3.4.1 Sperrlistenstatus

Sperrlisten werden von Customer Contract Partnern und Service Operatoren beim Hotlist Service (HLS) abgefragt und benutzt, um Berechtigungen zu sperren.

Hinweis: Welche Organisationen für den Sperrlistenstatus relevant sind wird über Produktakzeptanz wie beschrieben in 4.6.14.5.1 konfiguriert. Für den Super Admin sollten das in der Regel alle relevanten Organisationen aller Mandanten sein.

Der Listenstatus ist zeigt an, wann Listen zuletzt abgerufen wurden. Der Status ist in folgende Kategorien einzuordnen:

- „Aktuell“ bei Abruf des letzten Zyklus
- „Verzögert“ bei Abruf des vorletzten Zyklus
- „Nicht abgeholt“ sonst.

Die Statusanzeige muss aggregiert erfolgen und Abweichungen vom Sollzustand klar hervorheben.

Bei Auswahl einer Statuskategorie erfolgt die Navigation in eine Detailansicht mit entsprechender Filterung.

4.2.3.4.2 Aktionslistenstatus

Aktionslisten werden (executing) Customer Contract Partnern beim Product Owner System abgefragt und zum Anpassen von Berechtigungen benötigt.

Hinweis: Welche Organisationen für den Aktionslistenstatus relevant sind wird über das Aktionsmanagement wie beschrieben in 4.5.1 konfiguriert.

Der Listenstatus ist zeigt an, wann Listen zuletzt abgerufen wurden. Der Status ist in folgende Kategorien einzuordnen:

- „Aktuell“ bei Abruf innerhalb der letzten 24 Stunden
- „Verzögert“ bei Abruf innerhalb der letzten 48 Stunden
- „Nicht abgeholt“ bei Überschreitung von 48 Stunden

Die oben aufgeführten Zeiträume müssen pro Mandanten konfigurierbar sein.

Die Statusanzeige muss aggregiert erfolgen und Abweichungen vom Sollzustand klar hervorheben.

Bei Auswahl einer Statuskategorie erfolgt die Navigation in eine Detailansicht mit entsprechender Filterung.

4.2.4 Fachliches Monitoring

Eine zentrale Aufgabe des Product Owners ist das fachliche Monitoring der im System eingehenden Informationen, d.h. es werden standardisierte Prüfungen durchgeführt, um die Richtigkeit der eingehenden Informationen sicherzustellen. Das Monitoring teilt sich dabei in zwei Prozesse auf, zum einen in sofortige Prüfungen, die bei Eingang einer Nachricht in das System durchgeführt werden und zum anderen in nachgelagerte Prüfungen, welche zeitlich versetzt nach Erhalt der Nachricht stattfinden. Wird bspw. eine Kontrolle einer Berechtigung gemeldet, so wird geprüft, ob eine entsprechende Ausgabemeldung vorhanden ist. Die beiden Nachrichten kommen von unterschiedlichen Drittsystemen und können auch mit zeitlichem Abstand und in unterschiedlicher Reihenfolge eingehen, daher ist es sinnvoll, dass diese Prüfung nicht direkt nach Nachrichteneingang erfolgt.

In der Product Owner Reference System Specification “etiCORE SPEC-PO-RS_v3.0.0-rc.6 en”[4] ist das sofortige Monitoring in den Use Cases mit der Bezeichnung *handle * notification from product perspective* beschrieben. Diese finden sich in allen *Functionality Bundles*, die in der Spezifikation beschrieben sind.

Das nachgelagerte Monitoring ist in ((etiCORE definiert durch das sog. *Downstream Monitoring*, welches im Modell innerhalb des Product Owner Systems unter Downstream checks from Product Perspective (siehe [Spezifikationsmodell](#)) beschrieben ist.

4.2.4.1 Monitoring Konfiguration

Das System ermöglicht es die Alarmierung von Monitoring Vorfällen zeitweise zu deaktivieren. Während ein betroffenes Unternehmen mit der Endstörung beschäftigt ist, kann so die dauerhafte Alarmierung verhindert werden.

4.2.4.2 Monitoring Übersicht

Das System erzeugt für jeden Monitoring Vorfall einen Eintrag in einer Monitoring-Übersicht. Diese Übersicht zeigt alle verfügbaren Informationen pro Vorfall in der Übersicht an:

- Vorfall-ID
- Zeitpunkt des Vorfalls
- Nachrichtentyp (z.B. Entitlement Issued, Entitlement Inspected, ...)
- Inbound / Outbound Message
- Vorfall-Beschreibung und Warnungen
- Org-ID des Senders

- Org-ID des Empfängers
- ION-Message-Number
- Process-Instance-ID

Für jeden Eintrag der Übersicht stellt das System eine Detailansicht bereit, die dem Benutzer per Klick auf eine Schaltfläche angezeigt wird. Diese Detailansicht zeigt zum einen die geparsten Nachrichteninformation in menschlich lesbarer Form und zum anderen die Rohdaten der Nachricht. Dazu enthält die Detailansicht weitere Detailinformationen zur Warnmeldung inkl. eines direkten Links in die Zentrale Event-Datenbank zur weiteren Behandlung der Meldung. Sobald die zentrale Event-Datenbank verfügbar ist, muss das System diese Anbindung umsetzen. Für die Nachrichtentypen sind geeignete Kürzel zu verwenden, um die Darstellung in der Bedienoberfläche übersichtlich zu halten.

4.2.5 Meldungen / Anwendungsfälle Operatoren

Im Rahmen des fachlichen Monitorings können Vorfälle entstehen, die nicht automatisiert abgearbeitet werden können. Diese stellt das System in einer Meldungsübersicht bereit und kennzeichnet außerdem, welche Rolle (Administrator, Nutzer) in dem konkreten Vorfall eingreifen muss. In allen Fällen muss eine eigene Handlungsempfehlung nur für Klärfälle hinterlegt werden können. Das MPS muss dem Nutzer des Systems ermöglichen, diese Handlungsempfehlung auch selbst zu formulieren und zu hinterlegen. Ein Administrator muss für verschiedene Klärfall-Typen (siehe 4.2.5.2) Handlungsempfehlungen formulieren bzw. konfigurieren können.

Derartige Klärfälle müssen von den handelnden Rollen als behandelt quittiert werden können. Das Abschließen des Klärfalles (s.u.) ist für die Nachvollziehbarkeit festzuhalten in einer eigenen Historie. Dabei ist der Benutzer, der Zeitpunkt und die Referenz auf den Klärfall (s.u.) festzuhalten.

Für die Klärfälle ist eine entsprechende Bedienoberfläche zu realisieren. Details hierzu werden im Pflichtenheft festgelegt.

Zusammengefasste Meldungen zu Klärfällen sollen darüber hinaus per E-Mail an konfigurierbare E-Mail-Adressen der hinter der Rolle definierten Benutzer weitergeleitet werden.

4.2.5.1 Übersicht der Klärungsfälle im Monitoring

Im Monitoring sind Klärfälle im Spezifikationsmodell mit der Aktion „Create clarification case“ gekennzeichnet. Für Fälle, die den Product Owner und damit das MPS betreffen,

muss der Kontext in einem Clarification Case Register festgehalten werden. Einträge in diesem Register können abgearbeitet werden. Je nach Typ des Klärfalles (siehe 4.2.5.2) muss dann das MPS mit Hilfe des Kontextes den entsprechenden Anwendungsfall ermöglichen.

Je nach Typ des Klärfalles kann das Abschließen der Behandlung auch dazu führen, dass eine gekennzeichnete Nachricht wieder der Regelverarbeitung zugeführt wird. Dafür müssen Warnungen an Nachrichten entfernt werden können.

Die nachfolgenden Fälle sind jeweils Anwendungsfälle für den Mandant, welche manuelle Eingriffe erfordern. Diese Klärfälle können entweder durch eine Nachricht verursacht werden oder durch ein sonstiges Ereignis. Das MPS muss den Typen des Klärfalles festlegen und den passenden Kontext erzeugen.

Innerhalb der weiter unten aufgeführten Klärfälle muss es je nach Verlauf und Kontext möglich sein, folgende Anwendungsfälle manuell zu triggern:

- Demand Application Hotlisting (Sperranforderung Applikation)
- Demand Entitlement Hotlisting (Sperranforderung Berechtigung)
- Demand SAM Hotlisting (Sperranforderung SAM)
- Revoke Application Hotlisting Demand (Sperraufhebungsanforderung Applikation)
- Revoke Entitlement Hotlisting Demand (Sperraufhebungsanforderung Berechtigung)

4.2.5.2 Typen von Klärfällen

Folgende Typen von Klärfällen existieren:

- Timeout Warnung: Wartezeit überschritten
- Timeout Warnung bei ausgeführter Aktion: Wartezeit überschritten
- Signaturfehler statische Berechtigung
- Signaturfehler bei Chipkartentransaktion
- Signaturfehler bei Chipkartentransaktion bei ausgeführter Aktion
- Nachricht trotz Hotlist-Eintrag
- Kein Hotlist-Eintrag trotz Hotlisting-Demand
- Unbekanntes SAM oder unbekannte Applikation

4.2.5.3 Klärfälle als Anwendungsfälle

4.2.5.3.1 Musterfall

Kurzbeschreibung	Beschreibung des Klärfalles
Typ	Typ des Klärfalles
Auslöser	Welches Ereignis hat den Klärfall ausgelöst?
Problembeschreibung	Welches Problem entsteht bzw. besteht, was dann behoben werden muss?
Kontext	Benötigter Kontext, z.B. Referenzen auf Nachrichten, Hotlist-Einträge, etc.
Möglicher Status	Welche Zustände kann der Klärfall haben?
Rolle	Welche der Rollen Super-Administrator, Administrator, Nutzer ist erlaubt?
Unterstützung durch MPS	Was bietet das MPS, um diesen Klärfall zu bearbeiten?
Mögliche Nachbedingungen	<p>Wurde etwas durch die Klärung bewirkt? Mögliche Optionen sind</p> <ul style="list-style-type: none"> • Klärfall wurde auf „on hold“ gesetzt: ein für den Klärfall konfiguriertes Wartefenster startet erneut (z.B. bei Timeout Warnungen) • Klärfall wurde manuell auf „geklärt“ gesetzt („weggeklickt“), so dass er aus der Liste der Klärfälle verschwindet • Klärfall wurde bearbeitet: Hier muss es möglich sein, einen Freitext zu verfassen. Wenn eine bestimmte Maßnahme ergriffen wird, muss der Nutzer das auswählen können: Ticket erstellt, Hotlist Demand erstellt. • Klärfall geklärt: Es wurden Maßnahmen ergriffen, die den Klärfall final klären

4.2.5.3.2 Timeout Warnung bei Aktionsausführung

Kurzbeschreibung	Timeout Warnung in Nachricht für Aktionsausführung
Typ	Timeout Warnung bei ausgeführter Aktion, ggf. Wartezeit überschritten
Auslöser	Im Rahmen des Aktionsmanagements treffen ION-Nachrichten mit entsprechenden Notifications ein, in denen eine Timeout-Warnung enthalten ist. Das bedeutet, dass das erfolgreiche Ausführen der Aktion auf der Chipkarte nicht verifiziert werden konnte und der Ausführungsstatus unklar ist.
Problembeschreibung	Bei Timeout- oder Signatur-Warnungen kann eine Aktion nicht als ausgeführt gemeldet werden und verbleibt auf der Aktionsliste bis zur Lösung des Klärfalles. Bei Timeout-Warnungen wird ein

	konfigurierbares Zeitintervall gewartet, danach muss die Aktionsliste geprüft werden.
Kontext	Referenz auf die Nachricht, Referenz auf betroffene(n) Aktionslisteneinträge
Möglicher Status	„Timeout Aktionsausführung“, „Timeout Aktionsausführung, Wartezeit überschritten“, „Manuell geklärt“, „Automatisch geklärt“
Rolle	Klärung: Administrator; Betrachten, Auswerten: Administrator, Nutzer
Unterstützung durch MPS	Das MPS zeigt auf, dass Aktionseinträge aufgrund des Timeouts nicht entfernt werden können. Eine automatisierte Prüfung von nachfolgenden Nachrichten stellt fest, ob die Aktion ausgeführt wurde (z.B. Eingang eines Kontrollnachweises bei vorherigem Timeout der Ausgabe einer Berechtigung). Dann erfolgt eine automatische Klärung. Wurde die konfigurierbare Wartezeit überschritten, so wird der Administrator benachrichtigt und erhält die Möglichkeit, den Fall manuell zu klären. Dabei muss entschieden werden, ob die Aktionseinträge entfernt werden sollen oder nicht. Wenn die Analyse eine Häufung bei einem oder mehreren Terminals zeigt, muss im Ticket-System ein Ticket gegen den Verursacher (Terminalbetreiber) gestellt werden können.
Mögliche Nachbedingungen	On hold: die Wartezeit startet erneut Geklärt: Notifications als gültig markiert, Aktionseinträge entfernt

4.2.5.3.3 Signatur Warnung bei Aktionsausführung

Kurzbeschreibung	Signatur Warnung in Nachricht für Aktionsausführung
Typ	Signaturfehler bei Chipkartentransaktion bei ausgeführter Aktion
Auslöser	1. Im Rahmen des Aktionsmanagements treffen ION-Nachrichten mit entsprechenden Notifications ein, in denen bereits eine Signatur-Warnung enthalten ist. 2. Während der Verarbeitung der Attestation wird ein Problem mit der Signatur festgestellt und das MPS fügt die Warnung hinzu.
Problembeschreibung	Das bedeutet, dass das Ausführen der Aktion auf der Chipkarte nicht authentisch ist. Das Signatur-Zertifikat ist ungültig, unbekannt oder abgelaufen. Die Aktion verbleibt auf der Aktionsliste bis zur Lösung des Klärfalles.
Kontext	Referenz auf die Nachricht, Referenz auf betroffenen Aktionslisteneintrag
Möglicher Status	„Signaturfehler Aktionsausführung“, „Manuell geklärt“
Rolle	Klärung: Administrator; Betrachten, Auswerten: Administrator, Nutzer
Unterstützung durch MPS	Das MPS zeigt auf, dass ein Aktionseintrag aufgrund des Signaturfehlers nicht entfernt werden kann. Der Administrator wird benachrichtigt und erhält die Möglichkeit, den Fall manuell zu klären. Dazu bietet das MPS die Möglichkeit, im Ticket-System ein Ticket gegenüber dem Verursacher zu stellen. Final muss der Administrator

	entscheiden, ob der Aktionseintrag entfernt werden soll oder nicht und ob die betroffenen Attestations als gültig angesehen werden können. Das MPS kennzeichnet dann die Attestation dann als gültig.
Mögliche Nachbedingungen	Bearbeitet: Ticket gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert Bearbeitet: Hotlisting Demand gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert Geklärt: Notifications als gültig markiert, Aktionseinträge entfernt Geklärt: Notifications als ungültig markiert, Aktionseinträge bleiben bestehen

4.2.5.3.4 Signatur Warnung statische Berechtigung

Kurzbeschreibung	Signatur Warnung in Nachricht für statische Berechtigung
Typ	Signaturfehler statische Berechtigung
Auslöser	1. Im Rahmen der statischen Berechtigungen treffen ION-Nachrichten mit entsprechenden Notifications ein, in denen bereits eine Signatur-Warnung enthalten ist. 2. Während der Verarbeitung wird ein Problem mit der Signatur festgestellt und das MPS fügt die Warnung hinzu.
Problembeschreibung	Bei der Ausgabe einer statischen Berechtigung signiert das SAM die Berechtigung und signalisiert damit die authentische Ausgabe. Bei Eingang der Ausgabenachricht schlägt die Prüfung dieser Signatur fehl. Bei der Kontrolle wird die Signatur ebenfalls geprüft. Die Prüfung schlägt fehl. Damit ist die statische Berechtigung potenziell von einem nicht autorisierten SAM ausgegeben worden.
Kontext	Referenz auf die Nachricht
Möglicher Status	„Signaturfehler statische Berechtigung“, „Manuell geklärt“
Rolle	Klärung: Administrator; Betrachten, Auswerten: Administrator, Nutzer
Unterstützung durch MPS	Das MPS benachrichtigt den Administrator. Dieser erhält die Möglichkeit, den Fall manuell zu klären. Dabei muss entschieden werden, ob ein Hotlisting Demand SAM (Sperranforderung) gestellt wird. Zusätzlich besteht die Möglichkeit, im Ticket-System ein Ticket gegenüber dem Verursacher zu stellen.
Mögliche Nachbedingungen	Bearbeitet: Ticket gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert Bearbeitet: Hotlisting Demand gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert Manuell geklärt: z.B. nach Klärung im Ticket

4.2.5.3.5 Signatur Warnung bei Chipkarten-Transaktion (ohne Aktionsmanagement)

Kurzbeschreibung	Signatur Warnung in Nachricht
Typ	Signaturfehler bei Chipkartentransaktion

Auslöser	<p>1. Es treffen ION-Nachrichten mit entsprechenden Notifications ein, in denen bereits eine Signatur-Warnung enthalten ist. Die Notifications können sowohl Berechtigungen als auch Applikationen betreffen.</p> <p>2. Während der Verarbeitung der Attestation wird ein Problem mit der Signatur festgestellt und das MPS fügt die Warnung hinzu.</p>
Problembeschreibung	Bei (Trans-) Aktionen mit Berechtigungen oder Applikationen auf der Chipkarte kann die Signatur nicht geprüft werden. Das bedeutet, dass das Ausführen der Aktion auf der Chipkarte nicht authentisch ist. Das Signatur-Zertifikat ist ungültig, unbekannt oder abgelaufen.
Kontext	Referenz auf die Nachricht
Möglicher Status	„Signaturfehler“, „Manuell geklärt“
Rolle	Klärung: Administrator; Betrachten, Auswerten: Administrator, Nutzer
Unterstützung durch MPS	Das MPS benachrichtigt den Administrator. Dieser erhält die Möglichkeit, den Fall manuell zu klären. Dazu besteht die Möglichkeit, im Ticket-System ein Ticket gegenüber dem Verursacher zu stellen. Final muss entschieden werden, ob die betroffenen Attestations als gültig angesehen werden können.
Mögliche Nachbedingungen	<p>Bearbeitet: Ticket gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert</p> <p>Bearbeitet: Hotlisting Demand gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert</p> <p>Geklärt: Notifications als gültig markiert</p> <p>Geklärt: Notifications als ungültig markiert</p>

4.2.5.3.6 Unbekanntes SAM

Kurzbeschreibung	Im Monitoring kann für eine SAM-ID kein Besitzer ermittelt werden.
Typ	Unbekanntes SAM oder unbekannte Applikation
Auslöser	Für diverse Monitoring Prüfungen wird die Organisations-ID des SAM-Besitzers ermittelt. Dies geschieht durch die Anwendungsfälle <i>Retrieve Certificate over signing key</i> oder <i>Determine SAM owner</i> . Der Klärfall tritt auf, wenn zu der SAM-ID kein Besitzer ermittelt werden kann.
Problembeschreibung	Für eine SAM-ID kann kein Besitzer ermittelt werden.
Kontext	Referenz auf die Nachricht, Referenz auf die Nachricht / Fehlermeldung für den SAM-Lookup
Möglicher Status	„Unbekanntes SAM“, „Manuell geklärt“
Rolle	Klärung: Administrator, Nutzer; Betrachten, Auswerten: Administrator, Nutzer
Unterstützung durch MPS	Das MPS benachrichtigt den Administrator. Dieser erhält die Möglichkeit, den Fall manuell zu klären. Da es sich um einen sicherheitsrelevanten Fall handelt, kann im Ticket-System ein Ticket gegenüber VDV-ETS geöffnet werden.
Mögliche Nachbedingungen	<p>Bearbeitet: Ticket gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert</p> <p>Geklärt: Klärfall manuell auf „geklärt“ gesetzt</p>

4.2.5.3.7 Unbekannte Applikation

Kurzbeschreibung	Im Monitoring kann für eine Applikation-Instanz-ID kein Besitzer ermittelt werden.
Typ	Unbekanntes SAM oder unbekannte Applikation
Auslöser	Für diverse Monitoring Prüfungen wird die Organisations-ID des SAM-Besitzers ermittelt. Dies geschieht durch die Anwendungsfälle <i>Retrieve Certificate over signing key</i> oder <i>Determine application owner</i> . Der Klärfall tritt auf, wenn zu der Applikations-Instanz-ID kein Besitzer ermittelt werden kann.
Problembeschreibung	Für die Applikations-Instanz-ID eines User Mediums kann kein Besitzer ermittelt werden.
Kontext	Referenz auf die Nachricht, Referenz auf die Nachricht / Fehlermeldung für den Applikations-Lookup
Möglicher Status	„Unbekannte Applikation“, „Manuell geklärt“
Rolle	Klärung: Administrator, Nutzer; Betrachten, Auswerten: Administrator, Nutzer
Unterstützung durch MPS	Das MPS benachrichtigt den Administrator. Dieser erhält die Möglichkeit, den Fall manuell zu klären. Da es sich um einen sicherheitsrelevanten Fall handelt, kann im Ticket-System ein Ticket gegenüber VDV-ETS geöffnet werden
Mögliche Nachbedingungen	Bearbeitet: Ticket gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert Geklärt: Klärfall manuell auf „geklärt“ gesetzt

4.2.5.3.8 Berechtigung in Nachricht auf Hotlist

Kurzbeschreibung	Für eintreffende Nachrichten befindet sich die Berechtigung auf der Hotlist
Typ	Nachricht trotz Hotlist-Eintrag
Auslöser	Eine ION-Nachricht zu einer Berechtigung (außer Sperrnachweis) trifft ein. Diese Berechtigung befindet sich auf der Entitlement Hotlist.
Problembeschreibung	Wenn sich eine Berechtigung auf der Hotlist befindet, sollte außer einem Sperrnachweis zu dieser Berechtigung keine andere bzw. weitere Nachricht eintreffen. Insbesondere keine Kontrollnachweise. Dies wäre ein Indikator dafür, dass das Kontrollterminal zum Zeitpunkt der Kontrolle nicht die aktuelle Hotlist hatte.
Kontext	Referenz auf die Nachricht, Referenz auf Hotlist-Eintrag und Zyklus
Möglicher Status	„Gehotlistete Berechtigung“, „Manuell geklärt“
Rolle	Klärung: Administrator, Nutzer; Betrachten, Auswerten: Administrator, Nutzer
Unterstützung durch MPS	Das MPS benachrichtigt den Administrator/Nutzer. Dieser erhält die Möglichkeit, den Fall manuell zu klären. Dazu besteht die Möglichkeit, im Ticket-System ein Ticket gegenüber dem Verursacher (Operator Organisations-ID des Terminals) zu stellen.
Mögliche Nachbedingungen	Bearbeitet: Ticket gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert

	Geklärt: Klärfall manuell auf „geklärt“ gesetzt
--	---

4.2.5.3.9 Applikation in Nachricht auf Hotlist

Kurzbeschreibung	Für eintreffende Nachrichten befindet sich die Applikation auf der Hotlist
Typ	Nachricht trotz Hotlist-Eintrag
Auslöser	Eine ION-Nachricht zu einer Berechtigung oder Applikation (außer Sperrnachweis Applikation) trifft ein. Die relevante Applikations-Instanz-ID befindet sich auf der Application Hotlist.
Problembeschreibung	Wenn sich eine Applikation auf der Hotlist befindet, sollte außer einem Sperrnachweis zu dieser Applikation keine andere bzw. weitere Nachricht eintreffen. Insbesondere keine Kontrollnachweise zu Berechtigungen. Dies wäre ein Indikator dafür, dass das Kontrollterminal zum Zeitpunkt der Kontrolle nicht die aktuelle Hotlist hatte.
Kontext	Referenz auf die Nachricht, Referenz auf Hotlist-Eintrag und Zyklus
Möglicher Status	„Gehotlistete Applikation“, „Manuell geklärt“
Rolle	Klärung: Administrator, Nutzer; Betrachten, Auswerten: Administrator, Nutzer
Unterstützung durch MPS	Das MPS benachrichtigt den Administrator. Dieser erhält die Möglichkeit, den Fall manuell zu klären. Dazu besteht die Möglichkeit, im Ticket-System ein Ticket gegenüber dem Verursacher (Operator Organisations-ID des Terminals) zu stellen.
Mögliche Nachbedingungen	Bearbeitet: Ticket gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert Geklärt: Klärfall manuell auf „geklärt“ gesetzt

4.2.5.3.10 Timeout Warnung bei Nachrichten (ohne Aktionsmanagement)

Kurzbeschreibung	Timeout Warnung in Nachricht ohne Aktionsausführung.
Typ	Timeout Warnung: Wartezeit überschritten
Auslöser	Das MPS stellt fest, dass für Nachrichten mit Timeout-Warnungen die konfigurierbare Wartezeit abgelaufen ist. In dieser Zeit sind keine weiteren Nachrichten eingegangen, die zum automatischen Auflösen der Warnungen beitragen konnten.
Problembeschreibung	Nachrichten mit Timeout-Warnung sollen möglichst automatisiert wieder der Regelverarbeitung zugeführt werden. Dies wird mit der Untersuchung von Folgenachrichten erreicht (z.B. eintreffender Kontrollnachweis bei Ausgabe mit Timeout -> Ausgabe der Berechtigung hat funktioniert). Treffen keine Folgenachrichten ein, die

	den Fall klären können, so muss manuell entschieden werden, wie diese Nachrichten behandelt werden sollen.
Kontext	Referenz auf die Nachricht
Möglicher Status	„Timeout“, „Automatisch geklärt“, „Timeout Wartezeit überschritten“, „Manuell geklärt“,
Rolle	Klärung: Administrator, Nutzer; Betrachten, Auswerten: Administrator, Nutzer
Unterstützung durch MPS	Das MPS zeigt auf, dass Nachrichten mit Timeouts existieren, die nicht per automatisierter Prüfungen von nachfolgenden Nachrichten aufgelöst werden konnten. Wurde die konfigurierbare Wartezeit überschritten, so wird der Administrator/Nutzer benachrichtigt und erhält die Möglichkeit, den Fall manuell zu klären. Dabei muss entschieden werden, ob die Nachrichten ebenfalls auf „manuell geklärt“ gesetzt werden, und sie für die weitere Verarbeitung betrachtet werden sollen oder nicht. Wenn die Analyse eine Häufung bei einem oder mehreren Terminals zeigt, muss im Ticket-System ein Ticket gegen den Verursacher (Terminalbetreiber) gestellt werden können.
Mögliche Nachbedingungen	On hold: die Wartezeit startet erneut Geklärt: Notifications als gültig markiert

4.2.5.3.11 Kein Hotlist-Eintrag trotz Hotlisting Demand (Sperranforderung)

Kurzbeschreibung	Bei Hotlisting Demands (Sperranforderungen) für Berechtigungen, Applikationen oder SAMs ist die konfigurierbare Wartezeit abgelaufen, es wurden aber vom jeweiligen Eigentümer keine Einträge auf der Hotlist beauftragt.
Typ	Kein Hotlist-Eintrag trotz Hotlisting-Demand
Auslöser	Das MPS vergleicht die aktuellen Hotlists gegen Bestand an Hotlisting Demands. Nach der konfigurierbaren Wartezeit entsteht der Klärfall, wenn Hotlisting Demands existieren, zu denen kein Hotlist Eintrag gefunden wird.
Problembeschreibung	
Kontext	Referenz auf die Nachricht für den Hotlisting Demand, Referenz auf Hotlist-Zyklus
Möglicher Status	„Hotlisting demanded“, „Wartezeit überschritten“, „Manuell geklärt“,
Rolle	Klärung: Administrator, Nutzer; Betrachten, Auswerten: Administrator, Nutzer
Unterstützung durch MPS	Das MPS zeigt auf, dass Nachrichten für Hotlisting Demands existieren, für die es nach einer konfigurierbaren Wartezeit im Hotlist-Inventory (siehe 4.6.3) keine Einträge gibt. Wurde die konfigurierbare Wartezeit überschritten, so wird der Administrator oder Nutzer benachrichtigt und erhält die Möglichkeit, den Fall manuell zu klären.

	Dabei muss entschieden werden, ob ein erneuter Hotlisting Demand gestellt werden soll, ein Zurückziehen des Hotlisting Demands (z.B. nach telefonischer Klärung) erfolgen soll, oder eine Eskalation über das ESH erfolgen soll. In letzterem Fall muss das MPS einen JIRA-Eintrag mit dem richtigen Typen und Adressaten erstellen bzw. anstoßen können.
Mögliche Nachbedingungen	Bearbeitet: Ticket gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert Bearbeitet: Neuer Hotlisting Demand gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert Bearbeitet: Hotlisting Demand Revocation gegen Verursacher gestellt. Nach konfigurierbarer Wartezeit wird der Bearbeiter nochmal informiert Geklärt: Klärfall manuell auf „geklärt“ gesetzt

4.2.6 ION-Monitoring

Für das ION-Monitoring ergeben sich aufgrund ein- und ausgehender ION-Nachrichten mehrere Szenarien, die in den nachfolgenden Kapiteln aufgeführt werden.

4.2.6.1 Timeout und Wiederhol-Szenarien von ION-Nachrichten

Siehe dazu auch [2] Kap. 7.2 oder [Message Timeout and Retry Handling](#) im Modell.

Die ION-Spezifikation gibt vor, wie sich ein System bei Timeouts und für die Wiederholung von Nachrichten verhalten soll. In den nachfolgenden Kapiteln wird das auf MPS angewendet.

Wiederholversuche von ION-Nachrichten muss das MPS im ION-Nachrichtenregister (siehe 4.7.2) als Historie festhalten.

Im MPS müssen die Anzahl der Versuche und das Retry-Intervall konfigurierbar sein.

Nachfolgende Szenarien beziehen sich auf Zustände in ION-Nachrichten, die in 4.7.2.2 näher beschrieben werden.

4.2.6.1.1 MPS mit *Direct Timeout*

Nachrichten zwischen dem MPS und anderen Systemen werden in 4.7.2 gespeichert.

Ein direktes Timeout (siehe 4.7.2.2) beim MPS tritt auf, wenn das System auf der Gegenseite nicht in der vereinbarten Zeit reagiert. Dies kann sowohl bei synchroner als auch bei asynchroner Kommunikation auftreten (die in ((etiCORE mit Hilfe von 2 synchronen Calls abgebildet wird). Folgende Fälle können auftreten:

- Synchroner Kommunikation: Das MPS arbeitet in dem Fall als Initiator und Client gegenüber dem ION und wartet auf eine synchrone Rückmeldung (Antwort oder Exception)
- Asynchroner Kommunikation: Das MPS arbeitet in dem Fall als Client gegenüber dem ION und wartet auf eine synchrone Empfangsbestätigung (deliveryAcknowledgement oder deliveryRejection). Das kann bei Anfragen als Initiator der Fall sein (z.B. bei Weiterleitungen an den primary Customer Contract Partner pCCP) oder bei Rückmeldungen bei zuvor eingegangenen Nachrichten (z.B. Rückmeldung auf eine eingegangene Ausgabemeldung für eine Berechtigung)

In allen Fällen muss das MPS im Falle eines Timeouts oder eines Kommunikationsfehlers mithilfe des in der ION-Spezifikation beschriebenen Retry-Mechanismus versuchen, die betroffene Nachricht erneut zuzustellen (siehe auch [2] Kap 7.2.1.1 oder [Direct Timeout](#) im Modell).

Endgültig gescheiterte Versuche, eine Nachricht zuzustellen (Zustand verbleibt bei „Direct Timeout“, siehe 4.7.2.2), sind als ION-Monitoring-Fall zu kennzeichnen und erzeugen ab einem konfigurierbaren Schwellwert eine Warnung.

4.2.6.1.2 MPS mit *SLA-Timeout*

Beim MPS als Initiator eines Nachrichtenaustausches (siehe [2]) kann bei asynchroner Kommunikation das sogenannte „SLA-Timeout“ auftreten. SLA-Timeout bedeutet, dass innerhalb eines konfigurierbaren Zeitintervalls (z.B. 7 Tage) zu einer Anfrage im Zustand „Acknowledged“ oder „Acknowledged by CRE“ (siehe 4.7.2.2) keine Rückmeldung eingetroffen ist. Dazu muss ein Cron-Job regelmäßig prüfen, ob solche Anfragen im Nachrichtenregister existieren (siehe Kap. 4.7.2). Falls dies der Fall ist, müssen diese Anfragen auf den Zustand „SLA-Timeout“ (siehe 4.7.2.2) geändert werden. Das MPS kann dann diese Anfragen gemäß ION-Spezifikation dem Wiederholungszenario zuführen (siehe [2]). In „SLA-Timeout“ verbleibende Anfragen

- Führen ab einem konfigurierbaren Schwellwert zu einer Warnung
- Können im MPS als Report angefragt werden

4.2.6.2 Monitoring von Fehlerfällen im ION

Beim Nachrichtenaustausch über das ION können unterschiedliche Fehler entstehen, die nachfolgend aufgeführt werden. Für jedes dieser aufgeführten Szenarien muss ein jeweils

eigener Schwellwert pro Zeitintervall definiert werden können, ab dem eine ION-Monitoring Warnung erzeugt wird. Ohne Schwellwert wird sofort eine Warnung erzeugt.

Hierbei gibt es folgende Szenarien:

- 1) In das MPS einkommende Nachrichten lehnt das MPS mit einer Delivery-Rejection ab
- 2) In das MPS einkommende Nachrichten lehnt das MPS mit einer Business-Exception ab
- 3) Vom MPS ausgehende Nachrichten werden von der Gegenseite mit Delivery-Rejection abgelehnt
- 4) Vom MPS ausgehende Nachrichten werden von der Gegenseite mit einer Business Exception abgelehnt
- 5) Vom MPS ausgehende Nachrichten erhalten von der Gegenseite eine undefinierte Reaktion (z.B. eine Laufzeit-Exception)
- 6) In das MPS einlaufende synchrone Rückmeldungen sind valide ION-Nachrichten, können aber im MPS nicht verarbeitet werden:
 - a) Die ION-Message-ID befindet sich bereits im System
 - b) Die Zuordnung zu Empfängerrolle und Organisation ist nicht möglich
 - c) Die Korrelation in der Rückmeldung passt nicht zur ursprünglichen Anfrage

Für Fall 1 und 2 liegt die Ursache nicht im MPS. Hier muss das MPS mit Hilfe von Metriken bewirken, dass ab einer bestimmten konfigurierbaren Menge an Ablehnungen (pro konfigurierbare Zeit, z.B. pro Tag) eine Monitoring Warnung für den Operator entsteht, um den Fall zu untersuchen. Gegen den Verursacher muss ein Ticket im Ticket-System erstellt werden können.

Für Fall 3, 4 und 5 liegt die Ursache im MPS. Hierfür muss sofort eine Monitoring Warnung entstehen, um mögliche Fehler so schnell wie möglich zu beheben.

Für Fall 6 liegt die Ursache im System, welches die synchrone Antwort sendet. Über Status der synchronen Antwort (siehe Abbildung 7 in Kap. 4.7.2.2) und ION-Monitoring Warnung muss der Operator informiert werden. Gegen den Verursacher muss ein Ticket im Ticket-System erstellt werden können.

4.3 Stammdaten

Das System verwaltet zentrale Stammdaten, die als Grundlage für das Monitoring dienen.

4.3.1 Ansicht

Der Zugriff auf Stammdaten erfolgt mandantenweit für alle Nutzer eines Mandanten. Detaillierte Regelungen zu Benutzerrechten und Benutzerrollen sind im Abschnitt 4.4.2 beschrieben.

Übersichten auf Stammdaten (Organisationen, EFM-Produkte, CCP zu PO-Zuordnung) werden in tabellarischen Übersichten dargestellt. Die einzelnen Spalten jeder Tabelle sind von jedem Nutzer dynamisch konfigurierbar, d.h. Spalten können ein- bzw. ausgeblendet werden. Die getätigten Einstellungen sollen erhalten bleiben, bis sie vom Nutzer selbst geändert werden.

Die tabellarischen Übersichten unterstützen Sortier- und Filterfunktionen für alle dargestellten Datenfelder.

Einträge werden auch dann angezeigt, wenn einzelne Datenfelder leer, unvollständig oder fehlerhaft sind.

Für jede tabellarische Übersicht besteht die Möglichkeit, die aktuell dargestellten Daten in ein CSV-Format zu exportieren.

Aus der tabellarischen Übersicht kann in eine Detailansicht einzelner Datensätze gewechselt werden.

4.3.2 Erfassung und Pflege

Die Benutzeroberfläche muss eine übersichtliche Darstellung der Stammdaten und deren wesentlichen Attribute ermöglichen. Das System muss es berechtigten Nutzern ermöglichen, Stammdaten über eine grafische Benutzeroberfläche zu erstellen, zu bearbeiten, zu löschen und einzusehen. Die Erfassung aller in den Abschnitten 4.3.4.1 und 4.3.5.1 beschriebenen Attribute ist verpflichtend. Die Eingaben sind auf fachliche Konsistenz und Vollständigkeit zu prüfen.

4.3.3 Trennung der Mandanten

Die Stammdaten werden mandantenbezogen verwaltet, d.h. sie sind eindeutig einem Mandanten zugeordnet. Nutzer dürfen ausschließlich Stammdaten desjenigen Mandanten einsehen und bearbeiten, für den sie berechtigt sind.

4.3.4 Organisationsverwaltung

Die Organisationsverwaltung dient der Erfassung, Pflege und Konfiguration von Organisationen, die im Ticket-Ökosystem eines Verkehrsverbundes mit dem jeweiligen Mandanten interagieren.

Ziel der Organisationsverwaltung ist es, organisationsbezogene Informationen bereitzustellen, die für das Monitoring, die Validierung von Transaktionen sowie die fachliche Bewertung von Interaktionen zwischen Organisationen erforderlich sind.

Organisationen repräsentieren fachliche Akteure im Ticket-Ökosystem, insbesondere:

- Customer Contract Partner (CCP)
- Service Operator (SO)
- Product Owner (PO)

Nicht alle Organisationen sind für jeden Mandanten fachlich relevant. Die Einordnung erfolgt über die Produktakzeptanz wie beschrieben in Abschnitt 4.3.5.2.

4.3.4.1 Organisationsdefinition

Eine Organisation wird eindeutig über eine *OrgID* und etiCORE Rolle identifiziert und beschreibt einen fachlichen Akteur gemäß der etiCORE-Spezifikation.

Für jede Organisation müssen mindestens die folgenden Attribute in einer tabellarischen Übersicht verwaltet werden können:

- *OrgID*
- Rolle der Organisation, insbesondere CCP, SO und PO
- Kurzbezeichnung der Organisation
- StatAddress, (Angabe, ob eine statische oder dynamische Adresse vorhanden ist)
- Relevanz, (Angabe, ob die Organisation für den jeweiligen Mandanten relevant ist)

Die Felder OrgID, Rolle der Organisation und Kurzbezeichnung können nicht manuell geändert werden, sondern kommen aus der ((etiCORE OrganisationInformationList bzw. der ESH-Schnittstelle.

Der detaillierte fachliche und technische Aufbau einer Organisation ist nicht Bestandteil dieses Lastenheftes und wird vollständig durch die referenzierte etiCORE-Spezifikation beschrieben. Diese ist Bestandteil der Ausschreibungsunterlagen und verbindlich umzusetzen.

4.3.4.2 Weiterleitung an CCP deaktivieren

Nach ((etiCORE Spezifikation werden bestimmte *Notifications* an den jeweiligen primären CCP weitergeleitet. Diese Weiterleitung muss in der Ansicht zur Organisationsverwaltung aktiviert bzw. deaktiviert werden können. Das muss sowohl im Monitoring als auch in den Registern und Beständen berücksichtigt werden.

4.3.4.3 Detailansicht einer Organisation

Das System muss es Nutzern ermöglichen, aus der Übersicht auf eine Detailansicht einer Organisation zu wechseln.

Die Detailansicht muss mindestens folgende Informationen anzeigen:

- *OrgID*
- Organisationsbezeichnung und Kurzbezeichnung
- Rolle der Organisation
- Kontaktinformationen insbesondere eines technischen Ansprechpartners
- Konfigurationsattribute wie Relevanz, StatAddress und Weiterleitung an CCP

Die Detailansicht dient der vollständigen Einsicht in den Organisationsdatensatz und der gezielten Pflege einzelner Attribute.

4.3.5 EFM-Produktverwaltung

Die EFM-Produktverwaltung dient der Erfassung, Pflege und Bereitstellung von Produktinformationen. EFM-Produkte repräsentieren hierbei die Tarife und tariflichen Angebote, für die der Verkehrsverbund als Produktverantwortlicher agiert. Die im System gepflegten Daten zu den EFM-Produkten sind relevant für diverse Monitoring Prüfungen.

4.3.5.1 EFM-Produktdefinition

Für jedes EFM-Produkt müssen mindestens die folgenden Attribute in der Detailansicht verwaltet werden können:

- *ProductID*
- *ProductType*
- *ProductNumber*
- *OrgID* des Produktverantwortlichen
- Gültigkeitszeitraum
- Medienarten (z.B. Chipkarte, Barcode, NFC oder Motics Barcode, auch mehrere möglich pro EFM-Produkt)

- Bezeichnung
- Produktspezifischer Aufbau: *ProductParameters* und *ActionTariffParameters*
- *EntitlementIssuedMetaData*

Die *ProductID* besteht aus *OrgID*, *ProductType*, *ProductNumber*.

Der detaillierte fachliche und technische Aufbau eines EFM-Produktes ist nicht Bestandteil dieses Lastenheftes.

4.3.5.2 EFM-Produktakzeptanz

Zu jedem EFM-Produkt muss das System die Zuordnung des Produkts zu einem oder mehreren oder aller *CCP* oder *SO* ermöglichen. Es erfolgt die Zuordnung von Organisationen aus der im System bestehenden Organisationsverwaltung (Kapitel 4.3.4). Die Zuordnung wird dabei als sog. Produktakzeptanz bezeichnet und zeigt an, welche *CCP* das jeweilige Produkt ausgeben und somit auch im *HLS* sperren dürfen und welche *SO* das Produkt in der Kontrolle akzeptieren.

Die Zuordnung kann dabei zum einen produktübergreifend erfolgen, d.h. *CCPA* akzeptiert alle Produkte des *PO B*. Zum anderen kann die Zuordnung auch scharf auf Ebene der *Product-ID* erfolgen.

Auf Basis dieser Zuordnung wird das *HLS* konfiguriert und die Gesamtsperrrliste entsprechend gefiltert. Weitere Details dazu sind in Kapitel HLS-Produktkonfiguration (4.6.1) beschrieben. Dort ist auch eine beispielhafte Tabelle für die verschiedenen Arten der Zuordnung zu finden.

4.3.6 Zusätzliche Anforderungen für den nationalen Mandanten

Die VDV ETS betreibt für das Deutschland-Ticket einen nationalen Mandanten für das deutschlandweite Monitoring des Deutschland-Tickets wie beschrieben in Abschnitt 4.9. Dieser Mandant hat zusätzliche Anforderungen, die über die eines normalen Mandanten des Systems hinausgehen.

4.3.6.1 Zuordnung von regionalen Product Owner zu CCPs

Im nationalen Mandanten muss das System in den Stammdaten einer CCP-Organisation die Zuordnung zu 1-n PO Org-Ids für die Administratoren ermöglichen. Auf Basis dieser Zuordnung leitet das MPS die eingehenden Nachrichten des jeweiligen CCPs an den angegebenen PO weiter. Existieren mehrere dieser PO-Zuordnungen, muss in der Auflistung einer als primärer PO auswählbar sein. Der primäre PO erhält dann alle

Nachrichten, die nicht gesondert einem der weiteren PO zugeordnet werden. Diese Zuordnung erfolgt in der VDV-KA innerhalb der Ausgabetransaktion auf Basis des *berechtigungTarifbereichZusatz*. Die Entsprechung für das D-Ticket in ((etiCORE ist *entitlementIssuedMetadataExtension*.

4.4 Zugriff

4.4.1 SSO

MPS muss eine zentrale, sichere und standardisierte Benutzeranmeldung ermöglichen. Die Benutzer-Registrierung erfolgt in einem dritten System „Registration Portal“. MPS darf keine eigene Benutzer-Registrierung ermöglichen. Zu diesem Zweck muss das MPS vollständig in eine bestehende Keycloak Instanz integriert werden, um am Single Sign-On (SSO) teilzunehmen. Durch die Anbindung an Keycloak sollen Mandanten und deren Benutzer ohne separate lokale Benutzerverwaltung authentifiziert werden können.

MPS muss eine der folgenden durch Keycloak bereitgestellten Standardprotokolle unterstützen:

- OpenID Connect
- SAML

MPS muss in der Lage sein, die u.s. Infos aus dem AccessToken entsprechend bei der Authorization berücksichtigen

- Mandanten
- Rollen (siehe Kapitel 4.4.2)
- Benutzer

Diese Informationen müssen in dem MPS gespeichert werden zur Verwaltung von Benutzer und Mandanten (s. Kapitel 4.4.3 für die Benutzer und Mandantenverwaltung)

4.4.2 Benutzerrechte und Benutzerrollen

4.4.2.1 Übersicht

Rollen und Berechtigungen innerhalb des MPS gelten abhängig von der Rolle entweder:

- mandantenübergreifend (Systemebene) oder
- mandantenspezifisch (Mandantenebene).

Eine Trennung der Daten und Funktionen zwischen Mandanten ist sicherzustellen. Ausnahmen sind mandantenübergreifende Anwendungsfälle und konfigurierter Zugriff auf Teile des nationalen Mandanten.

Das System muss mindestens die folgenden Rollen unterstützen:

- Super-Administrator (mandantenübergreifend)
- Administrator (mandantenspezifisch)
- Nutzer (mandantenspezifisch)

Das System erhält die Information über die Rollen eines Benutzers aus dem SSO. Eine individuelle oder frei konfigurierbare Rollendefinition darüber hinaus ist nicht erforderlich. Die Rechtevergabe erfolgt ausschließlich rollenbasiert.

Das System muss sicherstellen, dass alle Rechte strikt gemäß der zugewiesenen Rolle durchgesetzt werden.

Die im System verwendeten technischen Rollen (Super-Administrator, Administrator, Nutzer) sind unabhängig von den fachlichen Rollen im Ticket-Ökosystem gemäß etiCORE-Spezifikation (z. B. Product Owner, Customer Contract Partner, Service Operator).

Die fachlichen Rollen und deren Beziehungen sind in der etiCORE Spezifikation beschrieben und sind nicht Bestandteil des Benutzerrechte- und Benutzerrollenmodells.

4.4.2.2 Super-Administrator

Super-Administratoren agieren auf Systemebene und sind nicht einem einzelnen Mandanten zugeordnet.

Das System muss folgende Rechte und Funktionalitäten für Super-Administratoren ermöglichen:

- Technische Überwachung des Gesamtsystems
- Fachliche Überwachung des Systems
- Zugriff auf Ansicht und Daten eines einzelnen Mandanten zu Supportzwecken

4.4.2.3 Administratoren

Administratoren sind einem konkreten Mandanten zugeordnet und verfügen über administrative Rechte innerhalb dieses Mandanten.

Das System muss folgende Rechte und Funktionalitäten für Administratoren ermöglichen:

- Administratoren müssen Zugriff auf alle Funktionen ihres Mandanten haben.

- Benutzerverwaltung über das ESH-System wie spezifiziert in Abschnitt 4.4.3.
- Konfiguration von (Cron) Jobs und HLS

Administratoren dürfen ausschließlich auf Daten und Funktionen ihres eigenen Mandanten zugreifen.

4.4.2.4 Nutzer

Nutzer sind einem Mandanten zugeordnet und stellen die regulären Anwender des Systems dar.

Nutzer müssen Zugriff auf alle fachlichen Funktionen des Systems haben, die zur Überwachung des Ticket-Ökosystems erforderlich sind.

Nutzer haben keinen Zugriff auf Konfiguration von (Cron) Jobs, kryptografischen Schlüsseln und HLS.

Nutzer dürfen keine Benutzerverwaltungs- oder systemadministrativen Funktionen ausführen.

Nutzer dürfen ausschließlich auf Daten ihres eigenen Mandanten zugreifen.

4.4.3 Benutzer- und Mandantenverwaltung

Die Registrierung sowie die Verwaltung der Mandanten und ihrer Nutzer werden vollständig durch das externe System ESH bereitgestellt und durchgeführt.

Das MPS muss über eine dedizierte Rest-Schnittstelle von ESH-Informationen zu Mandanten (wie z.B. u.a. Mandant Name, TenantId, OrgIDs) empfangen können. Auf Basis der über die ReST-Schnittstelle bereitgestellten Mandanteninformationen muss das MPS in der Lage sein, die entsprechenden Mandanten automatisiert anzulegen, temporär zu sperren und zu deaktivieren. Bei Deaktivierung müssen sämtliche Daten eines Mandanten archiviert werden. Die Archivierung darf keinen Datenverlust verursachen und muss revisionssicher erfolgen.

Das System ESH ist in das zentrale Single-Sign-On-System (SSO) Keycloak integriert. Die vollständige Benutzerverwaltung, einschließlich Authentifizierung und Autorisierung, erfolgt ausschließlich über Keycloak. MPS darf keine eigenständigen Benutzerkonten lokal führen, außer für technische Fallback-Szenarien (z. B. Systemadministration im Notfall).

Die Benutzerkonten müssen anhand von Informationen in Tokens (s. Kapitel 4.4.1) im MPS erstellt werden. Benutzerrollen und Berechtigungen werden im MPS dynamisch aus dem

Token übernommen. Änderungen an Rollen oder Attributen in Keycloak müssen sofort oder innerhalb eines definierten Refresh Intervalls wirksam werden. MPS darf keine sicherheitsrelevanten Daten (z. B. Passwörter) speichern.

Zur Absicherung dieser Schnittstelle muss das MPS eine gegenseitige TLS-Authentifizierung (mTLS) unterstützen.

In der Mandantenliste ist auch ETS zu finden. ETS arbeitet mandantenübergreifend und seine Mitarbeiter in der Regel als Super-Administrator.

4.5 Aktionsmanagement

Dieses Kapitel beschreibt die Integration des *Ordered Action Managements* in die Oberfläche des Systems.

4.5.1 Oberfläche: Konfiguration

Das System stellt für die Durchführung des Ordered Action Managements einen Bereich in der Benutzeroberfläche bereit. Dazu gehört die Konfiguration der *action list retrieval configuration*, die pro definiertem eCCP verwaltet werden muss. Diese Konfiguration wird an alle eCCP gesendet und enthält Information darüber ob und wann eine aktualisierte *Action List* zur Verfügung gestellt wird.

4.5.2 Oberfläche: Aktionslistenabruf

Das System stellt eine Übersicht der abgeholten Aktionslisten bereit. Diese Übersicht enthält folgende Informationen:

- Listennummer (*list cycle*)
- Zeitstempel (Zeitpunkt des Listenabrufs)
- CCP-Org-ID
- Detailansicht (Zeigt in einer weiteren Übersicht die enthaltenen Actions an)
- Export (das System stellt die jeweilige *Action List* als XML-Export bereit)

Die Übersicht muss die Suche nach bestimmten Einträgen ermöglichen.

4.5.3 Oberfläche: Order Inventory

Das System stellt eine Übersicht der im System registrierten Aktionsaufträge bereit.

Diese Ansicht repräsentiert die Daten aus dem Datastore *Order inventory*. Dieser Datenspeicher enthält alle im System vorhandenen aktiven Aktionsaufträge.

4.6 Sperrwesen

Das MPS muss mit dem Hotlist-Service (HLS) kommunizieren. Das umfasst den Bereich der Konfiguration sowie das Abholen und Übernehmen der Hotlists. Zusätzlich holt das MPS beim HLS regelmäßig den Report über korrekt abgeholte Hotlisten Seitens der Teilnehmer und wertet diesen aus.

Im Rahmen des Monitorings müssen Hotlisting-Demands (Sperranforderungen) gestellt werden, die an den Eigentümer der Entität zu richten sind. Bei Applikationen und Berechtigungen ist dies der primary Customer Contract Partner pCCP, bei SAMs kann der Eigentümer sowohl ein CCP als auch ein Service Operator (SO) sein. Ebenfalls an den Eigentümer der Entität gehen Hotlisting-Demand-Revocations (Aufhebungen von Sperranforderungen), die entweder unbeabsichtigte Sperranforderungen zurückziehen sollen oder im Rahmen von Klärfällen z.B. nach telefonischem Kontakt bestehende Sperranforderungen wieder aufheben können.

4.6.1 HLS-Produktkonfiguration

Die Produktkonfiguration legt im HLS eine Zuordnung fest, welche CCPs und SOs die Produkte des Mandanten akzeptieren (Akzeptanzkandidaten). Daraus resultiert:

- Die Entitlement-Hotlist wird vom HLS für den anfragenden CCP/SO entsprechend gefiltert und enthält nur Berechtigungen von unterstützten Produkten
- Der CCP kann nur Aufträge zu Entitlement-Hotlist-Einträgen stellen, wenn er das der Berechtigung zugrundeliegende Produkt in der HLS-Konfiguration akzeptiert

Dafür muss das MPS das HLS entsprechend konfigurieren.

Wie in 4.3.5.2 beschrieben, kann ein Mandant (PO) den Akzeptanzstellen per Organisations-ID des PO alle seine Produkte zuordnen, oder die Zuordnung auf einzelne Produkte beschränken.

Es gibt zusätzlich unterschiedliche räumliche Gültigkeiten von Produkten:

- Produkte für **lokal** begrenzte Berechtigungen: Diese Produkte sind nur in lokalen Tarifgebieten gültig und umfassen den Zuständigkeitsbereich von einem oder mehreren POs
- Produkte für **nationale** Berechtigungen (zurzeit das D-Ticket): Diese Produkte sind in ganz Deutschland gültig und müssen von jedem Verkehrsunternehmen akzeptiert werden. Daher erhält jedes abfragende Unternehmen hierzu alle Hotlist-Einträge

Bei Produkten für **lokal** begrenzte Berechtigungen sind Einträge auf der Hotlist nur für Verkehrsunternehmen interessant, bei denen das zugrundeliegende Produkt verwendet werden darf. Um die Hotlisten zu entlasten, werden die Hotlist-Einträge auf die Akzeptanzkandidaten gefiltert, so dass jedes teilnehmende Unternehmen nur die jeweils relevanten Hotlist-Einträge auf der Liste erhält.

Jeder Mandant (Product Owner, PO) muss dafür den Hotlist-Service entsprechend seiner Produkte und seiner teilnehmenden Unternehmen (SO + CCP) konfigurieren.

Bei Produkten für **nationale** Berechtigungen muss eine Konfiguration der Produkte nicht stattfinden. **Ausnahme:** eine Akzeptanzstelle (CCP) im Verbund des Mandanten vertreibt nur deutschlandweite Produkte, oder der Mandant ist nur für die Auswertung nationaler Berechtigungen zuständig. In dem Fall muss der Mandant alle relevanten Akzeptanzkandidaten konfigurieren. Somit muss insbesondere der zentrale Mandant alle Akzeptanzkandidaten (CCPs und SOs) mit Hilfe seiner Organisations-ID bei sich zuordnen. Hintergrund: Diese Information wird benötigt, wenn im Rahmen der Auswertung abgeholter Listen (siehe 4.6.7) die (zugeordneten) Akzeptanzkandidaten ausgewertet werden.

Die HLS-Konfiguration ist eng an die Produktverwaltung (siehe 4.3.5) gekoppelt. Die dort definierten Produkte müssen auch im HLS berücksichtigt werden. Des Weiteren ist auch die Organisationsverwaltung wichtig (siehe 4.3.4), da diese Grundlage ist für die Organisationen, denen Produkte zugeordnet werden sollen.

In der Stammdatenverwaltung ist die Zuordnung der SOs und CCPs zum PO-Mandanten festgelegt. Diese Zuordnung muss zusammen mit der Produktverwaltung als Grundlage für die HLS-Konfiguration dienen.

Dabei muss pro MPS-Mandanten eine Organisations-Produktzuordnung realisiert werden, die 1:1 der Konfiguration im HLS entspricht.

Wenn sich bei dieser Zuordnung etwas ändert, muss automatisch ein Abgleich an das HLS gesendet werden. Um dies sicher durchzuführen, wird vom HLS die Liste der aktuellen

Produktzuordnungen geholt und mit der internen Datenlage verglichen. Das Delta wird dann gebildet und in Form von Konfigurationsätzen an das HLS gesendet.

Zusätzlich zur automatischen Variante muss die Übertragung der Organisations-Produktzuordnung vom MPS an das HLS per Knopfdruck möglich sein (z.B. nach der ersten Erstellung der Zuordnung).

Die nachfolgende Tabelle zeigt ein Beispiel für einen MPS-Mandanten, dem als Akzeptanzkandidaten ein CCP mit der Organisations-ID 42 und ein SO mit der Organisations-ID 4711 zugeordnet sind. Der CCP akzeptiert alle Produkte des MPS-Mandanten, während der SO nur die Produkte 7, 9 und 13 akzeptiert. Damit würde der SO nur Hotlist-Einträge für Berechtigungen erhalten, denen die Produkte 7, 9, und 13 zugrunde liegen, während der CCP alle Produkte des MPS-Mandanten akzeptiert (alle Produkte, in denen als Organisations-ID der MPS-Mandant als PO eingetragen ist), die nicht einzeln aufgeführt werden müssen.

Organisation (Akzeptanzkandidat)	Rolle	Einzelprodukte 1..n	Alle Produkte
42	1 / CCP		Ja
4711	2 / SO	7, 9, 13	Nein

Die umzusetzenden Anwendungsfälle dazu sind

- *Add product acceptance entry to hotlist configuration* in [4]
- *Remove product acceptance entry from hotlist configuration* in [4]
- *Get product acceptance configuration list* in [4]

Wenn ein (Einzel-) Produkt von allen Akzeptanzkandidaten zu einem bestimmten Zeitpunkt entfernt werden soll (z.B. weil der Gültigkeitszeitraum ausläuft), so ist *Remove product acceptance from participants* in [4] zu verwenden.

4.6.2 Abholen von Hotlists

Jeder Mandant (PO) muss die für das PO-System vorgesehenen Hotlists abholen und in das Hotlist-Inventory überführen.

Die Häufigkeit und der Zeitpunkt muss Systemparameter steuerbar sein.

Folgende Hotlists sind pro Zyklus (zurzeit entspricht 1 Zyklus einem Tag in der Produktionsumgebung) abzuholen:

- Application-Hotlist (siehe [16])

- Entitlement-Hotlist
- Organisation-Hotlist
- SAM-Hotlist

Jeder Mandant muss die Informationen aus den Hotlists für einen konfigurierbaren Zeitraum (Default ist 7 Tage) in geeigneter Form aufheben. Insbesondere für das nachgelagerte Monitoring muss für untersuchte Nachrichten sichergestellt sein, dass für deren Zeitstempel die passenden Hotlists mit den entsprechenden Zyklen zur Verfügung stehen.

Der umzusetzende Anwendungsfall aus [4] ist

- *Update hotlist inventory from product perspective*

Hinweis: in der Staging-Umgebung ist die Zyklusdauer deutlich kürzer (zurzeit 15 Min). Das MPS muss also entsprechend konfigurierbar sein, so dass für die Staging-Umgebung die Hotlist-Informationen zur Verfügung stehen und ein geeignetes nachgelagertes Monitoring aufgesetzt werden kann.

4.6.3 Bestand an Hotlist-Einträgen (Hotlist-Inventory)

Das Hotlist-Inventory umfasst den Bestand der Hotlist-Einträge. Alle Arten von Hotlist-Einträgen werden gespeichert (siehe 4.6.2). Jede Hotlist ist mit einem Zyklus versehen, den das MPS in einer eigenen Entität abbildet (siehe 4.6.3.1). Diese Entität speichert die letzten 14 Zyklen mit entsprechender Referenz auf die einzelnen Hotlist-Einträge im Inventory. Auf diese Weise separiert das MPS die Datenbestände pro Zyklus im Inventory.

4.6.3.1 Zyklus, tabellarische Ansicht

Feld	Sortieren	Filter	Kurzbeschreibung	Anmerkung
Cycle-Number	X	X	Zyklus-ID für die Hotlists.	Der Zyklus gilt für alle Hotlist-Arten.
Cycle-Timestamp	X	X	Zeitstempel des Zyklus.	Alle Hotlist-Einträge mit einem Erfassungszeitpunkt < Cycle-Timestamp sind im Bestand enthalten.

4.6.3.2 Hotlist-Inventory, tabellarische Ansicht

Je nach Typ des Eintrages stellt das MPS nur die relevanten Felder dar.

Feld	Sortieren	Filter	Kurzbeschreibung	Anmerkung
Cycle-Number	X	X	Zyklus-ID für den Hotlist-Eintrag im Inventory. Referenz auf Zyklus-Entität.	Muss navigierbar sein zum Zyklus, siehe 4.6.3.1.
Hotlist-Entry Type	X	X	Typ des Hotlist-Entries	Typen sind Application, Entitlement, Organisation, SAM
Identifizier	X	X	Zusammen mit der Cycle-Number eine ID für den Hotlist-Entry	Application-Instance-ID, Entitlement-ID, Organisation-ID, SAM-ID
Blocking Mode		X	Sperrmodus des Eintrags	Nur für Berechtigungen und Applikationen
Transition Counter	X	X	Statuswechselzähler	Nur für Berechtigungen und Applikationen
SAM Action Counter	X	X	Aktionszähler des SAM	Nur für SAM-Einträge
SAM Entitlement Issuance Counter	X	X	Ausgabezähler des SAM	Nur für SAM-Einträge

4.6.4 Übertragung der Hotlist-Informationen in die Bestände

Wenn das MPS neue Hotlists abholt, aktualisiert es wie oben beschrieben das Hotlist-Inventory.

Gleichzeitig passt das MPS auch die Bestände (siehe 4.7.9) an.

Für jeden Eintrag (Berechtigung, Applikation, SAM), der sich auf den Hotlists befindet, wird der zugehörige Eintrag (Berechtigung, Applikation, SAM) im jeweiligen Bestand geprüft. Hat der Eintrag im Bestand einen der erlaubten Ausgangszustände (siehe Abbildung 13, Abbildung 14 und Abbildung 15), so wird der Status auf „Hotlisted“ gesetzt. Zusätzlich erfolgt dann ein Eintrag in die jeweilige Transition-Tabelle (siehe 4.7.10.1.3, 4.7.10.2.3 und 4.7.10.3.3), welche Hotlist (Zyklus-ID) zu welchem Zeitpunkt die Statusänderung des Bestands-Eintrags bewirkt hat. Bestands-Eintrag und Transition-Eintrag werden verknüpft. Folgende Verbindungen zwischen den Beständen und den Hotlists bestehen, bzw. werden dann per Transition-Eintrag verknüpft:

- Application-Hotlist
 - -> Eintrag in Historie des Applikations-Bestandes (Siehe [16], siehe 4.7.10.2), setzen des Bestand-Eintrags auf „(Application) Hotlisted“

- -> Eintrag in die Historie des Berechtigungsbestand für jede zugehörige Berechtigung, setzen des jeweiligen Bestand-Eintrags auf „Entitlement Hotlisted by Application“, siehe 4.7.10.1.
- Entitlement-Hotlist -> Eintrag in die Historie des Berechtigungsbestands, setzen des Bestand-Eintrags auf „Entitlement Hotlisted“, siehe 4.7.10.1
- SAM-Hotlist
 - -> Eintrag in die Historie des SAM-Bestandes, siehe 4.7.10.3 setzen des Bestands-Eintrages auf „Hotlisted“
 - -> Eintrag in die Historie des Berechtigungsbestand für jede zugehörige Berechtigung, setzen des jeweiligen Bestand-Eintrags auf „Entitlement Hotlisted by SAM“, siehe 4.7.10.1
- Organisation-Hotlist -> Dieser seltene Fall wird nicht betrachtet und muss händisch erfolgen.

4.6.5 Hotlisting-Demands (Sperranforderungen)

Im Monitoring entstehen bei den Prüfungen der Attestations aus den Notifications in bestimmten Situationen Hotlisting-Demands, die entweder für Berechtigungen, Applikationen oder SAM gestellt werden. Die Hotlisting-Demands können sowohl aus dem direkten Monitoring (immediate Checks) als auch aus dem nachgelagerten Monitoring (downstream Checks) entstehen.

4.6.5.1 Demand Application Hotlisting

Im Rahmen des Monitorings muss der Anwendungsfall *Demand application hotlisting* aus [4] umgesetzt werden. Wenn in den Monitoring-Prüfungen Inkonsistenzen auffallen, die auf die Applikation auf dem Nutzermedium (Chipkarte) hindeuten, so muss diese Applikation auf die Hotlist gesetzt werden (Beispiel: Status der Berechtigung nach dem Sperren ist nicht korrekt). Wurde ein Demand Application Hotlisting erfolgreich versendet und bestätigt, so müssen der eigene Applikations-Bestand (siehe 4.7.10.2) und die Statushistorie zur Applikation angepasst werden. Im passenden Bestand wird der Zustand auf „Hotlisting Demanded“ umgestellt. In der Historie erfolgt ein neuer Eintrag, der eine Referenz auf die gesendete Hotlisting Demand Nachricht erhält. Der Bestand für alle zugehörigen Berechtigungen wird in gleicher Weise angepasst. Der Zustand wird auf „Application hotlisting demanded“ gesetzt.

Hinweis: Im Direkten Monitoring führen bestimmte Prüfungen zu einem Hotlisting-Demand für eine Applikation. Das gilt für alle eingehenden Meldungen, die im Rahmen von *Handle Entitlement XX Notification from Product Perspective* (siehe [4]) verarbeitet werden.

Im nachgelagerten Monitoring führen folgende Anwendungsfälle potenziell zu *Demand application hotlisting* (siehe [4], Kap. 6.2):

- *Analyse entitlement history from product perspective*
- *Check entitlement notifications against issuance notification from product perspective*

4.6.5.2 Demand Entitlement Hotlisting

Im Rahmen des Monitorings muss der Anwendungsfall *Demand entitlement hotlisting* aus [4] umgesetzt werden. Im Umfeld der statischen Berechtigungen führen Inkonsistenzen in den Monitoring-Prüfungen dazu, dass diese Berechtigungen auf die Hotlist gesetzt werden müssen.

Wurde ein Entitlement Hotlisting Demand erfolgreich versendet und bestätigt, so müssen die Berechtigungsbestände (siehe 4.7.10.1) und die Statushistorie zur Berechtigung angepasst werden. Im passenden Bestand wird der Zustand auf „Hotlisting Demanded“ umgestellt. In der Historie erfolgt ein neuer Eintrag, der eine Referenz auf die gesendete Hotlisting Demand Nachricht erhält.

Hinweis: Im Direkten Monitoring führen bestimmte Prüfungen zu einem Hotlisting-Demand für eine Berechtigung. Das gilt für alle eingehenden Meldungen, die im Rahmen von *Handle Entitlement XX Notification from Product Perspective* (siehe [4]) verarbeitet werden.

Im nachgelagerten Monitoring führen folgende Anwendungsfälle potenziell zu *Demand entitlement hotlisting* (siehe [4], Kap. 6.2):

- *Check static entitlement notifications against issuance notification from product perspective*
- *Check static entitlement notifications for plausibility*

4.6.5.3 Demand SAM Hotlisting

Im Rahmen des Monitorings muss der Anwendungsfall *Demand SAM hotlisting* aus [4] umgesetzt werden. Dieser Anwendungsfall dient dazu, ein SAM bei festgestellten

Unregelmäßigkeiten beim Monitoring über den SAM-Besitzer auf die SAM-Hotlist setzen zu lassen.

Hat das MPS einen Demand SAM Hotlisting erfolgreich versendet und bestätigt, so müssen der SAM-Bestand (siehe 4.7.10.3) und die Statushistorie zum SAM angepasst werden. Im passenden Bestand wird der Zustand auf „Hotlisting Demanded“ umgestellt. In der Historie erfolgt ein neuer Eintrag, der eine Referenz auf die gesendete Hotlisting Demand Nachricht erhält.

Der Bestand für alle zugehörigen Berechtigungen wird in gleicher Weise angepasst. Der Zustand wird auf „SAM hotlisting demanded“ gesetzt.

Hinweis: Im nachgelagerten Monitoring führen folgende Anwendungsfälle potenziell zu *Demand SAM hotlisting* (siehe [4], Kap. 6.2):

- *Analyse entitlement history from product perspective*
- *Monitor SAMs from product perspective*

4.6.6 Hotlisting Demand Revocations (Sperraufhebungsanforderungen)

Als Gegenstück zu den Hotlisting Demands in Kap. 4.6.5 können Aufhebungsanforderungen gestellt werden. Damit kann manuell ein Hotlisting Demand bei einem Drittsystem rückgängig gemacht werden. Denkbar ist das durch Bearbeitung eines Klärfalles, siehe Kap. 4.2.5.3.

Hinweis: ein Zurücknehmen einer Sperranforderung für ein SAM ist nicht möglich.

4.6.6.1 Revoke Entitlement Hotlisting Demand

Dafür ist der Anwendungsfall *Revoke Entitlement Hotlisting Demand* aus [4] umzusetzen. Dieser Anwendungsfall kann im Rahmen eines Klärfalles aufgerufen werden. Eine Berechtigung im Bestand (siehe 4.7.10.1) wird mit diesem Anwendungsfall nach erfolgreichem Senden der Nachricht und der Bestätigung durch das Drittsystem wieder auf den Zustand *Entitlement OK* zurückgesetzt.

4.6.6.2 Revoke Application Hotlisting Demand

Dafür ist der Anwendungsfall *Revoke Application Hotlisting Demand* aus [4] umzusetzen. Dieser Anwendungsfall kann im Rahmen eines Klärfalles aufgerufen werden. Eine

Applikation im Bestand (siehe 4.7.10.2) wird mit diesem Anwendungsfall nach erfolgreichem Senden der Nachricht und der Bestätigung durch das Drittsystem wieder auf den Zustand *OK* zurückgesetzt.

4.6.7 Auswerten der Reports über abgeholte Hotlisten

Dieser Report erlaubt es dem MPS-Mandanten, für seine zugeordneten Organisation zu überprüfen, ob die Pflicht der regelmäßigen Abholung von Hotlists erfüllt wird. Dieser Report muss abhängig von der Zyklus-Konfiguration (in der Produktionsumgebung täglich) im Hotlist-Service regelmäßig vom MPS beim Hotlist-Service geholt werden.

Dazu muss der Anwendungsfall *Get unclaimed list information* (siehe [4], Kap 6.2.4) umgesetzt werden.

Das Ergebnis muss in einer geeigneten Entität gespeichert und dann ausgewertet werden. Die folgende Tabelle erklärt nur die Inhalte und stellt nicht unbedingt die gewünschte technische Umsetzung dar. Es muss pro Feld gefiltert und sortiert werden können.

Feld	Kurzbeschreibung	Anmerkung
Participant	Organisations-ID und Rolle des Teilnehmers (CCP oder SO), der dem MPS-Mandanten zugeordnet ist	Fremdschlüssel auf Organisation und Rolle in Kap. 4.3.4
Unclaimed List	Typ der Liste, die nicht abgeholt wurde, siehe auch <code>UnclaimedListTypeEnum</code> in [12]	
List Cycle Number	Zugehöriger Zyklus	
List Cycle Timestamp	Zugehöriger Zeitpunkt des Zyklus	
Status	Status für den Eintrag. Möglich sind „Offen“, „Gemeldet“ und „Geklärt“	Über den Status ist sichtbar, wie der Bearbeitungszustand im MPS ist, siehe unten
Text	Freitextfeld zum Eintragen einer Anmerkung, z.B. der Nummer des Tickets aus dem Ticket-System (z.Z. JIRA)	Idealerweise bietet die Schnittstelle zum Ticket-System die Übernahme der Ticket-ID

Per Konfiguration eines Schwellwertes pro Participant (z.B. 3 Zyklen für N offene Einträge) muss es möglich sein, dass das MPS den Benutzer benachrichtigt. Der MPS-Benutzer muss dann ein JIRA-Ticket gegen den Participant stellen können.

Zustände:

- „Offen“: der Eintrag ist seit der Übernahme in das MPS-System noch nicht bearbeitet worden

- „Gemeldet“: Gegen den Participant wurde ein JIRA-Ticket gestellt (optional)
- „Geklärt“: Der Fall ist geklärt, die Ursache ist behoben. Der direkte Statusübergang von „Offen“ auf „Geklärt“ ist erlaubt (z.B. Telefonat).

4.7 Register und Bestände

Das System stellt verschiedene Register und Bestände bereit, die strukturierte Sichten auf die im System verarbeiteten Daten ermöglichen.

Die Daten in den Registern und Beständen sind grundsätzlich den Mandanten (auch dem nationalen) zugeordnet. Wurden über das AssistanceCenter (siehe 4.9.3.1) Zuordnungen über weitere Organisationen gemacht, so können auch deren Daten aus dem nationalen Mandanten zusammen mit den Daten des aktuellen PO-Mandanten angezeigt werden.

Die Register dienen als Datengrundlage für Monitoring und manuelle Recherche und ermöglichen die Nachvollziehbarkeit von Tickets, Notifications und Prozessen sowie der Analyse von Fehlern, Inkonsistenzen und Abweichungen von den in der etiCORE-Spezifikation definierten Regeln. Weiter können diese Daten auch Grundlage für andere fachliche Nutzung sein wie z.B. die Überprüfung der Kontrollpflicht eines Dienstleisters.

Die Register stellen fachliche Sichten auf Systemdaten dar und nehmen keine zusätzliche fachliche Bewertung oder Interpretation vor.

Bestände sind aus den Registern abgeleitete Datenbestände einer Entität (Berechtigung, Applikation oder SAMs), deren virtuelle Zustände von äußeren Ereignissen geändert werden (Hotlisting, Sperren, Entsperren, etc.). Im Bestand ist somit immer der zuletzt bekannte Zustand einer Berechtigung, Applikation oder eines SAMs sichtbar.

4.7.1 Allgemein

Der Zugriff auf die Register und Bestände erfolgt mandantenweit für alle Nutzer eines Mandanten. Detaillierte Regelungen zu Rechten und Rollen sind im Abschnitt 4.4.2 beschrieben.

Jedes Register und jeder Bestand werden in einer tabellarischen Übersicht dargestellt. Die einzelnen Spalten der Tabelle sind von jedem Nutzer dynamisch konfigurierbar, d.h. Spalten können ein- bzw. ausgeblendet werden. Die getätigten Einstellungen sollen erhalten bleiben, bis sie vom Nutzer selbst geändert werden.

- Die tabellarischen Übersichten unterstützen Sortier- und Filterfunktionen für alle dargestellten Datenfelder.

- Einträge werden auch dann angezeigt, wenn einzelne Datenfelder leer, unvollständig oder fehlerhaft sind.
- Für jedes Register und jeden Bestand besteht die Möglichkeit, die Daten, welche den aktuellen Filterkriterien entsprechen in ein CSV-Format zu exportieren.
- Aus der tabellarischen Übersicht kann in eine Detailansicht einzelner Datensätze gewechselt werden.
- Bei zusammengesetzten Datentypen (z.B. Entitlement ID) können alle Felder einzeln in der Detailansicht betrachtet werden

4.7.2 ION-Nachrichtenregister (ION-Message Registry)

Das ION-Nachrichtenregister bildet sämtliche Interaktionen zwischen dem System und anderen Teilnehmern im ION. Es speichert alle ein- und ausgehenden Nachrichten, welche das MPS in Richtung ION sendet oder vom ION erhält.

Hinweis: Eine Anfrage entspricht in der ION-Spezifikation einem *Request*, eine Rückmeldung entspricht einer *Reply*. Die Rückmeldung kann entweder eine (reguläre) Antwort sein (ION: *Response*) oder eine Ausnahme/Exception (ION: *Business Exception*).

Das ION-Nachrichtenregister speichert nur reguläre ION-Nachrichten. Laufzeitfehler und unerwartete Ausnahmen werden nicht im Nachrichtenregister gespeichert. Sie werden im Systemlogging festgehalten.

Die ION-Nachrichten bestehen aus mehreren Anteilen (siehe auch [2]). Für die nachfolgenden Kapitel sind diese Anteile relevant und werden kurz erklärt:

1. Sicherheitsrelevante Anteile, z.B. Security-Header, (ION-)Signatur
2. Routing- und Identifikationsanteile (ION Message ID, Zeitstempel, Empfänger, Service)
3. Die Fachnachricht, meistens eine Notification (Meldung über Ausgabe, Kontrolle, Sperrung, etc.)
4. Innerhalb der Fachnachricht (wenn Notification) eine Attestation (signierter Anteil mit Transaktionsnachweis zu Ausgabe, Kontrolle, Sperrung, etc.)

Die Anteile 1 und 2 sind nur im Umfeld der ION-Kommunikation relevant, die Anteile 3 und 4 werden im Rahmen von Monitoring und Auswertungen weiterverarbeitet.

4.7.2.1 Nachrichtentypen in ION-Nachrichtenaustausch-Szenarien

Folgende Nachrichtentypen ergeben sich aus der ION-Spezifikation mit MPS als Initiator oder Processor (siehe [2], Kap. 2) und müssen als eigenständige Registereinträge geführt werden:

- Eingehende synchrone Anfrage (MPS ist Processor und Server)
- Direkt gesendete synchrone Antwort oder Exception (MPS ist Processor und Server)
- Eingehende asynchrone Anfrage (MPS ist Processor und Server)
- Ausgehende asynchrone Antwort oder Exception (MPS ist Processor und Client)
- Ausgehende synchrone Anfrage (MPS ist Initiator und Client)
- Direkt empfangene eingehende Antwort oder Exception (MPS ist Initiator und Client)
- Ausgehende asynchrone Anfrage (MPS ist Initiator und Client), z.B. bei Weiterleitung von Meldungen
- Eingehende asynchrone Antwort oder Exception (MPS ist Initiator und Server)

4.7.2.2 ION-Nachrichten-Zustände

Je nach Nachrichtentyp (siehe 4.7.2.1) können sich unterschiedliche Zustände ergeben, die auch ggf. das ION-Monitoring triggern (siehe 4.2.5). Die nachfolgenden Diagramme zeigen die Statusübergänge bei den entsprechenden Nachrichtentypen.

Status für Anfrage	Anmerkung
Sent	MPS als Initiator: Anfrage gesendet
Acknowledged	MPS als Initiator: Empfang vom Endpunkt bestätigt
Acknowledged by CRE	MPS als Initiator: Empfang von CRE bestätigt
Rejected	MPS als Initiator: Empfang von Gegenseite abgelehnt (relevant für ION-Monitoring)
Direct Timeout	MPS als Initiator: Direkter Timeout beim Senden (Retry anstoßen, bei Misserfolg relevant für das ION-Monitoring)
Error	MPS als Initiator: Unerwarteter Laufzeitfehler beim Empfang auf der Gegenseite (relevant für ION-Monitoring)
Response-Related	MPS als Initiator: Anfrage beantwortet und mit Antwort verknüpft
Exception-Related	MPS als Initiator: Anfrage beantwortet und mit Exception verknüpft (relevant für ION-Monitoring)
SLA-Timeout	MPS als Initiator: Keine Antwort nach X (konfigurierbar) Tagen (relevant für ION-Monitoring)
Received	MPS als Processor: Anfrage empfangen
Response-Related	MPS als Processor: Zu Anfrage wurde reguläre Antwort gesendet (final)
Exception-Related	MPS als Processor: Zu Anfrage wurde Exception gesendet (final)

Status für Rückmeldung	Anmerkung
Request-Correlated	MPS als Initiator: Die eingegangene Rückmeldung wurde mit der ursprünglichen Anfrage verknüpft (final)
Request-Correlated with Error	Im Falle einer synchronen Rückmeldung besteht nicht die Möglichkeit, diese Rückmeldung abzulehnen. Falls die Empfängerdaten nicht korrekt sind oder die Korrelations-ID (originalRequestCorrelationId) der Rückmeldung nicht zum Request passt oder die Korrelations-ID bereits im MPS existiert, entsteht dieser Status. Durch den synchronen Kontext kann die Rückmeldung trotzdem implizit dem Request zugordnet werden (siehe Abbildung 7). Es handelt sich aber um einen Klärfall im Sinne des ION-Monitorings (siehe 4.2.5).
Sent	MPS als Processor: asynchrone Rückmeldung gesendet
Acknowledged	MPS als Processor: Empfang vom Endpunkt bestätigt (final)
Acknowledged by CRE	MPS als Processor: Empfang von CRE bestätigt
Rejected	MPS als Processor: Empfang von Gegenseite abgelehnt (relevant für ION-Monitoring)
Direct Timeout	MPS als Processor: Direkter Timeout beim Senden der Rückmeldung (Retry anstoßen, bei Misserfolg relevant für das ION-Monitoring)
Error	MPS als Processor: Unerwarteter Laufzeitfehler beim Empfang der Rückmeldung auf der Gegenseite (relevant für ION-Monitoring)
Request-Correlated	MPS als Processor: Zustand einer gesendeten Rückmeldung, die mit der zuvor eingegangenen Anfrage verknüpft wurde (final)

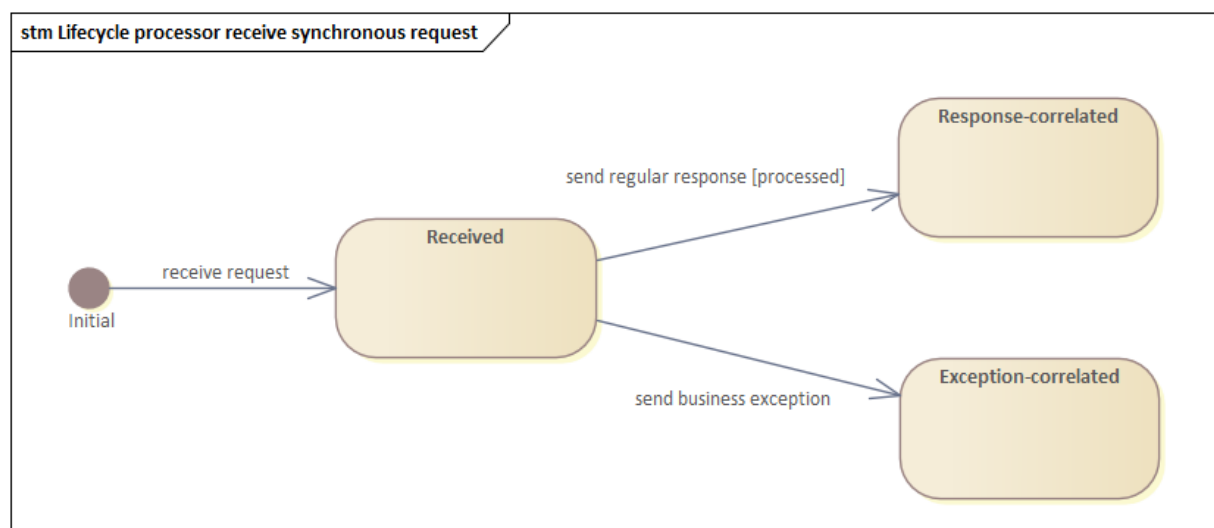


Abbildung 1: Statusübergänge einer empfangenen synchronen Anfrage

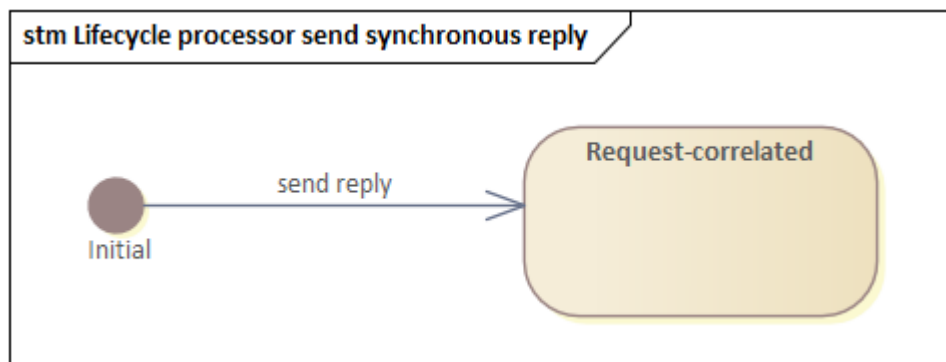


Abbildung 2: Statusübergänge einer gesendeten synchronen Rückmeldung

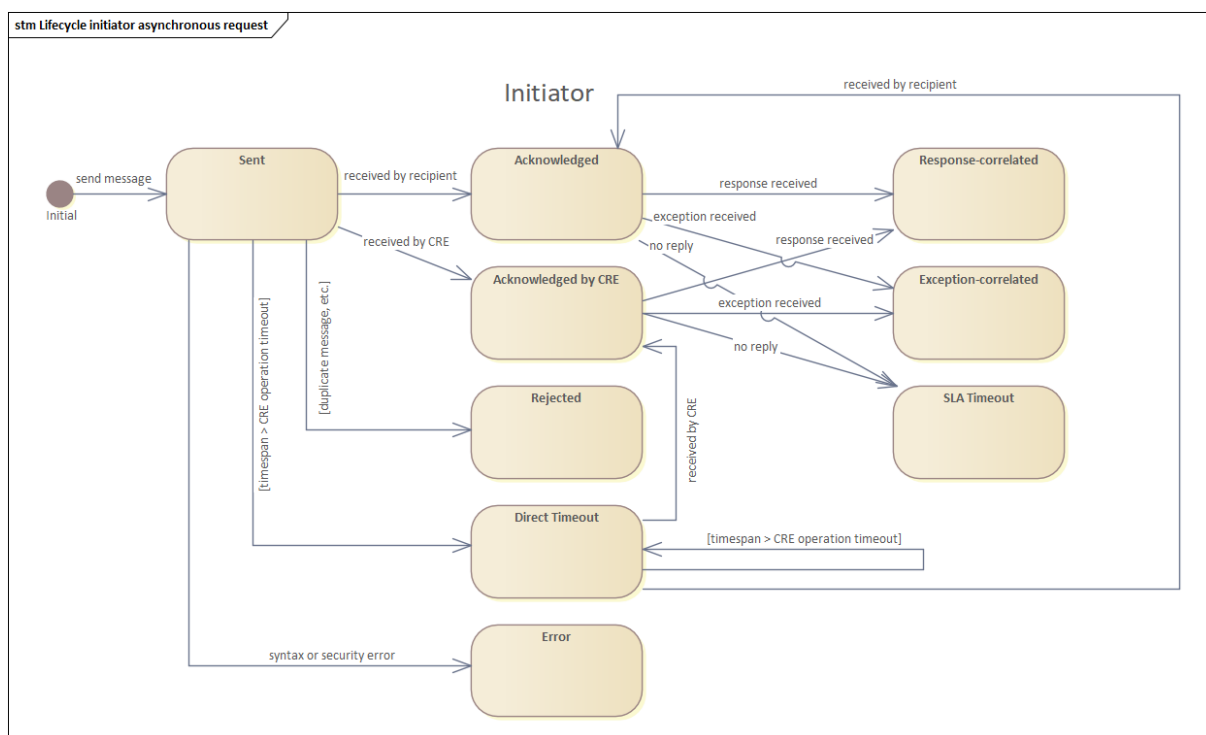


Abbildung 3: Statusübergänge einer gesendeten asynchronen Anfrage

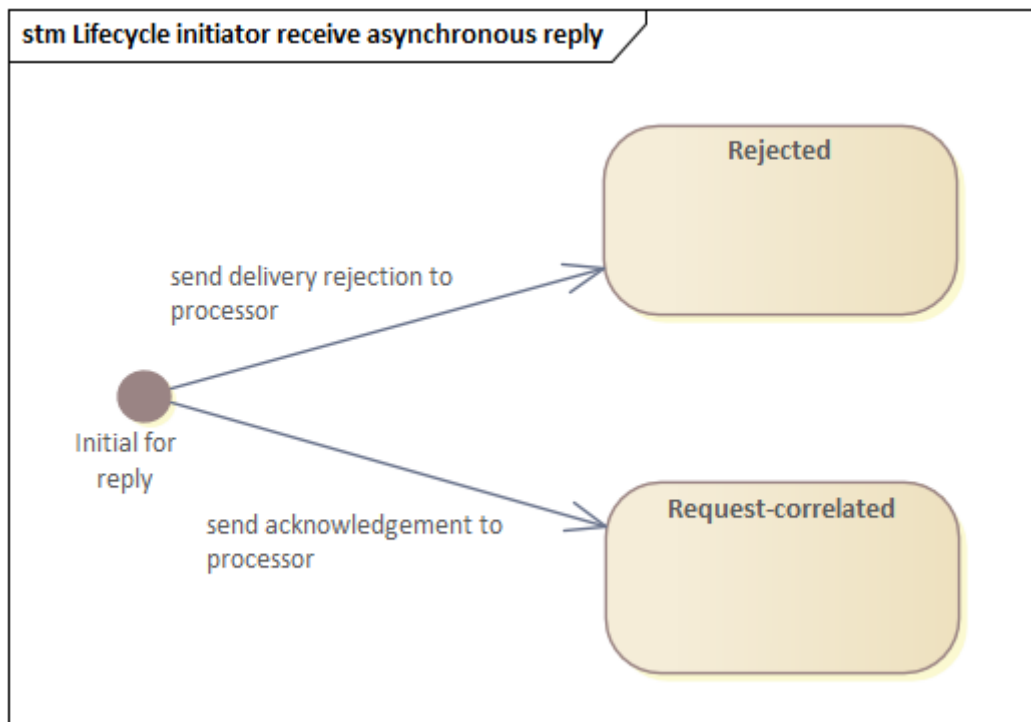


Abbildung 4: Statusübergänge einer empfangenen asynchronen Rückmeldung

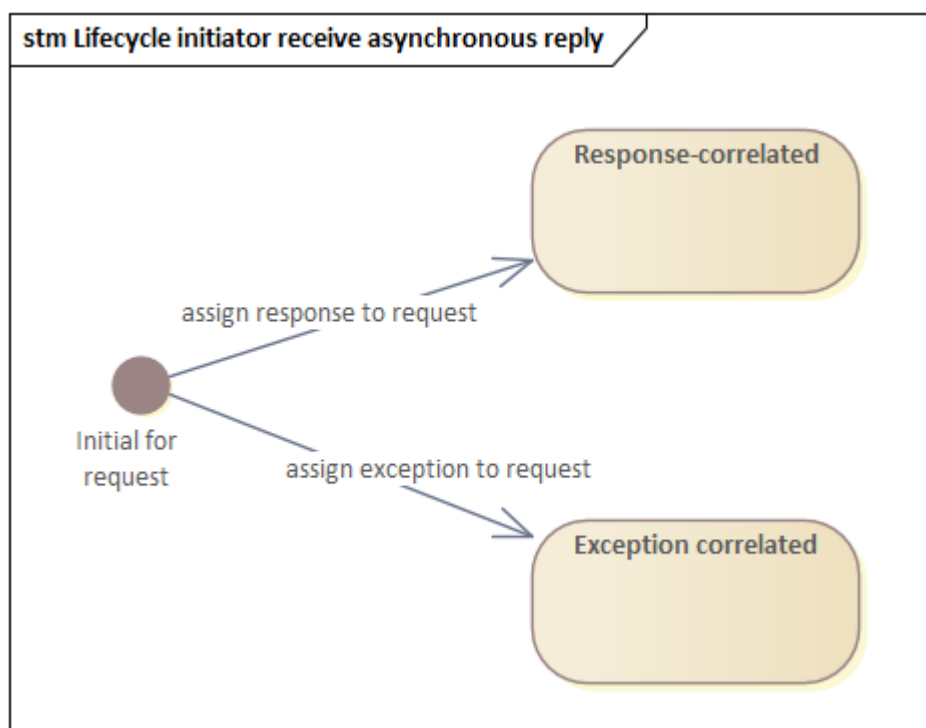


Abbildung 5: Statusübergänge der asynchronen Anfrage nach Verarbeitung und Zuordnung der Rückmeldung

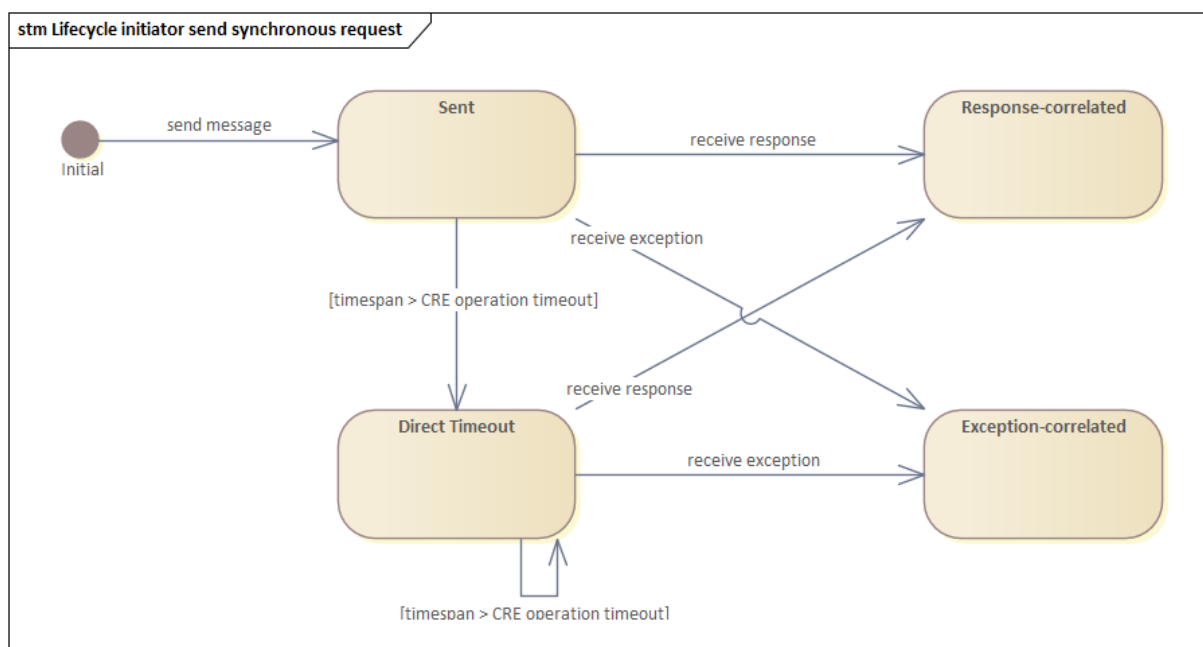


Abbildung 6: Statusübergänge einer gesendeten synchronen Anfrage

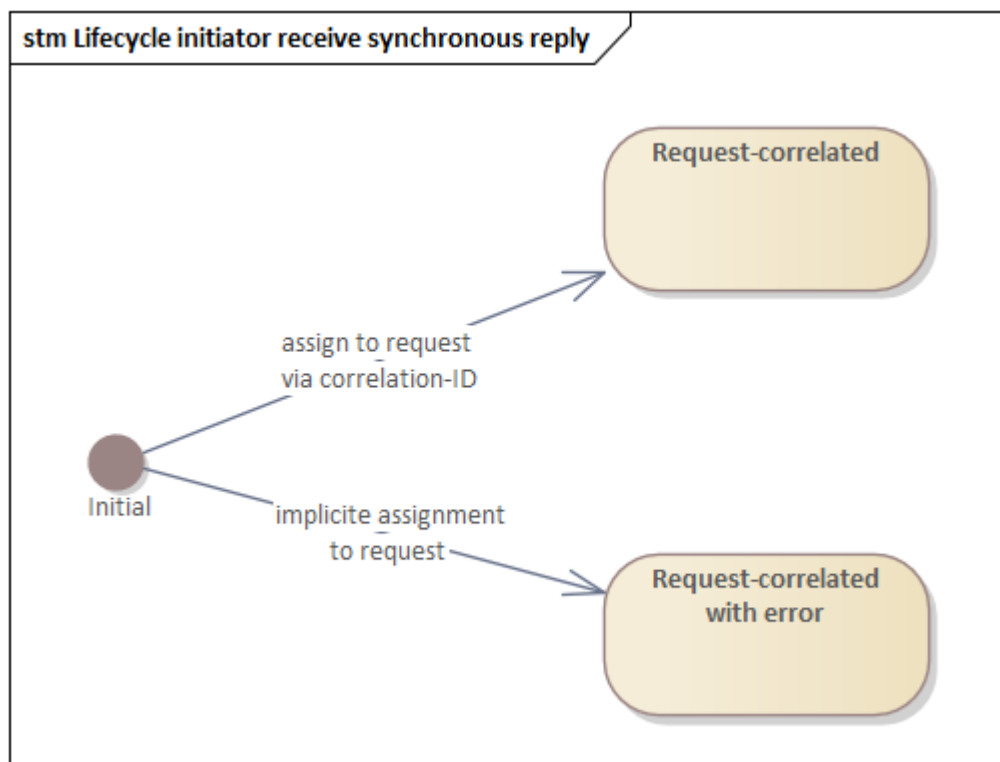


Abbildung 7: Zuordnung einer synchronen Rückmeldung

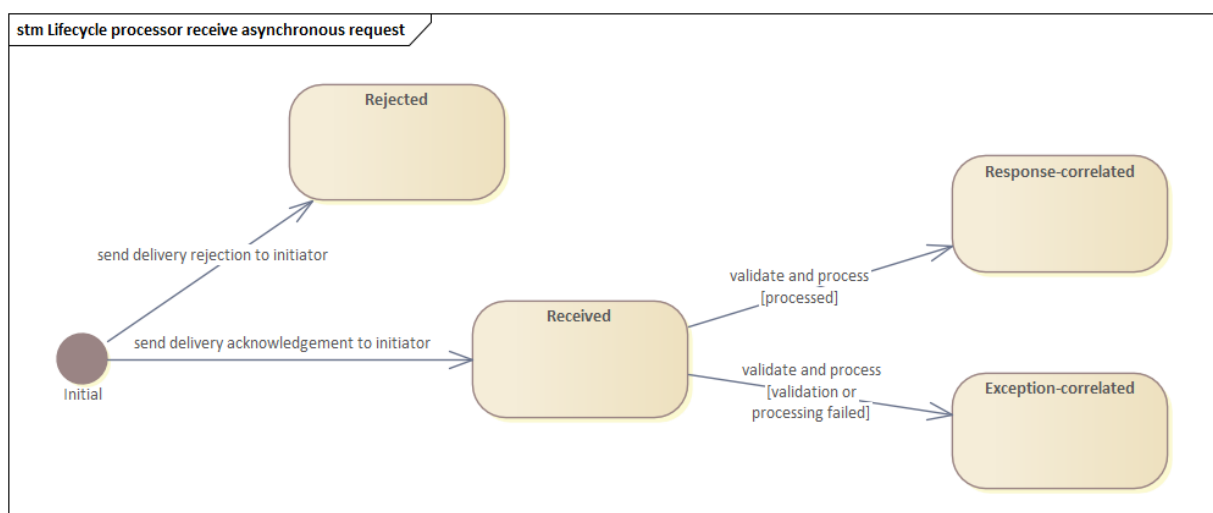


Abbildung 8: Statusübergänge einer empfangenen asynchronen Anfrage

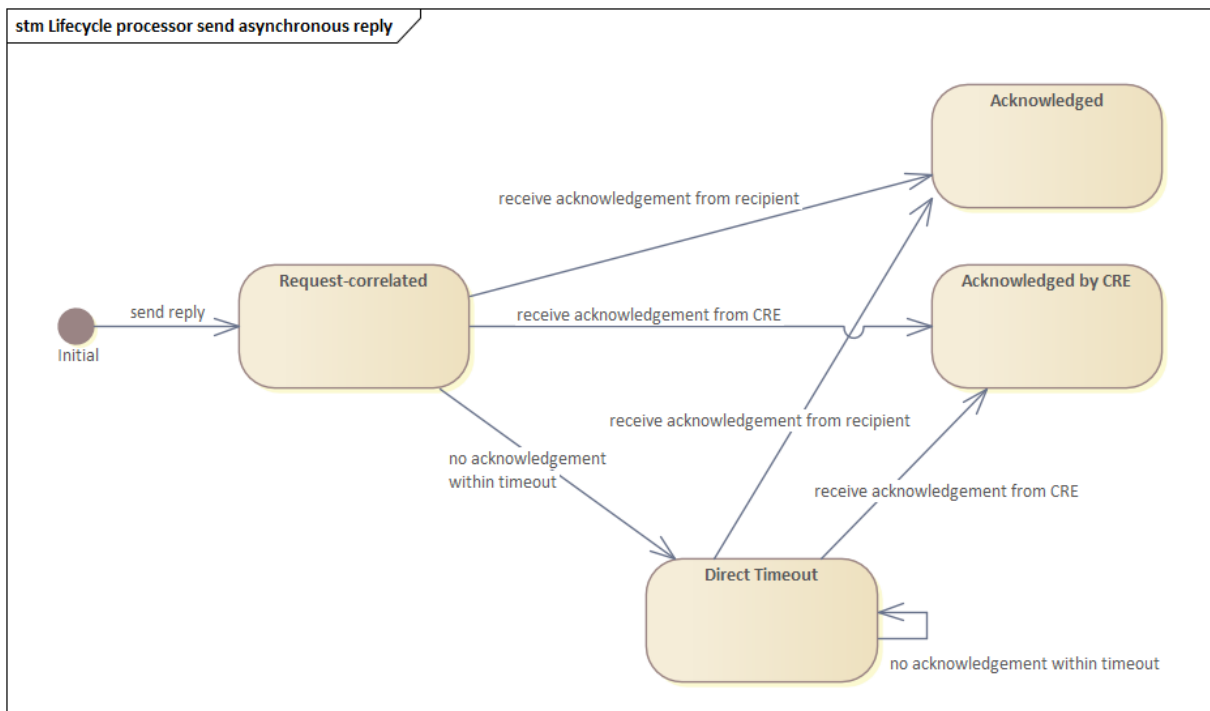


Abbildung 9: Statusübergänge einer gesendeten asynchronen Rückmeldung

4.7.2.3 Grundsätzliche Funktionalität

Es müssen folgende grundsätzliche Funktionalitäten durch das Nachrichten-Register bereitgestellt werden:

- Festhalten der jeweiligen asynchronen Teilnachrichten und der entsprechenden Bestätigung (deliveryAcknowledgement) oder Ablehnung (deliveryRejection) sowohl als Initiator als auch als Processor
- Verknüpfung von Anfrage und Rückmeldung (Antwort oder Exception) in allen beschriebenen Szenarien (aufgrund möglicher Fehlerfälle darf diese Verknüpfung nicht bzw. nicht ausschließlich über die ION-Message-ID erfolgen)
- Historie für die Wiederholung von Nachrichten bei Timeout
- Basis für Reports, ION-Monitoring und sonstige Anwendungsfälle, siehe auch Kap. 4.2.5 und 4.2.6.

Das Nachrichten-Register ist als Persistenz-Schicht umzusetzen.

4.7.2.4 Fachliche ION-Nachrichtentypen

Das MPS unterscheidet folgende fachliche Nachrichtentypen:

- (Eingegangene) Notification, ggf. mit Timeout Warnung
- (Eingegangene) Notification-Liste für Ausgaben, Kontrollen und Erfassungen (CICO)
- (Eingegangene) Notification aus Aktionsmanagement, ggf. mit Timeout Warnung
- (Eingegangene) Notification aus Aktionsmanagement (Timeout)
- (Eingegangene) Notification über einen Abbruch (nur bei Ausgabe einer Berechtigung)
- (Eingegangener) Auftrag zur Ausführung einer Aktion
- (Eingegangener) Auftrag zum Löschen einer Aktion
- (Eingegangene) Anfrage zum Senden einer Aktionsliste
- (Eingegangene) Aufträge zur Konfiguration der Hotlists
- (Gesendete) Weiterleitung von Notifications
- (Gesendete) Weiterleitung von Notifications für das Aktionsmanagement
- (Gesendete) Konfiguration für das Aktionsmanagement
- (Gesendeter) Hotlisting Demand
- (Gesendete) Hotlisting Demand Revocation
- (Gesendete) Konfiguration für den Hotlist-Service
- (Gesendete) Hotlist-Abrufe
- (Gesendete) Monitoring Nachricht
- (Gesendete) Nachrichten zum An- und Abmelden der Dienste
- Sonstige

4.7.2.5 Timeout der Transaktion auf dem UM und Abbrüche

Das MPS nimmt Timeouts (Warnungen in den Meldungen) und echte Abbrüche (nur bei Ausgabemeldung einer Berechtigung) entgegen und kennzeichnet diese entsprechend.

Die Timeouts mit Warnungen überführt das MPS in die passenden Register, um dort das nachgelagerte Monitoring (Cron-Job) zu ermöglichen. Dieser Cron-Job untersucht, ob die Timeout-Warnungen noch gerechtfertigt sind. Ergibt die Datenlage, dass die Transaktion auf dem UM durchgeführt wurde, so werden die Warnungen in den Registern jeweils gelöscht.

Der in ((etiCORE spezifizierte und umzusetzende Anwendungsfall dazu ist

- *Resolve notifications with timeout warnings*

Siehe auch [4].

4.7.2.6 Tabellarische Ansicht und Filterung

Die Visualisierung des Nachrichtenregisters erfolgt über eine Filterfunktion, welche dann zunächst eine Übersicht anzeigt, bei der nicht alle vorhandenen Felder der Nachricht gezeigt werden.

Durch Wählen einer Detailansicht (pro Zeile möglich) sind dann alle Felder anzuzeigen – auch die aus der Übersicht. Nachfolgende Tabelle zeigt die Felder und gibt an, ob diese in der Übersicht oder in der Detailansicht gezeigt werden. Zusätzlich ergeben sich Informationen („Zusatzinfo“), die sich aus dem logischen Kontext ergeben (z.B. ein virtueller Status, siehe auch 4.7.2.2).

Je nach ION-Nachrichtentyp (siehe 4.7.2.1) sind nicht alle Felder in der Übersicht oder in der Detailansicht gefüllt. Wenn die Felder aufgrund des ION-Nachrichtentyps „not applicable (n.a.)“ sind, so ist dies zu kennzeichnen, um diese Felder von leeren Feldern (z.B. bei optionalen Feldern) zu unterscheiden.

Alle unten aufgeführten Felder müssen sortierbar und filterbar sein, außer die Felder, die ausschließlich für die Detailansicht vorgesehen sind.

Feld	Kurzbeschreibung	Übersicht	Detail	Zusatz-Info	Anmerkung
Message Registry ID					Eindeutiger Schlüssel auf Eintrag. Wird für Referenzbeziehungen benötigt
Message Name	Verständlicher Name des Vorgangs, z.B. „Ausgabe Berechtigung“	X	X		
Technical Name	Name des Nachrichtenelements, z.B. notifyEntitlementIssued		X		
Message Type	Art der Nachricht in verständlicher Form, z.B. „Meldung“	X	X	X	Siehe 4.7.2.4
ION-Message Type	ION-Nachrichtentyp in verständlicher Form, z.B. „Asynchrone Anfrage“		X	X	Siehe 4.7.2.1
Action Timestamp	Zeitpunkt der (Trans)aktion auf dem Nutzermedium	X	X		
Retrieval Timestamp	Zeitpunkt des Eingangs der ION-Nachricht	X	X		
Sender-ID	Organisations-ID des Senders der Nachricht	X	X		

Feld	Kurzbeschreibung	Übersicht	Detail	Zusatz-Info	Anmerkung
Sender-Role	Rolle des Senders der Nachricht		X		
Sender-Service	Service des Senders als Abkürzung, z.B. ccp		X		Siehe entsprechende Aufzählung bei ion-enums.xsd in [12]
Receiver-ID	Empfänger-Organisations-ID	X	X		
Receiver-Role	Empfänger-Rolle als Rollen Code	X	X		Siehe ion-communication.xsd in [12]
ION-Message-Number	Identifiziert die ION-Nachricht zusammen mit Organisations-ID, Rolle und Service	X	X		Bildet zusammen mit Sender-Organisation, Sender-Rolle und Sender-Service die ION-Message-ID. Inhalt kann numerisch sein oder ein String, z.B. eine UUID
Repeat-Counter	Wiederholzähler für die Nachricht. Zeigt an, dass eine asynchrone Rückmeldung nicht vorhanden ist.		X		Wenn Wiederholung (>0), dann Referenz(en) auf bestehende Nachricht(en) beachten
Process-Instance-ID	ID für den gesamten Basic Process. Z.B. IssueEntitlement_<UUID>		X		Für Meldungen vom Terminal wird diese ID dort erzeugt und beibehalten. Für Hotlisting-Demands erzeugt das MPS die ID
Status	Status der Nachricht, z.B. „Received“	X	X	X	Siehe 4.7.2.2
Warning exists	Zeigt an, ob in der Nachricht Warnungen enthalten sind.	X	X		Wenn gefüllt, in Detailansicht zu öffnen. Warnungen können sowohl in Anfragen als auch Rückmeldungen enthalten sein
Fachdaten	TLV-Datensatz und XML-Metainformationen geparkt in geeigneter Ansicht. Ggf. Warnungen		X		Bei Details muss sich dazu eine eigene Ansicht öffnen. Bei eigenem Register Sprung dorthin
Application Instance ID	Applikations-Instanz-ID, auf die sich die aktuelle Nachricht bezieht	X	X		Aus den Fachdaten extrahiert, wenn dort vorhanden

Feld	Kurzbeschreibung	Übersicht	Detail	Zusatz-Info	Anmerkung
Entitlement-ID	Berechtigungs-ID, auf die sich die aktuelle Nachricht bezieht	X	X		Aus den Fachdaten extrahiert, wenn dort vorhanden
Bei Rückmeldungen					
Reference to Request	Bestimmt durch den Status „Request-Correlated“	X	X	X	siehe 4.7.2.2 Muss navigierbar sein
Acknowledgement	Bestimmt durch den Status „Acknowledged“ und „Rejected“, siehe 4.7.2.2 Inhalt z.B. „OK“ und „Not OK“	X	X	X	Nur bei asynchronen Nachrichten, eigene Ansicht bei Details, wo auch Zeitstempel und ggf. Fehlercode angezeigt werden.
Bei Anfragen					
Reference to Reply	Bestimmt durch den Status „Response-Correlated“ oder „Exception-Correlated“ (Referenz vorhanden)	X	X	X	siehe 4.7.2.2 Muss navigierbar sein
Bei Notification-Listen					
Reference to Extracted List	Je nach Art der Liste muss das MPS die zugehörigen Einträge im Ausgaberegister, Kontrolldatenregister oder Nutzungsregister anzeigen können		X		Muss navigierbar sein.

4.7.2.7 Detailansicht

Für jede Nachricht steht eine Detailansicht zur Verfügung.

Vollständige XML-Strukturen der Nachricht sollen abstrahiert dargestellt werden, um die Lesbarkeit zu erleichtern. Auf Wunsch muss das MPS diese Daten als XML-Struktur darstellen können („pretty print“ Format mit Einrückungen). Ebenfalls muss ein Export der Daten möglich sein. Das gilt insbesondere auch, wenn die ION-Nachricht eine (gepackte) Liste von Notifications beinhaltet (), oder im Antwortkontext eine Hotlist geliefert wurde. In diesen Fällen muss die entpackte Liste als XML exportiert werden können.

Soweit vorliegend, sind Fachdaten immer vollständig in der Detailansicht zu finden.

Werden diese dort angewählt, so kommt es darauf an, ob es hierfür ein eigenes Register gibt. Wenn ja, so wird der passende Eintrag im Register geöffnet (mit Navigationsmöglichkeit dorthin), wenn nein, so wird eine übersichtliche Ansicht der Felder und Werte gezeigt.

Insbesondere bei Notifications sind einzelne Felder (Attestations) im Original binär codiert (TLV-Format in DER Codierung). Der fachliche Inhalt wird dann sowohl in einer lesbaren Klartextdarstellung als auch in der Form angezeigt, in der er technisch übermittelt wurde, beispielsweise in Base-16-Kodierung.

Sind in den Fachdaten wiederum Listen (z.B. Warnungen, etc.) oder hierarchische Strukturen enthalten, so sind diese in geeigneten Unteransichten darzustellen.

Ansicht zu Nachrichtenbestätigungen (deliveryAcknowledgement) oder Ablehnungen (deliveryRejection): Hier muss der Zeitpunkt festgehalten werden, wann die Bestätigungen oder Ablehnung erfolgt ist. Zusätzlich muss bei Bestätigungen ersichtlich sein, ob die Bestätigung von der CRE oder vom Teilnehmersystem kam (wird durch den virtuellen Status „Acknowledged“ oder „Acknowledged by CRE“ abgebildet).

Sind in der entsprechenden ION-Nachricht Event-Codes enthalten (Fehler oder Warnung), so kann gemäß 4.10.5 auf Knopfdruck die Zusatzinformation zu diesem Event-Code abgerufen und in der Detailansicht dargestellt werden.

4.7.2.8 Datenübertragung in die Unterregister und Bestände

Wie beim Hotlist-Inventory, (siehe 4.6.4) muss das MPS für das Übertragen von Nachrichtenanteilen in die zustandsbehafteten Bestände (siehe 4.7.9) sorgen. Während das ION-Nachrichtenregister den Nachrichtenaustausch festhält, sollen die Unterregister und Bestände die fachliche Arbeit und das Monitoring im Hinblick auf die Nachrichteninhalte unterstützen.

Wie in 4.7.2 beschrieben, werden bestimmte Nachrichten in die Register und Bestände übertragen. In dem Fall handelt es sich um eingehende Notifications mit eingebetteten Attestations.

Nachfolgende Aufzählung zeigt, welche Notifications in welche Register und Bestände einfließen

- Notification über Ausgabe einer Berechtigung:
 - Anlegen eines Datensatzes im Ausgaberegister
 - Anlegen eines Datensatzes im Berechtigungsbestand
 - Anlegen eines Datensatzes für die Statushistorie mit Referenz auf das Ausgaberegister und die ION-Nachricht
 - Wenn noch nicht vorhanden, Anlegen eines Datensatzes im Applikations-Bestand bzw. in der Statushistorie

- Wenn noch nicht vorhanden, Anlegen eines Datensatzes im SAM-Bestand bzw. in der Statushistorie
 - Wenn die Notification aufgrund der Ausführung einer Aktion entstanden ist, so wird über die enthaltene Order-ID bzw. Order-Number die Aktionsliste (siehe 4.5) angepasst
- Notification-Liste über die Ausgabe von Berechtigungen
 - Für jeden Eintrag in der Liste
 - Anlegen eines Datensatzes im Ausgaberegister mit Referenz auf die ION-Nachricht mit der Notification-Liste
 - Anlegen eines Datensatzes im Berechtigungsbestand
 - Anlegen eines Datensatzes für die Statushistorie mit Referenz auf das Ausgaberegister und die ION-Nachricht mit der Notification-Liste
- Notification über Kontrolle einer Berechtigung
 - Anlegen eines Datensatzes im Kontrollregister
 - Ändern des Datensatzes im Berechtigungsbestand (Action Counter)
 - Anlegen eines Datensatzes für die Statushistorie mit Referenz auf das Kontrolldatenregister und die ION-Nachricht
 - Ggf. Anlegen eines Datensatzes im SAM-Bestand bzw. in der Statushistorie
- Notification-Liste über Kontrolle von Berechtigungen
 - Für jeden Eintrag in der Liste
 - Anlegen eines Datensatzes im Kontrollregister mit Referenz auf die ION-Nachricht mit der Notification-Liste
 - Ändern des Datensatzes im Berechtigungsbestand (Action Counter)
 - Anlegen eines Datensatzes für die Statushistorie mit Referenz auf das Kontrolldatenregister und die ION-Nachricht mit der Notification-Liste
 - Ggf. Anlegen eines Datensatzes im SAM-Bestand bzw. in der Statushistorie
- Notification über Erfassung einer Berechtigung
 - Anlegen eines Datensatzes im Nutzungsregister
 - Ändern des Datensatzes im Berechtigungsbestand (Action Counter)
 - Anlegen eines Datensatzes für die Statushistorie mit Referenz auf das Nutzungsregister und die ION-Nachricht
 - Ggf. Anlegen eines Datensatzes im SAM-Bestand bzw. in der Statushistorie
- Notification-Liste über das Erfassen von Berechtigungen

- Für jeden Eintrag in der Liste
 - Anlegen eines Datensatzes im Nutzungsregister mit Referenz auf die ION-Nachricht mit der Notification-Liste
 - Ändern des Datensatzes im Berechtigungsbestand (Action Counter)
 - Anlegen eines Datensatzes für die Statushistorie mit Referenz auf das Nutzungsregister und die ION-Nachricht mit der Notification-Liste
 - Ggf. Anlegen eines Datensatzes im SAM-Bestand bzw. in der Statushistorie
- Notification über die Sperrung einer Berechtigung
 - Anlegen eines Datensatzes im Meldungsregister für Berechtigungen
 - Ändern des Datensatzes im Berechtigungsbestand (Action Counter, Transition Counter, Status)
 - Anlegen eines Datensatzes für die Statushistorie mit Referenz auf die ION-Nachricht
 - Ggf. Anlegen eines Datensatzes im SAM-Bestand bzw. in der Statushistorie
- Notification über das Entsperren einer Berechtigung
 - Anlegen eines Datensatzes im Meldungsregister für Berechtigungen
 - Ändern des Datensatzes im Berechtigungsbestand (Action Counter, Transition Counter, Status)
 - Anlegen eines Datensatzes für die Statushistorie mit Referenz auf die ION-Nachricht
 - Ggf. Anlegen eines Datensatzes im SAM-Bestand bzw. in der Statushistorie
 - Wenn die Notification aufgrund der Ausführung einer Aktion entstanden ist, so wird über die enthaltene Order-ID bzw. Order-Number die Aktionsliste (siehe 4.5) angepasst
- Notification über das Terminieren einer Berechtigung
 - Anlegen eines Datensatzes im Meldungsregister für Berechtigungen
 - Ändern des Datensatzes im Berechtigungsbestand (Action Counter, Transition Counter, Status)
 - Anlegen eines Datensatzes für die Statushistorie mit Referenz auf die ION-Nachricht
 - Ggf. Anlegen eines Datensatzes im SAM-Bestand bzw. in der Statushistorie

- Wenn die Notification aufgrund der Ausführung einer Aktion entstanden ist, so wird über die enthaltene Order-ID bzw. Order-Number die Aktionsliste (siehe 4.5) angepasst
- Notification über den Abbruch einer Berechtigungsausgabe
 - Anlegen eines Datensatzes im Register für Ausgabeabbrüche von Berechtigungen

4.7.3 Register für Applikationsstatus (Application Status Registry)

Dieses Register wird mit [16], CR-407 “((etiCORE: Applikations-Monitoring und defekte Medien beim PO“ notwendig.

Für das erweiterte Applikations-Monitoring (siehe 4.12) werden Statusmeldungen für Applikationen mit Zustand ungleich „OK“ notwendig, durch die das MPS weiß, welche der Applikation zugeordneten Berechtigungen betroffen sind.

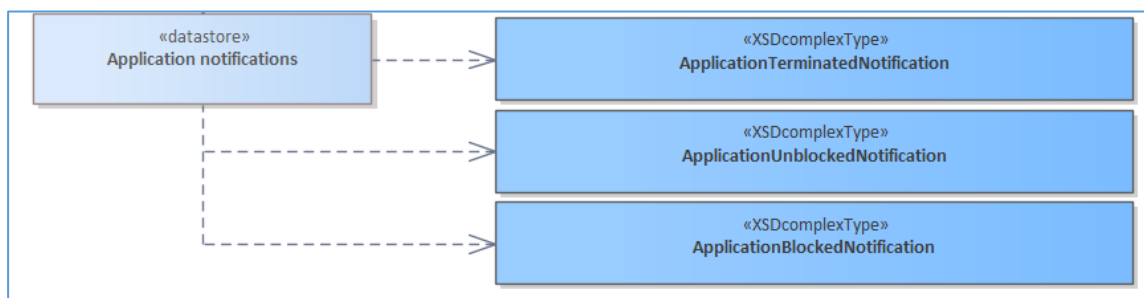


Abbildung 10: Meldungen für Applikationen

Abbildung 10 zeigt die unterschiedlichen Notifications für Applikationen, die mit [16] in das zentrale ESH einlaufen (nicht in das MPS). Diese Notifications dokumentieren jeweils eine Statusänderung, die im ESH festgehalten wird. Das MPS holt regelmäßig die aufbereitete Statusliste vom ESH und speichert die Einträge in der Application Status Registry, siehe 4.7.3.1. Dieser sich jeweils im MPS ergebende Status ist wichtig für das vollständige Monitoring von den Applikationen zugeordneten Berechtigungen (siehe 4.12).

Das MPS gleicht alle einlaufenden Meldungen für Statusänderungen mit dem Applikationsbestand ab (siehe 4.7.10.2). Zusätzlich bewirken die Registereinträge neue Einträge in den entsprechenden Statushistorien von Applikationen und Berechtigungen. Die nachfolgende Aufzählung beschreibt, was durch die jeweilige Zustandsänderung im MPS geschieht.

- Application Terminated: Die Applikation wurde endgültig zurückgegeben und kann nicht mehr verwendet werden. Alle zugehörigen Berechtigungen im Bestand (falls

noch vorhanden) sind dann als terminiert (Terminated By Application) zu kennzeichnen. Es erfolgt ein zusätzlicher Eintrag in die Statushistorie der Applikation, siehe 4.7.10.2.3. Es erfolgt jeweils ein zusätzlicher Eintrag in die Statushistorie der betroffenen Berechtigungen, siehe 4.7.10.1.3.

- **Application Blocked:** Die Applikation wurde gesperrt und kann nicht verwendet werden. Alle zugehörigen Berechtigungen im Bestand (falls vorhanden) sind dann als gesperrt (Blocked by Application) zu kennzeichnen, sofern sie einen geeigneten Ausgangszustand haben. Es erfolgt ein zusätzlicher Eintrag in die Statushistorie der Applikation, siehe 4.7.10.2.3. Es erfolgt jeweils ein zusätzlicher Eintrag in die Statushistorie der betroffenen Berechtigungen, siehe 4.7.10.1.3.
- **Application Unblocked:** Die Applikation wurde entsperrt und kann wieder verwendet werden. Diese Zustandsänderung zeigt sich aus nachvollziehbarkeitsgründen ebenfalls in der Liste vom ESH. Alle zugehörigen durch den alten Eintrag noch gesperrten Berechtigungen im Bestand (falls vorhanden) sind dann auf OK zurückzusetzen. Es erfolgt ein zusätzlicher Eintrag in die Statushistorie der Applikation, siehe 4.7.10.2.3. Es erfolgt jeweils ein zusätzlicher Eintrag in die Statushistorie der betroffenen Berechtigungen, siehe 4.7.10.1.3.

4.7.3.1 Tabellarische Ansicht

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Application Status Registry ID				Eindeutiger Schlüssel auf Eintrag	Wird für Referenzbeziehungen benötigt
Application Instance ID		X		Applikations-Instanz ID	
Application Transition Counter		X		Zustandsänderungszähler der Applikation	
Application Status		X		Status der Applikation	„Gesperrt“, „Terminiert“ oder „Entsperrt“ (Blocked, Terminated, Unblocked)
Action Timestamp	X	X		Zeitpunkt der Aktion der Zustandsänderung	
Eintrag Applikations-Bestand			X	Referenz auf den passenden Eintrag im Bestand der Applikationen	Muss navigierbar sein

4.7.3.2 Detailansicht und Verknüpfungen

Für die Applikations-Status-Einträge steht eine Detailansicht zur Verfügung. In oben aufgeführter Tabelle sind die Felder markiert, die ausschließlich in der Detailansicht sichtbar sind. Das MPS muss diese Felder aufarbeiten, so dass die Ansicht für den Benutzer verständlich ist und einen Mehrwert bietet. In der Detailansicht kann zusätzlich auf den Eintrag im Applikationsbestand (siehe 4.7.10.2) navigiert werden.

Alle oben aufgeführten Felder sind zusätzlich in der Detailansicht verfügbar.

4.7.4 Meldungsregister für Berechtigungen (Entitlement Notification Registry)

Dieses Register umfasst alle Notifications, die im Umgang mit Berechtigungen auftreten können (auch statische Berechtigungen und Berechtigungen aus dem Aktionsmanagement). Die nachfolgenden Register in 4.7.5, 4.7.7 und 4.7.8 (das Register für Abbrüche in 4.7.6 ist ein Sonderfall) sind Spezialregister dieses allgemeinen Registers. Trifft im Nachrichtenregister eine ION-Nachricht mit den Fachdaten einer Notification für Berechtigungen ein, so muss das MPS diese hier in geeigneter Form ablegen. Über einen Typ ist anzuzeigen, um welche Notification es sich handelt.

Für das in ((etiCORE spezifizierte Monitoring werden verschiedene Teilmengen aus diesem Register benötigt, die über die dedizierten Register aus 4.7.5, 4.7.7 und 4.7.8 hinausgehen. Das MPS muss diese Teilmengen durch geeignete Filter erzeugen können.

Abbildung 11 und Abbildung 12 zeigen die im Spezifikationsmodell definierten Notifications, die im Zusammenhang mit Berechtigungen auftreten können. Nachfolgend ist aufgeführt, ob die Notifications im allgemeinen Register oder in einem speziellen Register zu führen sind

- Entitlement Issued Notification -> Ausgaberegister
- Ordered Entitlement Issued Notification -> Ausgaberegister
- Static Entitlement Issued Notification -> Ausgaberegister
- Entitlement Issuing Aborted Notification -> Register für Ausgabeabbruch von Berechtigungen
- Static Entitlement Issuing Aborted Notification -> Register für Ausgabeabbruch von Berechtigungen
- Entitlement Inspected Notification -> Kontrolldatenregister
- Static Entitlement Inspected Notification -> Kontrolldatenregister

- Entitlement Blocked Notification -> Allgemeines Meldungsregister
- Ordered Entitlement Blocked Notification -> Allgemeines Meldungsregister
- Entitlement Unblocked Notification -> Allgemeines Meldungsregister
- Ordered Entitlement Unblocked Notification -> Allgemeines Meldungsregister
- Entitlement Terminated Notification -> Allgemeines Meldungsregister
- Ordered Entitlement Terminated Notification -> Allgemeines Meldungsregister
- Static Entitlement Terminated Notification -> Allgemeines Meldungsregister
- Entitlement Validated Notification -> Wenn umgesetzt: Allgemeines Meldungsregister
- User Tariff Parameters Changed Notification -> Wenn umgesetzt: Nutzungsregister
- Check-In Notification -> Wenn umgesetzt: Nutzungsregister
- Check-Out Notification -> Wenn umgesetzt: Nutzungsregister
- Account Based Payment Method Credited Notification -> Wenn umgesetzt: Allgemeines Meldungsregister
- Account Based Payment Method Debited Notification -> Wenn umgesetzt: Allgemeines Meldungsregister
- Stored Value Payment Method Debited Notification -> Wenn umgesetzt: Allgemeines Meldungsregister
- Stored Value Payment Method Credited Notification -> Wenn umgesetzt: Allgemeines Meldungsregister
- Stored Value Payment Method Reimbursed Notification -> Wenn umgesetzt: Allgemeines Meldungsregister
- Stored Value Payment Method Recharged Notification -> Wenn umgesetzt: Allgemeines Meldungsregister



Abbildung 11: Mögliche eingehende Notifications für Berechtigungen

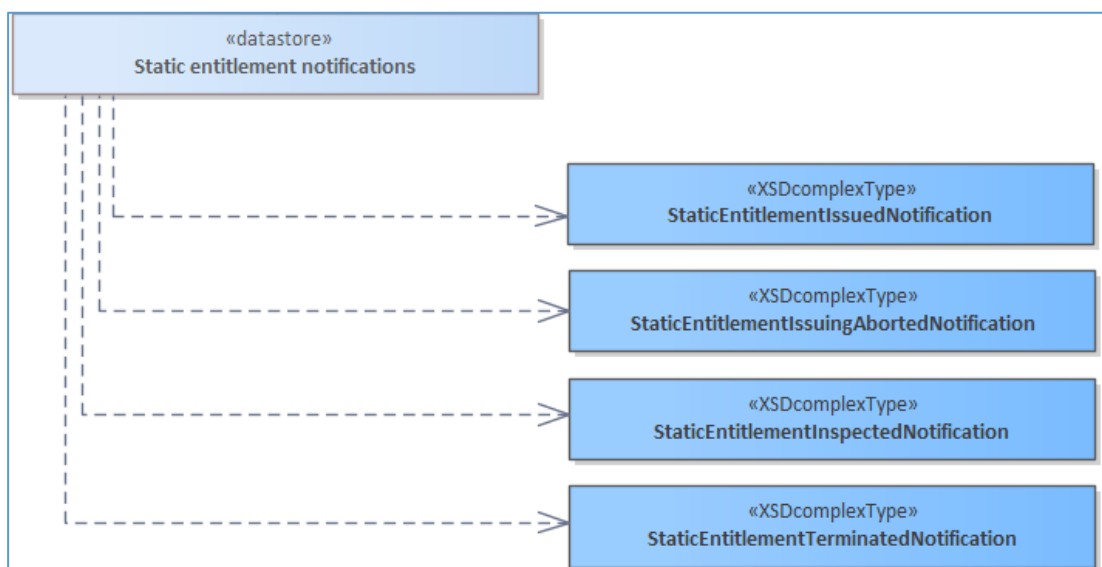


Abbildung 12: Mögliche eingehende Notifications für statische Berechtigungen

4.7.4.1 Tabellarische Ansicht

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Entitlement Registry ID				Eindeutiger Schlüssel auf Eintrag	Wird für Referenzbeziehungen benötigt
Spec Version	X	X		Verwendete Version der UM Spezifikation.	Wichtig für Zusammensetzung der Attestation und als Parser Information
Product-ID	X	X	X	Product-ID mit Product-Owner, Product Type und Product Number	Product Type zeigt, ob es sich um electronic Ticket, statische Berechtigung oder Payment Method handelt. Betrachten der einzelnen Felder in Details.
Entitlement-ID	X	X	X	Entitlement-ID mit ID des Herausgebers der Berechtigung (CCP-Organisation-ID), SAM-ID des ausgebenden SAMs, SAM Issuance Counter als Entitlement Number	Betrachten der einzelnen Felder in Details.
Order Number		X		Auftragsnummer aus dem Aktionsmanagement	Wenn die Meldung über das Aktionsmanagement stattgefunden hat.
Entitlement Status	X	X		Status der Berechtigung zum Zeitpunkt der Meldung	Der Status muss zur Fachlichkeit passen und ist Teil des Monitorings. Hier z.B. „OK“

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Application Instance ID	X	X	X	Applikations-Instanz-ID der Applikation, auf der die Berechtigung ausgegeben wurde	Betrachten der einzelnen Felder in Details.
Action Timestamp	X	X		Zeitpunkt der Ausgabe	
Terminal-ID	X	X		ID des Ausgabeterminals	
Operator-ID	X	X		Organisations-ID des Terminal-Betreibers	
Location-ID	X	X		ID des Ortes der Ausgabe	
Stored Value Current Balance			X	Aktueller auf der Karte verfügbarer Betrag	Optional, nur wenn Produkttyp SVPM entspricht.
Stored Value Maximum Balance			X	Auf der Karte maximal erlaubter Betrag	Optional, nur wenn Produkttyp SVPM entspricht.
Stored Value Autoload Threshold			X	Schwellwert des aktuellen Betrages auf der Karte, ab wann per Autoload automatisch aufgebucht wird	Optional, nur wenn Produkttyp SVPM entspricht.
Stored Value Autoload Amount			X	Betrag, der via Autoload automatisch aufgebucht wird	Optional, nur wenn Produkttyp SVPM entspricht.
Action Tariff Parameters			X	Tarifliche Informationen zur Action mit der Berechtigung	Muss für die Detailansicht aufbereitet werden
actionAmount	X	X		Betrag in der Aktion in Eurocent. Positiv oder negativ	Nur bei Payment
Vat Rate			X	Steuersatz für Kaufaktion	Nur bei Payment
Action Payment Parameters			X	Bei ((et)CORE konformen Ticket: Berechtigungs-ID und Produkt-ID, sonst Hexstring	Parameter für die Zahlung (erworbenes Ticket). Nur bei Payment
Warnung		X	X	0..N Warnungen, die an der Berechtigung hängen können	In der Übersicht muss gekennzeichnet sein, dass Warnungen vorliegen.
Eintrag Berechtigungs-Bestand			X	Referenz auf den passenden Eintrag im Berechtigungsbestand (4.7.10.1)	Muss navigierbar sein
ION-Message			X	Referenz auf die ION-Message zu diesem Registereintrag	Muss navigierbar sein. Es kann sich auch um eine Notification-Liste handeln.

4.7.5 Ausgaberegister (Issuance Registry)

Das Ausgaberegister bildet alle im System erfassten Ausgaben von Berechtigungen ab. Das MPS überträgt einkommende Nachrichten zu Berechtigungsausgaben in das Ausgaberegister. Zusätzlich legt das MPS einen neuen Datensatz für den Berechtigungs-Bestand an (siehe 4.7.10.1).

4.7.5.1 Tabellarische Ansicht

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Issuance Registry ID				Eindeutiger Schlüssel auf Eintrag	Wird für Referenzbeziehungen benötigt
Spec Version	X	X		Verwendete Version der UM Spezifikation.	Wichtig für Zusammensetzung der Attestation und als Parser Information
Product-ID	X	X	X	Product-ID mit Product-Owner, Product Type und Product Number	Product Type zeigt, ob es sich um electronic Ticket, statische Berechtigung oder Payment Method handelt. Betrachten der einzelnen Felder in Details.
Entitlement-ID		X	X	Entitlement-ID mit ID des Herausgebers der Berechtigung (CCP-Organisation-ID), SAM-ID des ausgebenden SAMs, SAM Issuance Counter als Entitlement Number	Betrachten der einzelnen Felder in Details.
Product Issuance Counter			X	Aktueller Zähler von Ausgaben pro SAM für den Product Owner des ausgegebenen Produkts.	Fortlaufend, ohne Lücken
Order Number		X		Auftragsnummer aus dem Aktionsmanagement	Wenn die Ausgabe über das Aktionsmanagement stattgefunden hat oder die Berechtigung über einen Massenpersonalisierer stattgefunden hat.
Entitlement Effective Time	X	X		Gültigkeitsbeginn der Berechtigung	
Entitlement Expiration Time	X	X		Gültigkeitsende der Berechtigung	Abgelaufene Berechtigungen sind zu kennzeichnen und nach einem konfigurierbaren Zeitraum aus den Registern zu entfernen

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Entitlement Status	X	X		Status der Berechtigung zum Zeitpunkt der Meldung	Der Status muss zur Fachlichkeit passen und ist Teil des Monitorings. Hier z.B. „OK“
Application Instance ID	X	X	X	Applikations-Instanz-ID der Applikation, auf der die Berechtigung ausgegeben wurde	Betrachten der einzelnen Felder in Details.
Action Timestamp	X	X		Zeitpunkt der Ausgabe	
Terminal-ID	X	X		ID des Ausgabeterminals	
Operator-ID	X	X		Organisations-ID des Terminal-Betreibers	
Location-ID	X	X		ID des Ortes der Ausgabe	
Stored Value Current Balance			X	Aktueller auf der Karte verfügbarer Betrag	Optional, nur wenn Produkttyp SVPM entspricht.
Stored Value Maximum Balance			X	Auf der Karte maximal erlaubter Betrag	Optional, nur wenn Produkttyp SVPM entspricht.
Stored Value Autoload Threshold			X	Schwellwert des aktuellen Betrages auf der Karte, ab wann per Autoload automatisch aufgebucht wird	Optional, nur wenn Produkttyp SVPM entspricht.
Stored Value Autoload Amount			X	Betrag, der via Autoload automatisch aufgebucht wird	Optional, nur wenn Produkttyp SVPM entspricht.
Product Parameters			X	Tarifliche und ggf. persönliche Informationen zur Berechtigung	Datenschutzrichtlinie: Die persönlichen Daten sind ggf. zu löschen. Diese Daten sind nur in der Detailansicht (siehe 4.7.5.2) verfügbar.
Infotext			X	Infotext der Berechtigung	
Warnung		X	X	0..N Warnungen, die an der Berechtigung hängen können	In der Übersicht muss gekennzeichnet sein, dass Warnungen vorliegen.
Aus Notification-Liste	X	X		Flag, ob der Eintrag aus einer Notification-Liste in der ION-Message entstanden ist.	Ja, wenn aus Liste, nein, wenn aus Einzelnachricht
Eintrag Berechtigungs-Bestand			X	Referenz auf den passenden Eintrag im Berechtigungsbestand (4.7.10.1)	Muss navigierbar sein
ION-Message			X	Referenz auf die ION-Message zu diesem Registereintrag	Muss navigierbar sein. Es kann sich auch um eine Notification-Liste handeln.

4.7.5.2 Detailansicht und Verknüpfungen

Für einzelne Ausgaben steht eine Detailansicht zur Verfügung. In oben aufgeführter Tabelle sind die Felder markiert, die ausschließlich in der Detailansicht sichtbar sind. Das MPS muss diese Felder aufarbeiten, so dass die Ansicht für den Benutzer verständlich ist und einen Mehrwert bietet.

Insbesondere das Feld „Product Parameters“ muss in der Detailansicht aufgearbeitet werden. Laut ((etiCORE-Spezifikation können hier folgende Daten enthalten sein, die entsprechend aufgearbeitet werden müssen. Die Art der Daten hängt vom Content-Flag ab, das in der u. g. Aufzählung mit aufgeführt ist:

- Typ 0: Inhalt wird lediglich als Hexstring dargestellt
- Typ 1, „TLV-EFS“: bisherige Tarifdaten. Darstellung der fachlichen Inhalte mit Hilfe eines geeigneten Parsers
- Typ 2-6, „Referenz-EFS“: bisheriger Referenz-EFS in verschiedenen Ausprägungen. Darstellung der fachlichen Inhalte mit Hilfe eines geeigneten Parsers
- Typ 7, „etiCORE-ET“: in ((etiCORE überarbeiteter Tarifdatensatz auf Basis des „TLV-EFS“. Darstellung der fachlichen Inhalte mit Hilfe eines geeigneten Parsers

In der Detailansicht kann zusätzlich auf die zugehörige ION-Nachricht navigiert werden.

Alle oben aufgeführten Felder sind zusätzlich in der Detailansicht verfügbar.

4.7.6 Register für Ausgabeabbruch von Berechtigungen

Register über Abbrüche, die SAM-Zähler verbraucht haben. Dies wird verwendet, um Lücken beim Monitoring zu plausibilisieren. Das MPS erzeugt einen Eintrag bei Eingang einer entsprechenden ION-Nachricht. Das gilt für Berechtigungen auf Chipkarte und statische Berechtigungen.

4.7.6.1 Tabellarische Ansicht

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Issuance Aborted Registry ID				Eindeutiger Schlüssel auf Eintrag	Wird für Referenzbeziehungen benötigt
Internal Error			X	Interne Fehlerbeschreibung	
Entitlement Type	X	X		Statische Berechtigung oder Berechtigung auf Chipkarte	Kann aufgrund der ION-Message gesetzt werden

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Entitlement-Issuance Counter		X		SAM Entitlement Issuance Counter des ausgebenden SAMs, bei dem der Abbruch passiert ist	
Application Instance ID	X	X	X	Applikations-Instanz-ID der Applikation, die beim Abbruch im Zugriff war	Betrachten der einzelnen Felder in Details.
Action Timestamp	X	X		Zeitpunkt des Abbruchs	
Terminal-ID	X	X		ID des Terminals	
Operator-ID	X	X		Organisations-ID des Terminal-Betreibers	
Location-ID	X	X		ID des Ortes des Abbruchs	
SAM-ID	X	X	X	ID des involvierten SAMs	Betrachten der einzelnen Felder in Details.
Product Owner Token		X		Information über das Token des Product Owners	
ION-Message			X	Referenz auf die ION-Message zu diesem Registereintrag	Muss navigierbar sein

4.7.6.2 Detailansicht und Verknüpfungen

Für einzelne Einträge steht eine Detailansicht zur Verfügung. In oben aufgeführter Tabelle sind die Felder markiert, die ausschließlich in der Detailansicht sichtbar sind. Das MPS muss diese Felder aufarbeiten, so dass die Ansicht für den Benutzer verständlich ist und einen Mehrwert bietet. In der Detailansicht kann zusätzlich auf die zugehörige ION-Nachricht navigiert werden.

Alle oben aufgeführten Felder sind zusätzlich in der Detailansicht verfügbar.

4.7.7 Kontrolldatenregister (Inspection Registry)

Das Kontrolldatenregister bildet alle im System erfassten Kontrollen (Inspections) ab.

4.7.7.1 Tabellarische Übersicht

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Inspection Registry ID				Eindeutiger Schlüssel auf Eintrag	Wird für Referenzbeziehungen benötigt
Spec Version	X	X		Verwendete Version der UM Spezifikation.	Wichtig für Zusammensetzung der Attestation und als Parser Information

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Product-ID	X	X	X	Product-ID mit Product-Owner, Product Type und Product Number	Product Type zeigt, ob es sich um electronic Ticket, statische Berechtigung oder Payment Method handelt. Betrachten der einzelnen Felder in Details.
Entitlement-ID		X	X	Entitlement-ID mit ID des Herausgebers der Berechtigung (CCP-Organisation-ID), SAM-ID des ausgebenden SAMs, SAM Issuance Counter als Entitlement Number	Aufgrund der enthaltenen SAM-ID lässt sich feststellen, ob es sich um eine Level-2 oder Level-3 Berechtigung handelt. Betrachten der einzelnen Felder in Details.
Entitlement Status	X	X		Status der Berechtigung zum Zeitpunkt der Meldung	Der Status muss zur Fachlichkeit passen und ist Teil des Monitorings. Hier z.B. „OK“
Entitlement Transition Counter		X		Zustandsänderungszähler der Berechtigung	
Entitlement Action Counter		X		Aktionszähler der Berechtigung	
Application Instance ID	X	X	X	Applikations-Instanz-ID der Applikation, die zu der kontrollierten Berechtigung gehört	Betrachten der einzelnen Felder in Details.
Action Timestamp	X	X		Zeitpunkt der Kontrolle	
Terminal-ID	X	X		ID des Kontrollterminals	
Operator-ID	X	X		Organisations-ID des Terminal-Betreibers	
Location-ID	X	X		ID des Ortes der Kontrolle	
Action Tariff Parameters			X	Tarifliche Informationen zur Action mit der Berechtigung	Muss für die Detailansicht aufbereitet werden
SAM-ID	X	X	X	ID des kontrollierenden SAMs	Bei statischen Berechtigungen ist die ID des kontrollierenden SAMs nicht gefüllt. Betrachten der einzelnen Felder in Details.
SAM Action Counter		X		Aktueller Aktionszähler Zähler des SAMs zum Zeitpunkt der Kontrolle	
Last SAM Action Data			X	SAM-ID und Action Counter des SAMs, welches zuletzt eine Aktion mit der Berechtigung durchgeführt hat	

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Warnung		X	X	0..N Warnungen, die an der Berechtigung hängen können	In der Übersicht muss gekennzeichnet sein, dass Warnungen vorliegen.
Eintrag Berechtigungs-Bestand			X	Referenz auf den passenden Eintrag im Berechtigungsbestand (4.7.10.1)	Muss navigierbar sein
Aus Notification-Liste	X	X		Flag, ob der Eintrag aus einer Notification-Liste in der ION-Message entstanden ist.	Ja, wenn aus Liste, nein, wenn aus Einzelnachricht
ION-Message			X	Referenz auf die ION-Message zu diesem Registereintrag	Muss navigierbar sein. Es kann sich auch um eine Notification-Liste handeln.

4.7.7.2 Detailansicht und Verknüpfungen

Für einzelne Kontrollen steht eine Detailansicht zur Verfügung. In oben aufgeführter Tabelle sind die Felder markiert, die ausschließlich in der Detailansicht sichtbar sind. Das MPS muss diese Felder aufarbeiten, so dass die Ansicht für den Benutzer verständlich ist und einen Mehrwert bietet. In der Detailansicht kann zusätzlich auf die zugehörige ION-Nachricht und auf den passenden Eintrag im Berechtigungsbestand navigiert werden.

Alle oben aufgeführten Felder sind zusätzlich in der Detailansicht verfügbar.

4.7.8 Nutzungsregister (Recording Registry)

Das Nutzungsregister bildet alle Recordings von Berechtigungen (Payment Methods) ab. Diese Recordings entstehen im Rahmen von IN/OUT in Form von Check-In und Check-Out-Notifications. Ebenfalls registriert werden Notifications zur Änderung von Nutzer-Tarif-Parametern.

4.7.8.1 Tabellarische Übersicht

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Recording Registry ID				Eindeutiger Schlüssel auf Eintrag	Wird für Referenzbeziehungen benötigt
Spec Version	X	X		Verwendete Version der UM Spezifikation.	Wichtig für Zusammensetzung der Attestation und als Parser Information

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Product-ID	X	X	X	Product-ID mit Product-Owner, Product Type und Product Number	Product Type zeigt, ob es sich um electronic Ticket, statische Berechtigung oder Payment Method handelt. Betrachten der einzelnen Felder in Details.
Type	X	X		Check-In, Check-Out oder Änderung der Nutzer-Tarif-Parameter	Explizites Feld für bessere Übersicht.
Entitlement-ID		X	X	Entitlement-ID mit ID des Herausgebers der Berechtigung (CCP-Organisation-ID), SAM-ID des ausgebenden SAMs, SAM Issuance Counter als Entitlement Number	Aufgrund der enthaltenen SAM-ID lässt sich feststellen, ob es sich um eine Level-2 oder Level-3 Berechtigung handelt. Betrachten der einzelnen Felder in Details.
Entitlement Status	X	X		Status der Berechtigung zum Zeitpunkt der Meldung	Der Status muss zur Fachlichkeit passen und ist Teil des Monitorings. Hier z.B. „OK“
Entitlement Transition Counter		X		Zustandsänderungszähler der Berechtigung	
Entitlement Action Counter		X		Aktionszähler der Berechtigung	
Application Instance ID	X	X	X	Applikations-Instanz-ID der Applikation, die zu der erfassten Berechtigung gehört	Betrachten der einzelnen Felder in Details.
Action Timestamp	X	X		Zeitpunkt der Kontrolle	
Terminal-ID	X	X		ID des Recording-Terminals	
Operator-ID	X	X		Organisations-ID des Terminal-Betreibers	
Location-ID	X	X		ID des Ortes des Recordings	
Stored Value Current Balance					Optional, nur wenn Produkttyp SVPM entspricht.
Action Amount				Betrag, der aufgrund der Aktion verwendet wurde. Bei Abbuchung negativ	Optional, nur wenn Produkttyp SVPM entspricht.
Action Payment Parameters			X	Bestehend aus Line Variant ID, Trip-ID, Initial-Trip-Segment, Current Stop ID und und Paid Amount	Die Daten müssen für die Detailansicht aufbereitet bzw. auf einzelne Felder aufgeteilt werden
Action Tariff Parameters			X	Tarifliche Informationen zur Action mit der Berechtigung	Muss für die Detailansicht aufbereitet werden

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
SAM-ID	X	X	X	ID des SAMs für das Recording	Betrachten der einzelnen Felder in Details.
SAM Action Counter		X		Aktueller Aktionszähler Zähler des SAMs zum Zeitpunkt des Recordings	
Last SAM Action Data			X	SAM-ID und Action Counter des SAMs, welches zuletzt eine Aktion mit der Berechtigung durchgeführt hat	
Warnung		X	X	0..N Warnungen, die an der Berechtigung hängen können	In der Übersicht muss gekennzeichnet sein, dass Warnungen vorliegen.
Eintrag Berechtigungs-Bestand			X	Referenz auf den passenden Eintrag im Berechtigungsbestand (4.7.10.1)	Muss navigierbar sein
Aus Notification-Liste	X	X		Flag, ob der Eintrag aus einer Notification-Liste in der ION-Message entstanden ist.	Ja, wenn aus Liste, nein, wenn aus Einzelnachricht
ION-Message			X	Referenz auf die ION-Message zu diesem Registereintrag	Muss navigierbar sein. Es kann sich auch um eine Notification-Liste handeln.

4.7.8.2 Detailansicht und Verknüpfungen

Für einzelne Erfassungen (Check-In / Check-Out) steht eine Detailansicht zur Verfügung. In oben aufgeführter Tabelle sind die Felder markiert, die ausschließlich in der Detailansicht sichtbar sind. Das MPS muss diese Felder aufarbeiten, so dass die Ansicht für den Benutzer verständlich ist und einen Mehrwert bietet. In der Detailansicht kann zusätzlich auf die zugehörige ION-Nachricht und auf den passenden Eintrag im Berechtigungsregister navigiert werden.

Alle oben aufgeführten Felder sind zusätzlich in der Detailansicht verfügbar.

Hinweis: eine aggregierte Ansicht für eine spätere tarifliche Best-Price-Berechnung wird im Rahmen dieses Lastenheftes nicht betrachtet.

4.7.9 Product Owner Token

Das Product Owner Token besteht aus der Organisations-ID des Product Owners und einem Zähler (pro SAM) für die Ausgabe einer Berechtigung basierend auf einem Produkt dieses Product Owner.

Die Summe über alle Product Issuance Counter, die für die SAMs mit entsprechendem Product Owner Token gemeldet werden, ergibt die Gesamtmenge aller ausgegebenen Berechtigungen der beteiligten SAMs.

Diese Summe muss das MPS zur Verfügung stellen.

Folgende Tabelle fasst die Daten für die Nutzung der Product Issuance Counter zusammen. Diese Tabelle muss das MPS analog zu den Beständen pflegen und zur Verfügung stellen. Der Product Issuance Counter bezieht sich immer auf die Organisations-ID des POs des aktuellen Mandanten und somit auf das Product Owner Token.

4.7.9.1 Tabellarische Ansicht

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
PO Org ID	X	X		Organisations-ID des Product-Owners	Es ist möglich, dass ein Mandant für sein(e) PO-System(e) mehrere Organisations-IDs hat. Das kann hier unterschieden werden.
Product Issuance Counter	X	X		Aktueller Ausgabezähler	Wird jeweils aus dem neuesten Ausgabenachweis extrahiert (Zähler in der Entitlement Struktur)
SAM	X	X	X	Entsprechendes SAM aus dem Bestand	Muss zum SAM navigierbar sein, bzw. dessen Status mit anzeigen
Entitlement			X	Entsprechende Berechtigung im Bestand, passend zum Product Issuance Counter	Muss zur Berechtigung navigierbar sein und in der Detailansicht die Felder anzeigen

4.7.10 Zustandsbehaftete Bestände

Die nachfolgenden Bestände bilden virtuelle Entitäten ab. Das sind Entitäten, die dem Mandanten in der Rolle PO nicht gehören (Berechtigungen, Applikationen, SAMs), aber aufgrund der eingehenden Nachrichten erstellt bzw. gefüllt werden können. Weitere eintreffende Nachrichten oder auch Hotlist-Einträge können den Zustand eines Eintrages im Bestand verändern. Bei jeder Zustandsänderung der Nachricht wird zusätzlich ein Eintrag in einer Transition-Tabelle erzeugt, die die Änderungshistorie festhält. Dieser Eintrag enthält den Grund für die Zustandsänderung (Referenz auf Nachricht oder Hotlist-

Eintrag), das Datum sowie wichtige Metainformationen, die vom Typ der Transition abhängen (z.B. die Zyklus-ID bei einem Hotlist-Eintrag).

Die nachfolgenden Bestände werden also mit Eintreffen der Nachrichten nach und nach aufgebaut bzw. geändert.

4.7.10.1 Bestand an Berechtigungen (Entitlement Inventory)

Der Berechtigungsbestand stellt alle im System bekannten Berechtigungen dar. Bei Eintreffen einer Nachricht, die sich auf eine Berechtigung bezieht, wird der Bestand angepasst. Damit enthält der Bestand für die jeweilige Berechtigung immer den letzten Stand, während die Historie bzw. die Nachvollziehbarkeit des aktuellen Stands in der passenden Transition-Tabelle bzw. im jeweiligen Bestand zu finden ist.

4.7.10.1.1 Mögliche Zustände

Folgende Zustände sind möglich:

- Entitlement OK: Berechtigung ist ausgegeben ist aktiv
- Entitlement Blocked: Gesperrt
- Entitlement Terminated: Berechtigung wurde zurückgegeben. Zurückgenommene Berechtigungen sind zu kennzeichnen und nach einem konfigurierbaren Zeitraum aus den Beständen zu entfernen
- Entitlement Hotlisting Demanded: Eine Sperranforderung wurde im Rahmen des Monitorings versendet. Wird die Sperranforderung abgelehnt, so wird der Zustand zurück auf „OK“ gesetzt. Die Ablehnung führt zu einem neuen Eintrag in der Transitiontabelle mit Verweis auf die Ablehnung.
- SAM Hotlisting Demanded: bei der Untersuchung einer Meldung für die Berechtigung wurde ein SAM-Problem festgestellt und eine Sperranforderung für das SAM gesendet
- Application Hotlisting Demanded: bei der Untersuchung einer Meldung für die Berechtigung wurde ein Application-Problem festgestellt und eine Sperranforderung für die Application gesendet
- Entitlement hotlisted: Im Hotlist-Inventory existiert ein Eintrag für die Berechtigung
- Entitlement hotlisted by SAM: Im Hotlist-Inventory existiert ein Eintrag für ein mit der Berechtigung involviertes SAM
- Entitlement hotlisted by Application: Im Hotlist-Inventory existiert ein Eintrag für die Applikation, zu der die Berechtigung gehört. **Hinweis:** beim Zurücksetzen des Status muss der zuletzt bekannte Wert verwendet werden!

- Entitlement Blocked by Application: Die zugehörige Applikation wurde gesperrt, damit ist auch die Berechtigung virtuell mit gesperrt und darf z.B. zur Einnahmeaufteilung o.Ä. nicht berücksichtigt werden. **Hinweis:** beim Zurücksetzen des Status muss der zuletzt bekannte Wert verwendet werden!
- Entitlement Terminated by Application: Die zugehörige Applikation wurde terminiert. Damit ist auch die Berechtigung virtuell terminiert, falls dies zuvor beim pCCP nicht korrekt für die Berechtigung ausgeführt wurde und darf z.B. zur Einnahmeaufteilung o.Ä. nicht berücksichtigt werden.

Die möglichen Statusübergänge finden sich in Abbildung 13: Mögliche Zustände von Berechtigungen. Zustandsänderungen werden in der Statushistorie festgehalten (siehe 4.7.10.1.3).

Wichtig: Durch Race-Conditions können sich Nachrichten überholen. Es muss also ein Eintrag mit jedem Zustand (außer *XX Hotlisting Demanded*) neu angelegt werden können, wenn die Berechtigung noch nicht im Bestand ist. Dies ist im Diagramm aus Verständnisgründen nicht dargestellt.

4.7.10.1.2 Tabellarische Ansicht

www.eticket-deutschland.de

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
				Organisation-ID), SAM-ID des ausgebenden SAMs, SAM Issuance Counter als Entitlement Number	zur Vollständigkeit. Betrachten der einzelnen Felder in Details. Aufgrund der enthaltenen SAM-ID lässt sich feststellen, ob es sich um eine Level-2 oder Level-3 Berechtigung handelt
Issuance Registry ID				Eintrag im Ausgaberegister, der initial zu diesem Eintrag geführt hat (initiales Anlegen nach Ausgabe)	Navigierbar zum entsprechenden Eintrag ins das Ausgaberegister
Entitlement Effective Time	X	X		Gültigkeitsbeginn der Berechtigung	Kann aus dem Ausgaberegister-Eintrag übernommen werden. Hier zur Vollständigkeit.
Entitlement Expiration Time	X	X		Gültigkeitsende der Berechtigung	Kann aus dem Ausgaberegister-Eintrag übernommen werden. Hier zur Vollständigkeit. Abgelaufene Berechtigungen sind zu kennzeichnen und nach einem konfigurierbaren Zeitraum aus den Registern zu entfernen
Entitlement Inventory Status	X	X		(virtueller) Status der Bestandseintrages für die Berechtigung	Siehe 4.7.10.1.1
Entitlement Transition Counter	X	X		Zustandsänderungszähler der Berechtigung	Fortlaufend, ohne Lücken
Entitlement Action Counter	X	X		Aktionszähler der Berechtigung	
Application Instance ID	X	X	X	Applikations-Instanz-ID der Applikation, zu der die Berechtigung gehört	Navigierbar auf den passenden Eintrag im Applikations-Bestand. Betrachten der einzelnen Felder in Details.
Stored Value Current Balance			X	Aktueller auf der Karte verfügbarer Betrag	Optional, nur wenn Produkttyp SVPM entspricht.
Stored Value Maximum Balance			X	Auf der Karte maximal erlaubter Betrag	Optional, nur wenn Produkttyp SVPM entspricht.
Stored Value Autoload Threshold			X	Schwellwert des aktuellen Betrages auf der Karte, ab wann per Autoload	Optional, nur wenn Produkttyp SVPM entspricht.

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
				automatisch aufgebucht wird	
Stored Value Autoload Amount			X	Betrag, der via Autoload automatisch aufgebucht wird	Optional, nur wenn Produkttyp SVPM entspricht.
Product Parameters			X	Tarifliche und ggf. persönliche Informationen zur Berechtigung	Kann aus dem Ausgaberegister-Eintrag übernommen werden. Hier zur Vollständigkeit. Datenschutzrichtlinie: Die persönlichen Daten sind ggf. zu löschen. Diese Daten sind nur in der Detailansicht verfügbar.
Warnungen		X	X	O..N Warnungen, die an der Berechtigung hängen können	In der Übersicht muss gekennzeichnet sein, dass Warnungen vorliegen.
Anzahl Kontrollen			X		Wird mit jedem Kontrollnachweis hochgezählt
Anzahl Nutzungen			X		Wird mit jeder Nutzung (Check-In oder Check-Out) hochgezählt

4.7.10.1.3 Statushistorie im Bestand

Feld	Navigierbar	Kurzbeschreibung	Anmerkung
Entitlement-ID	X	Referenz auf Entitlement-ID im Berechtigungsregister	
ION-Message	X	Referenz auf die ION-Message mit der Nachricht, die zur Statusänderung geführt hat	Das können eingehende, aber auch ausgehende Nachrichten sein, wie z.B. bei gesendeten Hotlisting Demands
Inspection Registry ID	X	Kontrollregister-Eintrag, der zur Statusänderung geführt hat	Falls es sich um eine Kontrolle gehandelt hat.
Recording Registry ID	X	Nutzungsregister-Eintrag, der zur Statusänderung geführt hat	Falls es sich um eine Nutzung gehandelt hat.
Application Status Registry ID	X	Register-Eintrag für Applikationsstatus, der zur Statusänderung geführt hat	Falls sich die betroffene Berechtigung auf einer jetzt als gesperrt oder terminiert gemeldeten Applikation befindet
Hotlist Cycle ID		Referenz auf den Hotlist-Inventory-Cycle, der zur Statusänderung geführt hat	Status auf "Hotlisted" oder zurück auf „OK“, wenn der Eintrag nicht mehr enthalten ist.

Feld	Navigierbar	Kurzbeschreibung	Anmerkung
Order ID		Auftragsnummer aus dem Aktionsmanagement zusammen mit der CCP-Organisations-ID	Wenn das Aktionsmanagement die Änderung der Berechtigung herbeigeführt hat.
Transition-Timestamp		Zeitpunkt der Änderung im Bestand	
Old Status		Vorheriger (Virtueller) Status des Bestands-Eintrages vor dem aktuellen Eintrag in die Historie	Siehe 4.7.10.1.1
New Status		Aktueller (virtueller) Status des Bestands-Eintrages nach dem erfassten Ereignis für die Änderung	Siehe 4.7.10.1.1. Status kann den gleichen Wert wie vorher haben, z.B. nach eingegangenem Kontrollnachweis.
Old Entitlement Action Counter		Action Counter im Bestands-Eintrag vor der Änderung im Bestand	
New Entitlement Action Counter		Action Counter im Bestands-Eintrag nach der Änderung im Bestand	Status kann den gleichen Wert haben, wenn keine echte (Trans-)Aktion stattgefunden mit der Berechtigung hat (z.B. von „Entitlement OK“ auf „Entitlement Hotlisted“)
Old Entitlement Transition Counter		Transition Counter vor der Änderung im Bestand	
New Entitlement Transition Counter		Transition Counter nach der Änderung im Bestand	Counter kann den gleichen Wert wie vorher haben, z.B. nach eingegangenem Kontrollnachweis.

4.7.10.2 Bestand an Applikationen (Application Inventory)

Das MPS füllt den Applikations-Bestand mit Hilfe der eingehenden Ausgabenachweise für Berechtigungen (notityEntitlementIssued), da nur bei dieser Nachricht die Applikations-Instanz-ID geliefert wird. Wenn im Rahmen des Monitorings Informationen zum Eigentümer der Applikation abgerufen werden, so werden diese ebenfalls dort abgelegt. Des Weiteren werden die Zustände zu Applikationen ausgewertet (z.B. Sperrung) und im Bestand eingetragen.

Wird im Rahmen des Monitorings ein Hotlisting-Demand (Sperranforderung) gestellt, so entsteht eine Zustandsänderung auf „Hotlisting Demanded“ und über die Transitiontabelle ein Verweis auf die ausgegangene Hotlisting-Demand Nachricht. Wird die Sperranforderung abgelehnt, so wird der Zustand zurück auf „OK“ gesetzt. Die Ablehnung führt zu einem neuen Eintrag in der Transitiontabelle mit Verweis auf die Ablehnung. Das gilt auch für alle betroffenen Berechtigungen.

Bei Aktualisierung der Application-Hotlist muss das MPS die Einträge ebenfalls anpassen.

4.7.10.2.1 Mögliche Zustände

Folgende Zustände sind im MPS möglich, nicht bekannte Zustände in Klammern:

- OK, Ready to use: Applikation ist ausgegeben und aktiv. Der Status „OK“ ist eine Annahme, solange kein Hotlisting aktiv ist
- Hotlisting Demanded: Eine Sperranforderung für die Applikation wurde im Rahmen des Monitorings versendet
- Hotlisted: Im Hotlist-Inventory wurde ein Eintrag gefunden
- Blocked: Gesperrt siehe [16]
- Terminated: Applikation wurde zurückgegeben, siehe [16]

Abbildung 14 zeigt die möglichen Statusübergänge.

Wichtig: Durch Race-Conditions können sich Nachrichten überholen. Es muss also ein Eintrag mit jedem Zustand (außer Hotlisting demanded) neu angelegt werden können, wenn die Applikation noch nicht im Bestand ist. Dies ist im Diagramm aus Verständnisgründen nicht dargestellt.

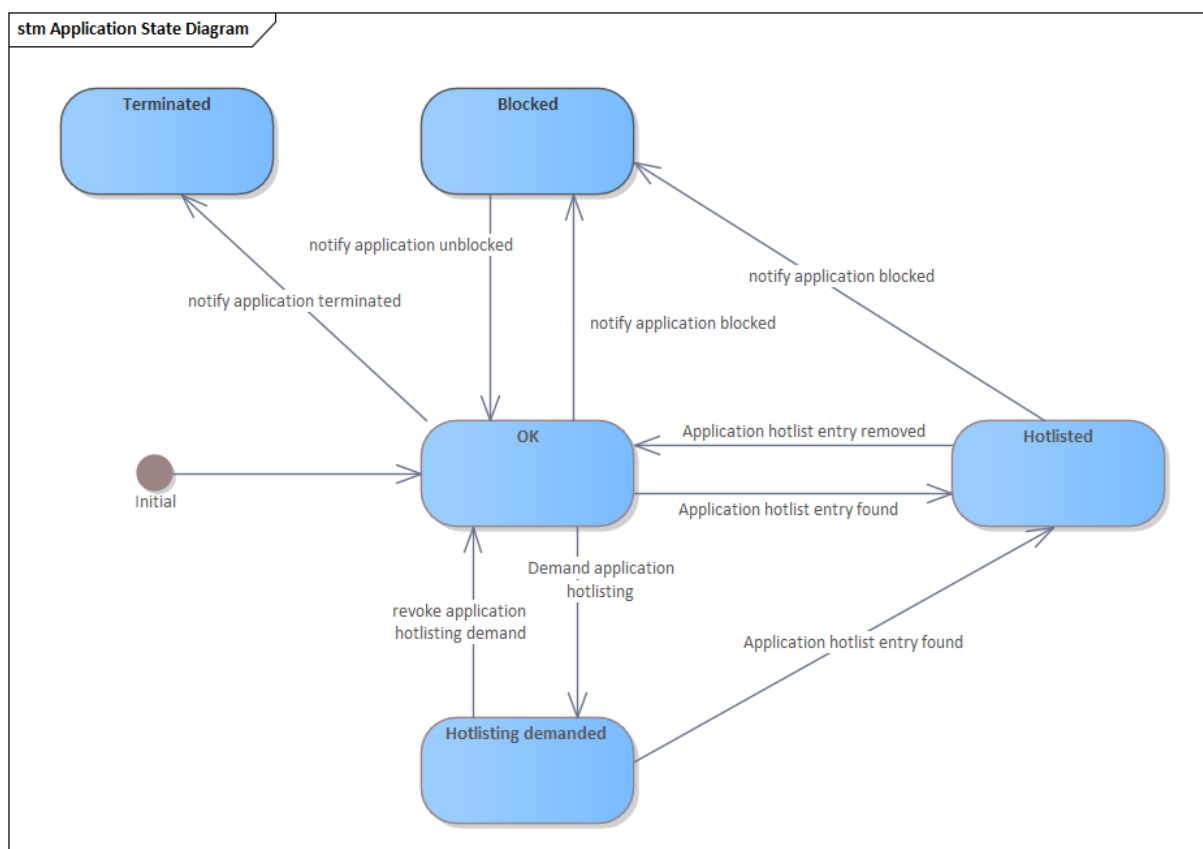


Abbildung 14: Mögliche Zustände einer Applikation im Bestand

4.7.10.2.2 Tabellarische Ansicht

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Applikations-Instanz-ID	X	X	X	Applikations-Instanz-ID bestehend aus Organisation-ID des Herstellers, Subject Role und Subject Number	Betrachten der einzelnen Felder in Details.
Applikations-Eigentümer	X	X		Bestehend aus Organisation und Rolle.	Wenn über eine Abfrage der Eigentümer bestimmt wurde, so trägt das MPS die Organisation hier ein. Die Rolle ist immer CCP.
Application Effective Time	X	X		Gültigkeitsbeginn der Applikation	Kann bei der Anfrage nach dem Applikationseigentümer aus dem CV-Zertifikat bei Abfrage extrahiert werden. Das geschieht in der Regel aber nur, wenn ein Hotlisting-Demand gestellt wurde oder Berechtigungen zu einem

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
					defekten Medium abgefragt werden.
Application Expiration Time	X	X		Gültigkeitsende der Applikation	Kann bei der Anfrage nach dem Applikationseigentümer aus dem CV-Zertifikat bei Abfrage extrahiert werden. Das geschieht in der Regel aber nur, wenn ein Hotlisting-Demand gestellt wurde oder Berechtigungen zu einem defekten Medium abgefragt wurden. Abgelaufene Applikationen sind zu kennzeichnen und nach einem konfigurierbaren Zeitraum aus den Registern und Beständen zu entfernen
Application Status	X	X		(Virtueller) Status im Bestand für die Applikation	Siehe 4.7.10.2.1
Application Transition Counter	X	X		Zustandsänderungszähler der Applikation	Das Feld kann gesetzt werden, wenn ein Hotlist-Eintrag für diese Applikation besteht. In dem Fall ist der Zähler bekannt. Ebenfalls kann das Feld bei einer registrierten Statusänderung (siehe 4.7.3) gesetzt werden.
Entitlements			X	1..n Berechtigungen, die zu der Applikation gehören.	Darstellung einer Liste mit navigierbaren Einträgen aus dem Berechtigungsbestand (siehe 4.7.10.1)

4.7.10.2.3 Statushistorie im Bestand

Feld	Navigierbar	Kurzbeschreibung	Anmerkung
Applikations-Instanz-ID	X	Referenz auf Applikations-Instanz-ID im Applikations-Bestand	
ION-Message	X	Referenz auf die ION-Message mit der Nachricht, die zur Statusänderung geführt hat	Das können eingehende (z.B. die erste Ausgabe einer Berechtigung auf dieser Applikation), aber auch ausgehende Nachrichten sein, wie z.B. bei gesendeten Hotlisting Demands
Application Status Registry ID	X	Applikation-Statusregister-Eintrag, der zur Statusänderung geführt hat	

Feld	Navigierbar	Kurzbeschreibung	Anmerkung
Hotlist-Inventory-Cycle		Referenz auf den Hotlist-Inventory-Cycle, der zur Statusänderung geführt hat	Status auf "Hotlisted" oder zurück auf „OK“, wenn der Eintrag nicht mehr enthalten ist.
Transition-Timestamp		Zeitpunkt der Änderung	
Old Status		Status des Bestands-Eintrages vor der Änderung im Bestand	Siehe 4.7.10.2.1
New Status		Status des Bestands-Eintrages nach der Änderung im Bestand	Siehe 4.7.10.2.1
Old Application Transition Counter		Transition Counter vor der Änderung im Bestand	Z.B. aus altem Hotlist-Eintrag
New Application Transition Counter		Transition Counter nach der Änderung im Bestand	Kann den gleichen Wert haben wie der alte Zähler.

4.7.10.3 Bestand an SAMs (SAM Inventory)

Der SAM-Bestand enthält keine MPS-eigenen SAMs (in etiCORE besitzt der PO keine SAMs) sondern wird über die eintreffenden Nachrichten gefüllt.

Beim Eintreffen von Nachrichten wertet das MPS die zugehörigen SAM-Action-Data und die SAM-ID aus der Entitlement-ID aus der Attestation aus und legt entweder einen neuen Datensatz an, wenn das SAM noch nicht bekannt ist, oder ändert den vorhandenen Datensatz. In dem Fall legt das MPS zusätzlich einen Datensatz für die Statushistorie an.

4.7.10.3.1 Mögliche Zustände

Folgende Zustände sind im MPS möglich:

- OK: SAM ist aktiv. Der Status OK ist eine Annahme, solange kein Hotlisting aktiv ist. Über andere Zustände ist das MPS nicht informiert.
- Hotlisting Demanded: Eine Sperranforderung wurde im Rahmen des Monitorings versendet. Wird die Sperranforderung abgelehnt, so wird der Zustand zurück auf „OK“ gesetzt. Die Ablehnung führt zu einem neuen Eintrag in der Transitiontabelle mit Verweis auf die Ablehnung. Das gilt auch für alle betroffenen Berechtigungen.
- Hotlisted: Im Hotlist-Inventory wurde ein Eintrag gefunden

Abbildung 15 zeigt die möglichen Statusübergänge.

Wichtig: Es muss ein Eintrag mit Zustand OK oder Hotlisted neu angelegt werden können, wenn das SAM noch nicht im Bestand ist. Dies ist im Diagramm aus Verständnisgründen nicht dargestellt.

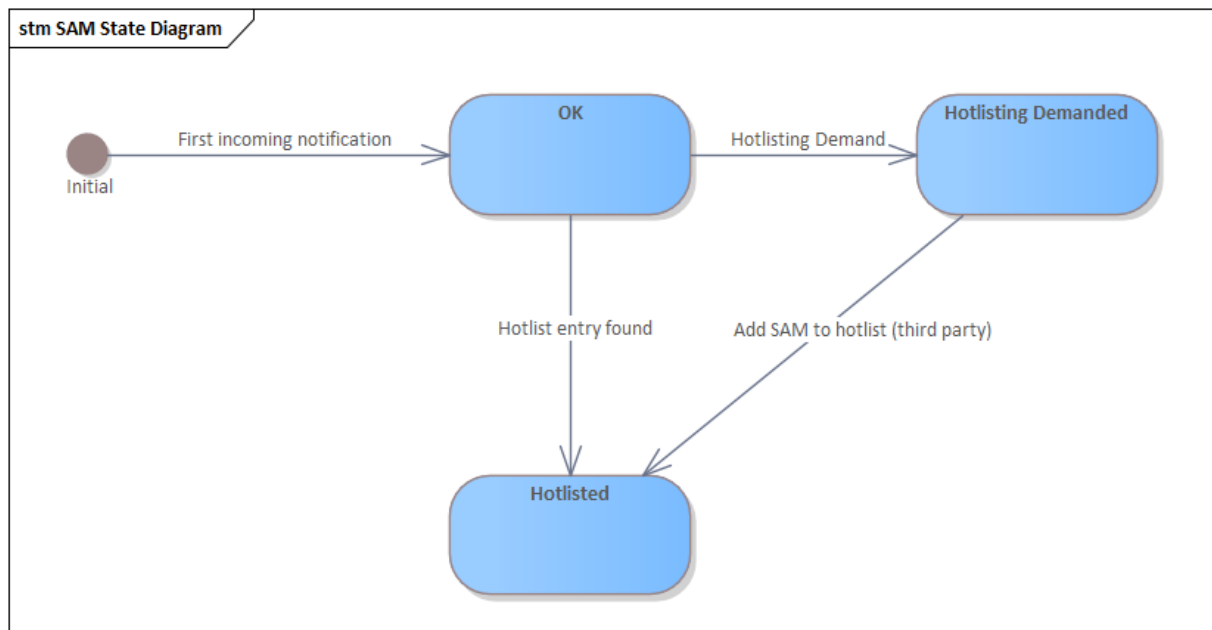


Abbildung 15: Mögliche Zustände eines SAMs im Bestand

4.7.10.3.2 Tabellarische Ansicht

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
SAM-ID	X	X	X	Applikations-Instanz-ID des SAM („SAM-ID“) bestehend aus Organisation-ID des Herstellers, Subject Role und Subject Number	Betrachten der einzelnen Felder in Details.
SAM-Eigentümer	X	X		Bestehend aus Organisation und Rolle. Ggf. leer, wenn keine Abfrage erfolgt ist.	Wenn über eine Abfrage der Eigentümer bestimmt wurde, so trägt das MPS die Organisation hier ein. Die Rolle wird bei der Antwort mitgeliefert (CCP oder SO).
SAM Effective Time	X	X		Gültigkeitsbeginn des SAMs	
SAM Expiration Time	X	X		Gültigkeitsende des SAM	Abgelaufene SAMs sind zu kennzeichnen und nach einem konfigurierbaren Zeitraum aus den Registern und Beständen zu entfernen
SAM-Status	X	X		(Virtueller) Status des SAMs im Bestand	Siehe 4.7.10.3.1
SAM Action Counter	X	X		Aktionszähler des SAMs	Fortlaufend. Wird aus SAM Action Data der

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
					Attestations (außer Ausgabe) extrahiert
Product Issuance Counter	X	X		Aktueller Ausgabezähler, wenn bekannt	Wird jeweils aus dem neuesten Ausgabenachweis extrahiert (Zähler in der Entitlement Struktur)

4.7.10.3.3 Statushistorie im Bestand

Feld	Navigierbar	Kurzbeschreibung	Anmerkung
SAM-ID	X	Referenz auf die SAM-ID im SAM-Bestand	
ION-Message	X	Referenz auf die ION-Message mit der Nachricht, die zur Statusänderung geführt hat	Das können eingehende, aber auch ausgehende Nachrichten sein, wie z.B. bei gesendeten Hotlisting Demands
Ausgaberegister-Eintrag	X	Referenz auf den Ausgaberegistereintrag, der zur Statusänderung gehört	X-OR: Letzter Eintrag, der zum Ausgeben einer Berechtigung auf diesem SAM geführt hat
Kontroll-Register-Eintrag	X	Referenz auf den Kontrollregistereintrag, der zur Statusänderung gehört	X-OR: Letzter Eintrag, der zur Kontrolle einer Berechtigung mit diesem SAM geführt hat
Nutzungsregister-Eintrag	X	Referenz auf den Nutzungsregistereintrag, der zur Statusänderung gehört	X-OR: Letzter Eintrag, der zur Erfassung (Nutzung) einer Berechtigung mit diesem SAM geführt hat
Hotlist-Inventory-Cycle		Referenz auf den Hotlist-Inventory-Cycle, der zur Statusänderung geführt hat	
Transition-Timestamp		Zeitpunkt der Änderung	
Old Status		Status vor der Änderung im Bestand	
New Status		Status nach der Änderung im Bestand	
Old SAM Action Counter		Action Counter vor der Änderung im Bestand	Z.B. aus altem Hotlist-Eintrag
New SAM Action Counter		Action Counter nach der Änderung im Bestand	
Old Product Issuance Counter		Product Issuance Counter vor der Änderung im Bestand	
New Product Issuance Counter		Product Issuance Counter nach der Änderung im Bestand	

4.8 Logbücher

Das System stellt in einem Bereich Logbücher bereit, die die Nachvollziehbarkeit und Integrität des Systems sicherstellen und damit wichtige Informationen protokollieren.

Dazu gehören die folgenden drei Logbucharten.

4.8.1 Joblogbuch

Die einzelnen Prüfroutinen im Monitoring, aber auch automatisierte Prozesse, wie das Abholen der Sperrliste durch das System am Hotlistservice (HLS) oder die Datenarchivierung, werden in sog. Jobs durchgeführt. Jede Ausführung eines solchen Jobs soll im System protokolliert werden und den Benutzern der jeweiligen Mandanten auf der Benutzeroberfläche angezeigt werden. Folgende Informationen soll das Joblogbuch anzeigen:

- Job-ID
- Name des Jobs
- Startzeitpunkt
- Endzeitpunkt
- Nächster geplanter Start (falls bereits geplant)
- Zustand (Fertig/Fehler/Warnung/Wird ausgeführt)

4.8.2 Änderungslogbuch

Das Änderungslogbuch soll alle Änderungen im System erfassen.

Das Änderungslogbuch ermöglicht die Nachvollziehbarkeit von Änderungen durch Benutzer aller Rollen: Super-Administrator, Administrator und Nutzer. Änderungen an folgenden Informationen und Daten werden in diesem Logbuch protokolliert:

- Stammdaten
 - Organisationen
 - Produktdaten
- Jobsteuerung
- Meldungen / Klärfälle

Die Übersicht enthält folgende Informationen:

- Zeitpunkt der Änderung
- Ausführender Benutzer
- Geändertes Datenobjekt
- Datensatz vor der Änderung
- Datensatz nach der Änderung
- Detailansicht des Datensatzes

Die Detailansicht zeigt eine Auflistung der geänderten Attribute inkl. des vorherigen Wertes.

4.9 Nationaler Mandant

Der nationale Mandant im MPS dient als PO-System für nationale Tickets insbesondere das Deutschlandticket. Im Rahmen des zentralen Monitorings des Deutschlandtickets benötigt der nationale Mandant zusätzliche Rechte und Funktionalitäten wie im Folgenden beschrieben.

4.9.1 Funktionsprüfung

Die Funktionsprüfung ist verpflichtende Voraussetzung für die Freischaltung eines CCP oder SO an den nationalen Mandanten (siehe Abschnitt 4.9) im MPS und darf erst begonnen und abgeschlossen werden, sobald folgende Voraussetzungen und Vorgaben erfüllt sind:

- Erfolgreich abgeschlossener Anschalttest an das ION und muss für jedes in Betrieb genommene System erfolgen. Sicherstellung der erfolgreichen An- und Abmeldung an die CRE, sowie der bidirektionalen Kommunikation.
- Die Funktionsprüfung wird nur im Level 2 ausgeführt.
- Ohne erfolgreiche ausgeführte Funktionsprüfung im Level 2 wird eine Kommunikation von Verkehrsunternehmen in den Rollen 1 und 2 mit dem MPS im Level 3 mit einem Fehler abgelehnt.
- Die relevanten Testfälle werden mit WSS (Web Service Security) durchgeführt.
- Registrierung zur Funktionsprüfung über das vom Auftraggeber benannte Jira Ticket-/Servicemanagement-System mit Angabe von OrgID, Rolle und Mandant.
- Die Ergebnisse der Funktionsprüfung werden in dem Ticket-/Servicemanagement-System protokolliert.
- Das Ergebnisprotokoll beinhaltet die Liste der auszuführenden Testfälle und die einzelnen Ergebnisse, sowie das daraus resultierenden Gesamtergebnis.

4.9.1.1 Ablaufplan Funktionsprüfung

- Voraussetzung: Die Funktionsprüfung kann erst begonnen werden, nachdem der Anschalttest erfolgreich abgeschlossen wurde.
- Anmeldung zum Funktionstest: Das Verkehrsunternehmen erstellt ein Jira-Ticket zur Anmeldung für den Funktionstest in Jira Service Management. Das Ticket enthält folgende Angaben: OrgID, Rolle und relevanten Testfälle.
- Start des Funktionstests: ETS-Mitarbeiter starten den Funktionstest über die Portalseite.
- Ergebnisdokumentation: Nach Abschluss des Funktionstests wird ein PDF-Dokument mit dem Ergebnis erstellt und als Anhang an das entsprechende Jira-Ticket angehängt.
- Fehlerbehandlung: Sollten im Funktionstest Fehler auftreten, wird das Verkehrsunternehmen informiert. Nach ggf. erforderlichen Anpassungen der Einstellungen kann der Funktionstest wiederholt werden.
- Freischaltung: Nach erfolgreich bestandenem Funktionstest wird das Verkehrsunternehmen informiert und für den Wirkbetrieb auf Level 3 freigeschaltet.

4.9.1.2 Testfälle

Mit der Registrierung zur Funktionsprüfung gibt der jeweilige CCP oder SO an, ob mit dem System Chipkarten und/oder statische Berechtigungen verarbeitet werden. Nach der Registrierung wird dann für den jeweiligen CCP oder SO konfiguriert, welche Testfälle absolviert werden müssen.

Die Prüfkriterien:

- Nachricht wird syntaktisch valide versendet und akzeptiert
- fachlicher Inhalt entspricht der Vorgabe und Zuordnung
- Eintrag im Nachrichtenregister (siehe 4.7.2) mit Nachrichten-Zustand (siehe 4.7.2.2)

4.9.1.2.1 Testfälle CCP

Für ein CCP Back-Office-System sind folgende Testfälle durchzuführen.

4.9.1.2.1.1 Berechtigung

Berechtigung ausgeben: *notifyEntitlementIssued*

Berechtigung zurücknehmen: *notifyEntitlementTerminated*

4.9.1.2.1.2 Statische Berechtigung

Statische Berechtigung ausgeben: *notifyStaticEntitlementIssued*

Statische Berechtigung zurücknehmen: *notifyStaticEntitlementTerminated*

4.9.1.2.1.3 Berechtigung Ordered Action Management eCCP

Ausgabe einer Berechtigung über Ordered Action Management:

notifyOrderedEntitlementIssued

Rücknahme einer Berechtigung über Ordered Action Management:

notifyOrderedEntitlementTerminated

4.9.1.2.1.4 Aufträge Ordered Action Management oCCP

Auftrag zur Ausgabe einer Berechtigung: *orderEntitlementIssuance*

Auftrag zur Zurücknahme einer Berechtigung: *orderEntitlementTermination*

Auftrag zur Sperrung einer Berechtigung: *orderEntitlementBlocking*

Auftrag zur Entsperrung einer Berechtigung: *orderEntitlementUnblocking*

4.9.1.2.1.5 Bezahlmethoden

Benachrichtigung, dass mit WEB gezahlt wurde:

notifyStoredValuePaymentMethodDebited

Benachrichtigung, dass das Konto belastet wurde:

notifyAccountBasedPaymentMethodDebited

4.9.1.2.1.6 Blocking und Unblocking

Benachrichtigung, dass ein Terminal eine Berechtigung gesperrt hat:

notifyEntitlementBlocked

Benachrichtigung, dass ein Terminal eine Berechtigung entsperrt hat:

notifyEntitlementUnblocked

4.9.1.2.2 Testfälle SO

Für ein SO Back-Office-System sind folgende Testfälle durchzuführen.

4.9.1.2.2.1 Kontrolle Berechtigung und statische Berechtigung

Berechtigung Kontrolldaten verarbeiten: *notifyEntitlementInspected*

Statische Berechtigung Kontrolldaten verarbeitet: *notifystaticEntitlementInspected*

Berechtigung wurde erfolgreich validiert: *notifyEntitlementValidated*

Berechtigung wurde gesperrt: *notifyEntitlementBlocked*

4.9.1.2.3 CICO

Check in: *notifyCheckin*

Check out: *notifyCheckout*

4.9.2 Regionale Filterbarkeit von Aktionslisten im nationalen Mandanten

Das System stellt im nationalen Mandanten eine Konfigurationsmöglichkeit bereit, um die dort bereitgestellte *Action List* vor dem Versand an den *executing CCP* regional zu filtern.

Die *Action List* im nationalen Mandanten enthält Aufträge, die das Deutschland-Ticket betreffen. Somit kann die *Action List* im nationalen Mandanten sehr groß werden. Damit die Datenmenge für die Terminals handelbar bleibt, muss das System anhand der Filterkonfiguration die *Action List* für den *executing CCP* filtern.

Die Konfiguration sieht vor, dass in den Stammdaten für einen *executing CCP* konfiguriert werden kann, von welchen beauftragenden *CCPs* Aufträge auf der *Action List* enthalten sein sollen. Ist die Konfiguration nicht definiert, so erhält der *executing CCP* die komplette *Action List* zugestellt. Die Konfiguration muss in der Stammdatenverwaltung umgesetzt sein und ist ausschließlich für *executing CCPs* verfügbar.

4.9.3 MPS – Zentrale

Hinweis: Auf Anforderung der Branche wurde für das Zentrale PV-System der VDV-KA eine sog. ZPVS-Zentrale als Weboberfläche, für die an das ZPVS angebundene Verkehrsunternehmen, bereitgestellt, welche diesen den Zugriff auf die durch KVP und DL gemeldeten KA-Transaktionen erlaubt und zeigt, wie der Status der Prüfroutinen innerhalb des Monitorings ist. Zudem ist die Zentrale an das JIRA-System der VDV ETS angebunden, um zu Meldungen im Durchlauf der Prüfroutinen automatisiert Tickets zu erzeugen.

Zusätzlich zu den KVP und DL können die regionalen Produktverantwortlichen als sog. Assistenzzentren (AZ) auftreten, um bei der Abarbeitung der Monitoring Vorfälle, die zu dem AZ zugewiesenen KVP und DL gehören, zu unterstützen.

Analog dazu soll das MPS im nationalen Mandanten den Zugriff auf die D-Ticket Daten in ((etiCORE ermöglichen. Der Zugriff erfolgt auf Basis von besonderen Benutzerrollen, die im Folgenden beschrieben werden. Der Zugriff beschränkt sich dann auf den nationalen Mandanten, dessen Daten auf Basis der Org-ID Zuordnung entsprechend gefiltert sind.

4.9.3.1 Rollen und Rechte im nationalen Mandanten

Das System setzt dazu die drei Rollen *CCP*, *SO* und *AssistanceCenter(AC)* um.

Diese drei Rollen haben lesenden Zugriff auf die Daten im nationalen Mandanten des MPS.

Dieser Zugriff ist wie folgt beschränkt:

- *CCP*: Die Benutzer innerhalb der Rolle *CCP* haben Zugriff auf das Nachrichtenregister und das Monitoring zu Nachrichten, die *Entitlements* und *Inspections* derselben betreffen, die durch den *CCP* ausgegeben worden sind.
- *SO*: Die Benutzer innerhalb der Rolle *SO*, haben Zugriff auf das Nachrichtenregister und das Monitoring zu Nachrichten, die der jeweilige *SO* in den zentralen Mandanten des MPS gesendet hat.
- *AssistanceCenter*: Die Benutzer innerhalb der Rolle *AC* haben Zugriff auf das Nachrichtenregister und das Monitoring zu Nachrichten, die dem *AC* zugeordneten *CCP* und *SO* gehören. Die Zuweisung erfolgt im ESH.

Die *CCP*, *SO* und *AC* können durch die Zuweisung der jeweiligen Org-ID bei der Bearbeitung von auftretenden Klärfällen im Monitoring mitarbeiten.

Ein Benutzer in der Rolle des Assistance Centers ist dabei für POs (oder andere Organisationen) gedacht, die nach Login in das MPS zusätzlichen Einblick auf die nationalen Daten anderer via AssistanceCenter zugeordneter Organisationen im MPS haben möchten und insbesondere im Falle eines regionalen POs ein eigenes System betreiben.

Ist der regionale PO ein Mandant im MPS, so kann über das AssistanceCenter der Zugriff auf die Daten im nationalen Mandanten über zugeordnete CCPs oder SOs gesteuert werden. Innerhalb des MPS-Mandanten kann dann ohne gesonderten Login neben den regionalen Daten auch lesend auf die Daten im nationalen Mandanten der via AssistanceCenter zugeordneten Organisationen zugegriffen werden. Das gilt insbesondere für die Register und Bestände (siehe 4.7).

4.9.4 Optional: Zugriff des nationalen Mandanten auf regionale POs für das D-TICKET

Das Deutschland-Ticket wird in der Regel mit der PO-Org-ID 3000 ausgegeben und wird daher an den nationalen Mandanten im MPS gemeldet. Es ist allerdings auch zulässig, dass Deutschland-Ticket mit der regionalen PO-Org-ID auszugeben, wenn diese Ausgaben und

Kontrollen an das heutige Zentrale PV-System (ZPVS) durch den regionalen PV gemeldet werden.

Sollte dies auch mit ((etiCORE weiterhin zulässig sein, so muss der nationale Mandanten Zugriff auf die Deutschland-Ticket Daten in den regionalen Mandanten haben. Eine Weiterleitung wie im heutigen ZPV-System ist nicht sinnvoll, da die Mandanten dieselbe Datenbank verwenden und der Zugriff so einfacher zu realisieren ist.

Das System muss daher den Zugriff des nationalen Mandanten auf Deutschland-Ticket bezogene Berechtigungen und Kontrollen ermöglichen. Die Zuordnung kann anhand der Product-ID und dem mit dem Deutschland-Ticket verbundenen *productNumber* Bereichs erfolgen.

4.9.5 Optional: Integration von D-Tickets im UIC-FCB Format

Das System muss Nachrichten und Daten, die zu Deutschland-Tickets im UIC Format *Flexible Content Barcode nach UIC 918-9* annehmen und verarbeiten können. Dies kann durch die Filterung der Daten anhand einer der Deutschlandtarifverbund-GmbH (DTVG) zugeordneten *CCP Org-ID* erfolgen, oder in einer dedizierten Ansicht innerhalb des nationalen Mandanten des MPS.

Zum aktuellen Zeitpunkt dieser Ausschreibung ist nicht klar, ob die DTVG Unternehmen Ausgaben und/oder Kontrollen an den nationalen Mandanten des MPS senden werden.

Sofern diese Anforderung konkreter wird, wird eine definierte Spezifikation der gemeldeten Daten zur Verfügung gestellt werden. Die Umsetzung innerhalb des nationalen Mandanten des MPS, erfolgt dann auf Basis dieser Spezifikation.

4.10 Zusatzinformationen zu spezifizierten Warnungen und Fehlern

Das MPS als mandantenfähiges PO-System ist mit einer großen Anzahl Nachrichten konfrontiert. Dabei ist zu unterscheiden, dass zum einen Nachrichten eintreffen können, die Warnungen oder fachliche Fehler enthalten können. Zum anderen sendet das MPS selber - zum Teil automatisiert - spezifizierte Nachrichten mit Warnungen oder fachlichen Fehlern im Rahmen des Monitorings an Dritte bzw. legt bestimmte Informationen ab.

Überall dort, wo Warnungen oder fachliche Fehler involviert sind, muss das MPS ermöglichen, die Systembenutzer mit erweiterten Zusatzinformationen zu unterstützen.

Fehler und Warnungen sind in ((etiCORE mit sprechenden und spezifikationsweit eindeutigen Event-Strings abgebildet, die ohne weitere Information bereits eine gewisse Aussagekraft besitzen.

Beispiel 1: E_PO_RECEIVER_IS_NOT_PRODUCT_OWNER_OF_OBJECT (Das MPS verwendet diesen Event-Identifizier selbst)

- E = Error, führte zu einer Ablehnung der Nachricht: das MPS hat die Nachricht nicht verarbeitet
- PO = Umfeld des Product Owners
- RECEIVER_IS_NOT_PRODUCT_OWNER_OF_OBJECT: Das in der Nachricht befindliche Objekt (z.B. eine Berechtigung) gehört nicht zum Empfänger, dem Product Owner, z.B. ist ein unbekanntes Produkt enthalten. Eine Beschreibung in dieser oder ähnlicher Form kann dann per Abruf angefordert werden

Beispiel 2: E_CCP_RECEIVER_IS_NOT_ENTITY_OWNER (Das MPS erhält diesen fachlichen Fehler beim Weiterleiten vom CCP-System)

- E = Error, führte zu einer Ablehnung der Nachricht: das CCP-System hat die Nachricht nicht verarbeitet
- CCP = Umfeld des Customer Contract Partners
- RECEIVER_IS_NOT_ENTITY_OWNER: Das in der Nachricht befindliche Objekt (z.B. eine Berechtigung) gehört nicht zum Empfänger, dem CCP, z.B. ist eine andere Organisation-ID in der Berechtigungs-ID referenziert. Eine Beschreibung in dieser oder ähnlicher Form kann dann per Abruf angefordert werden
- Zusätzlich in diesem Beispiel erhält das MPS für seine Benutzer eine Information mit einem Lösungsvorschlag. Hier könnte dieser z.B. sein „Prüfen der Berechtigung. Bei Abweichung des CCP vom Empfänger der ION-Nachricht Empfänger anpassen und die Nachricht erneut senden.“

Die Zusatzinformationen inklusive Lösungsvorschlag werden von einer zentralen Stelle abgerufen (siehe 4.10.5).

4.10.1 Events in Nachrichten aus dem ION-Nachrichtenregister

Im Nachrichtenregister werden ein- und ausgehende ION-Nachrichten abgelegt, die potenziell fachliche Fehler- und Warnungen enthalten können. In der jeweiligen Detailansicht, muss dann die Zusatzinformation zu diesem Event angefordert und dargestellt werden (siehe 4.10.5).

4.10.2 Warnungen in den verschiedenen Entitlement-Notification-Registern

In den Registern für Ausgabe, Nutzung und Kontrolle können Warnmeldungen enthalten sein, die bereits von Drittsystemen erzeugt wurden. Für diese Warnungen muss in der Detailansicht der Abruf der Zusatzinformation erfolgen.

4.10.3 Events beim Monitoring

Beim Monitoring sind in erster Linie Warnungen involviert.

Hierbei können beim direkten Monitoring Warnungen entstehen, die dann in die Rückmeldung an das Initiator-System integriert werden. Dies wird im Bereich des ION-Nachrichtenregisters abgedeckt. Beim nachgelagerten Monitoring entstehen Warnungen, die dann als ION-Nachrichten an Dritte gesendet werden. Auch dies wird im Bereich des ION-Nachrichtenregisters abgedeckt.

4.10.4 Warnungen im Bestand

Im Bestand von Applikationen und insbesondere von Berechtigungen können Warnungen gespeichert sein. Für diese Warnungen erfolgt in der Detailansicht ein Abruf der Zusatzinformationen.

4.10.5 Abruf der Event-Information und Lösungsvorschlag

Für den Abruf steht ein zentraler Dienst zur Verfügung, der mit Hilfe des ION-Protokolls angesprochen werden kann. Anfrage und Antwort werden dabei nicht protokolliert. Der Inhalt der Antwort wird extrahiert und an geeigneter Stelle (s.o.) im MPS zusammen mit der Event-ID angezeigt.

Eingaben (Anfrage):

- Event-Identifizier als String
- Gewünschte Sprache (de oder en)
- Anwendungskontext: Dieser Kontext wird noch im Rahmen der MPS-Umsetzung geklärt. Hintergrund ist, dass die Antwort für dasselbe Event bei unterschiedlichem Anwendungskontext unterschiedliche Lösungsvorschläge enthalten kann
- Flag, ob die Lösungsempfehlung benötigt wird oder nicht: Nicht immer wird der Lösungsvorschlag benötigt, z.B. dann, wenn das MPS selbst der Erzeuger des Events ist.

Ausgaben (Antwort in der geforderten Sprache):

- Kategorie (Fehler oder Warnung)
- Bereich (z.B. Product Owner)
- Fehlerbeschreibung
- Lösungsvorschlag (wenn angefordert)

Eingaben und Ausgaben sind in XML-Form. Insbesondere die Ausgabe kann dann leicht in eine Detailmaske einfließen.

4.11 Negativnachweise

Voraussetzung für das Applikations-Monitoring ist die Genehmigung von [15] CR-405 „(((etiCORE: Weiterleiten von Negativnachweisen“ durch die Teilnehmerversammlung am 05.05.2026.

Negativnachweise sind Nachrichten über ungültige Berechtigungen, die bei den allgemeinen Prüfungen bei Kontakt mit den Nutzermedien bzw. bei Kontrollen und Erfassungen entstehen.

Bei (((etiCORE sind diese Nachrichten unter „Extended Logging“ = erweitertes Logging zusammengefasst, wobei hier auch ungültige Applikationen gemeldet werden. Die Nachrichten für ungültige Applikationen sind für das MPS nicht relevant.

(((etiCORE sieht beim Zugriff auf das Nutzermedium eine ganze Anzahl Prüfungen vor, deren Ergebnis jeweils über den enthaltenen Validierungscode spezifiziert ist und beim Fehlschlagen einer der Prüfungen in einer Nachricht für das extended Logging resultiert. Nicht alle diese Nachrichten sind für das MPS relevant. Sie werden im Hintergrundsystem vor dem Senden an das MPS nach Validation Code gefiltert (siehe 4.11.1.1).

4.11.1 Senden der Meldungen an das MPS

Bisher werden diese Nachrichten von den Terminals an das jeweils zuständige Hintergrundsystem weitergeleitet. Der CR in [15] stellt sicher, dass die oben aufgeführten Nachrichten in geeigneter Form an den PO -in unserem Fall an das MPS – weitergeleitet werden.

An das MPS werden nur Negativnachweise gesendet, die bestimmte Validierungscodes enthalten (siehe 4.11.1.1). Die Prüfung/Auswertung dieser Codes wird in 4.11.5 beschrieben.

4.11.1.1 Für das MPS relevante Validierungscodes

Die nachfolgende Tabelle zeigt die für das MPS relevanten Validierungscodes, die in den Negativnachweisen enthalten sind. Die Prüfungen bzw. Auswertungen zu den Codes sind in 4.11.5 beschrieben.

Wert	Kurzbeschreibung
1	Inauthentic Data
3	Spatially Invalid
4	Invalid Personal Entitlement
5	Hotlisted SAM for static Entitlement
6	Hotlisted Organisation for static Entitlement
12	Hotlisted static Entitlement
13	Hotlisted Motics Application
14	SCE-ID found in static entitlement without Motics
16	SCE-ID in static entitlement with Motics does not match SCE-ID in certificate

4.11.2 Entgegennahme der Meldungen

Das MPS muss die Nachrichten vom CCP oder SO empfangen und für das Monitoring aufbereiten. Die Nachrichten müssen im Nachrichtenregister gespeichert werden. Zusätzlich werden sie in das Register für Negativnachweise übertragen, siehe 4.11.4.

4.11.3 Weiterleiten der Meldungen

Das MPS muss nach dem Empfangen und Verarbeiten der Negativnachweise diese Nachweise an den zuständigen primary CCP weiterleiten – falls sie nicht bereits von ihm kommen. Die Weiterleitungen müssen im Nachrichtenregister festgehalten werden.

4.11.4 Register für Negativnachweise

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Notification Type	X	X		Typ der Meldung	Entitlement, Static Entitlement oder (Motics-) Application
Entitlement-ID		X		Entitlement-ID aus der Extended Logging Meldung (nur beim Typ „Entitlement“ und „Static Entitlement“)	
Application Instance ID		X		Applikations-Instanz-ID zu der Berechtigung	Nicht gesetzt bei statischer Berechtigung ohne Motics. Mit Motics ist das die SCE-ID

Feld	Sortieren	Filter	Details	Kurzbeschreibung	Anmerkung
Validation Code	X	X		Code, der das Prüfergebnis widerspiegelt.	Siehe dazu 4.11.1.1
Action Timestamp	X	X		Zeitpunkt der Prüfung	
Terminal-ID	X	X		ID des Ausgabeterminals	
Operator-ID	X	X		Organisations-ID des Terminal-Betreibers	
Location-ID	X	X		ID des Ortes der Prüfung	
ION-Message			X	Referenz auf die ION-Nachricht zu diesem Registereintrag	Muss navigierbar sein zur eingegangenen ION-Nachricht
Inspection Registry Entry			X	Referenz auf Eintrag im Kontrollregister	Dieser Eintrag existiert nur, wenn die Kontrolle bis zum Fehlschlagen der tariflichen Prüfung durchgeführt wurde und somit ein Kontrollnachweis gesendet wurde (Validation Code 3 und 4)

4.11.5 Monitoring-Prüfungen

Grundsätzlich können aufgrund der eingehenden Negativnachweise Monitoring-Prüfungen und Auswertungen gemacht werden:

- Bei Ablehnung von statischen Berechtigungen aufgrund von Hotlist-Einträgen kann die Menge und die räumliche Verbreitung der Fälschungen/Kopien ermittelt werden
- Die Ablehnung von Motics-Applikationen kann ausgewertet werden
- Falsch ausgestellte statische Berechtigungen mit/ohne Motics werden sichtbar
- Gründe für das Scheitern tariflicher Prüfungen, deren Anzahl sowie ggf. räumliche Häufungen werden sichtbar gemacht

Aufgrund der übermittelten Negativnachweise können abhängig vom Validierungscode (siehe 4.11.1.1) Monitoring-Prüfungen oder Auswertungen vorgenommen werden. Alle Negativnachweise werden an den zuständigen CCP weitergeleitet, daher müssen keine zusätzlichen *notifyEvents* Nachrichten aus dem Monitoring gesendet werden. Für die Häufung muss es pro Prüfung und betroffener Organisation einen Schwellwert geben, ab dem vom MPS eine Auswertungsmeldung geschrieben wird. Diese Auswertungsmeldungen

fasst das MPS in einem Report zusammen und stellt diese dem Benutzer nach dem Monitoring der Negativnachweise zur Verfügung.

- Nicht authentische Daten bei Berechtigung oder Applikation (1): Hier wurde betrügerisch versucht, Daten auf dem Nutzermedium zu fälschen.
- Örtlich ungültig (3): Hier kann eine Häufung ein Zeichen für ein schwer verständliches Tarifgebiet oder Produkt sein. Durch Referenz auf den Kontrollnachweis (Inspection Registry Entry) kann auch das zugrundeliegende Produkt ermittelt werden.
- Persönlich ungültig (4): Hier könnte bei Häufung Betrug aufgedeckt werden, z.B. bei fehlendem Personalausweis oder Abweichung von Kundendaten im Ticket. Durch Referenz auf den Kontrollnachweis (Inspection Registry Entry) kann auch das zugrundeliegende Produkt ermittelt werden.
- SAM auf Hotlist (5): offenbar sind immer noch statische Berechtigungen (Tickets), die von einem gehotlisteten SAM signiert wurden, in Umlauf. Hier könnten bei Häufung Betrug, Systemfehler oder fehlerhafte Prozesse zugrunde liegen.
- Organisation auf Hotlist (6): offenbar sind immer noch statische Berechtigungen (Tickets), die von einer gehotlisteten Organisation ausgegeben wurden, in Umlauf
- Statische Berechtigung auf der Hotlist (12): eine statische Berechtigung wurde auf die Hotlist gesetzt. Wenn nun Negativnachweise - ggf. auch örtlich getrennt - auftreten, kann dadurch im Nachgang erkannt werden, dass Kopien der Berechtigung im Umlauf waren
- Applikation auf dem Smartphone für Motics basierte Berechtigungen (13): Es wurde versucht, eine bereits gehotlistete Applikation auf dem Smartphone weiterhin zu nutzen
- In einer statischen Berechtigung wurde eine SCE-ID eingebettet, obwohl der Motics Kopierschutz-Container nicht verwendet wurde (14): Softwarefehler im Ausgabeterminal
- In einer statischen Berechtigung wurde eine SCE-ID eingebettet, die nicht zu der SCE-ID im Zertifikat passt (16): Softwarefehler im Ausgabeterminal oder Betrugsversuch

4.12 Applikations-Monitoring

4.12.1 Voraussetzungen

Voraussetzung für das Applikations-Monitoring ist die Genehmigung von [16], CR-407 “(((etiCORE: Applikations-Monitoring und defekte Medien beim PO“ durch die Teilnehmerversammlung am 05.05.2026.

Mit der Umsetzung von [16] holt das MPS die Hotlist für Applikationen (siehe 4.6.2). Zusätzlich holt das MPS vom ESH-System die Liste der chipkartenbasierten Applikationen, deren Zustand <> „OK“ ist (siehe 4.7.3). Diese Listen werden zentral für alle Mandanten geholt und in die Bestände übertragen.

Zusammen mit den impliziten Notifications, welche die Applikations-Instanz-IDs enthalten (Ausgabe, etc.), spiegeln die Bestände dann vollständig und korrekt die aktuellen Zustände der Applikationen wider.

Für das Applikations-Monitoring sind also die folgenden Voraussetzungen notwendig:

- Das MPS holt regelmäßig die Applikations-Hotlist vom HLS und wertet für seinen Applikations-Bestand aus.
- Das MPS muss die Statusliste für chipkartenbasierte Applikationen regelmäßig vom ESH abholen und in seinen Bestand integrieren. Dabei muss immer der Bestand durch die neueste Statusliste ersetzt werden. Applikationen beim MPS mit dem Zustand „Gesperrt“, deren Applikations-Instanz-ID nicht (mehr) in der ESH-Statusliste und nicht in der Hotlist enthalten ist, muss auf den Zustand „OK“ zurückgesetzt werden. Die dazugehörigen Berechtigungen werden wieder auf den Ursprungszustand zurückgesetzt. Dabei werden die zuletzt bekannten Zustände der Berechtigungen im MPS-Monitoring wiederhergestellt (es dürfen also nicht alle Berechtigungen „entsperrt“ werden, nur weil dies jetzt für die Applikation gemeldet wird).

4.12.2 Monitoring-Prüfungen

Grundlage für das Monitoring ist der Bestand an Applikationen (siehe 4.7.10.2), der für jede Applikation den zuletzt bekannten Zustand enthält.

- Bei allen Meldungen von Berechtigungen:
 - ist die zugehörige Applikation auf der Hotlist? -> Hotlist nicht aktuell beim Meldungserzeuger.

- ist die zugehörige Applikation im Zustand „Gesperrt“ oder „Terminiert“? -> ggf. ist eine Kopie der Applikation im Umlauf
- Das Register für Berechtigungen kann jetzt vollständig geführt werden, da auch die Zustände „Hotlisted“ und „Gesperrt“ und „Terminiert“ der übergeordneten Applikation berücksichtigt werden können. Berechtigungen auf einer solchen Applikation werden automatisch mit gleichem Zustand angenommen wie die übergeordnete Applikation
- Ist eine Applikation nach dem Einarbeiten der Zustandsliste aus dem ESH noch auf der Hotlist, so kommt der primäre CCP seiner Pflicht nicht nach, terminierte oder gesperrte Applikationen von der Hotlist zu entfernen
- **Hinweis:** Damit wird auch ein mandantenübergreifendes Monitoring von Applikationen möglich, auf denen sich Berechtigungen mit Produkten verschiedener POs als Mandanten des MPS befinden

4.12.3 Handhabung verlorener Medien

Bei verlorenen Medien stellt der zuständige primary CCP eine Hotlisting Order („add application to hotlist“) ein, so dass für die Applikation ein Hotlist-Eintrag vorliegt. Dies kann z.B. auf Wunsch des Kunden geschehen.

Bei Erfüllung der Voraussetzungen unter 4.12.1 erhält das MPS die Hotlist-Einträge für verlorene Medien. Damit brauchen verlorene Medien in MPS keine Sonderbehandlung.

4.13 Auskunft über Berechtigungen / Defekte Medien

Das MPS kann angefragt werden, um aus seiner Sicht gültige Berechtigungen für eine übergebene Applikations-Instanz-ID zu ermitteln. Dabei werden nur gültige Berechtigungen gemeldet. Dies kann z.B. zur Unterstützung eines EBE-Prozesses beim SO genutzt werden, z.B. bei defekten Medien. Dazu muss der optionale Anwendungsfall *Determine valid entitlements for given app instance ID* in [4] umgesetzt werden.

Das MPS muss folgende Aspekte beachten, wenn es zu einer übermittelten Applikationsinstanz-ID Berechtigungen suchen und zurückliefern soll:

1. Das MPS prüft für die übergebene Applikations-Instanz-ID in seinem Bestand für Applikationen, ob die Applikation den Zustand „Hotlisted“, „Gesperrt“ oder „Terminiert“ hat

2. Das MPS prüft, ob die Applikation zu der Applikations-Instanz-ID noch gültig ist und schaut dazu in den Bestand (4.7.10.2). Falls dort der Zeitraum nicht eingetragen ist, erfolgt automatisch eine Abfrage über LDAP zum Nutzermedium-Zertifikat
3. Das MPS prüft, ob zu der Applikations-Instanz-ID Berechtigungen im Bestand vorliegen

Für jede Berechtigung:

4. Berechtigung ist zeitlich gültig (zum Zeitpunkt der Anfrage)
5. Berechtigung ist nicht gesperrt
6. Berechtigung befindet sich nicht auf der Hotlist
7. Berechtigung gehört nicht zu einem offenen Klärfall (z.B. Timeout bei Ausgabe)
8. Kein mit der Berechtigung involviertes SAM befindet sich auf der Hotlist
9. Keine mit der Berechtigung involvierte Organisation befindet sich auf der Hotlist

Verbleibende Berechtigungen werden als Liste in der Antwort zurückgegeben.

Für Punkt 1. Ist das Applikations-Monitoring aus 4.12 Voraussetzung.

Hinweis: Der primary CCP erhält vom Teilnehmer, der das defekte Medium erfasst hat, eine Sperranforderung (Hotlisting Demand) für die Applikation mit dem Sperrgrund „22 – Defective Medium“ (bereits in etiCORE spezifiziert). Damit ist der primary CCP über den Sachverhalt informiert. Durch die Nachricht (Sperranforderung) zu dem defekten Medium kann der pCCP automatisch Betrugsversuche auf Kundenseite erkennen, insbesondere weil er die Informationen zu den Sperrnachweisen für Applikationen hat. Der primary CCP stellt danach die Applikation per Hotlisting Order in die Hotlist beim HLS ein. Damit sind defekte Medien zeitnah - aber nicht in Echtzeit - auf der Hotlist.

4.14 Mandantenübergreifende Produktanerkennung

Das System muss Produktinformationen über mehrere Mandanten hinweg verknüpfen können.

An den Grenzen der Verbundräume der PO gibt es in der Praxis Anerkennungsregeln für Produkte aus anderen Verbünden. Damit diese Anerkennung nicht zu Warnungen innerhalb des Monitorings führt, stellt das System, über die Zuordnung in der Produktverwaltung (Kapitel 4.3.5), Konfigurationsmöglichkeiten für die Verknüpfung bzw. Definition von Anerkennungsregeln von Produkten anderer PO zur Verfügung.

4.15 Online-ALISE

Als Ergänzung zur Bereitstellung der *Action Lists* für die CCP-S (*Customer Contract Partner Back-Office Order Execution Module*) muss das MPS den CCP-T (*Customer Contract Partner Terminal Order Execution Module*) die Möglichkeit bieten, auf das aktuelle (also nicht zykel-basierte) *Order Inventory* (Hinweis: mit *Order Inventory* ist der [folgende Datastore aus der etiCORE-Spezifikation](#) gemeint) zuzugreifen. Diese Funktionalität wird mittels CR-403 “(((etiCORE: Online-Zugriff auf das Aktionsmanagement“ [14] in (((etiCORE integriert. Das MPS muss CR-403 “(((etiCORE: Online-Zugriff auf das Aktionsmanagement“ [14] vollständig konform (fully conformant) umsetzen.

Die Kommunikation zwischen den *Terminals* und dem MPS muss wie in Delegated authorisation framework [18] beschrieben erfolgen. Das MPS ist in diesem Konzept ein *Resource Server*. Diese Architektur wird für das MPS wie folgt ausgestaltet:

- Die *Resource* in diesem Konzept ist das *Order Inventory* eines Mandanten.
- Das MPS muss den Use Case *Managing access to a resource* umsetzen, indem es den Mandanten die Möglichkeit bietet, festzulegen, die *Terminals* welcher CCP (identifiziert durch ihre *Org ID*) auf das *Order Inventory* des Mandanten zugreifen dürfen. (Die etiCORE-Rolle zur *Org ID* ist immer CCP.)
- Das MPS muss den Use Case *Updating the list of Authorisation Servers* umsetzen.
- Das MPS muss den Use Case *Accessing a Resource* umsetzen. Die Fachdaten einer solchen Anfrage bestehen ausschließlich aus einer *UM App Instance ID*. Die Fachdaten einer solchen Antwort bestehen ausschließlich aus einer optionalen Liste von zu dieser *UM App Instance ID* vorliegenden *Action List Entries*, deren *Order* im *State Active* ist. (Hinweis: *Action List Entries* sind Bestandteil der *Orders*, den *State* führt das MPS zusätzlich.) Das MPS muss den Zugriff sowohl mandantenscharf als auch mandantenübergreifend ermöglichen, beispielsweise durch Anbieten eines übergreifenden Endpunkts und je eines mandantenscharfen Endpunkts pro Mandanten. Bei Zugriff über den übergreifenden Endpunkt muss das MPS die *Order Inventories* all jener Mandanten berücksichtigen, die dem anfragenden CCP den Zugriff auf ihr *Order Inventory* gewährt haben.

4.16 JIRA Integration

Das System setzt die Integration des JIRA Service Desk der Firma Atlassian um, sodass durch die bearbeitenden Benutzer zu Monitoring-Vorfällen JIRA-Tickets erzeugt werden

können. Diese können dann, durch die betroffenen Unternehmen bearbeitet und gelöst werden. Die Zuweisung der Bearbeiter in JIRA erfolgt auf Basis der existierenden SSO-Benutzer in ESH und JIRA.

Die Anbindung des Jira Service Management Systems erfolgt über die Jira Service Management API JIRA Service Management API [19].

Der verwendete Atlassian Mandant nutzt das in Kapitel 4.4.1 beschriebene SSO-Verfahren. Die im JIRA verwendeten Benutzer, werden über das ESH-System verwaltet.

4.17 ION An-/Abmeldung

Das MPS muss - wie in [etiCORE](#) gefordert - dem Mandanten die Möglichkeit bieten, jeden Dienst des Mandanten einzeln an- und abzumelden. Das MPS muss den Zielzustand per Mandantenwunsch dauerhaft speichern. Bevor das MPS ordnungsgemäß nicht mehr erreichbar sein wird (z. B. aufgrund Wartung, Stilllegung), muss es alle von den Mandanten angemeldeten Dienste abmelden. Sobald das MPS wieder erreichbar ist, muss es genau die Dienste wieder anmelden, die laut Mandantenwunsch angemeldet sein sollten (entspricht denen, die es zuvor kurz vor der Wartung abgemeldet hat).

4.18 Sperrlisten für Dritte

Das MPS muss sicherstellen, dass jeder Mandant seine Sperrlisten nur für autorisierte Dritt-Anbieter automatisiert und standardisiert bereitstellen kann.

Die im Kapitel 4.6.3 beschriebenen Sperrlisten aus den jeweiligen Hotlist Inventories werden durch das MPS automatisch exportiert und in den jeweiligen mandantenspezifischen FTP-Bereich abgelegt. In dem Bereich sind Sperrlisten aus den letzten n Zyklen zu finden. Die Zahl n muss konfigurierbar für Systembetreiber sein. Das MPS muss sicherstellen, dass ältere Sperrlisten automatisch aus dem FTP-Server entfernt werden.

Dritt-Anbieter müssen über einen definierten technischen Zugriffspunkt (FTP-Server) jederzeit auf die für sie relevanten Sperrlisten zugreifen können. Der FTP-Server muss sichere Übertragungsprotokolle wie SFTP oder FTPS unterstützen. Sollte ein anderes Übertragungsprotokoll in Frage kommen, dann muss der Softwarehersteller dies mit ETS abstimmen.

Zusätzlich muss der Mandant-Administrator im MPS in der Lage sein, selbstständig Zugänge für Dritt-Anbieter zu erstellen, zu verwalten und zu kontrollieren. Die Verwaltung

der Zugriffsdaten muss für Mandanten einfach und ohne tiefgehendes technisches Know-how bedienbar sein.

Der Mandant Admin muss über die Funktionen des MPS in der Lage sein:

- FTP-Zugangskonten für Dritt-Anbieter anzulegen.
- Jedem Dritt-Anbieter den mandantenspezifischen Ordner als Zugriffsbereich zuzuweisen.
- Zugangsdaten (Benutzername, Passwort, Token oder Zertifikat) zu generieren und an den Dritt-Anbieter via MPS weiterzugeben.
- Zugängen zu sperren, entsperren oder Zugangsdaten zu erneuern.

Zugriffe auf Sperrlisten müssen protokolliert werden, um nachvollziehen zu können, welcher Dritt-Anbieter (z.B. anhand Zugangsdaten) wann auf welche Dateien zugegriffen hat.

MPS muss sicherstellen, dass Drittanbieter-Systeme Sperrlisten im MPS ausschließlich lesen oder abrufen/herunterladen dürfen. Der Mandant darf lesen oder abrufen/herunterladen und löschen.

4.19 Optional: Anbindung von Online-Ticketspeichern

Das System ermöglicht die Anbindung von externen Berechtigungs- bzw. Tokenspeichern, an einzelne Mandanten,

Im Rahmen des Themas Account-Based-Ticketing bzw. Server-Based-Ticketing, werden die Berechtigungs- bzw. *Entitlement*-Daten nicht mehr auf dem *Usermedium*, sondern Online in einem Ticketspeicher vorgehalten. Ein solcher Ticket- und Token-Speicher muss für das Monitoring direkt an das PO-System angebunden werden.

Solche Ticketspeicher werden derzeit noch spezifiziert und werden Tokens, welche auf Berechtigungen in den verschiedenen Systemen referenzieren und ggf. die zugehörigen Berechtigungen selbst enthalten. Dies können auch CheckIn-Tokens auf Basis von Kredit- oder Girokarten sein.

5 Grafische Oberflächen

Die grafischen Oberflächen werden hinsichtlich Gestaltung, Bedienkonzept und Nutzerführung in gemeinsamer Abstimmung zwischen Auftragnehmer und Auftraggeber in den in Kapitel 2.2 Workshops zur Ausarbeitung grafischer Oberflächen spezifiziert. Für das System ESH liegen bereits grafische Mockups in Figma [17] vor, die als gestalterische Referenz in den Workshops heranzuziehen sind.

5.1 Allgemeine Gestaltungsprinzipien

Die Benutzeroberfläche muss übersichtlich, konsistent und modern gestaltet sein. Sie hat eine klare visuelle Hierarchie aufzuweisen und den Nutzer bei der Orientierung und Bedienung zu unterstützen.

Die Gestaltung und Bedienung der Benutzeroberfläche muss sich an den aktuellen Regeln der Softwareergonomie nach ISO 9241 orientieren. Dialoge und Interaktionselemente sind, soweit möglich, barrierearm und barrierefrei umzusetzen.

Die Benutzeroberfläche ist responsiv zu gestalten, sodass eine sinnvolle Nutzung auf unterschiedlichen Bildschirmgrößen sowie Mobilgeräten möglich ist, sofern dem keine fachlichen oder technischen Einschränkungen entgegenstehen.

Interaktionen, visuelle Rückmeldungen sowie Zustände von Elementen sind konsistent und nachvollziehbar umzusetzen.

5.2 Sprache

Die primäre Sprache des MPS ist Deutsch. Das System muss so gestaltet sein, dass eine spätere Ergänzung weiterer Sprachen über Konfigurationsdateien möglich ist und jeder Nutzer seine Sprache selbst über das MPS aus den hinterlegten Sprachen wählen kann. Das Auswählen einer anderen Sprache muss nahtlos alle Texte in jeglichen Ansichten und Dialogen auf die gewählte Sprache übersetzen. Ausgenommen von der Übersetzung sind lediglich Daten.

5.3 Typografie

Unterschiedliche Textelemente wie Überschriften, Fließtexte, Hinweise und ergänzende Informationen müssen visuell klar unterscheidbar sein.

Die Typografie muss eine gute Lesbarkeit gewährleisten und die Strukturierung von Inhalten unterstützen.

5.4 Farben und visuelle Gestaltung

. Das Farbschema des Systems wird innerhalb der in Kapitel 2.2 definierten Workshops festgelegt. Dies umfasst insbesondere Primär- und Sekundärfarben, Akzentfarben sowie Farben für Status- und Hinweismeldungen. Farben sind konsistent einzusetzen.

5.5 Navigation und Seitenstruktur

Die Hauptnavigation muss eine klare Struktur der verfügbaren Funktionen ermöglichen.

Ergänzende Navigationselemente wie Breadcrumbs, Stepper oder kontextbezogene Navigationen sind, sofern vorgesehen, gestalterisch einheitlich umzusetzen.

5.6 Interaktionselemente

Buttons und vergleichbare Interaktionselemente sind hinsichtlich Form, Größe, Farbgebung und Zustandsdarstellung werden innerhalb der in Kapitel 2.2 definierten Workshops festgelegt..

Eingabefelder, Auswahlfelder und weitere Formularelemente sind gestalterisch und hinsichtlich ihres Interaktionsverhaltens konsistent umzusetzen.

Formulare sind klar strukturiert darzustellen. Hinweise, Validierungen und Rückmeldungen sind verständlich und einheitlich zu gestalten.

5.7 Tabellen und Listen

Tabellen- und Listenansichten werden hinsichtlich Aufbau, Darstellung und Interaktion innerhalb der in Kapitel 2.2 definierten Workshops festgelegt.. Geforderte Aktionsmöglichkeiten wie z.B. das Ausblenden von Spalten in gewissen Ansichten sind so umzusetzen, dass sie sich nahtlos in das Look and Feel des Systems einfügen.

Unterschiedliche Zustände wie leere Inhalte, Ladezustände oder Fehlersituationen sind einheitlich darzustellen.

Filter-, Such- und Auswahlkomponenten werden gestalterisch und konzeptionell innerhalb der in Kapitel 2.2 definierten Workshops festgelegt.. Aktive Filter oder Einschränkungen müssen für den Nutzer klar erkennbar sein.

Für jede tabellarische Übersicht besteht die Möglichkeit, die aktuell dargestellten Daten in ein CSV-Format zu exportieren.

5.8 Hinweise, Meldungen und Statusanzeigen

Hinweise, Warnungen, Fehlermeldungen und Bestätigungen sind einheitlich zu gestalten und klar voneinander zu unterscheiden. Die Darstellung wird innerhalb der in Kapitel 2.2 definierten Workshops festgelegt und müssen dem Nutzer verständliche Informationen bereitzustellen.

5.9 Avatare und benutzerbezogene Darstellungen

Darstellungen von Benutzern, Avataren oder benutzerbezogenen Informationen werden innerhalb der in Kapitel 2.2 definierten Workshops festgelegt.

5.10 Referenz

Die Figma-Mockups [17] des Systems ESH gelten als maßgebliche gestalterische Referenz. Im Verlauf der Umsetzung ist sicherzustellen, dass relevante Weiterentwicklungen des ESH-Designs berücksichtigt werden.

Hinweis: Die Nutzung von vue.js und PrimeVue wird empfohlen, um möglichst einfach die Benutzerführung und Optik des ESH zu adaptieren.

6 Schnittstellen

Das MPS muss eine Vielzahl an Schnittstellen umsetzen. Das Schaubild in Abschnitt 1.4 gibt bereits einen Überblick.

Die Kommunikation des MPS mit den folgenden Systemen muss über das *ION* erfolgen (Details siehe ((etiCORE Interface Specification, Release Candidate 6 [12]):

- *Hotlist Service System*
- *Service Operator System*
- *Customer Contract Partner System*
- *eTicket Security Hub*
- *Central Routing Engine*

Für diese Kommunikation muss der ION-Adapter eingesetzt werden. Dieser wird beigestellt. Der ION-Adapter bietet einen simplen Endpunkt für das MPS, um Nachrichten

ins *ION* zu schicken und erwartet einen Endpunkt pro adaptiertem *etiCORE Service* für eingehende Nachrichten aus dem *ION*. Jede Instanz des ION-Adapters adaptiert genau eine Kombination aus *Organisation ID* und *etiCORE Rolle*. Durch den Einsatz des ION-Adapters entfällt auch die Notwendigkeit für das MPS, auf die *ION-PKI* zuzugreifen, weil diese Aufgabe vom ION-Adapter übernommen wird.

Für das Onboarding neuer Mandanten ist eine weitere Schnittstelle zwischen MPS und ESH erforderlich.

Siehe [18] Delegated authorisation framework für die Kommunikation zwischen *Terminals* und dem *MPS*.

Die Kommunikation zwischen den Third parties und dem MPS muss via FTP mit geeigneter Sicherungsschicht erfolgen. Für die fachlichen Details siehe Abschnitt 4.18 Sperrlisten für Dritte.

Die Kommunikation zwischen MPS und Media PKI muss via LDAPS erfolgen. Details siehe [etiCORE Spec.](#)

Die Kommunikation zwischen MPS und SSO muss über Open ID Connect oder SAML erfolgen.

Die Kommunikation zwischen MPS und Jira Service Management muss über die von Atlassian angebotene Schnittstelle erfolgen.

7 Datenmodelle

Die nachfolgenden Kapitel beschreiben das Zusammenspiel von Registern und Beständen sowie dem Hotlist-Inventory bzw. dem Sperrwesen. Die Benutzerverwaltung inklusive Rechte- und Rollen-Konzept ist nicht Bestandteil dieses Kapitels. Es handelt sich um eine logische Darstellung und nicht um eine technische Vorgabe zu einem normalisierten Datenbankmodell. Es dient in erster Linie zum besseren Verständnis für die Relationen zwischen den Entitäten.

Insbesondere muss das reale Datenmodell mit technischen Schlüsseln (statt der fachlichen IDs) umgesetzt werden. Diese Schlüssel werden hier ebenfalls nicht gezeigt.

7.1 Übersicht

Abbildung 16 zeigt die Übersicht eines logischen Datenmodells für die Register, Bestände und HLS-Konfiguration sowie Teile der Organisations- und Produktverwaltung. Die gezeigten Verknüpfungen entsprechen den Beschreibungen aus 4.6.1 und 4.7.

Die dargestellten Entitäten enthalten aus Darstellungsgründen keine Attribute. Die Attribute sind den Texten in den Einzelkapiteln bzw. den tabellarischen Darstellungen zu entnehmen.

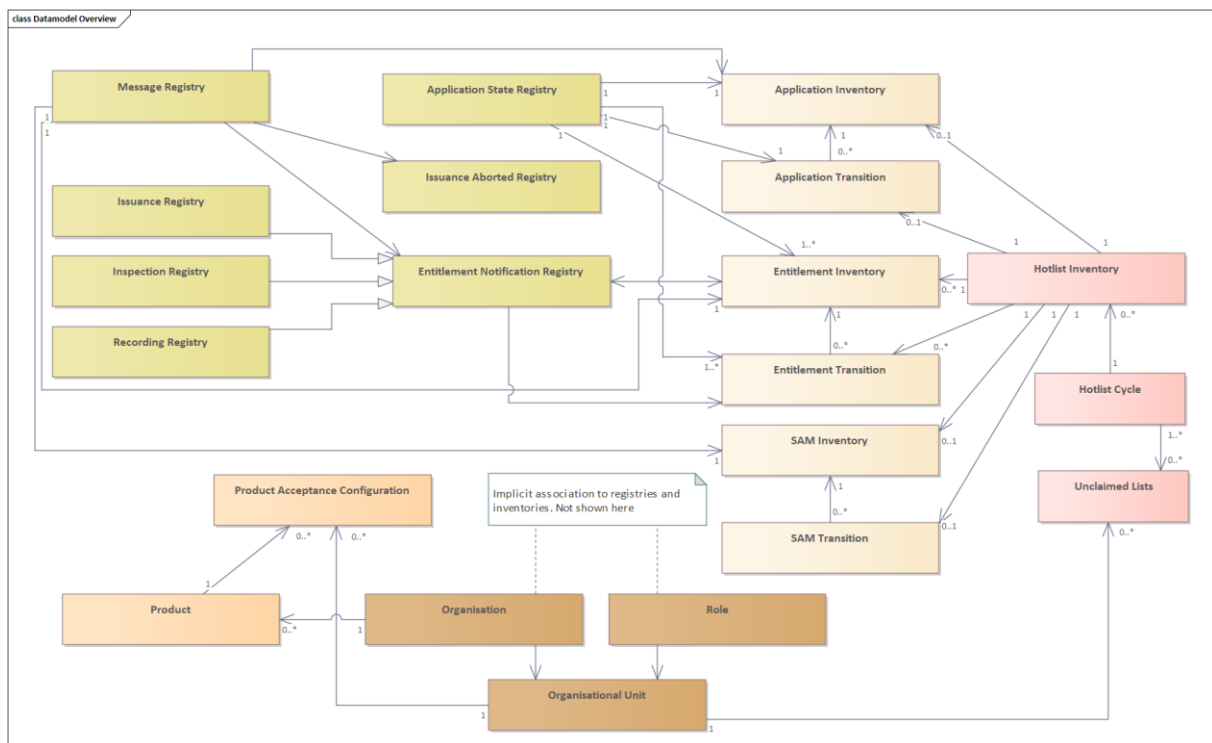


Abbildung 16: Datenmodell für Register, Bestände und HLS Konfiguration

7.2 Benötigte Stammdaten

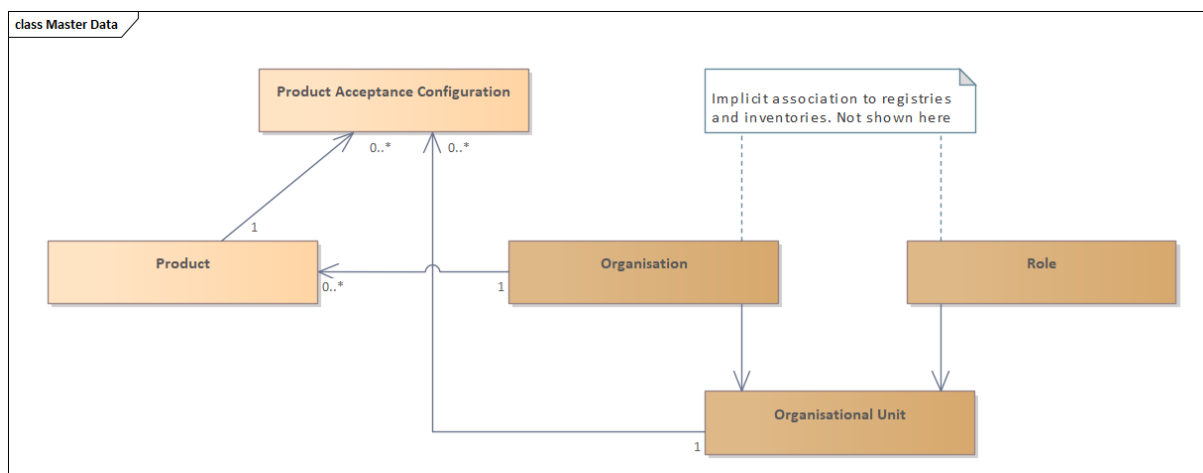


Abbildung 17: Stammdaten Organisationen und Produkte

7.2.1 Organisationsverwaltung

Siehe auch 4.3.4. Hier wird nochmal die Verknüpfung zwischen den Organisationen und Rollen gezeigt. Die Entität dazu ist die Organisationseinheit (Organisational Unit, Kombination aus Organisation und Rolle).

7.2.2 Produktverwaltung

Siehe auch 4.3.5. Hier wird die Entität für die Produkte gezeigt.

7.3 Register

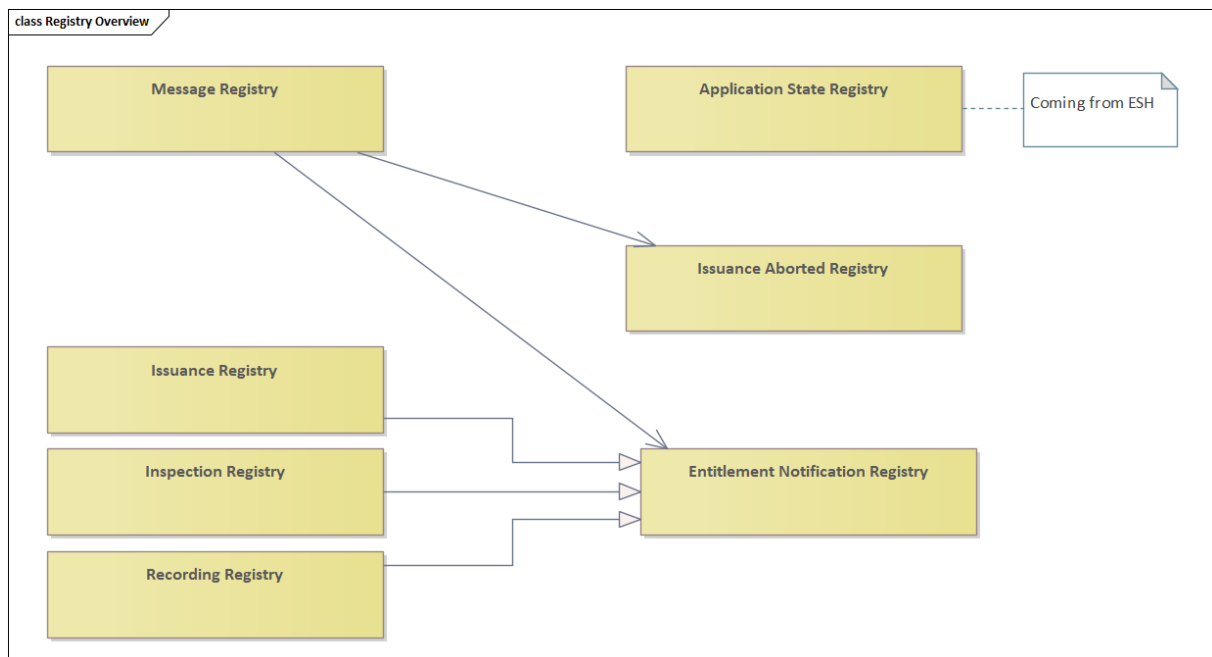


Abbildung 18: Register im MPS

Die Register sind in Kap. 4.7 beschrieben. Das ION-Nachrichtenregister speichert die ION-Nachrichten. Zugehörige Register-Einträge werden in die zuständigen Unterregister transferiert. Die Register für Ausgabe, Kontrolle und Nutzung sind Spezialfälle des Registers für Berechtigungsmeldungen. Abbrüche von Berechtigungsausgaben werden in einem eigenen Register geführt, welches das MPS direkt über das ION-Nachrichtenregister befüllt.

Jeder Registereintrag hat eine Verknüpfung zu seiner übergeordneten ION-Nachricht. Damit kann vom Registereintrag zur ION-Nachricht navigiert werden. Des Weiteren ist jeder Registereintrag mit dem aktuellen Bestandseintrag verknüpft. Z.B. zeigt ein Kontrollnachweis auf den aktuellen Eintrag für die Berechtigung (inklusive Historie).

7.4 Bestände (Inventories)

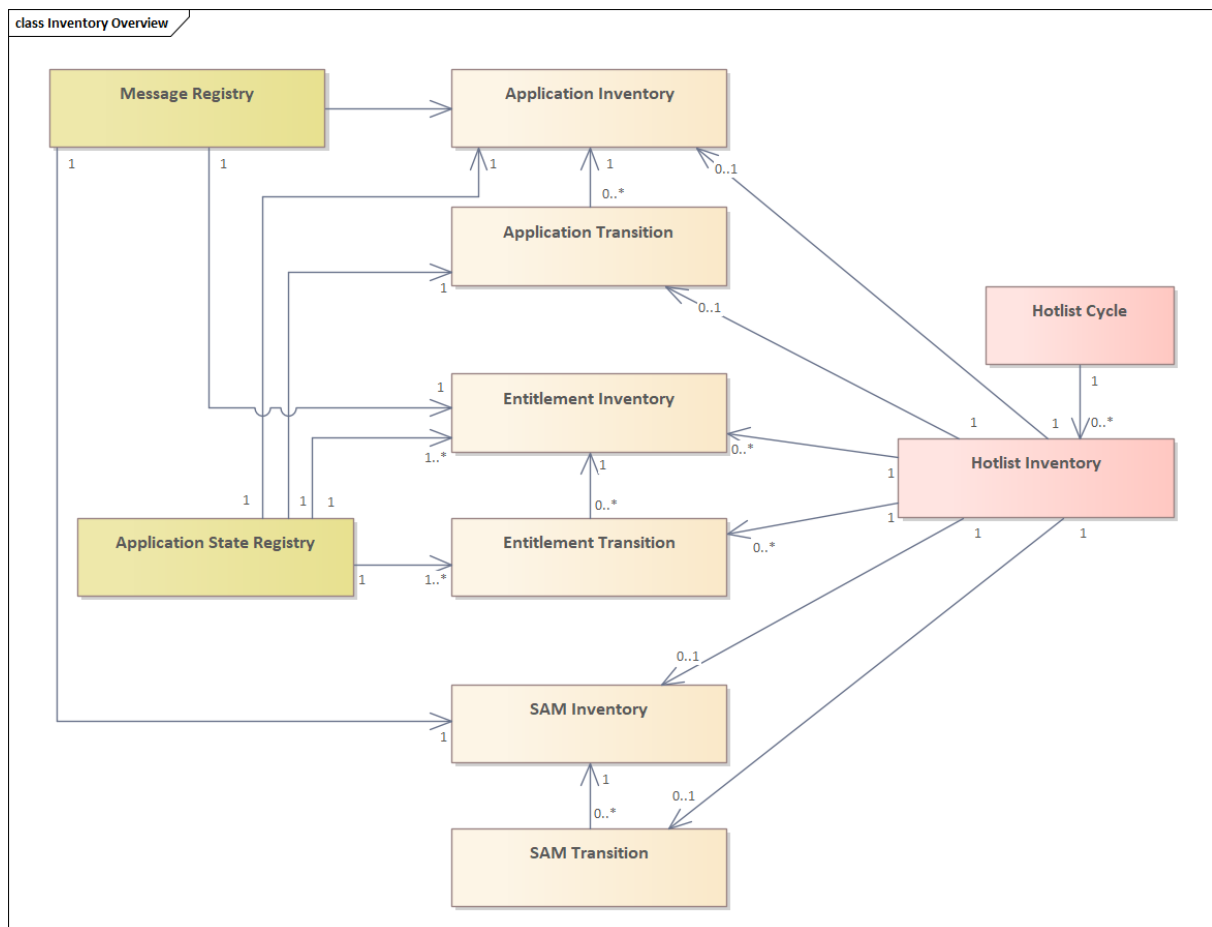


Abbildung 19: Bestände für Berechtigungen, Applikationen, SAMs und Hotlist-Einträgen

Abbildung 19 zeigt die Übersicht der verschiedenen Bestände. Die Bestände werden vom MPS implizit über die Notifications aus dem ION-Nachrichtenregister gefüllt (Berechtigung, Applikation und SAM) bzw. über das Abholen der Hotlists (Hotlist-Eintrag-Bestand). Die Bestände für Berechtigung, Applikation und SAM haben eigene Statusübergang-Historien. Diese sind mit dem Hotlist-Eintrag-Bestand verknüpft, falls ein Hotlist-Eintrag besteht.

Des Weiteren sind die Bestände und Statusübergang-Historien mit den Registern verknüpft. Dadurch wird festgelegt, welcher Registereintrag zu einer Änderung in der Historie geführt hat.

8 Mandantenfähigkeit

Die Mandantenfähigkeit ist eine zentrale Eigenschaft des Systems, da mehrere Verkehrsverbünde (Mandanten) innerhalb einer Lösung betrieben werden sollen. Jeder Mandant repräsentiert ein im ESH registriertes Unternehmen mit der etiCORE Rolle Product Owner wie beschrieben im etiCORE Rollenmodell. Die konkrete technische Umsetzung (z. B. Single-Instance-Multi-Tenant, getrennte Instanzen, hybride Ansätze) ist nicht Bestandteil des Lastenheftes und wird bewusst dem Auftragnehmer überlassen. Maßgeblich ist ausschließlich die Erfüllung der nachfolgend beschriebenen Anforderungen. In der Initialphase ist mit ca. 20–30 Mandanten zu rechnen. Maximal werden nicht mehr als 60 Mandanten erwartet.

8.1 Begriffsdefinition Mandant

Ein Mandant einer *Registered Company* mit einem Teilnehmer Vertrag mit der etiCORE Rolle PV im ESH in der Regel einem Verkehrsverbund bzw. einer organisatorisch und fachlich abgegrenzten Einheit innerhalb des Ökosystems. Ein Mandant kann mehrere OrgIDs umfassen. Die Information über die Zuordnung von OrgIDs zu einem Mandanten kommt aus dem ESH-System wie beschrieben in 4.4.3.

Jeder Mandant agiert eigenständig, verfügt über eigene Stammdaten, Konfigurationen, Nutzerberechtigungen und operative Daten (z. B. Transaktionen, Kontrollen, Fehlermeldungen), sofern nicht explizit anders beschrieben.

8.2 Grundanforderungen an die Mandantenfähigkeit

Das System muss folgende grundlegende Eigenschaften der Mandantenfähigkeit erfüllen:

- **Trennung der Mandanten:** Daten, Konfigurationen und Prozesse eines Mandanten müssen logisch von denen anderer Mandanten getrennt sein. Ein Mandant darf ausschließlich auf die ihm zugeordneten Daten zugreifen, sofern keine explizit freigegebenen mandantenübergreifenden Anwendungsfälle oder Daten (z.B. über das AssistanceCenter konfiguriert, siehe 4.9.3.1) vorliegen.
- **Einheitliche Servicelevel:** Für alle Mandanten gelten identische Anforderungen an Verfügbarkeit, Performance und Aufbewahrungsfristen. Unterschiedliche mandantenspezifische Servicelevel oder Betriebsparameter sind nicht vorgesehen.

- **Sicherheit:** Die Mandantenfähigkeit muss den Schutz sensibler Daten gewährleisten. Insbesondere sind unautorisierte Zugriffe zwischen Mandanten technisch und organisatorisch auszuschließen.
- **Monitoring und Betrieb:** Der Betrieb muss eine mandantenspezifische Überwachung (z. B. Fehlerraten, Datenvolumen, ggf. Systemzustand,) ermöglichen, ohne andere Mandanten offenzulegen.

Die Anforderungen sind genauer in den einzelnen Bereichen innerhalb der Qualitätsanforderungen "MPS_Qualitätsanforderungen_V0.9.pdf" [1] beschrieben.

9 Mitgeltende Dokumente

- [1] Qualitätsanforderungen "MPS_Qualitätsanforderungen_V0.9.pdf"
- [2] ION-Specification "etiCORE SPEC-ION_v3.0.0-rc.6 en"
- [3] Main Specification "etiCORE SPEC-MAIN_v3.0.0-rc.6 en"
- [4] Product Owner Reference System Specification "etiCORE SPEC-PO-RS_v3.0.0-rc.6 en"
- [5] Hotlist Service System Specification "etiCORE SPEC-Hotlist_v3.0.0-rc.6 en"
- [6] Customer Contract Partner Reference Terminal Specification "etiCORE SPEC-CCP-RT_v3.0.0-rc.6 en"
- [7] Customer Contract Partner Reference System Specification "etiCORE SPEC-CCP-RS_v3.0.0-rc.6 en"
- [8] Service Operator Reference System Specification "etiCORE SPEC-SO-RS_v3.0.0-rc.6 en"
- [9] (((eTicket Security Hub Specification "etiCORE SPEC-ESH_v3.0.0-rc.6 en"
- [10] Central Routing Engine Specification "etiCORE SPEC-CRE_v3.0.0-rc.6 en"
- [11] (((etiCORE Media PKI Specification "etiCORE SPEC-Media-PKI_V1.0.0"
- [12] [\(\(\(etiCORE Interface Specification](#), Release Candidate 6
- [13] [\(\(\(etiCORE Specification Model](#), Release Candidate 6
- [14] [CR-403](#) "(((etiCORE: Online-Zugriff auf das Aktionsmanagement"
- [15] [CR-405](#) „(((etiCORE: Weiterleiten von Negativnachweisen"
- [16] [CR-407](#) "(((etiCORE: Applikations-Monitoring und defekte Medien beim PO"
- [17] Figma UI Elemente "Layout Allgemeine Elemente (Stand_ 08.09.2025).png"
- [18] Delegated authorisation framework v1.1
- [19] [JIRA Service Management API](#)
- [20] Anlage_2_Erklärung_über_technische_und_funktionale_Eigenschaften

