gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Übergreifende Richtlinien zum Betrieb der TI

Version:	1.7.4
Revision:	\main\rel_online\rel_ors1\68
Stand:	06.05.2015
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemRL_Betr_TI]

Dokumentinformationen

Änderungen zur Vorversion

In das vorliegende Dokument wurden Korrekturen aus der Prozessablaufsimulation eingearbeitet.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	29.06.12		zur Abstimmung freigegeben	PL P77
0.6.0	07.09.12		zur Abstimmung freigegeben	PL P77
1.0.0	15.10.12		zur Abstimmung freigegeben	gematik
	06.11.12		Einarbeitung Kommentare aus übergreifender Konsistenzprüfung	P77
1.1.0	12.11.12		freigegeben	gematik
1.1.1	15.02.13		CR 168 Lösungszeiten im Anwendersupport eingearbeitet	P77
1.1.9	22.04.13		zur Abstimmung freigegeben	gematik
			Einarbeitung Kommentare LA	P77
1.2.0 RC	30.05.13		zur Freigabe empfohlen	PL P77
1.2.0	06.06.13		freigegeben	gematik
1.2.1	08.08.13		Einarbeitung gemäß Änderungsliste	PL P77
1.3.0	15.08.13		freigegeben	gematik
1.3.1	29.09.13	Anhang B	CR 662: Anpassung Regelungen zum Reporting und Notfallmanagement für RU	P77
1.4.0	25.09.13		freigegeben	gematik
1.4.1	09.12.13	Kap. 2.3.1	Einarbeitung C_719 - um eine Klarstellung ergänzt	gematik
1.5.0	17.12.13		freigegeben	gematik
1.5.1	07.02.14	4.3.2, 8.7	Einarbeitung Fehlerkorrekturen: C_2025: fehlende Zeile 5 mit Messgröße in Struktur des Performance-Reports eingefügt C_2026: Detaillierung der Strukturvorgabe für Incident-Dokumentation im Datenfeld 16 "Incident Worklog":	gematik
			Losübergreifende Synchronisation	PL P77
1.6.0	21.02.14		freigegeben	gematik
1.6.1	04.06.14	2.5	Einarbeitung Änderungen aus P11: C_4136:	P77

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
		8.4.5, 9.4.4 8.6, 9.8 2.3.1 8.5.6 9.10 4.3 3.4.2	- Konvention zum csv Datenschema ergänzt und präzisiert - Erhöhung der fortlaufenden Nr. für Incidents und Problems auf 5 Stellen - Präzisierung der Vorgaben zur Incident- und Problemdokumentation C_4137 - Konfigurationsreport in zwei Einzelreports aufgeteilt, neue Dateinamen eingefügt C_4139 - Einführung neuer Incidentstatus: „gelöst“ C_4140 - Adhoc Reporting: Pflicht zur Übermittlung von Fehlerlogs, Systemprotokollen der Produktinstanzen und lokalen Incidents an den SBV C_4141 - Präzisierung der Vorgaben zum Performance Report, Fehlerkorrektur Datenschema C_4142 - SL-Report: Fehlerkorrektur zur Einheit der Auswertedauer	
1.7.0	04.07.14		freigegeben	gematik
1.7.1	03.09.14	9.8	Tab_Betr_TIP_021, Zeile 11/Spalte Feldname Problem – Beschreibung statt Problem Beschreibung	gematik
	03.02.15		Einarbeitung von Korrekturen aus der Prozessablaufsimulation	gematik
1.7.2	04.02.15		Abstimmung mit den Auftragnehmern	gematik
1.7.3	18.02.15		zur Abstimmung freigegeben	gematik
	25.03.15		Einarbeitung der Änderungen zur Einführung der Zentralen Informationsdrehscheibe	gematik
1.7.4	08.04.15		zur Abstimmung freigegeben	gematik
			Einarbeitung Kommentierung	
1.7.4 RC 2	28.04.15		zur Freigabe empfohlen	gematik
1.7.4	06.05.15		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen 2

Inhaltsverzeichnis 4

1 Einordnung des Dokuments 9

1.1 Zielsetzung 9

1.2 Zielgruppe 10

1.3 Geltungsbereich 10

1.4 Abgrenzung des Dokuments 10

1.5 Methodik 11

2 Prozessübergreifende Regelungen 12

2.1 Prozessübergreifende Begriffserläuterungen 12

2.1.1 Information, Eskalation, Report 12

2.1.2 Teilnehmer-ID (TID) 13

2.2 Prozessübergreifende Kommunikation 13

2.3 Reporting 16

2.3.1 Konsolidiertes Reporting 16

2.3.2 Ad-hoc Reporting 18

2.3.3 Service Level Requirements (SLR) 18

2.4 Auditierung von Anbietern und Herstellern 19

2.5 Konvention zur Übermittlung von Prozessdaten 19

2.5.1 Basisfeldtypen von Prozessdaten 24

3 Service Level Management (SLM) 26

3.1 Betrachtungsgegenstand des übergreifenden SLM 26

3.2 Begriffserläuterungen 27

3.2.1 Service Level Requirements 27

3.3 Grundsätze des übergreifenden SLM 27

3.3.1 Gliederung des SLM in Service Level Cluster 27

3.4 Prozessdurchführung übergreifendes SLM 28

3.4.1 Messung der Service Level 28

3.4.2 Bereitstellung des Service Level Reports 29

3.4.3 Service Review 30

4 Performance Management (PERF) 31

4.1 Betrachtungsgegenstand des übergreifenden PERF 31

4.2 Begriffserläuterungen 32

4.2.1 Performance 32

4.3 Prozessdurchführung des übergreifenden PERF 32
4.3.1 Messung der Performance 32
4.3.2 Bereitstellung des Performance Reports 32
4.3.3 Bereitstellung von Ad-hoc Performance Reports 33
4.3.4 Service Level Requirements (SLR) 33

5 Change & Release Management (CHG & RLM) 34

5.1 Betrachtungsgegenstand des übergreifenden CHG & RLM 35

5.2 Begriffserläuterungen 35

5.3 Prozessdurchführung übergreifendes RLM 35

5.4 Prozessdurchführung übergreifendes CHG 37
5.4.1 Eigeninitiierten Produktänderungsbedarf feststellen 39
5.4.2 Vorprüfung durchführen 39
5.4.3 lokalen Produkt-Change durchführen & abschließen 39
5.4.4 Eigeninitiierten Produkt-RfC aufzeichnen 40
5.4.5 Produkt-RfC registrieren 40
5.4.6 Produkt-RfC bewerten & autorisieren 41
5.4.7 Produkt-Change umsetzen 42
5.4.8 Produkt-Change abschließen 45

5.5 Service Level Requirements (SLR) 45

5.6 Informationspflichten 45

5.7 Dokumentation 46

5.8 Eskalationen 46

5.9 Prozessreporting (Vorgangsdaten) CHG 47

6 Configuration Management (CM) 49

6.1 Betrachtungsgegenstand des übergreifenden CM 50

6.2 Begriffserläuterungen 50
6.2.1 Konfigurationselement (Configuration Item, CI) 50
6.2.2 Konfiguration 51
6.2.3 TI-Konfigurationsdatenbank 51
6.2.4 Konfigurationsdaten 51

6.3 Prozessdurchführung zur Bereitstellung von Konfigurationsdaten 51
6.3.1 Prozessreporting (Konfigurationsdaten) CM 51
6.3.2 Bereitstellung Ad-hoc Report 54

6.4 Obliegenheiten SBV/GBV TI 55

7 Knowledge Management (KM) 56

7.1 Betrachtungsgegenstand des KM 57

7.2 Begriffserläuterungen 57
7.2.1 Wissensdatenbank (WDB) 57

7.3 Prozessdurchführung Bereitstellung der Produktinformation 57
7.3.1 Bereitstellung der Produktinformation 57

7.4 Obliegenheiten SBV/GBV TI 58

8 Incident Management (INC) 59

8.1 Betrachtungsgegenstand des übergreifenden INC 60

8.2 Begriffserläuterungen 60
8.2.1 Lokaler Incident 60
8.2.2 Übergreifender Incident 60
8.2.3 Anwendersupport 61
8.2.4 Anbieter-/Herstellersupport 61
8.2.5 Supportverantwortung 61
8.2.6 Lösungsverantwortung 61

8.3 Grundsätze des übergreifenden INC 62
8.3.1 Zentrale INC-Koordinierung durch den GBV TI 62
8.3.2 Übergabe der Lösungsverantwortung 62
8.3.3 Incident-Melder 62
8.3.4 Incident-Bearbeiter 62
8.3.5 Betroffener Anwender 63

8.4 Prozessdurchführung Anwendersupport INC 63
8.4.1 Incident-Erstmeldung im Anwendersupport 63
8.4.2 Vorprüfung im Anwendersupport 63
8.4.3 Ablehnung im Anwendersupport 64
8.4.4 Lösung und Schließung im lokalen Incident Management 64
8.4.5 Interne Erfassung, Kategorisierung & Priorisierung übergreifender Incidents 66
8.4.6 strukturierte Informationsübermittlung übergreifender Incidents 70
8.4.7 Schließung übergreifender Incidents 70
8.4.8 Service Level Requirements (SLR) 71

8.5 Prozessdurchführung Anbieter-/Herstellersupport INC 73
8.5.1 Feststellung, Lösung und Schließung im lokalen INC 73
8.5.2 qualifizierte Incident-Erstmeldung im Anbieter-/Herstellersupport 73
8.5.3 Vorprüfung im Anbieter-/Herstellersupport 74
8.5.4 Ablehnung im Anbieter-/Herstellersupport 75
8.5.5 Lösung übergreifender Incidents 76
8.5.6 Schließung übergreifender Incidents 77
8.5.7 interne Dokumentation übergreifender Incidents 78
8.5.8 strukturierte Informationsübermittlung übergreifender Incidents 78
8.5.9 Service Level Requirements (SLR) 78

8.6 Informationspflichten 80

8.7 Dokumentation 81

8.8 Eskalationen 87

8.9 Prozessreporting (Vorgangsdaten) INC 88

8.10 Obliegenheiten SBV/GBV TI 89

9 Problem Management (PRO) 90

9.1 Betrachtungsgegenstand des übergreifenden PRO 91

9.2 Begriffserläuterungen 92
9.2.1 Problem 92

9.2.2 Lokales Problem 92
9.2.3 Übergreifendes Problem 92
9.2.4 Problemerkennender 92
9.2.5 Problemlösungsverantwortlicher 92
9.2.6 Lösungsunterstützender 93

9.3 Grundsätze des übergreifenden Problem Managements 93
9.3.1 Zentrale PRO Koordinierung durch den SBV TI 93

9.4 Prozessdurchführung problemerkennende Anbieter und Hersteller 93
9.4.1 Problemerkennung 93
9.4.2 Vorprüfung 93
9.4.3 Lösung und Schließung im lokalen Problem Management 94
9.4.4 Erfassung, Kategorisierung & Priorisierung übergreifender Probleme 95
9.4.5 Anfrage zur Unterstützung übergreifender Probleme 96
9.4.6 Ermittlung der Problemlösungsverantwortung bei übergreifenden Problemen 96
9.4.7 Problemschließung 97
9.4.8 Service Level Requirements (SLR) 97

9.5 Prozessdurchführung lösungsunterstützende Anbieter und Hersteller 98
9.5.1 Vorprüfung 98
9.5.2 Ablehnung 99
9.5.3 Unterstützung Problembearbeitung 99
9.5.4 Service Level Requirements (SLR) 99

9.6 Prozessdurchführung problemlösungsverantwortlicher Anbieter und Hersteller 100
9.6.1 Vorprüfung 100
9.6.2 Ablehnung 101
9.6.3 Problem Ursachenanalyse 101
9.6.4 Anfrage zur Bereitstellung der Testumgebung bei SBV 101
9.6.5 Anfrage zu Produkttypvorgaben 101
9.6.6 Problem Lösungsentwicklung und -implementierung 102
9.6.7 Schließung übergreifendes Problem 102
9.6.8 Service Level Requirements (SLR) 104

9.7 Informationspflichten 104

9.8 Dokumentation 105

9.9 Eskalationen 110

9.10 Obliegenheiten SBV/GBV TI 111

9.11 Prozessreporting (Vorgangsdaten) PRO 111

9.12 Obliegenheiten lösungsunterstützende SV/SBV 112
9.12.1 Vorprüfung 112
9.12.2 Ablehnung 112
9.12.3 Unterstützung Problembearbeitung 112

10 Notfallmanagement 113

10.1 Betrachtungsgegenstand des übergreifenden Notfallmanagement 113

10.2 Begriffserläuterungen 114
10.2.1 Notfall 114
10.2.2 lokaler Notfall 114

10.2.3 TI-Notfall 114
10.2.4 TI-Notfallvorsorge 114
10.2.5 TI-Notfallmaßnahme 115
10.2.6 Notbetrieb 115
10.2.7 TI-Notfallbewältigung 115
10.2.8 Emergency Management Committee (EMC) 115
10.2.9 Lösungsteam 116

10.3 Grundsätze des übergreifenden Notfallmanagements 116
10.3.1 Kommunikation des übergreifenden Notfallmanagements 116
10.3.2 zentrale Koordination von TI-Notfällen durch das EMC 116

10.4 Prozessdurchführung Notfallvorsorge 116
10.4.1 Analyse der Auswirkungen möglicher Notfälle der Produktinstanzen 116
10.4.2 Entwicklung und Pflege der Notfallvorsorgedokumentation 117
10.4.3 Umsetzung Vorkehrungen zur Notfallvorsorge 117

10.5 Prozessdurchführung TI-Notfallbewältigung 117
TI-Notfallerkennung 118
10.5.1 Eskalation TI-Notfälle 119
10.5.2 Sofortmaßnahmen TI-Notfälle 119
10.5.3 Bewältigung TI-Notfälle 119
10.5.4 Koordination der TI-Notfallbewältigung durch SBV 119
10.5.5 Wiederherstellung 120
10.5.6 Rollback-Verfahren 121
10.5.7 Nachbearbeitung/Notfallauswertung 121
10.5.8 Service Level Requirements (SLR) 121

10.6 Informationspflichten 122

10.7 Dokumentation 122

Anhang A – Verzeichnisse 124

A1 – Abkürzungen 124

A2 – Glossar 125

A3 – Abbildungsverzeichnis 125

A4 – Tabellenverzeichnis 125

A5 - Referenzierte Dokumente 126
A5.1 – Dokumente der gematik 126
A5.2 – Weitere Dokumente 127

Anhang B – Management der Test- und Referenzumgebung im ORS1 128

Anhang C – Webservice-Schnittstelle 132

1 Einordnung des Dokuments

1.1 Zielsetzung

Die vorliegenden „Übergreifenden Richtlinien zum Betrieb der TI“ definieren die betrieblichen Mitwirkungspflichten und Schnittstellen zur übergreifenden Zusammenarbeit der Teilnehmer der TI im IT-Servicemanagement (ITSM) auf prozessualer Ebene. Teilnehmer der TI sind Anbieter, Hersteller, Service Provider und weitere, für Ihre Fachanwendungen, Services, Produkte oder Leistungen verantwortlichen Serviceeinheiten, die in und für die TI entsprechend zugelassen und beauftragt sind. Die Mitwirkung der gematik erfolgt über explizit benannte Rollen (z. B. Servicebetriebsverantwortlicher - SBV). Die Richtlinien treffen keine Vorgaben zu internen ITSM-Prozessen der einzelnen Teilnehmer der TI.

Folgende Prozesse werden betrachtet:

- Service Level Management: Regelungen für das Management zur Definition, Kontrolle sowie Optimierung der Service Level über alle Betriebseinheiten hinweg,
- Performance Management: Regelungen für das Management zur Sicherstellung einer adäquaten Dimensionierung und SLA konformer Leistungserbringung der TI,
- Change & Release Management: Regelungen für das Management von Änderungen der TI-Plattform-Services und Anwendungsservices sowie Regelungen für das Management zur Überführung von Releases in den Wirkbetrieb,
- Configuration Management: Regelungen für das Management der für die TI-Plattform-Services und Anwendungsservices erforderlichen Beschreibungsdaten,
- Knowledge Management: Regelungen für das Management von Informationen aus dem und für den Wirkbetrieb der TI-Plattform-Services und Anwendungsservices,
- Incident Management: Regelungen für den Umgang mit Störungen, die zu einer Qualitätsminderung der TI-Plattform-Services oder der Anwendungsservices führen können,
- Problem Management: Regelungen für das Management von unbekannten Ursachen einer eingetretenen/möglichen Störung und nachhaltiger Beseitigung der identifizierten Störungsursachen,
- Notfallmanagement: Regelungen für die Notfallvorsorge und die Notfallbewältigung der TI-Plattform-Services und der Anwendungsservices.

In Kapitel 2 werden die prozessübergreifenden Begriffe und Grundsätze, die Regelungen zum Reporting und die Zuordnung der ITSM-Prozesse zu den ITIL-Lebenszyklusphasen

eingeführt. Es werden die betrieblichen Rollen definiert und deren Verantwortungsteilung beschrieben. Zugleich werden den Rollen Teilaufgaben zugeordnet, die sich aus den Aufgabenbereichen des Betriebs der TI ergeben.

Die Aufgabenbereiche sind an ITIL® V3 angelehnt. Alle Aufgabenfelder werden in Form von übergreifenden IT-Service-Management-Prozessen mit den jeweiligen Aufgaben und Zielen vorgestellt. Sie orientieren sich an den ITIL-Lebenszyklusphasen des „Service Design“ zur Erstellung, Weiterentwicklung und Pflege von Vorgaben, der „Service Transition“ zur Überführung der Vorgaben in den Wirkbetrieb und der „Service Operation“ in der Unterstützung des Wirkbetriebs der TI-Services.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von Produkten.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur (TI) des Deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzung des Dokuments

Nicht alle ITSM-Prozesse gemäß ITIL® V3 sind im Rahmen dieses Richtliniendokumentes geregelt. Dies ergibt sich insbesondere

- durch die Fokussierung auf die Mitwirkungspflichten durch Anbieter und Hersteller im Wirkbetrieb der TI,
- durch Umsetzungsanforderungen, die ausschließlich durch ein spezifisches Reporting umzusetzen sind und in Folge innerhalb der spezifischen Betriebskonzepte ausgeprägt werden.

Aus oben genannten Gründen sind innerhalb dieses Dokumentes folgende ITSM-Prozesse nicht geregelt:

- Service Design: Weiterentwicklung der TI, Information Security Management

- Service Transition: Subprozesse des Change Managements (On-/Offboarding zentraler Produktinstanzen, Inbetriebnahme und Änderung dezentraler Produktinstanzen der TI), Testmanagement
- Service Operation: Operativer Betrieb und Überwachung.

Regelungen für Anwender und PEDs (Professionelle Endnutzernahe Dienstleister) werden nicht definiert.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet. Sie werden im Dokument wie folgt dargestellt:

⌦ **GS-A_xxxx Titel der Afo**

Text / Beschreibung. ⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Prozessübergreifende Regelungen

In diesem Kapitel werden Begriffe und Regelungen eingeführt, die für alle nachfolgend beschriebenen ITSM-Prozesse Gültigkeit haben.

Begriffe, die im Kontext des übergreifenden Betriebes einer Konkretisierung bedürfen, werden in diesem Dokument in den Kapiteln „Begriffserläuterungen“ definiert. Dabei wird zwischen prozessübergreifenden und prozessspezifischen Begriffserläuterungen unterschieden.

Prozessübergreifende Begriffserläuterungen werden zentral in diesem Dokument eingeführt und sind über alle in diesem Dokument beschriebenen ITSM-Prozesse hinweg gültig.

Prozessspezifische Begriffserläuterungen werden prozessspezifisch eingeführt und sind nur im Kontext des jeweiligen ITSM Prozesses gültig.

Ergänzende Informationen mit nicht normativem Inhalt, die zum Fördern des gemeinsamen Verständnis der ITSM-Teilnehmer (siehe Kapitel 2.1.2) beitragen (z.B. Prozessablaufdiagramme, ergänzende Beschreibungen oder Kontaktinformationen), werden bei Bedarf im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank (siehe Kapitel 7.2.1) bereitgestellt.

2.1 Prozessübergreifende Begriffserläuterungen

Dieses Kapitel ist für Anbieter und Hersteller informativ.

2.1.1 Information, Eskalation, Report

- **Information:** Bei einer Information handelt es sich um eine für den jeweiligen Empfänger strukturierte und aufbereitete Sammlung von Daten, die - zu festgelegten Prozesszeitpunkten - durch den Versender an definierte Adressaten verschickt werden.
- **Eskalation:** Eine Eskalation wird angestoßen, um die gefährdete Zielerreichung dennoch sicherzustellen. In den Richtlinien wird unter dem Begriff „Eskalation“ prinzipiell eine hierarchische Eskalation verstanden. Eine Eskalation beinhaltet ähnliche Merkmale wie eine strukturierte Information.
    - Funktionale „Eskalationen“ sind im Umfang der definierten ITSM-Prozesse Zuweisungen bzw. Weiterleitungen von speziellen Aufgaben an andere Prozessbeteiligte.
- **Report:** Bei einem Report handelt es sich um eine für den jeweiligen Empfänger strukturierte und aufbereitete Sammlung von Daten, die nach der originären Prozessdurchführung - zu festgelegten Zeitpunkten oder ad-hoc - durch den Versender an definierte Adressaten verschickt werden.

2.1.2 Teilnehmer-ID (TID)

Die Teilnehmer-ID identifiziert die Teilnehmer im Betrieb der TI (Beteiligte am IT-Servicemanagement gemäß dieser Richtlinie) eineindeutig. Sie ist vom Typ „String [5]“ und wird von gematik vergeben. Die ID über alle Teilnehmer wird in Listenform von der gematik im Rahmen des Knowledge Managements veröffentlicht. Ist eine Hersteller-ID/Anbieter-ID gemäß [gemSpec_OM] vorhanden, wird sie verwendet.

2.2 Prozessübergreifende Kommunikation

Um eine möglichst reibungslose Prozesskommunikation und effiziente Prozessdurchführung zwischen den Anbietern und Herstellern (A/H) und zu den zuständigen Serviceverantwortlichen (SV) bzw. Servicebetriebsverantwortlichen (SBV) sicherzustellen, werden nachfolgend die übergreifenden Anforderungen für die Bereitstellung von Kommunikationsschnittstellen und Ansprechpartnern definiert. Die Kommunikationsschnittstelle und die Ansprechpartner bilden den SPOC (Single Point of Contact) des jeweiligen Anbieters bzw. Herstellers im Rahmen der Prozesskommunikation.

Die zuständigen SV/SBV errichten ihrerseits Kommunikationsschnittstellen und stellen Ansprechpartner im Rahmen der Prozesskommunikation zur Verfügung. Die Übersicht der im übergreifenden ITSM zu verwendenden Kontaktdaten (E-Mail-Adressen, Telefonnummern) wird im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank hinterlegt.

Die nachfolgenden Anforderungen an die Kommunikation zwischen den Prozessbeteiligten basieren auf einer ursprünglich vorgesehenen bilateralen Kommunikation via E-Mail und dem Austausch strukturierter csv-Dateien. Um jedoch für alle Beteiligten eine einheitliche und transparente Daten- und Prozesskonsistenz für die übergreifenden ITSM-Prozessabläufe im Incident-, Problem- und Change-Management zu erreichen, wird mit der Zentralen Informationsdrehscheibe (ZID) ein zentrales ITSM-System zur Verfügung gestellt. Dieses bildet die zentrale Kommunikationsschnittstelle für alle Prozessbeteiligten. Wichtig ist, dass die ZID nur die übergreifenden Kommunikationsprozesse unterstützt (keine lokalen Prozesse) und hier auch nur die Kommunikationsvorgänge im Incident-, Problem- und Change-Management. Für Teilnehmer, die sich in den übergreifenden INC- und PRO-Prozessen für die Benutzung des Webportals entscheiden, kann hingegen die ZID zum führenden ITSM-System werden. Auch diese Teilnehmer müssen den INC „lokal“ dokumentieren, d. h. in diesem Fall in der ZID. Die Dokumentation sollte allerdings bereits vollständig in der ZID vorliegen.

Die ZID stellt für den gesicherten Austausch und die Generierung von Prozessinformationen mehrere Schnittstellen zur Verfügung. Ein Prozessbeteiligter kann im Incident- und Problem-Management über die ZID dabei entweder (weiterhin) seine Kommunikationsschnittstelle durch die Versendung von E-Mails mit angehängten csv-Dateien einrichten, oder er realisiert den Austausch mit der ZID über eine Webservice-Schnittstelle oder er entscheidet sich für die manuelle Bedienung im Webportal. Grundsätzlich besteht die Möglichkeit, Incidents, Problems und Changes im Webportal der ZID einzusehen.

Die ZID stellt im Incident- und Problem-Management sicher, dass über die vom Prozessbeteiligten einmalig vorab getroffene Entscheidung des Kommunikationsweges

(E-Mail mit CSV oder Webservice oder Webportal) sämtliche der im Folgenden beschriebenen Kommunikationsschritte abgebildet werden.

Bei der Kommunikation im Change Management wird im Wesentlichen davon ausgegangen, dass die Informationsübermittlung zwischen den Prozessbeteiligten per E-Mail ohne CSV-Dateien erfolgt. Daher bietet die ZID für diesen Prozess keine Webservice-Schnittstelle an, sondern es steht ausschließlich das Webportal der ZID zur Verfügung. Die Benutzung des Webportals für übergreifende Produkt-RfCs bzw. Produkt-Changes steht jedoch jedem Anbieter und Hersteller frei. Falls sich ein Anbieter oder Hersteller im Rahmen des Change Managements für die Nutzung des Webportals entscheidet, sind die für diesen Prozess definierten Übermittlungs- und Dokumentationspflichten auch möglichst durchgehend in der ZID zu erfüllen.

Der Zugriff auf die Webservice-Schnittstelle und das Webportal der ZID durch die Anbieter und Hersteller wird durch Eingabe von Melder-individuellen Anmeldeinformationen (Anmeldenamen und Passwort) abgesichert. Zusätzlich wird der Zugriff auf definierte IP-Adress-Bereiche beschränkt, wobei der IP-Adress-Bereich nachvollziehbar dem entsprechenden Anbieter bzw. Hersteller zuzuordnen sein muss. Weiterhin wird die Datenübertragung durch ein Server-Zertifikat abgesichert.

Bei Ausfall der ZID oder anderen vom GBV/SBV zur Verfügung gestellten Kommunikationsschnittstellen bzw. Informationssystemen, hat die Absicherung der Kommunikation durch die Anbieter und Hersteller zu erfolgen.

⌦ **GS-A_4085 Etablierung von Kommunikationsschnittstellen durch die A/H**

Anbieter und Hersteller MÜSSEN im Rahmen der übergreifenden Betriebsprozesse geeignete Kommunikationsschnittstellen etablieren. Diese Schnittstellen MÜSSEN neben der Erreichbarkeit sicherstellen, dass die Übermittlung der definierten strukturierten Prozessdaten im Rahmen der ZID durchführbar ist. Der Informationsaustausch per E-Mail zwischen TI-Teilnehmern hat verschlüsselt mittels S/MIME (Secure / Multipurpose Internet Mail Extensions) zu erfolgen. Die für die Kommunikation notwendigen Zertifikate werden über das Knowledge Management den ITSM-Beteiligten TI-Teilnehmern zur Verfügung gestellt.

Anbieter und Hersteller MÜSSEN alle im Rahmen der prozessübergreifenden Kommunikation zu versendenden E-Mails auf ihre Größe überprüfen. Dabei MUSS grundsätzlich sichergestellt sein, dass E-Mails die Größe von 5 MB nie überschreitet. Eine Ausnahme stellen E-Mails mit dem Adressaten SBV/GBV mit einer maximalen Größen von 20 MB dar.

Weiterführend sind folgende Regelungen zu beachten:

- Der Betreff einer E-Mail ist immer der Dateiname der in der E-Mail angehängten csv-Datei.
- Bei der Anwendung von E-Mail-Komprimierung:
  - CSV-Dateien sind von Komprimierungsmaßnahmen ausgeschlossen
  - Komprimierung der Dateianhänge im zip-Datei-Format
  - Mit „normaler“ Kompression/Kompressionsstärke
  - Mit Kompressionsmethode/-verfahren „Deflate“ (#4.4.5 - compression method 8)

- Unverschlüsselt, d. h. ohne Passwort
- Nicht selbst-entpackend (d.h. zip als exe)

- Die ZID wird immer mit der Empfängeradresse des ZID-Postfaches des adressierten Teilnehmers antworten.⌫

⌦ **GS-A_4086 Erreichbarkeit von Kommunikationsschnittstellen der A/H**

Anbieter und Hersteller MÜSSEN die Kommunikationsschnittstellen während der festgelegten Servicezeiten erreichbar halten und einer regelmäßigen Eingangsprüfung und Bearbeitung unterziehen. ⌫

Die Service Level Requirements zu den Servicezeiten werden in den jeweiligen ITSM Prozessen dieses Dokumentes definiert.

⌦ **GS-A_4087 Erreichbarkeit der Kommunikationsschnittstelle bei Rufbereitschaften außerhalb der Servicezeiten der A/H**

Bei Anbietern bzw. Herstellern, bei denen Rufbereitschaften etabliert werden sollen, MUSS die Kommunikationsschnittstelle während der vereinbarten Rufbereitschaftszeiten stetig erreichbar sein und regelmäßiger Eingangsprüfung und Bearbeitung durch den Anbieter und Hersteller unterliegen. ⌫

⌦ **GS-A_4088 Bereitstellung eines technischen Ansprechpartners durch A/H**

Anbieter und Hersteller MÜSSEN im Rahmen der übergreifenden Betriebsprozesse allen Prozessbeteiligten einen technischen Ansprechpartner bereitstellen. ⌫

⌦ **GS-A_4089 Bereitstellung eines kaufmännischen Ansprechpartners durch A/H**

Anbieter und Hersteller MÜSSEN im Rahmen der übergreifenden Betriebsprozesse allen Prozessbeteiligten einen kaufmännischen Ansprechpartner bereitstellen. ⌫

⌦ **GS-A_4892 Eingangsbestätigung für den Melder**

Dem Übermittler/Erfasser der Prozessdaten muss unverzüglich eine Eingangsbestätigung übermittelt werden, bei den übergreifenden Prozessen im Incident-, Problem- und Change-Management verläuft die Kommunikation über die ZID. Für per Web-Service bzw. Webportal angebundene Empfänger entfällt diese Pflicht, hier übernimmt die ZID das Ausstellen einer Eingangsbestätigung an den per CSV-angebundenen Absender (über die ZID-Postfachadresse des Empfängers). Die „technischen Empfangsbestätigungen“ werden durch eine einheitliche Notation in der Betreffzeile der E-Mail gekennzeichnet. Die Betreffzeile ist wie folgt zu kodieren:

- [<Präfix>␣<originaler Betreff der Nachricht >]
- In der Empfangsbestätigung ist KEINE csv-Datei anzufügen!
- Mailformat ist Plain-Text
- Es darf auf eine empfangene Eingangsbestätigung keine erneute Eingangsbestätigung generiert werden.
- Der <Präfix> hat zu lauten „#ERHALTEN#“ ⌫

⌦ **GS-A_4090 Kommunikationssprache zwischen den Prozessbeteiligten**

Anbieter und Hersteller MÜSSEN im Rahmen der Prozesskommunikation sowohl schriftlich als auch mündlich in deutscher Sprache kommunizieren. Dies gilt insbesondere für die durch diese Richtlinien geregelte Kommunikation an den Prozessschnittstellen (bspw. mittels E-Mails, Formularen). ⌫

⌦ **GS-A_4091 Dokumentationssprache**

Anbieter und Hersteller MÜSSEN alle im Rahmen der übergreifenden Betriebsprozesse zu erstellenden Dokumentationen in deutscher Sprache verfassen. ⌫

2.3 Reporting

Zur Unterstützung der strategischen und operativen Betriebsführung sowie zur Überwachung der Einhaltung von Vorgaben ist durch Anbieter und Hersteller ein Reporting zu etablieren. In diesem Kapitel werden hierzu die übergreifenden Anforderungen sowie der inhaltliche Aufbau an das regelmäßige, konsolidierte Reporting sowie an das unregelmäßige Ad-hoc-Reporting beschrieben. In den spezifischen Betriebskonzepten können weitere Einzelreports des konsolidierten Reportings definiert werden.

2.3.1 Konsolidiertes Reporting

Ziel des konsolidierten Reportings ist die Bereitstellung der relevanten Reporting-Inhalte in einem einheitlichen Verfahren sowie deren strukturierte Übermittlung an den SBV.

Der konsolidierte Report setzt sich aus insgesamt **acht Einzelreports** zusammen. Die Inhalte des Reports werden durch die in der folgenden Tabelle referenzierten Kapitel bzw. Dokumente definiert. Werden für einen Einzelreport keine Inhalte definiert, bzw. sind diese für den jeweiligen Produkttyp nicht relevant, muss der entsprechende Einzelreport nicht übermittelt werden.

Tabelle 1: Tab_Betr_TIP_025 Bestandteile des konsolidierten Reportings

Reportbezeichnung	Inhalt	Format / Struktur siehe
Service Level Report (SL Report)	Kennzahlen zu Performance, Prozess und Serviceerbringung	Kapitel 3
Performance Report (PERF Report)	Kennzahlen zu technischen Messgrößen gemäß [gemSpec_Perf] für Bearbeitungszeit, Durchsatz und Verfügbarkeit	Kapitel 4.3.2
Change Report (CHG Report)	Vorgangs- und prozessbezogene Daten der Change-Prozesse	Kapitel 5.9
Configuration Report (CM Report)	Konfigurationsdaten zu Produkt und produktverantwortlicher Organisation	Kapitel 6
Incident Report (INC Report)	Kennzahlen zu den Incidents	Kapitel 8
Problem Report (PRO Report)	Kennzahlen zu den Problems	Kapitel 9

Reportbezeichnung	Inhalt	Format / Struktur siehe
Datenschutz Report (DSM Report)	Vorgangsdaten und Kennzahlen des Datenschutzmanagements. Die Kennzahlen des Datenschutz Reports werden nicht als SLR ausgeprägt und sind daher nicht im Service Level Report enthalten	[gemSpec_DSM]
Security Report (ISM Report)	Vorgangsdaten und Kennzahlen des Informationssicherheitsmanagements. Die Kennzahlen des Security Reports werden nicht als SLR ausgeprägt und sind daher nicht im Service Level Report enthalten	[gemSpec_ISM]

Neben den inhaltlichen Aspekten, die primär in den jeweiligen ITSM-Prozessen bzw. -Prozesskapiteln geregelt werden, gelten für das konsolidierte Reporting, übergreifende Regelungen, die insbesondere die Struktur, die Reportingfrequenz, als auch die Übermittlung des konsolidierten Reports an den SBV regeln:

⌦ **GS-A_4092 Übermittlung des konsolidierten Reports**

Anbieter und Hersteller MÜSSEN folgende Reports im Rahmen des konsolidierten Reports per E-Mail an den SBV oder den durch den SBV benannten Empfänger bzw. Funktionspostfächer übermitteln: Service Level Report, Performance Report, Change Report, Configuration Report, Incident Report, Problem Report, Datenschutz Report, Security Report.

Anbieter von Fachdiensten VSDM liefern keinen Datenschutz Report und keinen Security Report. ⌫

⌦ **GS-A_4093 Dateinamen der Einzelreports im konsolidierten und Ad-hoc Reporting**

Anbieter und Hersteller MÜSSEN die an den SBV zu übermittelnden Einzelreports innerhalb des konsolidierten Reportings sowie zu übermittelnden den Ad-hoc Report eineindeutig mit folgenden Dateinameninhalten

- Jahr und dem Monat (JJJJMM)
- der Reportart, Konsolidiertes Reporting (KR) oder Ad-hoc Report (AR)
- der Bezeichnung des Einzelreports bei konsolidiertem Reporting (KR) oder inhaltliche Zuordnung beim Ad-hoc-Report (SL, PERF, CHG, CM, INC, PRO, DSM, ISM), wobei der Konfiguration-Report (CM) wie folgt zu differenzieren ist
    - CMPO für Konfiguration-Report zum CI „Produktverantwortliche Organisation“
    - CMPR für Konfiguration-Report zum CI „Produkt“
- Teilnehmer-ID des Herstellers oder Anbieters bzw. weiterer Beteiligter im Betrieb der TI (TID)

- der fortlaufenden Versionsnummer (VNR) (Hochzählung der Versionsnummer bei Veränderung der übermittelten Daten zum vorherigen Einzelreport oder zum vorherigen Ad-hoc Report)

und nach dem Schema für Konsolidiertes Reporting (KR) „JJJJMM-KR-SL/PERF/CHG/CMPO/CMPR/INC/PRO/DSM/ISM-TID-VNR“ erstellen.

(Beispiel: 201209-KR-SL-12345-01)

oder nach dem Schema für Ad-hoc Report (AR) „JJJJMM-AR-SL/PERF/CHG/CMPO/CMPR/INC/PRO/DSM/ISM-TID-VNR“ erstellen.

(Beispiel: 201209-AR-SL-12345-01 oder 201210-AR-PERF-12345-01).⌫

2.3.2 Ad-hoc Reporting

Neben der regelmäßigen Zusendung des konsolidierten Reportings kann der SBV Ad-hoc, also außerplanmäßige, Reports anfordern. Dabei kann der Servicebetriebsverantwortliche (SBV) oder der Gesamtbetriebsverantwortliche der TI (GBV TI) auf den vorhandenen Vorgangsdaten-/Kennzahlenpool aus den Einzelreports des konsolidierten Reportings zurückgreifen oder andere Kennzahlen (innerhalb eines zumutbaren Umfangs für den Anbieter und Hersteller) abfragen. Entsteht die Notwendigkeit zur Erhebung weiterer Messgrößen, werden diese gemeinsam mit den betroffenen Anbietern und Herstellern individuell abgestimmt.

⌦ **GS-A_4095 Übermittlung von Ad-hoc Reports**

Anbieter und Hersteller MÜSSEN den vom SBV angeforderten Ad-hoc Report per E-Mail an den SBV oder den durch den SBV benannten Empfänger übermitteln. ⌫

⌦ **GS-A_4096 Weiterbearbeitbarkeit und Auswertbarkeit des Ad-hoc Reports**

Anbieter und Hersteller MÜSSEN den vom SBV angeforderten Ad-hoc Report in einem weiterbearbeitbaren und auswertbaren Format an den SBV oder den durch den SBV benannten Empfänger versenden. ⌫

⌦ **GS-A_4097 Dateiformat und -struktur des Ad-hoc Reports**

Anbieter und Hersteller SOLLEN, sofern nicht abweichend vereinbart, für den angeforderten Ad-hoc Report in dem vom SBV vorgegebenen Dateiformat und vorgegebenen Dateistruktur verwenden. Dateiformat und Dateistruktur richtet sich dabei nach den Vorgaben für Struktur und Format des konsolidierten Reportings. ⌫

⌦ **GS-A_4099 Zulieferungszeit des Ad-hoc Reports an den SBV oder GBV TI**

Anbieter und Hersteller MÜSSEN den Ad-hoc Report, sofern nicht abweichend mit dem SBV vereinbart, unverzüglich an den SBV versenden. ⌫

2.3.3 Service Level Requirements (SLR)

⌦ **GS-A_4094 Service Level Requirements Serviceerbringung**

Anbieter und Hersteller MÜSSEN innerhalb des konsolidierten Reportings einmal im Monat spätestens zum 5. Werktag des Folgemonats die Reports an den

jeweiligen SBV oder den durch den SBV benannten Empfänger übermitteln. Service Level werden in den spezifischen Betriebskonzepten produkttypspezifisch ausgeprägt. ⌫

2.4 Auditierung von Anbietern und Herstellern

Es besteht die Notwendigkeit anlassbezogene Audits durchzuführen. Audits werden durchgeführt, wenn die Prozesskommunikation zwischen den am Betrieb beteiligten Anbietern und Herstellern nachhaltig gestört bzw. die Serviceerbringung gegenüber dem Anwender bzw. Versicherten gefährdet ist.

Die Audits dienen der Prüfung der korrekten Umsetzung der Richtlinien insbesondere mit dem Ziel Schnittstellen-/Prozessprobleme zwischen Anbietern oder Herstellern zu identifizieren. Die Erkenntnisse der anlassbezogenen Audits können zur Optimierung der Richtlinien führen, um die Reibungsverluste im Zusammenspiel der Anbieter und Hersteller untereinander zu minimieren.

⌦ **GS-A_4855 Auditierung von Anbietern und Herstellern**

Anbieter und Hersteller (außer Anbieter von Fachdiensten VSDM) MÜSSEN Auditierungen durch den zuständigen SBV sowie den GBV TI zur Überprüfung der Einhaltung von Produktvorgaben ermöglichen und angemessen unterstützen.

Das Audit darf im Rahmen der Prüfungsdurchführung nicht gegen gesetzliche Vorgaben verstoßen, denen Anbieter und Hersteller unterliegen.

Umfang und Zeitpunkt des Audits hat der GBV TI bzw. der zuständige SBV mit dem zuständigen SV abzustimmen. Der zuständige SV muss der Durchführung des Audits zustimmen. ⌫

2.5 Konvention zur Übermittlung von Prozessdaten

⌦ **GS-A_5200 Konvention zu Dateinamen zur Übermittlung von Incident- und Problemdokumentationen**

1. Für die Zusendung der CSV- Dateien gilt:

Anbieter und Hersteller MÜSSEN die Namen der csv-Dateien wie folgt bilden:

<Zeitstempel>_<ITSM-Prozess>_<Referenznummer>_<Meldungstyp>_<TID>.csv

- <Zeitstempel> Zeitpunkt der Übermittlung YYYYMMDDThhmmss+/-hh (gemäß ISO 8601)
- <ITSM-Prozess> Bezeichnung des zugrundeliegenden ITSM-Prozesses: „INC“ für Incidentmanagement bzw. „PRO“ oder Problemmanagement
- <Referenznummer> fortlaufende Nummer der Dokumentation des zugrundeliegenden Incidents oder Problems gemäß GS-A_3880 oder Problems gemäß GS-A_3961
- <Meldungstyp>

- o „WE“: Weiterleitung im Sinne der funktionalen Eskalation mit Übergang der Lösungsverantwortung
- o „AN“ Annahme des übergreifende Incidents oder Problems gemäß GS-A_3904 und übergreifenden Problemen gemäß GS-A_3975
- o „AL“ Ablehnung von übergreifen Incidents oder Problems gemäß GS-A_3905 und übergreifendenden Problemen gemäß GS-A_3976 und GS-A_3982
- o „RQ“: Anfrage ohne Übergang der Lösungsverantwortung
- o „ES“: Eskalation an den SBV oder GBV TI
- o „SI“: Statusinformation an den SBV oder GBV TI
- o „NI“ Nachreichen von Informationen zum übergreifenden Incident / Problem- in beide Richtungen – siehe Beispiele

- <TID> Teilnehmer-ID des Service Providers der aktuell den Versand der strukturierten Information vornimmt / TID des E-Mail-Absenders

2. Die Nutzung der Webservice-Schnittstelle erfolgt durch eine Kopplung der lokalen Ticket-/Informationssysteme mit der ZID, der alleinige Austausch von XML-Dateien wird nicht unterstützt. Die Anbieter und Hersteller arbeiten dabei nach dem Pull-Prinzip und fragen Daten zyklisch ab. Aktiv werden von der ZID keine Webservices der Anbieter und Hersteller angesprochen.

   Die für den Aufbau des csv-Dateinamens definierten Daten sind beim Senden als Pflichtfelder zu übermitteln. Eine Reihenfolge ist dabei nicht zu beachten. Es gelten die Vorgaben an die Webservice-Schnittelle gemäß den Tabellen Tab_Betr_TIP_040, Tab_Betr_TIP_041, Tab_Betr_TIP_042, Tab_Betr_TIP_043 (siehe Anhang C).

   Bei fehlerhaften oder fehlenden Angaben erfolgt als Antwort in der Webservice-Schnittstelle von der ZID eine Fehlermeldung mit Hinweis auf den/die Fehler bzw. die fehlenden Felder oder erwarteten Daten. Die Übermittlung eines neuen Incidents oder Problems, d. h. die übermittelte Incident- oder Problem-Referenznummer ist neu und in der ZID noch nicht vorhanden, kann nur mit dem Meldungstyp „WE“ (Weiterleitung) erfolgen.

   Weitere Beispiele werden in der Wissensdatenbank dokumentiert.

3. Für die Erfassung der Prozessdaten im Webportal gelten die Inhaltsdefinition für das übergreifende Incident Management (siehe GS-A_3882) und für das übergreifende Problem Management (siehe GS-A_4000). Das Webportal der ZID stellt darüber hinaus sicher, dass für die Nutzer des Webportals die notwendigen Prozessdaten aller notwendigen Meldungstypen sowie Eingangsbestätigungen durch die ZID selbst erzeugt werden, d.h. es ist keine Erzeugung bspw. von Statusinformationen (Meldungstyp SI) parallel zur ZID notwendig. Ebenso werden durch das Webportal die weiteren für die Prozessverarbeitung notwendigen Daten wie die Referenznummer gemäß GS-A_3880 bzw. GS-A_3961 erzeugt. Die im Webportal befüll- und verarbeitbaren Daten entsprechen grundlegend denen in den CSV-Dateien. Die konkrete Umsetzung und Darstellung des Webportals kann als Beispielbeschreibung der Wissensdatenbank entnommen werden. ⌫

Um doppelte Einträge im Worklog zu verhindern und damit die Entwicklung eines Ticketverlaufes möglichst einfach nachzuvollziehen, ist grundsätzlich zu empfehlen,

ausschließlich die letzte Änderung des Worklogs aus dem lokalen ITSM-System in das übergreifende ITSM zu übermitteln.

Incident Management:

Tabelle 2: Tab_Betr_TIP_028 Übersicht Meldungstypen – Incident Management

Meldungstyp	Anwendungsfall	Beschreibung anhand Beispielen
WE	Weiterleitung im Sinne der funktionalen Eskalation mit Übergang der Lösungsverantwortung	• Eröffnung eines übergreifenden Incidents (Eröffnung im Sinne einer Zuweisung und nicht im Sinne einer Neueröffnung) • Lösungsverifikation/Lösung • Ggf. Schließung
NI	Nachreichen von Informationen (Keine Änderung der Lösungsverantwortung)	• Während der Bearbeitung eines übergreifendes Incidents/Problems treffen zusätzliche Informationen beim Melder ein, diese sollen an den Bearbeiter weitergegeben werden. • Zur Lösung eines übergreifenden Incidents werden noch zusätzlich Informationen benötigt • Der betroffene Anwender hat Nachfragen zu einem bestehenden übergreifenden Incident • … • Fazit: das Nachreichen von Informationen zu einem übergreifenden Incident kann sowohl vom Melder zum Bearbeiter, als auch von Bearbeiter zum Melder stattfinden.
AN	Annahme eines übergreifenden Incidents (Übernahme der Lösungsverantwortung)	• TI-Teilnehmer bekommt einen Incident zugewiesen und bestätigt durch den Meldungstyp die Annahme der Incidentbearbeitung
AL	Ablehnung eines übergreifenden Incidents (Keine Änderung der Lösungsverantwortung)	• TI-Teilnehmer bekommt einen Incident zugewiesen und lehnt die Bearbeitung ab
ES	Eskalation an den SBV oder GBV TI (Keine Änderung der Lösungsverantwortung)	• Eskalation
SI	Statusinformation an den SBV oder GBV TI	• Lokaler Incident Prio 1 und 2 • Übergreifender Incident Prio 1, 2, 3 und 4

Problem Management:

Tabelle 3: Tab_Betr_TIP_029 Übersicht Meldungstypen – Problem Management

Meldungstyp	Anwendungsfall	Beschreibung anhand Beispielen
WE	Weiterleitung im Sinne der funktionalen Eskalation mit	• Eröffnung eines übergreifenden Problems (Eröffnung im Sinne einer Zuweisung und nicht

Meldungstyp	Anwendungsfall	Beschreibung anhand Beispielen
	Übergang der Lösungsverantwortung	im Sinne einer Neueröffnung) • Lösungsverifikation/Lösung • Schließung
NI	Nachreichen von Informationen (Keine Änderung der Lösungsverantwortung)	• Während der Bearbeitung eines übergreifendes Incidents/Problems treffen zusätzliche Informationen beim Melder ein, diese sollen an den Bearbeiter weitergegeben werden. • Zur Lösung eines übergreifenden Problems werden noch zusätzlich Informationen benötigt • Der betroffene Anwender hat Nachfragen zu einem bestehenden übergreifenden Problem • … • Fazit: das Nachreichen von Informationen zu einem übergreifenden Problem kann sowohl vom PLE zum PLV, als auch von PLV zum PLE stattfinden.
AN	Annahme eines übergreifenden Problems (Übernahme der Lösungsverantwortung)	• TI-Teilnehmer bekommt einen Problem zugewiesen und bestätigt durch den Meldungstyp die Annahme der Problembearbeitung
AL	Ablehnung eines übergreifenden Problems (Keine Änderung der Lösungsverantwortung)	• TI-Teilnehmer bekommt einen Problem zugewiesen und lehnt die Bearbeitung ab
RQ	Anfrage ohne Übergang der Lösungsverantwortung	• Anfrage auf Unterstützung im übergreifenden Problem Management (sowie ggf. Ablehnung der Anfrage) (Hinweis: Vor Verwendung des Meldungstyps RQ MUSS bereits ein PLV gefunden worden sein, anderenfalls darf dieser Meldungstyp nicht verwendet werden.)
ES	Eskalation an den SBV oder GBV TI (Keine Änderung der Lösungsverantwortung)	• Eskalation
SI	Statusinformation an den SBV oder GBV TI	• Lokales Problem Prio 1 und 2 • Übergreifendes Problem Prio 1, 2, 3, 4

⌦ GS-A_5248 Konventionen zur Struktur von Prozessdaten~~csv-Dateien~~

1. Für CSV- Dateien gilt :

   Anbieter und Hersteller MÜSSEN die Struktur der CSV-Dateien für Statusinformationen und Eskalationen sowie der Prozesskommunikation nach den Vorgaben aus [RFC4180] und den nachfolgenden Konkretisierungen bauen:

- In der ersten Zeile sind die Feldnamen (Header) und ab der zweiten Zeile sind die zu übermittelnden Werte enthalten (Datensatz). Diese sind durch Semikolon (ASCII-59) zu trennen.
- Zeichensatzkodierung UTF-8 ohne ByteOrderMark liefern.
- Sämtliche Feldinhalte innerhalb der csv-Datei (d.h. die Inhalte der Datensätze UND die Inhalte des Headers) sind in ASCII-34-Zeichen zu setzen (Quoting).
- Leere Felder müssen quotiert werden.
- Innerhalb der Feldinhalte ist jedes ASCII-34-Zeichen durch ASCII-39-Zeichen zu ersetzen.
- Zeilendelimiter ist die Zeichenfolge ASCII-13-Zeichen (Carriage return), ASCII-10-Zeichen (Line feed).
- Comments sind nicht zugelassen.
- Leere Zeilen sind nicht zugelassen.
- Leerzeichen am Rand von Feldinhalten werden nicht ignoriert, d.h. sie sind vom Sender zu entfernen, wenn sie nicht intendiert sind.
- Ist in einem Feldinhalt kein Zeichen enthalten, wird das als NULL-Wert, d.h. nicht gefüllter Feldwert interpretiert.
- Der auf Grundlage von Basisfeldtypen (Tabelle 5: Tab_Betr_TIP_030 Basisfeldtypen von csv-Dateien) festgelegte Wertebereich in Spalte „Typ“ muss erfüllt werden.
- Als Basis für Datums- und Zeitformate dient die ISO-Norm 8601.
- Folgende Formate sind zu benutzen:
    - für Werte innerhalb der csv-Datei: YYYY-MM-DDThh:mm:ss±hh
    - als Bestandteil eines Dateinamens: YYYYMMDDThhmmss±hh
- Jede Datei darf im Rahmen der Prozesskommunikation nur einen Datensatz enthalten. Reports dürfen mehrere Datensätze enthalten.

2. Für den Webservice gelten die gleichen Konventionen zur Struktur und das Webservice Schemata gemäß dem Anhang C.
3. Für die Erfassung der Prozessdaten im Webportal werden die Konventionen im entsprechenden Formular dargestellt. ⌫

⌦ **GS-A_5249 Reservierte Zeichen in den Prozessdaten ~~csv-Datensätzen~~**

Anbieter und Hersteller MÜSSEN die in Tabelle 4: Tab_Betr_TIP_026 reservierte Zeichen Ersetzungstabelle benannten Zeichenketten in den [String] Basisfeldtypen der zu übermittelnden Prozessdaten der Incident- und Problemdokumentationen vermeiden und entsprechend ersetzen. ⌫

Tabelle 4: Tab_Betr_TIP_026 reservierte Zeichen Ersetzungstabelle

reservierte Zeichen	Muss ersetzt werden durch	Begründung
#	<Hash>	Reserviertes Zeichen, für die Feldtrennung. Sie müssen ersetzt werden durch den Text <Hash>.
Zeilen-umbruch	 	Zeilenumbrüche in Inhaltsfeldern erhöhen die Fehlerwahrscheinlichkeit beim Einlesen der CSV-Datei durch das Zielsystem. Sie müssen ersetzt werden durch den Text
Doppeltes Anführungs-zeichen (ASCII 34)	’ (ASCII 39)	Reserviertes Zeichen, für die Markierung der Inhalte von Feldern. Sie müssen ersetzt werden durch ein „Einfaches Anführungszeichen“.
<tr>	löschen	Reservierte Zeichen, für eine Datensatztrennung im Inhaltsfeld. Die Zeichen müssen gelöscht werden.
</tr>	löschen	Reservierte Zeichen, für eine Datensatztrennung im Inhaltsfeld. Die Zeichen müssen gelöscht werden.

2.5.1 Basisfeldtypen von Prozessdaten

Tabelle 5 definiert Basisfeldtypen, die in konkreten Definitionen fachlicher Tabellen referenziert werden. In der Definition der fachlichen Tabellen können diese Basisfeldtypen weiter durch Constraints konkretisiert werden, z. B. durch Einschränkung auf eine fachlich definierten Wertemenge.

Tabelle 5: Tab_Betr_TIP_030 Basisfeldtypen von csv-Dateien

Basisfeldtyp	Definition	Beispiel
[String]	Beliebige Zeichenkette mit den Anforderungen aus GS-A_5249	Hello World
[Date]	Gemäß [ISO-Norm 8601] folgendes Format auf Grundlage der lokalen Zeit gegenüber UTC: YYYY-MM-DDThh:mm:ss±hh	2015-02-23T01:47:36+01
[Date]	als Bestandteil eines Dateinamens: YYYYMMDDThhmmss±hh	20150223T014736+01
[Integer]	+-nnnnnnnnn	88888888
[Double]	+-nnnnn,nnn	2,456
[Auswahlfeld], (auswahl1), (auswahl2), (auswahl n)	Es ist immer nur ein Wert von Auswahl n gültig. Beispiel :[Auswahlfeld], (ja), (nein)	ja
[Telefonnummer]	[String] DIN 5008	+49 30 40041-999
[hh.mm]	Uhrzeit: zwei Stellen für Stunde, zwei Stellen für Minuten gemäß [ISO-Norm 8601]	12:30
[hhhh:mm:ss]	Dauer in Stunden, zwei Stellen für	0012:04:10

Basisfeldtyp	Definition	Beispiel
	Minuten, zwei Stellen für Sekunden	

3 Service Level Management (SLM)

Mit Hilfe des Service Level Management (SLM) werden die Service Level über alle Betriebseinheiten definiert, kontrolliert und optimiert.

Ziele des übergreifenden SLM sind:

- die vereinbarten Service Level zu messen, um die Sicherstellung der aktuell vereinbarten (technischen und prozessualen) Qualität zu gewährleisten.
- die gemessenen Service Level zu analysieren und zu optimieren, um zukünftig die Sicherstellung der IT-Service-Qualität und Performance - möglichst effizient - zu gewährleisten.

Abbildung 1: SLM - Prozessausschnitt „Service Level Management“ veranschaulicht den anbieter- und herstellerrelevanten Prozessausschnitt.

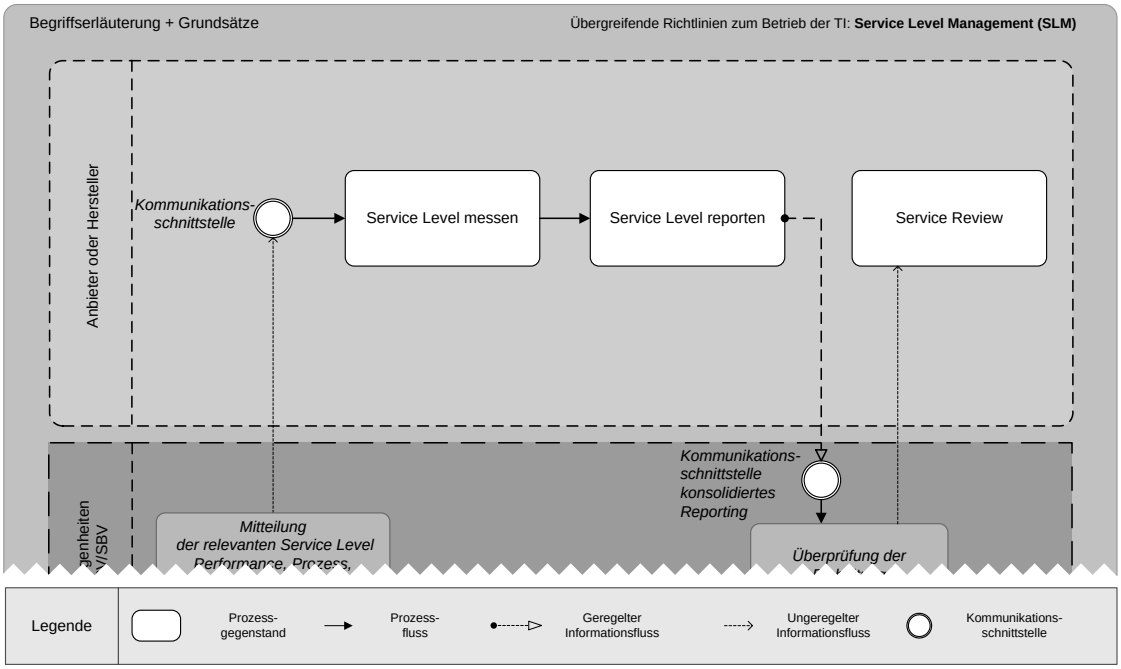


Abbildung 1: SLM - Prozessausschnitt „Service Level Management“

3.1 Betrachtungsgegenstand des übergreifenden SLM

Grundlage und Arbeitsmittel für die Aufgabenwahrnehmung des Service Level Managements durch den SBV und den GBV TI sowie der damit verknüpften Zielerreichung ist der Service Level Report des konsolidierten Reportings (siehe Kapitel 2.3.1 „Konsolidiertes Reporting“).

Betrachtungsgegenstand des übergreifenden SLM sind daher die Regelungen, welche zum Reporting der Service Level im Rahmen des Service Level Reportings festzulegen sind.

3.2 Begriffserläuterungen

3.2.1 Service Level Requirements

Service Level Requirements enthalten die inhaltlichen, als auch schematischen Anforderungen (Qualitätsdimension, Beschreibung der Qualitätsdimension, Ausprägungstyp) für die durch Anbieter oder Hersteller zu messenden Service Level.

Die in der Richtlinie definierten, durch Anbieter und Hersteller zu messenden, Service Level Requirements werden innerhalb der spezifischen Betriebskonzepte ausgeprägt, mit Werten hinterlegt und bilden damit die vollständigen, durch Anbieter oder Hersteller zu erreichenden Service Level ab.

3.3 Grundsätze des übergreifenden SLM

Die nachfolgenden Grundsätze bilden die übergeordneten Regelungen des übergreifenden Service Level Managements für Anbieter und Hersteller.

3.3.1 Gliederung des SLM in Service Level Cluster

Innerhalb des Service Level Managements wird in drei verschiedene Service Level Cluster unterschieden:

- **Service Level Performance** - hierunter werden alle zu messenden technischen Kennzahlen (bspw. hinsichtlich Bearbeitungszeit, Durchsatz und Verfügbarkeit) zusammengefasst.

  Dabei wird die Service Level Performance in den spezifischen Betriebskonzepten nach folgendem Schema gebildet:

Tabelle 6: Tab_Betr_TIP_023 SLM - Service Level "Performance"

Service Level ID	Bezeichnung Service Level	Beschreibung	Typ	Beispiel
wird je Kennzahl vergeben	Performance-Kenngröße	zu messende Performance je Performance-Größe	[Double]	2,465

- **Service Level Prozess** - hierunter werden alle prozessbezogen zu messenden Service Level Requirements der übergreifenden ITSM-Prozesse mit Fokus auf die Prozessqualität (bspw. Reaktionszeit) zusammengefasst.

In dem vorliegenden Dokument sind diese mit „Prozess“ gekennzeichneten SLRs

- für das Incident Management den Kapiteln 8.4.8 „Service Level Requirements (SLR)“ und 8.5.9 „Service Level Requirements (SLR)“ zu entnehmen,
- für das Problem Management den Kapiteln 9.4.8 „Service Level Requirements (SLR)“, 9.5.4 „Service Level Requirements (SLR)“ und 9.6.8 „Service Level Requirements (SLR)“ zu entnehmen,

- für das Change Management dem Kapitel 5.5 „Service Level Requirements (SLR)“ zu entnehmen.
- **Service Level Serviceerbringung** - hierunter werden alle qualitativen, servicebezogen zu messenden Service Level Requirements der übergreifenden ITSM-Prozesse mit dem Schwerpunkt auf die Serviceerbringung (bspw. Rufbereitschaft) zusammengefasst.

In dem vorliegenden Dokument sind diese mit „Serviceerbringung“ gekennzeichneten SLRs

- für das konsolidierte Reporting dem Kapitel 2.3.3 „Service Level Requirements (SLR)“ zu entnehmen,
- für das Incident Management den Kapiteln 8.4.8 „Service Level Requirements (SLR)“ und 8.5.9 „Service Level Requirements (SLR)“ zu entnehmen,
- für das Problem Management den Kapiteln 9.4.8 „Service Level Requirements (SLR)“, 9.5.4 „Service Level Requirements (SLR)“ und 9.6.8 „Service Level Requirements (SLR)“ zu entnehmen,
- für das Performance Management dem Kapitel 4.3.4 „Service Level Requirements (SLR)“ zu entnehmen,
- für das Notfallmanagement dem Kapitel 10.5.8 „Service Level Requirements (SLR)“ zu entnehmen.

3.4 Prozessdurchführung übergreifendes SLM

Innerhalb der jeweiligen ITSM-Prozessbeschreibungen dieses Dokumentes sind, abhängig vom Prozess, verschiedene Service Level Requirements beschrieben, die durch den Anbieter und Hersteller zu messen, zu berichten und zu optimieren sind. Da die Service Level Requirements in diesem Dokument ausschließlich die schematischen Inhalte, als Grundlage der Service Level darstellen, werden diese innerhalb der spezifischen Betriebskonzepte mit Werten hinterlegt und bilden erst damit die vollständige Anforderung als Service Level.

Während des Wirkbetriebs werden diese spezifischen, durch Anbieter und Hersteller zu messenden und zu berichtenden Requirements dann durch den Serviceverantwortlichen fortgeschrieben und gepflegt sowie deren Einhaltung durch den SBV überwacht.

3.4.1 Messung der Service Level

⌦ **GS-A_4100 Messung der Service Level**

Anbieter und Hersteller MÜSSEN zur Kontrolle und Optimierung der vereinbarten Service Level alle Service Level innerhalb der Cluster „Service Level Performance“, „Service Level Prozess“ und „Service Level Serviceerbringung“ messen. ⌫

3.4.2 Bereitstellung des Service Level Reports

⌦ GS-A_4101 Übermittlung der Service Level Messergebnisse

Anbieter und Hersteller MÜSSEN die Service Level Messergebnisse im Rahmen des konsolidierten Reportings an die durch den SBV benannte Kommunikationsschnittstelle übermitteln. ⌫

⌦ GS-A_4102 Dateistruktur des Service Level Reports

Anbieter und Hersteller MÜSSEN Service Level Messungen nach folgendem Schema (die Reihenfolge ist verbindlich) für den Service Level Report aufbereiten:

Tabelle 7: Tab_Betr_TIP_002 SLM - Reportinhalte Service Level Report

#	Spaltenname	Beschreibung	Typ	Beispiel
1	Teilnehmer ID	ID des A/H bzw. weitere Beteiligte im Betrieb der TI	[String]	
2	Produktkürzel	Produktkürzel gemäß gemSpec_OM	[String]	
3	Betriebsumgebung	Gibt die zugehörige Betriebsumgebung des SLA an. Für übergreifende SLA – wie z.B. organisatorische SLA – ist die Betriebsumgebung „Alle“ zu verwenden	[Auswahlfeld], (RU), (TU), (PU), (Alle)	Alle
4	Service Level ID	ID des Service Level	[String]	
5	Bezeichnung Service Level	Bezeichnung des Service Levels	[String]	
6	Messwert	erreichter Wert, gemessen gemäß der Messvorgaben	[Double]	2,456
7	Einheit Ergebniswert	Einheit des Ergebniswertes	[String]	[s] oder [%]oder ….
8	Soll Wert	zu erreichender Zielwert gemäß Service Level	[Double]	2,456
9	Einheit Soll Wert	Einheit des Soll-Wertes	[String]	[s] oder [%]oder ….
10	Abweichung	bei Unterschreitung der vereinbarten Service Level	[Double]	2,456
11	Einheit Abweichung	Einheit der Abweichung	[String]	[s] oder [%]oder ….
12	Auswertungsstart	Zeitpunkt, an dem die Ermittlung bzw. die Messung für den Service Level gestartet wurde	[Date]	
13	Auswertungsende	Zeitpunkt, an dem die Ermittlung bzw. die Messung	[Date]	

#	Spaltenname	Beschreibung	Typ	Beispiel
		für den ServiceLevel beendet wurde		
14	Grund für Abweichung	qualifizierte Beschreibung für den Grund der Abweichung vom Soll-Wert	[String]	
15	Getroffene Maßnahmen	Nennung und qualifizierte Beschreibung der bereits erfolgten Mitigationsmaßnahmen, um zukünftig den Soll-Wert zu erreichen	[String]	
16	Geplante Maßnahmen	Nennung und qualifizierte Beschreibung der geplanten Mitigationsmaßnahmen, um zukünftig den Soll-Wert zu erreichen	[String]	

⌫

⌦ **GS-A_4103 Dateiformat des Service Level Reports**

Anbieter und Hersteller MÜSSEN den an den SBV zu versendenden Service Level Report im CSV-Format übermitteln.

Anbieter und Hersteller MÜSSEN bei den an den SBV zu versendenden Reports GS-A_5248 beachten.⌫

Für die Webportal-nutzenden Teilnehmer wird der Service Level Report (Prozess und Serviceerbringung) über die ZID zur Verfügung gestellt.

3.4.3 Service Review

Service Reviews werden zur Feststellung von notwendigen Optimierungsaktivitäten - sowohl auf Ebene der Vorgaben als auch auf Ebene der Umsetzung - durchgeführt. Service Reviews erfolgen bei Bedarf und werden durch den SBV einberufen. Die Art der Durchführung des Service Reviews wird durch den SBV festgelegt (bspw. Telefonkonferenz, E-Mail). Präsenztermine für Anbieter und Hersteller werden durch den SBV, soweit möglich, vermieden und nur einberufen, sofern eine Notwendigkeit hierfür besteht.

Anbieter und Hersteller, die Optimierungsaktivitäten eigenverantwortlich definiert haben, erfassen diese im Service Level Report.

⌦ **GS-A_4397 Teilnahme am Service Review**

Anbieter und Hersteller MÜSSEN am Service Review teilnehmen und die bilateral besprochenen Optimierungsaktivitäten umsetzen.⌫

4 Performance Management (PERF)

Das Performance Management fasst die ITIL-Prozesse „Capacity Management“ und „Availability Management“ zusammen. Dabei hat das Performance Management zum Ziel, adäquate Kapazitäten und die geforderten Verfügbarkeiten für die TI zu gewährleisten.

Um dieses Ziel zu unterstützen, müssen Anbieter Performance-Messungen durchführen und diese an die zuständige servicebetriebsverantwortliche Instanz berichten. Die entsprechenden Analysen und Optimierungen im Design werden durch den SBV initiiert bzw. vorgenommen. Interne Optimierungsmaßnahmen der Anbieter sind nicht Bestandteil der Richtlinie und werden vorausgesetzt.

Dieses Kapitel enthält ausschließlich Anforderungen an Anbieter von zentralen Produkten der TI.

Abbildung 2: PERF - Gesamtüberblick „Performance Management“ veranschaulicht den anbieter- und herstellerrelevanten Prozessausschnitt und gibt eine Zuordnung der einzelnen Prozessinhalte zu den nachfolgenden Kapiteln.

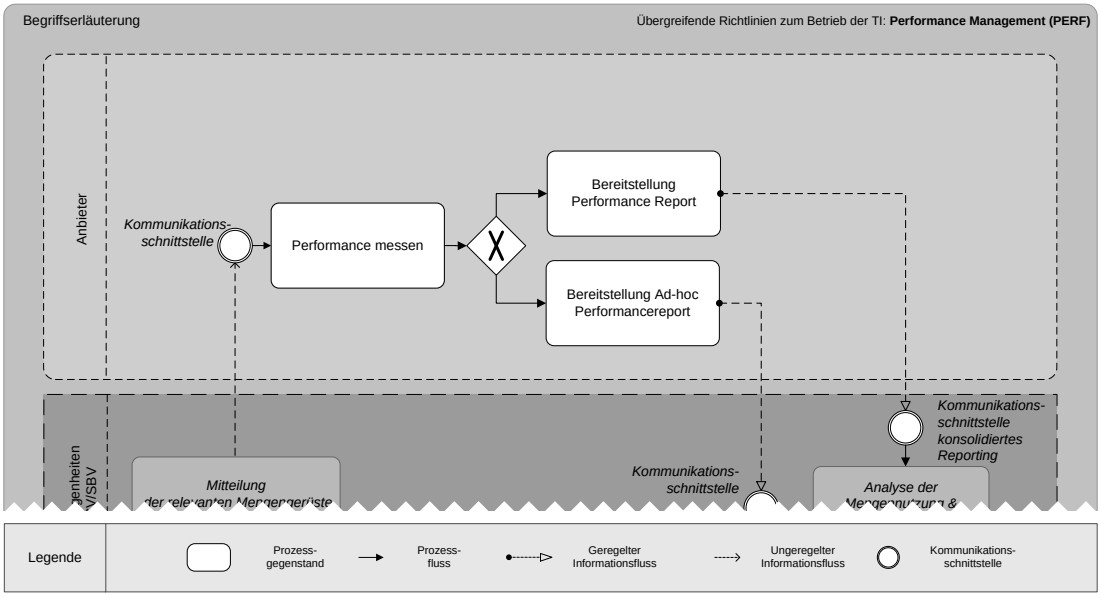


Abbildung 2: PERF - Gesamtüberblick „Performance Management“

4.1 Betrachtungsgegenstand des übergreifenden PERF

Fokus der nachfolgenden Performance-Management-Regelungen im übergreifenden Betrieb sind die durch die Anbieter durchzuführenden Performance-Messungen und das dazugehörige Reporting an die servicebetriebsverantwortliche Instanz. Die Performance-Messungen der dezentralen Produkte werden nicht betrachtet.

4.2 Begriffserläuterungen

4.2.1 Performance

Die Performance umfasst gemäß [gemSpec_Perf] die Dimensionen Bearbeitungszeit, Durchsatz und Verfügbarkeit.

4.3 Prozessdurchführung des übergreifenden PERF

Zur Sicherung der notwendigen Leistungen und Kapazitäten in der geforderten Verfügbarkeit, zur rechtzeitigen Einleitung von notwendigen Schritten zur Leistungsanpassung sowie zur Vermeidung von Überkapazitäten in der TI müssen Anbieter Performance-Messungen durchführen und die Ergebnisse berichten.

Die Messergebnisse dienen dabei

- im ersten Schritt der Analyse der aktuellen Performance sowie der Prognoseerstellung für zukünftige Performance-Anforderungen der Anwendungsservices und des TI-Plattform Services und
- im zweiten Schritt der - falls erforderlich - Anpassung der Kapazität, um Überkapazitäten oder bestehende bzw. drohende Engpässe zu kompensieren und die vereinbarten Service Level aufrechterhalten zu können.

4.3.1 Messung der Performance

Die Messungen erfolgen innerhalb der lokalen Systeme und Prozesse des Anbieters und müssen die Vorgaben (bspw. Messvorschriften) gemäß [gemSpec_Perf] für die Messung der Performance einhalten.

4.3.2 Bereitstellung des Performance Reports

⌦ **GS-A_4106 Reportinhalte und Format des Performance-Reports**

Anbieter MÜSSEN Performance-Messungen nach folgendem Schema (die Reihenfolge ist verbindlich) an den zuständigen SBV übermitteln:

Tabelle 8: Tab_Betr_TIP_003 PERF - Reportinhalte von Performance Messungen

#	Spaltenname	Beschreibung	Typ	Beispiel
1	Teilnehmer ID	ID des A/H bzw. weitere Beteiligte im Betrieb der TI	[String]/	
2	Produktkürzel	Produktkürzel gemäß gemSpec_OM	[String]/	
3	Betriebsumgebung	Gibt die Betriebsumgebung an, in welcher das Produkt im Messintervall gemessen wurde. Werden Messwerte für Produkte bzw. Produktbestandteile (z.B. SZZP) geliefert, so ist die Betriebsumgebung „Alle“ zu verwenden	[Auswahlfeld], (RU), (TU), (PU), (Alle)	Alle

#	Spaltenname	Beschreibung	Typ	Beispiel
4	Performance Kenngroesse	Ausgeprägter Bezeichner der Performance-Kenngröße gemäß Tab_gemSpec_Perf_Performance-Kenngroessen [gemSpec_Perf#Anh.C]	[String]	PDT03-S06-D1-G01-Z06
5	Messwert	ermittelter Wert aus der Performance-Messung für das angegebene Messintervall [Auswertungsstart / -ende] bzw. Zeitstempel	[Integer] oder [Date]	
6	Messgroesse	Messgröße des Performance-Wertes gemäß [gemSpec_Perf]	[String]	
7	Auswertungsstart	Zeitpunkt, ab dem die Messung für den Wert gestartet ist	[Date]/	
8	Auswertungsende	Zeitpunkt, an dem die Messung für den Wert beendet wurde	[Date]/	

Der Performance-Report ist als CSV-Datei zu übermitteln. Anbieter und Hersteller MÜSSEN bei den an den SBV zu versendenden Reports die AFO GS-A_5248 beachten.Tausendertrennzeichen werden nicht verwendet. ⌫

4.3.3 Bereitstellung von Ad-hoc Performance Reports

⌦ **GS-A_4108 Inhalt von Ad-hoc Reports**

Anbieter MÜSSEN für das Ad-hoc Reporting Daten aus dem vorhandenen Performance-Kenngrößen-Pool des Performance Reports oder andere - durch den SBV benannte - Kennzahlen (innerhalb eines zumutbaren Umfangs für den Anbieter) dem SBV bereitstellen. Für die Bereitstellung der Reports gelten die Regelungen gemäß „GS-A_4097“. Entsteht die Notwendigkeit zu Erhebung weiterer Kennzahlen, werden diese gemeinsam mit den betroffenen Anbietern und Herstellern individuell abgestimmt.⌫

4.3.4 Service Level Requirements (SLR)

⌦ **GS-A_4109 Service Level Requirements Anbieter-Performance-Messungen**

Anbieter MÜSSEN mindestens folgende Service Level messen und berichten:

Tabelle 9: Tab_Betr_TIP_004 PERF-Performance-Messungen Anb. „Serviceerbringung”

ID	Qualitätsdimension	Beschreibung	Typ	Beispiel
PERF_1	Anzahl der Monate der Datenaufbewahrung von Performance-Messungen	Datenaufbewahrung von Performance-Messungen in Monaten	[integer]	6

Service Level werden in den spezifischen Betriebskonzepten produkttypspezifisch ausgeprägt. ⌫

5 Change & Release Management (CHG & RLM)

Das Release Management hat die Überführung von Releases in den Wirkbetrieb zur Aufgabe. Es koordiniert die Entwicklung, den Test, die Verifikation sowie das Deployment der durch das Service Design definierten und geplanten Funktionen. Das Release Management stellt sicher, dass ein Release ausschließlich aus zugelassenen sowie aus einem Satz zu einander kompatibler Konfigurationseinheiten besteht.

Das Change Management hat die Aufgabe sicherzustellen, dass alle Änderungen an Produkten und den darauf basierenden Services kontrolliert durchgeführt werden. Innerhalb des Change Managements werden Änderungsanträge (Requests for Change) aufgezeichnet, bewertet sowie autorisiert und die daraus resultierenden Umsetzungen als Änderungsanforderungen (Change) koordiniert.

Da ein Release im Kontext der TI aus einer Vielzahl von Changes besteht, sind beide ITSM-Prozesse eng miteinander verzahnt und werden innerhalb dieses Dokumentes integrativ beschrieben. Die nachfolgende Abbildung veranschaulicht hierzu Regelungen des übergreifenden Change & Release Managements und verdeutlicht den für Anbieter und Hersteller relevanten Prozessausschnitt.

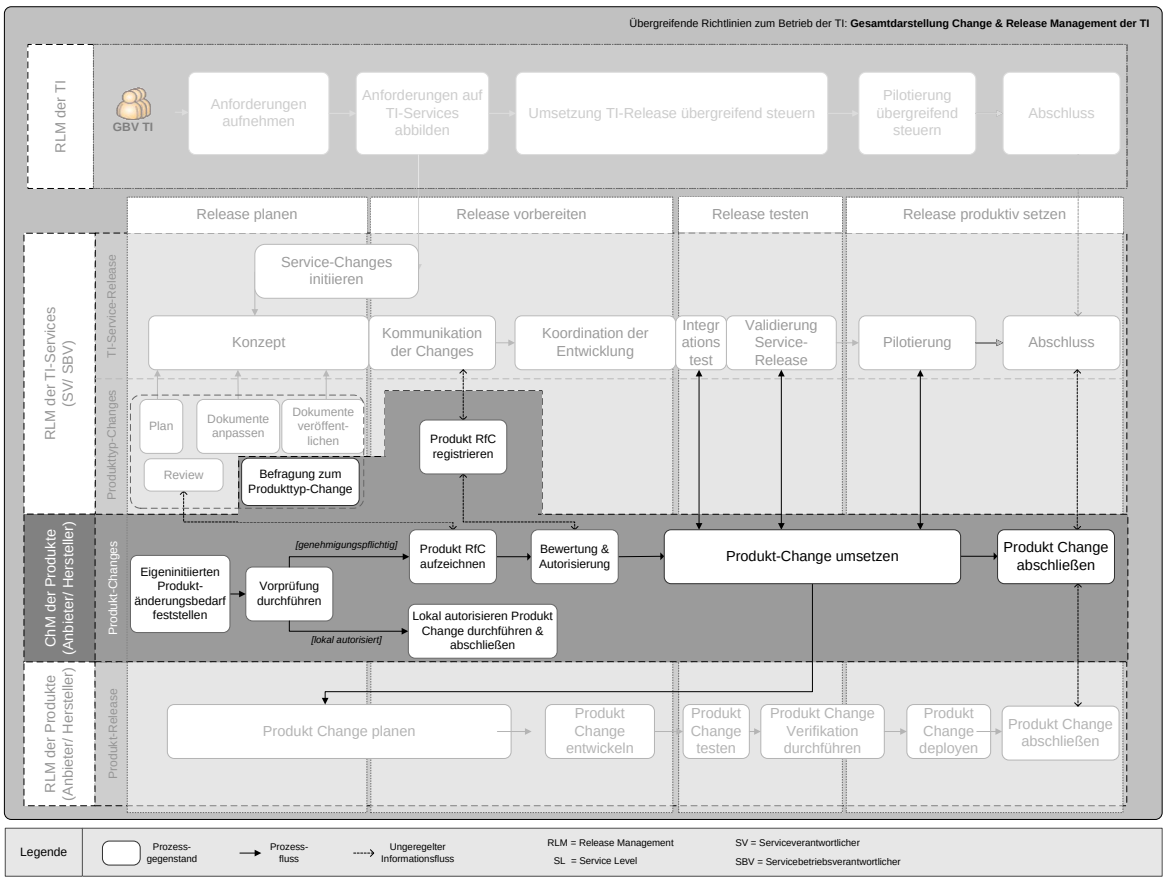


Abbildung 3: CHG & RM - Gesamtkontext "Change & Release Management"

5.1 Betrachtungsgegenstand des übergreifenden CHG & RLM

In diesem Abschnitt wird das übergreifende Change Management für Produkte sowie die im Change Management Prozess enthaltenen Übergabepunkte zum und vom Release Management der Produkte geregelt.

Das Change & Release Management der anderen Level (TI, Service, Produkttyp) wird innerhalb dieser Richtlinie nur insoweit dargestellt, wie es zur Einordnung des Produkt-Levels in den Gesamtkontext notwendig ist.

Das „lokale“ Release Management der Produkte in Verantwortung der Anbieter und Hersteller wird in dieser Richtlinie nur insofern geregelt, wie es zur Sicherstellung der ordnungsgemäßen Umsetzung des Change & Release Managements notwendig ist.

Nicht weiter betrachtet wird das Release Management der TI in Verantwortung des GBV TI.

5.2 Begriffserläuterungen

Die Begriffe **RfC, Change Request** und **Änderungsantrag** werden synonym verwendet.

Die Begriffe **Change** und **Änderungsanforderung** werden synonym verwendet.

Korrigierender Change: Bei einem korrigierenden Change handelt es sich um Korrekturänderungen der TI bzw. des Services bzw. des Produkttyps bzw. des Produktes.

Erweiterungs-Change: Bei einem Erweiterungs-Change handelt es sich um ergänzende Änderungen der TI bzw. des Services bzw. des Produkttyps bzw. des Produktes.

Übergreifender Change- und Releasekalender: Der Change- und Releasekalender ist Bestandteil der betriebsunterstützenden Verfahren und Systeme der Telematikinfrastruktur.

Der Change- und Releasekalender dient allen am Betrieb der TI Beteiligten dazu, sich über anstehende und durchgeführte Änderungen und Releasewechsel informieren zu können. Er ist zugleich ein Organisations- und Planungsinstrument im Rahmen des Change & Release Managements. Er ersetzt nicht die aktive Steuerung von Changes und Releasewechseln in der TI, sondern ermöglicht eine langfristige Vorschau auf geplante Änderungen und ist ein zusätzliches Hilfsmittel bei der Analyse von Störungsursachen bezüglich der Identifikation von Seiteneffekten bereits umgesetzter Änderungen.

Anbieter und Hersteller können bspw. zur erneuten Verifikation von Change- und Releaseplanungen oder zur Analyse von Störungsursachen den Change- und Releasekalender nutzen.

5.3 Prozessdurchführung übergreifendes RLM

In einem Release werden unterschiedliche Services zu einem TI-Release bzw. unterschiedliche Produkttypen und Produkte zu einem Service-Release

zusammengefasst, die zum gleichen Releasetermin im Rahmen eines einheitlichen Releaseprozesses produktiv gesetzt werden.

Der Begriff Release ist in diesem Zusammenhang im Sinne eines Containers zu verstehen, der die einzelnen Service-, Produkttyp- oder Produktversionen enthält. Das übergreifende Release Management erfolgt auf den Ebenen:

- Release Management der TI,
- Release Management der TI-Services,
- Release Management der Produkte.

Auf der Ebene der Services und Produkttypen wird ein Release in der Regel mehrere Änderungen beinhalten. Auf Ebene der Produkte kann ein Release bereits aus einer Änderungen bestehen.

Jede dieser Ebenen prägt ihr eigenes Release Management aus, so dass Umfang, Aufgaben, Stakeholder und Betroffene je nach Gegenstand der Releases variieren.

Release Management der TI:

Das **Release Management der TI** verantwortet die strategische Releaseplanung für die TI. Auf dieser Ebene steht der Planungsaspekt im Vordergrund, der Funktionsumfang eines TI-Releases wird vereinbart und die Bereitstellung sowie Implementierung wird mit den Stakeholdern abgestimmt. Die Planung der TI-Releases legt den zeitlichen Rahmen und die Termine für die Ebene Release Management der TI-Services fest. Diese Termine werden im Change- und Releasekalender dokumentiert. Der Test und die Überführung der TI-Releases in den Wirkbetrieb werden in enger Kooperation mit der Ebene Release Management der TI-Services durchgeführt. Verantwortlich für das Release Management der TI ist der GBV TI.

Beispiel für TI-Release: Das ORS1-Release als Gesamtmenge aller bereitzustellenden Anwendungs- und Basisservices auf Basis der Produkttyp-Spezifikationen und den realisierten, implementierten und zugelassenen Produkten im Wirkbetrieb, mit dem dazugehörigen und freigegebenen Dokumentenset. Ein Release Label zu diesem TI-Release ist derzeit noch nicht festgelegt.

Da das Release Management der TI ausschließlich durch den GBV TI durchgeführt wird, wird es in dieser Richtlinie nicht weiter betrachtet.

Release Management der TI-Services:

Auf der Ebene des **Release Managements der TI-Services** planen und koordinieren die serviceverantwortlichen Instanzen (Rolle SV) die Bereitstellung, den Test und die Überführung von Service Releases und Produkttyp-Changes in den Wirkbetrieb.

Der SV wird während der Anpassung der Produkttypen - bei Bedarf - bei Anbietern und Herstellern eine Befragung zum geplanten Produkttyp-Change durchführen. Die Befragung wird sich insbesondere auf die Kriterien Machbarkeit (inkl. Kompatibilität) und Kostenwirkung (inkl. Migrationsaufwand) fokussieren.

⌦ **GS-A_4414 Beteiligung von Herstellern und Anbietern an der Bewertung von Produkttyp-Changes mittels Befragung**

Anbieter und Hersteller MÜSSEN bei der Befragung zu geplanten Produkttyp-Changes durch den SV mitwirken und den SV in seiner Releaseplanung beratend unterstützen. ⌫

Beispiel für TI-Service-Release: Das Release des Anwendungsservices VSDM als Gesamtmenge aller auf Basis der Produkttyp-Spezifikationen zugelassenen Produkte, die genau den Anwendungsservice VSDM bilden. Die zugelassenen Produkte sind als Produktinstanzen im Wirkbetrieb implementiert, mit dem dazugehörigen und freigegebenen Dokumentenset. Das Release Label zu diesem TI-Service-Release ist derzeit noch nicht festgelegt.

Release Management der Produkte:

Das operative **Release Management der Produkte** verantworten die Hersteller und Anbieter. Die Entwicklung der Produkte, ihr Test und die Überführung der Produktinstanzen in den Wirkbetrieb müssen die Produkttyp-Spezifikationen, die Vorgaben aus dem übergeordneten Service Release sowie die Änderungsaufträge aus dem Change Management beachten.

Beispiel für Produkt-Release: Die fertige, veröffentlichte und zugelassene Version eines Produktes eines Herstellers oder Anbieters wird als Produkt-Release bezeichnet. Beispiele für zugelassene Produkt-Releases finden sich auf der Homepage der Zulassungsstelle der gematik.

5.4 Prozessdurchführung übergreifendes CHG

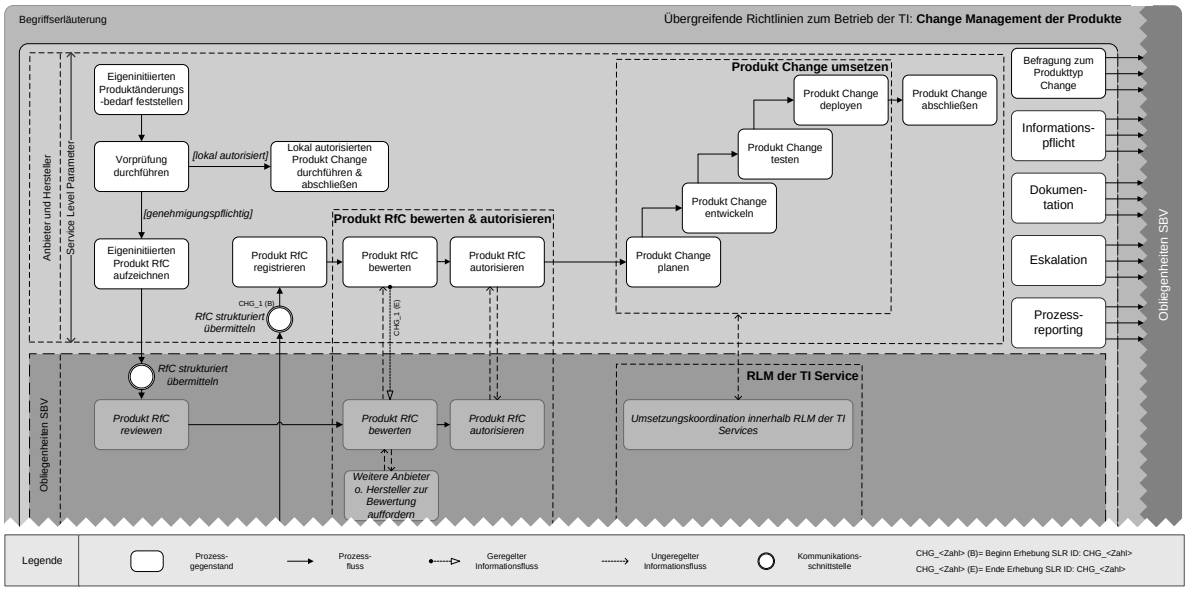


Abbildung 4: CHG - Gesamtüberblick „Change Management der Produkte“

Im Rahmen des übergreifenden Change Managements verantworten die Anbieter und Hersteller (in Abstimmung mit dem SBV) das Change Management der Produkte.

Alle Produktänderungen werden

- durch das lokale Change Management des Anbieters und Herstellers koordiniert und
- innerhalb des lokalen Release Managements des Anbieters und Herstellers umgesetzt.

Innerhalb des übergreifenden Change Managements wird dabei grundsätzlich in zwei Produkt-Change-Typen unterschieden:

- in lokal autorisierte Changes (informationspflichtig im Rahmen des Configuration Managements)
- und in genehmigungspflichtige Changes.

Die Entscheidung, um welchen Change Typ es sich handelt, muss innerhalb der Vorprüfung des Produktänderungsbedarfs (siehe Kapitel 5.4.2 „Vorprüfung durchführen“) erfolgen.

Sofern nicht anders ausgewiesen, werden nachfolgend die für Anbieter und Hersteller relevanten Regelungen zur Identifikation des Change Typs sowie des Prozessablaufs für genehmigungspflichtige Changes dargelegt.

Eine Übersicht aller RfCs und deren Status wird in einem FSC (Forward Schedule of Change) über die Wissensdatenbank zur Verfügung gestellt. Weiterhin werden RfCs abhängig von ihrem Status im CAB (Change Advisory Board) besprochen.

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt

Die Kommunikation und der Informationsaustausch zur Durchführung des Change-Prozesses erfolgt aus Gründen der Flexibilität sowie aufgrund der individuellen Ausprägungsmöglichkeiten je Produkt-RfC bzw. Change-Durchlauf weitgehend per E-Mail, aber auch telefonisch, in Form von Telefonkonferenzen oder auch durch Besprechungen vor Ort. Die im Folgenden aufgeführten Anforderungen hinsichtlich der Übermittlung von Informationen der Anbieter und Hersteller an den SBV erfolgen dabei grundsätzlich per E-Mail, es sei denn, es werden nähere Angaben für das zu wählende Kommunikationsmedium gemacht.

Jeder übergreifende Produkt-RfC bzw. Produkt-Change wird in formaler Form in der ZID gespeichert. Speicherung und Statusänderungen des Produkt-RfCs bzw. des Produkt-Changes werden durch den SBV vorgenommen.

Anbieter und Hersteller haben über das zur Verfügung gestellte Webportal der ZID die Möglichkeit, diejenigen Produkt-RfCs bzw. Changes einzusehen, an denen sie beteiligt sind. Ein Rollen- und Berechtigungskonzept der ZID regelt dabei die Einsichtnahme und den Zugriff auf die relevanten Datensätze. Des Weiteren wird den Anbietern und Herstellern im Webportal der ZID die Möglichkeit eröffnet, alle in diesen Richtlinien angegebenen formalen Informationen und Prozessschritte, welche die Kommunikation mit dem SBV berühren (z. B. Beantragung eines Produkt-RfCs, Autorisierung des Produkt-RfCs, Vorgangsdaten zu Produkt-Changes speichern), direkt über das Webportal der ZID vorzunehmen. Die Erläuterungen erfolgen in den jeweiligen Abschnitten.

Die im Folgenden definierten Dokumentations- und Übermittlungspflichten der am jeweiligen Produkt-RfC bzw. Produkt-Change beteiligten Anbieter und Hersteller obliegen weiterhin ausschließlich den Anbietern und Herstellern selbst.

5.4.1 Eigeninitiierten Produktänderungsbedarf feststellen

Eigeninitiierte Produktänderungsbedarfe können durch verschiedene Einflussfaktoren bei den Anbietern und Herstellern festgestellt werden (bspw. Korrekturbedarfe aus dem lokalen/übergreifenden Incident Management oder Problem Management, oder auch Ergänzungsbedarfe des Produktes, die der Anbieter oder Hersteller festgestellt hat).

An die Feststellung von Produktänderungsbedarfen innerhalb der lokalen Change-Prozesse des Anbieters und Herstellers werden keine Anforderungen gestellt.

5.4.2 Vorprüfung durchführen

⌦ **GS-A_4398 Vorprüfung von durch Anbieter oder Hersteller festgestellten Produktänderungsbedarfen**

Anbieter und Hersteller MÜSSEN jeden festgestellten Produktänderungsbedarf einer Vorprüfung gemäß der unten abgebildeten Tabelle unterziehen. Dabei ist - durch Feststellung der Wechselwirkungen mit anderen Produkten sowie der Abweichung von Produkttypvorgaben - zu prüfen, ob es sich um eine genehmigungspflichtige oder einen lokal autorisierte Produktänderung handelt.

Tabelle 10: Tab_Betr_TIP_024 CHG - Vorprüfung lokal./genehmig. Produktänderungsbedarf

Change Typ	Wechselwirkungen mit anderen Produkten (an den Schnittstellen)	Abweichung von Produkttypvorgaben
lokal autorisiert	Nein	Nein
genehmigungspflichtig	Nein	Ja
genehmigungspflichtig	Ja	Nein
genehmigungspflichtig	Ja	Ja

⌫

Sofern es sich um einen genehmigungspflichtigen Produktänderungsantrag handelt, müssen Anbieter und Hersteller einen Produkt-RfC gemäß den Anforderungen in Kapitel 5.4.4 „Eigeninitiierten Produkt-RfC aufzeichnen“ aufzeichnen.

Sofern es sich um einen lokal autorisierten Änderungsantrag handelt, erfolgt die weiterführende Bearbeitung - ohne weitere Genehmigung durch den SBV - im lokalen Change Management des Anbieters. (siehe Kapitel 5.4.3 „lokalen Produkt-Change durchführen & abschließen“)

5.4.3 lokalen Produkt-Change durchführen & abschließen

An das Management lokal autorisierter Produkt-Changes (s. Tabelle 10: Tab_Betr_TIP_024 CHG - Vorprüfung lokal./genehmig. Produktänderungsbedarf) werden

keine Anforderungen gestellt. Der zuständige SBV ist nach Durchführung des lokal autorisierten Changes zu informieren.

⌦ **GS-A_4399 Übermittlung von Produktdaten nach Abschluss von lokal autorisierten Produkt-Changes**

Anbieter und Hersteller MÜSSEN nach dem Abschluss (nach der Produktivsetzung des Produkt-Changes als Produkt) von lokal autorisierten Produkt-Changes den Änderungsdatensatz der Produktdaten an den SBV übermitteln. ⌫

5.4.4 Eigeninitiierten Produkt-RfC aufzeichnen

⌦ **GS-A_4400 Produkt-RfC aufzeichnen & an SBV übermitteln**

Anbieter und Hersteller MÜSSEN für genehmigungspflichtige Produktänderungen über ein vom SBV zur Verfügung gestelltes Formular einen Produkt-RfC erstellen und an die vom SBV bereitgestellte Kommunikationsschnittstelle übermitteln oder den Produkt-RfC direkt über eine im Webportal der ZID eingerichtete, Erfassungsmaske manuell eingeben. Erfasst der Anbieter oder Hersteller den Produkt-RfC direkt im Webportal der ZID, wird die formale Beantragung und Übermittlung an den SBV ebenfalls über das Webportal der ZID angestoßen.

(Zur Erstellung des Produkt-RfCs stellt der SBV den Anbietern und Herstellern ein Formular zur Verfügung.) ⌫

Der SBV wird den Erhalt des vom Anbieter oder Hersteller versendeten Produkt RfC quittieren, eine über alle Anbieter und Hersteller eindeutige ID vergeben, an den Antragsteller zurückmelden. Im Falle des per Formular (d. h. per E-Mail) übermittelten Produkt-RfC trägt der SBV diesen gemäß den Angaben des Anbieters oder Herstellers vor der Quittierung in das Webportal der ZID ein. Der SBV wird dann den Produkt-RfC in angemessener Zeit formal und inhaltlich prüfen (insbesondere auf Vollständigkeit, Durchführbarkeit und Redundanz mit bereits angenommenen, aktuell zu prüfenden und abgelehnten Produkt RfCs).

Bei Zustimmung wird der SBV den Produkt-RfC zur Bewertung freigeben. Die Freigabe erfolgt durch den SBV im Webportal der ZID. Der SBV wird daraufhin dem Anbieter oder Hersteller die Freigabe des Produkt-RfC per E-Mail mitteilen.

Bei Ablehnung (Stornierung) (bspw. wegen Nichtdurchführbarkeit) des Produkt-RfCs wird der SBV dies dem Anbieter oder Hersteller unter Angabe von Gründen mitteilen. Die Ablehnung wird formal vom SBV in der ZID dokumentiert.

5.4.5 Produkt-RfC registrieren

Ein Produktänderungsbedarf kann - neben Anbietern und Herstellern - vom SBV festgestellt werden (bspw. durch Änderungen am Produkttyp). Der SBV registriert den Produkt-RfC in der ZID und übermittelt ihn per E-Mail an den bzw. die von ihm ausgewählten Anbieter und Hersteller verbunden mit der Aufforderung zur inhaltlichen Prüfung. Der Produkt-RFC ist damit noch nicht zur Bewertung freigegeben. Erst nach positiver inhaltlicher Prüfung und Rückmeldung durch den Anbieter oder Hersteller kann der Produkt-RfC durch den SBV zur Bewertung freigegeben werden.

⌦ **GS-A_4401 Registrierung von durch den SBV übermittelten Produkt-RfCs**

Anbieter und Hersteller SOLLEN durch den SBV übermittelte Produkt-RfCs vor der Bewertungsphase inhaltlich prüfen und das Ergebnis ihrer Prüfung – nach den mit der Registrierung und Anfrage zur Prüfung festgelegten zeitlichen Vorgaben des SBV – an ihn übermitteln.

(Die Registrierung dient insbesondere der Kenntnisnahme der anstehenden Produktänderung, der Prüfung auf Vollständigkeit, Kosten und Machbarkeit sowie der Vorbereitung der sich anschließenden gemeinsamen Bewertung des Produkt-RfC.) ⌫

5.4.6 Produkt-RfC bewerten & autorisieren

Sowohl vom Anbieter oder Hersteller aufgezeichnete, genehmigungspflichtige Produkt-RfCs (die vom SBV zur Bewertung freigegebenen wurden), als auch vom SBV an Anbieter und Hersteller übermittelte Produkt-RfCs werden durch betroffene Anbieter und Hersteller sowie dem SBV bewertet werden. Die Autorisierung des genehmigungspflichtigen Produkt-RfC erfolgt im Konsens zwischen dem realisierenden Anbieter bzw. Hersteller und dem zuständigen SBV. Der SBV hat sich die notwendigen Genehmigungen des SV und GBV TI vor der Autorisierung einzuholen.

Übergreifende Ziele der gemeinsamen Bewertung sind:

- finale Schärfung/Konkretisierung/Feststellung der Produkt-RfC-Inhalte, insbesondere zu Zeitraumplanung, Ressourcenaufwand & -planung, Kosten, Machbarkeit, Nutzen, Priorität, Risiken, Backout-/Fehlerkorrekturplan, Zulassungsrelevanz (inkl. relevanter Testverfahren, Testumgebungen & Testmanagement), Zuordnung zum Produktrelease bzw. TI-Service-Release
- sowie Festlegung der Verbindlichkeit von Termin- und Umsetzungszusagen.

Sollten Anbieter und Hersteller mit dem SBV keine Einigung bei der Bewertung erzielen können, besteht die Möglichkeit der Eskalation an den GBV TI (siehe Kapitel 5.8 „Eskalationen“).

Die Durchführung der Bewertung kann mittels der Einberufung eines CAB (Change Advisory Board) erfolgen. Die Form und die zeitlichen Intervalle des CAB werden durch den SBV festgelegt (bspw. Telefonkonferenz, E-Mail-Verteiler). Präsenztermine für Anbieter und Hersteller werden durch den SBV, soweit möglich, vermieden und nur einberufen, sofern eine Notwendigkeit hierfür besteht oder die Mehrheit der im CAB beteiligten Anbieter und Hersteller dieses wünschen.

⌦ **GS-A_4402 Mitwirkungspflicht bei Bewertung von Produkt-RfCs**

Anbieter und Hersteller MÜSSEN bei der Bewertung von Produkt-RfCs mitwirken. Die Mitwirkung erfolgt innerhalb eines CAB oder bilateral zwischen Anbieter oder Hersteller und SBV. ⌫

Ist die Bewertung des Produkt-RfCs durch Anbieter und Hersteller sowie SBV inhaltlich abgeschlossen, müssen die am Produkt-RfC beteiligten Rollen (Anbieter/Hersteller und SBV) eine Autorisierung (Freizeichnung) des Produkt-RfCs vornehmen. Der SBV wird sich bei Bedarf - vor seiner Autorisierung - mit dem GBV TI abstimmen.

Die Autorisierung durch die Anbieter und Hersteller erfolgt per E-Mail an den SBV oder mittels eines im Webportal der ZID bereitgestellten Autorisierungsvorgangs. Erfolgt die Autorisierung per E-Mail an den SBV, nimmt der SBV - nach Erhalt der Autorisierung des betroffenen Anbieter oder Hersteller - die Autorisierung für diesen formal im Webportal der ZID vor.

Vor der Change-Umsetzung muss der Produkt-RfC sowohl vom SBV als auch vom Anbieter/Hersteller formal autorisiert sein.

Ab diesem Zeitpunkt ist der Produkt-RfC als Produkt-Change freigegeben - die ID des Produkt-RfCs wird zur ID des Produkt-Changes. Der SBV informiert die Anbieter und Hersteller per E-Mail über die vollständig abgeschlossene Autorisierung.

5.4.7 Produkt-Change umsetzen

Genehmigte Produkt-Changes werden im Rahmen eines TI-Service-Releases umgesetzt und übergreifend durch den SBV koordiniert.

⌦ **GS-A_4415 Aktualisierung des Vorgangsdatenreports**

Anbieter und Hersteller MÜSSEN die interne Dokumentation des Vorgangsdatenreports für genehmigte Produkt-Changes stetig aktuell halten und auf Anfrage an den SBV übermitteln. Die Aktualisierung der Dokumentation erfolgt anlassbezogen, der Worklog ist spätestens zu jedem Statuswechsel des Produkt-Changes zu ergänzen. ⌫

Die für den Vorgangsdatenreport erforderlichen Dokumentationspflichten (siehe Kap. 5.9) können vom Anbieter oder Hersteller auch im Webportal der ZID vorgenommen werden. In diesem Fall kann die Übermittlungspflicht an den SBV - bei entsprechend vorgenommener Dokumentation - im Webportal der ZID ausgeführt werden.

⌦ **GS-A_4418 Übermittlung von Abweichungen vom Produkt-RfC**

Anbieter und Hersteller, die während Change-Umsetzung des genehmigten Produkt-Changes Abweichungen zur Planung im Produkt-RfC feststellen, MÜSSEN diese unverzüglich dem SBV melden. ⌫

Bei einer festgestellten Abweichung des dem aktuellen Produkt-Change zugrunde liegenden Produkt-RfCs wird der SBV entscheiden müssen, welche Konsequenzen die Feststellung bzw. Abweichung auf die weitere Durchführung des Produkt-Changes hat und welche Maßnahmen zu treffen sind. Dazu wird sich der SBV bei Bedarf mit den beteiligten Anbietern und Herstellern (und dem GBV TI) beraten. Die Ergebnisse werden vom SBV in der ZID dokumentiert, ebenso wie eine eventuelle Status-Änderung des Produkt-Changes (bspw. Stornierung). Die Anbieter und Hersteller werden vom SBV hierüber abschließend per E-Mail informiert.

Die Umsetzung des Produkt-Changes setzt sich im Wesentlichen aus den nachfolgenden vier Prozessschritten zusammen. Die einzelnen Prozessschritte entsprechen dabei dem jeweiligen Status, den ein Produkt-Change im Zuge der Umsetzungsphase annehmen kann.

Die formale Änderung des Status eines Produkt-Changes wird vom SBV in der ZID vorgenommen und von ihm entsprechend an die beteiligten Anbieter und Hersteller per E-Mail kommuniziert. Einem Statuswechsel geht dabei eine übereinstimmende Einschätzung des aktuellen Sachstandes der Beteiligten voraus. Eine formale

Autorisierung des SBV zur Änderung eines Status (z. B. durch die beteiligten Anbieter und Hersteller) erfolgt nicht.

1. Produkt-Change planen

⌦ **GS-A_4416 Planung von Produkt-Changes gemäß Produkt-RfC**

Anbieter und Hersteller MÜSSEN die Produktentwicklung, den Produkttest, das Produkt-Deployment sowie den Abschluss des genehmigten Produkt-Changes planen und dabei die gemeinsam mit dem SBV festgelegten Termine und Inhalte des Produkt-RfCs zum Produkt-Change beachten. ⌫

Zur Umsetzung von mehreren Changes an einem Produkt können Anbieter und Hersteller genehmigte Produkt-Changes an einem Produkt zu einem Produkt-Release bündeln. Diese Produkt-Releases können auch lokal autorisierte Produkt-Changes enthalten, die Anbieter und Hersteller eigenständig initiiert haben.

Weiterhin ist während der Bewertung des genehmigten Produkt-RfCs eine Grobplanung für die Umsetzung entwickelt worden. Diese ist durch den Anbieter und Hersteller innerhalb dieser Phase weiter zu konkretisieren, stetig zu aktualisieren und bei Bedarf dem SBV zur Verfügung zu stellen.

⌦ **GS-A_4417 Stetige Aktualisierung von Planungs- und Realisierungsdaten**

Anbieter und Hersteller MÜSSEN die interne Dokumentation der Planungs- und Realisierungsdaten von genehmigten Produkt-Changes stetig aktuell halten und auf Anfrage an den SBV übermitteln. ⌫

2. Produkt-Change entwickeln

⌦ **GS-A_4419 Nutzung der Testumgebung**

Anbieter und Hersteller MÜSSEN die Anforderungen an die Nutzung der Testumgebung sowie die geplante Belegung der Testumgebung für ihre Produkttests mit dem SBV abstimmen.⌫

Die Testumgebung wird hinsichtlich der Nutzung durch die testdurchführende Instanz (siehe Testkonzept) koordiniert. Der SBV stimmt sich mit der testdurchführenden Instanz ab.

⌦ **GS-A_4420 Übermittlung der lokalen Testergebnisse**

Anbieter und Hersteller MÜSSEN - sofern mit dem SBV vereinbart - die finalen Ergebnisse der beim Anbieter oder Hersteller lokal durchgeführten Tests von genehmigten Produkt-Changes an den SBV übermitteln. ⌫

3. Produkt-Change testen

⌦ **GS-A_4421 Zulassung und Abnahme von entwickelten Produkt-Changes**

Anbieter und Hersteller MÜSSEN für ihre entwickelten Produkte die vom SBV vorgegebenen Tests absolvieren und die notwendigen Zulassungen für die Erprobung bzw. den Produktivbetrieb erlangen. ⌫

Der Abschluss des Tests ist erfolgt, wenn der Hersteller/Anbieter das Produkt (Produkt-Release) in den jeweiligen Umgebungen getestet hat und durch die testkoordinierende Instanz des SBV der Einsatz in der Produktivumgebung freigegeben wurde.

4. Produkt-Change einführen

Das Deployment eines Produkt-Changes im Service Release wird durch den SBV zeitlich und verfahrenstechnisch koordiniert. Anbieter und Hersteller müssen das Deployment des Produkt-Changes gemäß den Vorgaben vom SBV durchführen und stetig deren Einhaltung prüfen.

Das Deployment beinhaltet bei

- dezentralen Produkten die Bereitstellung zur Nutzung (inkl. Rollout).
- zentralen Produkten die Inbetriebnahme in die Produktivumgebung.

⌦ **GS-A_4422 Überführung von Produkten durch Anbieter und Hersteller in den Wirkbetrieb**

Anbieter und Hersteller MÜSSEN die von ihnen verantworteten Produkte zu den vereinbarten Test- und Releaseterminen in die Testumgebungen und die Wirkbetriebsumgebung überführen und dabei die Vorgaben der SBV zum übergeordneten Service Release erfüllen.

(Eine Vorgabe des SBV kann sein, dass Änderungen an dezentralen Produkten über den zentralen Konfigurationsdienst bereitgestellt werden müssen.) ⌫

Vom SBV genehmigte Wartungsfenster werden von der Verfügbarkeitsberechnung des betroffenen Produkts ausgenommen. Bei genehmigungspflichtigen Änderungen wird die Koordination der Wartungsfenster im Rahmen der Planung und Umsetzung des Changes durch den SBV vorgenommen.

⌦ **GS-A_4423 Abstimmung von Wartungsfenster für genehmigungspflichtige Änderungen**

Anbieter MÜSSEN Wartungsfenster für genehmigungspflichtige Änderungen mit dem SBV abstimmen. ⌫

⌦ **GS-A_4424 Umsetzung des Fallbackplans**

Anbieter und Hersteller MÜSSEN einen Fallbackplan nach den Vorgaben des SBV erstellen und umsetzen.

(Die Notwendigkeit eines Fallbackplans wird i.d.R. gemeinsam mit dem SBV während der Bewertung des genehmigungspflichtigen Produkt-RfCs festgelegt. Sollten Abweichungen von dem dort definierten Vorgehen notwendig sein, wird der SBV dies an die Anbieter und Hersteller kommunizieren.) ⌫

Produkt-Change-Umsetzung abbrechen

Ein genehmigungspflichtiger Produkt-Change kann ausschließlich durch den SBV abgebrochen werden (bspw. durch im Nachgang festgestellte Fehlannahmen im Produkt RfC).

Der SBV storniert dabei formal den Produkt-Change in der ZID. Die beteiligten Anbieter und Hersteller werden daraufhin durch den SBV in formalisierter Form über den Abbruch eines Produkt-Changes per E-Mail benachrichtigt.

5.4.8 Produkt-Change abschließen

⌦ **GS-A_4425 Übermittlung von Optimierungsmöglichkeiten zur Umsetzung von genehmigten Produkt-Changes an den SBV**

Anbieter und Hersteller MÜSSEN Potenziale für mögliche Optimierungen zukünftiger Durchführungen von Produkt-Changes dem SBV mitteilen. ⌫

⌦ **GS-A_4404 Übermittlung von Produktdaten nach Abschluss von genehmigungspflichtigen Produkt-Changes**

Anbieter und Hersteller MÜSSEN nach dem Abschluss (nach der Produktivsetzung des Produkt-Changes als Produkt) von genehmigten Produkt-Changes den Änderungsdatensatz der Produktdaten an den SBV übermitteln. ⌫

5.5 Service Level Requirements (SLR)

⌦ **GS-A_4405 Service Level Requirements Anbieter und Hersteller für genehmigungspflichtige Produkt-Changes**

Aufbauend auf die in den jeweiligen Verträgen geregelten Servicezeiten MÜSSEN Anbieter und Hersteller für genehmigte Produkt-Changes mindestens folgende Service Level messen:

Tabelle 11: Tab_Betr_TIP_005 CHG - Change Management - SLP "Prozess"

ID	Qualitätsdimension	Beschreibung	Typ	Beispiel
CHG_1	Reaktionszeit Produkt- RfC-Bewertung	Zeitdauer während der Servicezeit, innerhalb der eine Bewertung & Rückmeldung an den SBV auf einen an ihn übersandten Produkt-RfC erfolgen muss	~~Zeit~~ [hhhh:mm:ss]	0002:00:00

Service Level werden in den spezifischen Betriebskonzepten produkttypspezifisch ausgeprägt. ⌫

Die SLR-Berichtsdaten können von Anbietern oder Herstellern im Webportal der ZID generiert und zur Erstellung exportiert werden. Voraussetzung hierzu ist, dass die Rückmeldung der Anbieter und Hersteller auf Bewertungsanfragen des SBV durchgängig im Webportal der ZID erfolgen.

5.6 Informationspflichten

⌦ **GS-A_4406 Aktualität des Change- & Releasekalenders**

Anbieter und Hersteller MÜSSEN den SBV bei Änderungen der Umsetzungsplanung und -durchführung sowie bei Abweichungen im Change-/Releasekalender zu einem Produkt-Change/-Release unverzüglich informieren, damit dieser den Change-/Releasekalender aktualisieren kann. ⌫

5.7 Dokumentation

Die Dokumentation des Change Managements dient insbesondere der Steuerung und der Schaffung der Nachvollziehbarkeit von Produkt-Changes.

Für die ordnungsgemäße Umsetzung der Dokumentation ist ausschließlich der Anbieter und Hersteller verantwortlich.

⌦ **GS-A_4407 Bereitstellung der Dokumentation des Change Managements für genehmigungspflichtige Produkt-Changes**

Anbieter und Hersteller MÜSSEN für jeden genehmigungspflichtigen Produkt-Change eine Change-Dokumentation anlegen und an den SBV übermitteln. Die Change-Dokumentation setzt sich aus dem jeweils zu dem Produkt-Change dazugehörigen Produkt-RfC sowie der nachvollziehbaren Dokumentation der Change-Umsetzung zusammen. ⌫

Die in der Umsetzungsphase des Produkt-Changes seitens der Anbieter und Hersteller bestehende Dokumentationspflicht kann, soweit sie die für den Vorgangsdatenreport erforderlichen Daten betrifft (siehe Kap. 5.9), vom Anbieter bzw. Hersteller im Webportal der ZID vorgenommen werden. In diesem Fall kann die Übermittlungspflicht an den SBV – bei entsprechend vorgenommener Dokumentation – im Webportal der ZID ausgeführt werden.

Die darüber hinausgehende Dokumentation (Projektpläne, Entwicklungsdaten, Testergebnisse, Logfiles etc.) erfolgt weiterhin Anbieter- bzw. Hersteller-intern, die Kommunikation dieser Daten oder Dokumente erfolgt in der Regel außerhalb der ZID.

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

5.8 Eskalationen

⌦ **GS-A_4408 Eskalation für genehmigte Produkt-Changes während der Test- oder Deploymentdurchführung**

Anbieter und Hersteller KÖNNEN bei schwerwiegenden Konflikten während der Test- oder Produktivsetzungsdurchführung von genehmigten Produkt-Changes eine hierarchische Eskalation an den SBV einleiten, wenn

- während der Tests oder der Produktivsetzung Fehler festgestellt werden, deren Ursache der Hersteller oder Anbieter nicht ohne übergreifende Koordination durch den SBV beheben kann,
- die Auswirkung eines Fallbacks nicht lokal auf den Produkt-Change beschränkt ist. ⌫

⌦ **GS-A_4409 Eskalation für genehmigte Produkt-Changes während der Bewertung von Produkt-Changes**

Anbieter und Hersteller KÖNNEN bei schwerwiegenden Konflikten während der Bewertung der notwendigen Anpassungen an Produkten, d.h. während der Bewertung von Produkt-Changes, eine hierarchische Eskalation an den GBV TI

einleiten, wenn zu verbindlichen Termin- und Umsetzungszusagen keine Einigung zwischen SBV und Anbieter oder Hersteller des Produktes erzielt werden kann. ⌫

5.9 Prozessreporting (Vorgangsdaten) CHG

Das Prozessreporting dient voranging der Übermittlung des aktuellen Status zu einem Produkt-Change.

Ist der Status des Produkt-Changes innerhalb der Vorgangsdaten des Prozessreportings auf „abgeschlossen“ gesetzt worden, muss der Produkt-Change damit letztmalig innerhalb des konsolidierten Reports berichtet werden und wird nicht mehr in Folgereports erwähnt.

⌦ **GS-A_4410 Bereitstellung von Vorgangsdaten für genehmigte Produkt - Changes**

Anbieter und Hersteller MÜSSEN für jeden Produkt-Change einen Datensatz für das Vorgangsdatenreporting anlegen.

(Die Anlage muss mit der Aufzeichnung oder dem Erhalt (eigeninitiiert oder durch den SBV übermittelt) für jeden genehmigungspflichtigen Produkt-RfC erfolgen.) ⌫

⌦ **GS-A_4411 Reportinginhalte des Change-Management-Prozessreportings**

Anbieter und Hersteller MÜSSEN Vorgangsdatenreports nach folgenden, vorgegebenen Struktur erstellen:

Tabelle 12: Tab_Betr_TIP_006 CHG - Reportinginhalte des CHG-Prozessreportings

#	Feldname	Inhalt	Typ	Beispiel
1	Teilnehmer ID	ID des A/H bzw. weitere Beteiligte im Betrieb der TI	[String]	
2	Produkt Change ID	ID des Produkt-RfC bzw. nach Autorisierung des Produkt-Changes	[String]	
3	Status	Aktueller Status des RfC/Changes.	[Auswahlfeld], (Beantragt) , (In Bewertung), (Autorisiert), (In Planung), (In Entwicklung), (In Test), (In Deployment), (Implementiert), (Storniert), (Abgebrochen)	Beantragt
4	Produktzielversion	Produkt-Change wird umgesetzt in folgender Produktzielversion des Produkt-Releases	[String]	
5	In Plan	Produkt-Change liegt in der vereinbarten Planung. Beispielhafte Planabweichungsgründe, die nicht	[Auswahl], (Ja), (Nein)	Ja

		für alle TI-Teilnehmer gleichermaßen relevant sind, können sein: Zeit, Ressourcen, Kosten.		
6	Bemerkungen zum Fortschritt	Freitext für Bemerkungen zum Fortschritt Bei den Status „Storniert“ bzw. „Abgebrochen“ sind mindestens folgende Details zu ergänzen: Status: „Storniert“ – Bemerkung: „Storniert wegen Durchführung xyz, wird neu geplant.“ Status: „Abgebrochen“ – Bemerkung: „Abgebrochen, siehe Incident xyz“	[String]	

⌫

⌦ **GS-A_4412 Bereitstellung der Change-Management-Vorgangsdaten mittels Prozessreporting**

Anbieter und Hersteller MÜSSEN die an den SBV zu versendenden Change Management Report im csv-Format übermitteln.

Anbieter und Hersteller MÜSSEN bei den an den SBV zu versendenden Change Management Reports die AFO GS-A_5248 beachten. ⌫

Werden vom Anbieter oder Hersteller die für das Prozessreporting erforderlichen Daten lückenlos im Webportal der ZID gepflegt, kann das Reporting vom Anbieter oder Hersteller aus der ZID heraus erfolgen.

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

6 Configuration Management (CM)

Um den Gesamtbetriebsverantwortlichen der TI und den Serviceverantwortlichen Informationen über die für die Erbringung von TI-Services erforderlichen Konfigurationselemente (Configuration Items, CI) und deren Beziehungen untereinander bereitzustellen, ist ein Configuration Management (CM) zu etablieren. Über das Configuration Management stehen für die Prozesse und Aufgaben über den gesamten Lebenszyklus der Services konsistente Daten und Informationen zur Verfügung.

Die nachfolgende „Abbildung 5: CM - Beziehung TI-Konfigurations-DB & lokal. Konfigurationssys. der A/H“ veranschaulicht den allgemeinen Aufbau der TI-Konfigurationsdatenbank. Der jeweilige Anbieter und Hersteller übermittelt Informationen zu den von ihm verantworteten CI (Produkt) an den SBV. Der SBV konsolidiert die produktspezifischen Konfigurationsdaten und pflegt die TI Konfigurationsdatenbank sowie die CI Relationen (Erstellung und Aktualisierung). Das übergreifende Configuration Management wird durch den GBV TI etabliert. Der GBV TI stellt das Konfigurationsmodell inklusive der Relationen zur Verfügung. Dazu wird eine TI- Konfigurationsdatenbank als betriebsunterstützendes System implementiert. Die Dokumentation der anbieter- bzw. herstellerspezifischen Konfiguration der IT-Architektur der Produkte obliegt dem Anbieter und Hersteller in seinem lokalen Konfigurationssystem. Dabei bilden die Produkte das Bindeglied zwischen der TI-Konfigurationsdatenbank und den lokalen Konfigurationssystemen der Anbieter und Hersteller.

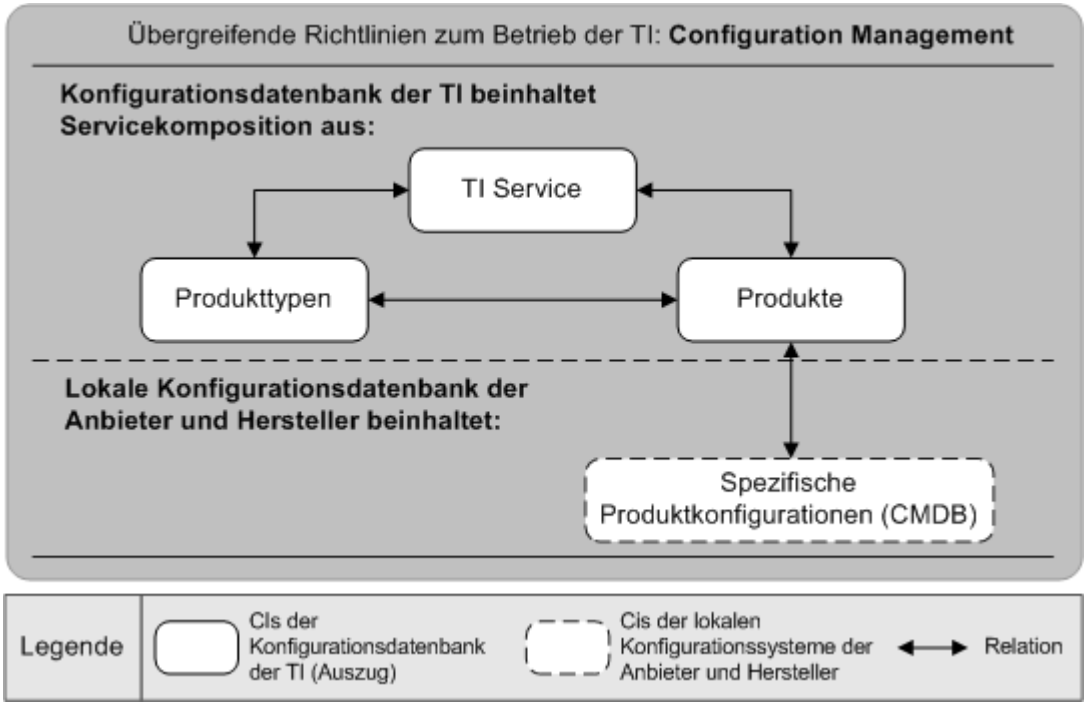


Abbildung 5: CM - Beziehung TI-Konfigurations-DB & lokal. Konfigurationssys. der A/H

Im Fokus der nachfolgenden Regelungen stehen die Mindestanforderungen zum Informationsaustausch zwischen lokalem CM und TI-Konfigurationsdatenbank.

Die nachfolgende Abbildung veranschaulicht die Regelungen des Configuration Managements im anbieter- und herstellerrelevanten Prozessausschnitt mit Fokus auf die Aufgaben der Anbieter und Hersteller und gibt eine Zuordnung der einzelnen Prozessinhalte zu den nachfolgenden Kapiteln.

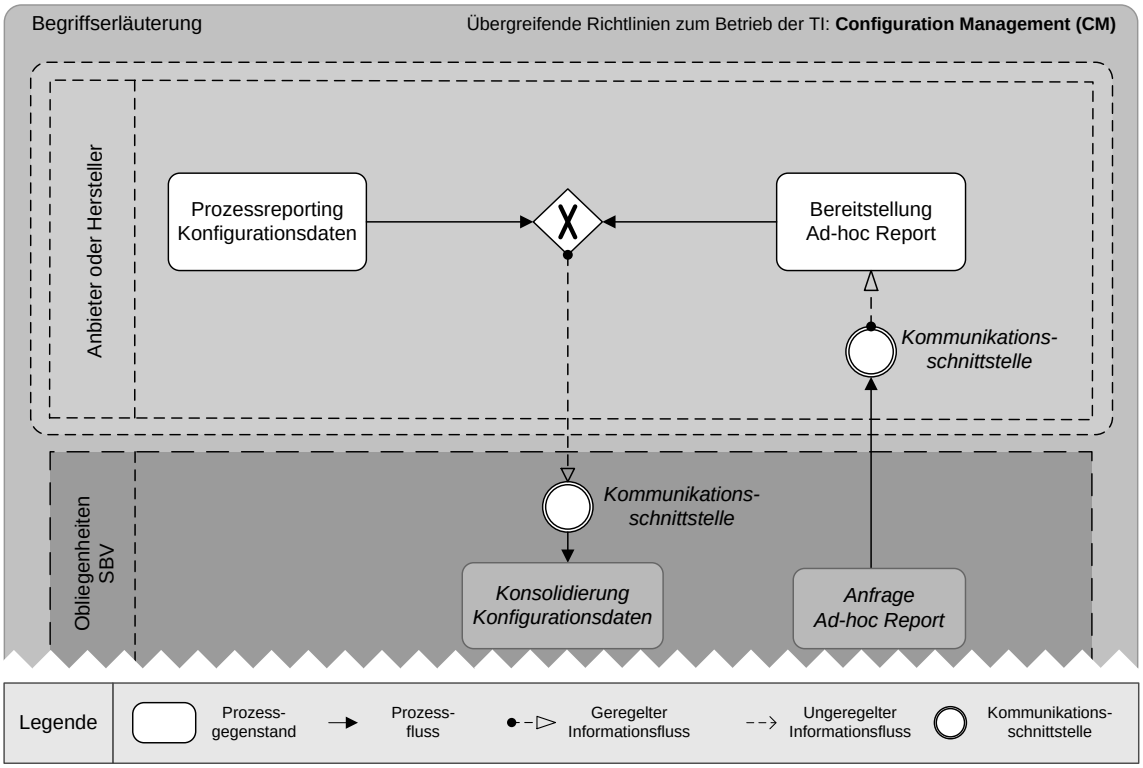


Abbildung 6: CM - Gesamtüberblick "Configuration Management“

6.1 Betrachtungsgegenstand des übergreifenden CM

Fokus der nachfolgenden Configuration-Management-Regelungen im Betrieb ist die Bereitstellung der Konfigurationsdaten durch Anbieter und Hersteller.

6.2 Begriffserläuterungen

6.2.1 Konfigurationselement (Configuration Item, CI)

Ein Konfigurationselement (Configuration Item, CI) ist eine formalisierte Beschreibung einer zum Betrieb erforderlichen Komponente, über deren gesamten Lebenszyklus hinweg. Konfigurationselemente werden durch das Configuration Management strukturiert, dokumentiert und in einer Datenbank zusammengefasst und gepflegt.

Beispiele für CIs sind Services, Produkte, Produkttypen, produktverantwortliche Organisationen und Prozess- und Betriebsdokumentationen.

6.2.2 Konfiguration

Die Konfiguration ist eine Bezeichnung für eine Gruppe von Konfigurationselementen, die miteinander verbunden für die Erbringung eines Service oder eines umfangreichen Teils eines Service eingesetzt werden.

6.2.3 TI-Konfigurationsdatenbank

Die TI-Konfigurationsdatenbank ist ein Werkzeug, welches die Konfigurationsdaten der TI-Services enthält, die der Gesamtbetriebsverantwortliche der TI zur Entscheidungshilfe und zur Steuerung des übergreifenden IT-Service-Managements der TI benötigt.

6.2.4 Konfigurationsdaten

Konfigurationsdaten sind die Attribute zu einem CI. In dieser Richtlinie werden für Anbieter und Hersteller folgende Minimaldaten für CIs festgelegt:

- CI „Produktverantwortliche Organisation“: Allgemeine Informationen zu einem Anbieter und Hersteller, bspw. Anschrift und Ansprechpartner.
- CI „Produkt“: Produktspezifische Konfigurationsdaten der Anbieter und Hersteller, bspw. Produktname, -version, -beschreibung etc.

In spezifischen Betriebskonzepten werden weitere CIs bzw. ergänzende Informationen zu CIs festgelegt.

6.3 Prozessdurchführung zur Bereitstellung von Konfigurationsdaten

6.3.1 Prozessreporting (Konfigurationsdaten) CM

Anbieter und Hersteller führen Änderungen kontrolliert im Rahmen des Change & Release Managements durch. Nach erfolgter Änderung werden Konfigurationsdaten aktualisiert und dem SBV eine konsistente Informationsbasis bereitgestellt.

Die Beziehung zwischen lokalem CM und TI-Konfigurationsdatenbank (vgl. Abbildung 5: CM - Beziehung TI-Konfigurations-DB & lokal. Konfigurationssys. der A/H) werden für die von Anbieter und Herstellern verantworteten CI weiter verdeutlicht: in „Abbildung 7: CM - A/H-relevanter Ausschnitt TI-Konfigurationsdatenbank“ werden die Relationen dieser CI dargestellt und die durch die Anbieter und Hersteller zu liefernden CI Daten tabellarisch aufgezeigt.

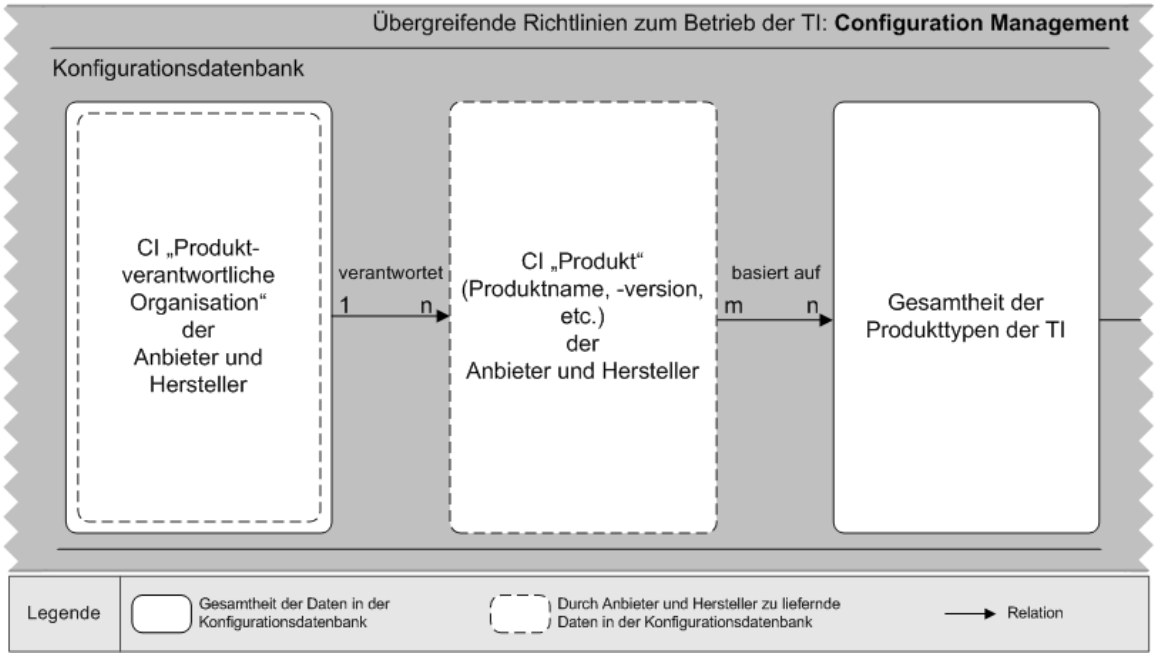


Abbildung 7: CM - A/H-relevanter Ausschnitt TI-Konfigurationsdatenbank

CI „Produktverantwortliche Organisation“

GS-A_4112 Datenbereitstellung für CI „Produktverantwortliche Organisation“

Anbieter und Hersteller MÜSSEN folgende Daten für das CI „Produktverantwortliche Organisation“ an den SBV übermitteln:

Tabelle 13: Tab_Betr_TIP_007 CM - CI „Produktverantwortliche Organisation“

Parameter	Beschreibung	Typ	Beispiel
Teilnehmer ID	ID des A/H bzw. weitere Beteiligte im Betrieb der TI	[String]	
A/H Name	Name des A/H	[String]	gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
Anschrift	Anschrift des A/H (Land, PLZ und Stadt, Straße Hausnummer)	[String]␣ [Integer]␣[String] [String]␣[String]	Deutschland 10117 Berlin Friedrichstraße 136
Name Support MA	Vor- und Nachname des Support/technischen Ansprechpartners	[String]	Max Mustermann
Telefonnummer Support MA	Telefonnummer des Support/technischen Ansprechpartners	[Telefonnummer]	+49 30 40041-999

Parameter	Beschreibung	Typ	Beispiel
E-Mail Adresse Support MA	E-Mail Adresse des Support/technischen Ansprechpartners	[String]	max.mustermann@gematik.de
Name kaufmännischer MA	Vor- und Nachname des kaufmännischen Ansprechpartners	[String]	Ute Mustermann
Telefonnummer kaufmännischer MA	Telefonnummer des kaufmännischen Ansprechpartners	[Telefonnummer]	+49 30 40041-999
E-Mail Adresse kaufmännischer MA	E-Mail-Adresse des kaufmännischen Ansprechpartners	[String]	ute.mustermann@gematik.de

⌫

⌦ **GS-A_4113 Datenänderung für CI „Produktverantwortliche Organisation“**

Anbieter und Hersteller MÜSSEN bei Datenänderung des CIs „Produktverantwortliche Organisation“ einen Report im CSV-Format an den SBV versenden. ⌫

CI „Produkt“

⌦ **GS-A_4114 Datenbereitstellung für CI „Produkt“**

Anbieter und Hersteller MÜSSEN bei jeder Datenänderung für das CI „Produkt“ einen Änderungsdatensatz an den SBV übermitteln. Anbieter und Hersteller MÜSSEN Daten des CIs „Produkt“ für jede neue Produktversion nach folgendem Schema übermitteln:

Tabelle 14: Tab_Betr_TIP_008 CM - „CI Produkt“

Parameter	Beschreibung	Typ	Beispiel
Teilnehmer ID	ID des A/H bzw. weitere Beteiligte im Betrieb der TI	[String]	
Produktname	Bezeichnung des Produktes durch den Anbieter/Hersteller (Handelsname)	[String]	
Produktversion	Versionsnummer des Produktes	[String]	Dezentral 0.0.1:1.2.3 Zentral 0.0.1-255
Produktkürzel	Produktkürzel gemäß gemSpec_OM	[String]	
Aktueller Status	Aktueller Status des Produktes.	[Auswahlfeld], (Geplant), (Produktiv) ,(IM Test), (Stillgelegt)	

Vorheriger Status	Vorheriger Status des Produktes	[String]	
Beschreibung der Änderungen	Beschreibung der durchgeführten Änderungen zu Vorversion und ID(s) der/ des Changes (CHG_ID) Es sind sämtliche Changes mit inhaltlichem Bezug zu der neuen Produktversion – getrennt nach lokalen und übergreifenden Changes - aufzuführen und als solche eindeutig zu kennzeichnen.	[String]	
Weitere versionierte Produktbestandteile	Anbieter/Herstellerspezifische Angaben, z.B. Versionierung der Komponenten (Firmware, Hardware etc.)	[String]	
Produkttyp	Zugrunde liegender Produkttyp	[String]	
Produkttypversion	Zugrunde liegende Produkttypversion	[String]	
Betriebsumgebung	Eingesetzt in Betriebsumgebung	[Auswahlfeld], (RU), (TU), (PU)	

⌫

Im spezifischen Betriebskonzept werden bei Bedarf weitere produkttypspezifische Attribute aufgezeigt und beschrieben.

⌦ **GS-A_4115 Datenänderung für CI „Produkt“**

Anbieter und Hersteller MÜSSEN bei Datenänderung des CIs „Produkt“ einen Report im CSV-Format an den SBV versenden. ⌫

6.3.2 Bereitstellung Ad-hoc Report

⌦ **GS-A_4116 Bereitstellung Ad-hoc Report**

Anbieter und Hersteller MÜSSEN dem SBV auf Anfrage kurzfristig Konfigurationsdaten für Produkte und Produktinstanzen im Rahmen des Ad-hoc Reportings zur Verfügung stellen.

Inhalt und Format wird im Bedarfsfall mit den betroffenen Anbietern und Herstellern individuell abgestimmt.⌫

6.4 Obliegenheiten SBV/GBV TI

Obliegenheiten des SBV:

- Der SBV ist verantwortlich für die Konsolidierung der von Anbietern oder Herstellern erhaltenen Konfigurationsdaten und die Pflege der TI-Konfigurationsdatenbank.
- Der SBV wird im Rahmen des Configuration Managements an Anbieter und Hersteller Mitteilungen bzgl. der Änderungsanforderungen zu Konfigurationsdaten versenden.

Obliegenheiten des GBV TI:

- Der GBV TI veröffentlicht die Listen der Teilnehmer-IDs sowie der zugelassenen Produkte.

7 Knowledge Management (KM)

Durch den Gesamtbetriebsverantwortlichen der TI wird ein Knowledge Management (KM) etabliert, um den support-leistenden Organisationen die TI-Produktinformationen für die Ursachenanalyse und Lösungsfindung von Incidents und Problemen bereitzustellen. Diese Produktinformationen werden in der Wissensdatenbank bereitgestellt. Die Wissensdatenbank soll dabei als erste Anlaufstelle für support-leistende Organisationen dienen.

Im Knowledge Management abgelegte Produktinformationen sollen Anbieter und Hersteller sowie Anwender oder PED's in der TI bei der Klärung im Betrieb bzw. bei der Nutzung auftretender Fragestellungen unterstützen. Anbieter und Hersteller sind verpflichtet, diese Informationen bereitzustellen.

Die nachfolgende Abbildung veranschaulicht die Regelungen des Knowledge Managements im anbieter- und herstellerrelevanten Prozessausschnitt und mit Fokus auf die durch Anbieter und Hersteller zu unterstützenden Betriebsaufgaben in einem Schaubild.

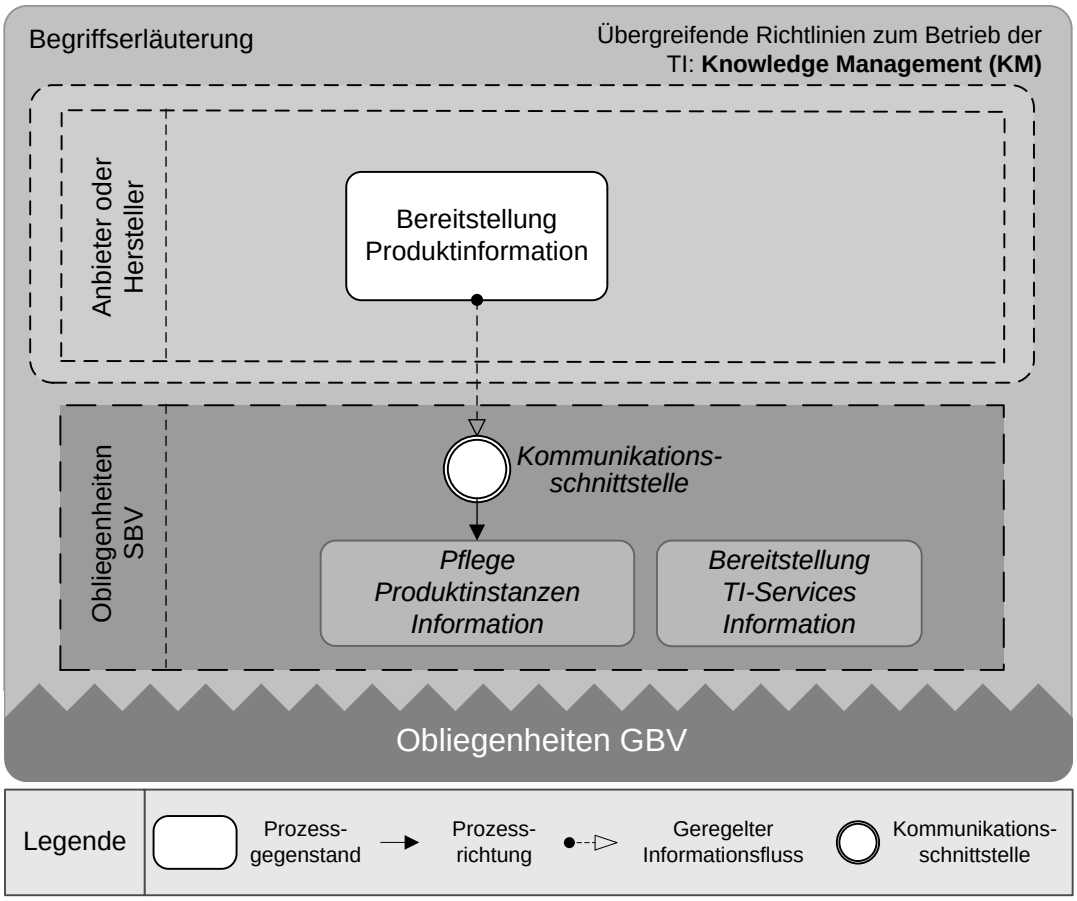


Abbildung 8: KM - Gesamtüberblick "Knowledge Management"

7.1 Betrachtungsgegenstand des KM

Fokus der nachfolgenden Regelungen des Knowledge Managements ist die nicht-normative regelnde Informationsbereitstellung der anbieter- oder herstellerbezogenen Produktinformationen, insbesondere zu Support-Schnittstellen und Ansprechpartnern.

7.2 Begriffserläuterungen

7.2.1 Wissensdatenbank (WDB)

Die Wissensdatenbank der TI wird durch den GBV TI bereitgestellt und unterstützt Anbieter und Hersteller sowie Anwender und PED im Falle einer Störung dabei, mehr Informationen über die möglichen Störungsursachen und möglichen Lösungen der Produkte zu erhalten und den für die Fehlerbehebung Verantwortlichen zu identifizieren und zu kontaktieren.

Die Wissensdatenbank soll in der initialen Ausbaustufe folgende Informationen bereitstellen:

- Erläuterung zu Fehlercodes aus Produkttypspezifikation
- Hinweise auf mögliche Ursachen sowie möglichen Lösungen des Fehlers
- Kontaktinformationen der lösungsverantwortlichen sowie problemlösungs-unterstützenden Anbieter und Hersteller

7.3 Prozessdurchführung Bereitstellung der Produktinformation

7.3.1 Bereitstellung der Produktinformation

⌦ **GS-A_4117 Bereitstellung der Produktinformation**

Anbieter und Hersteller KÖNNEN für Nutzer ihrer Produkte (Anwender oder PEDs sowie Anbieter und Hersteller) Produktinformationen über die möglichen Störungsursachen und Lösungen der Produkte an den SBV übermitteln. ⌫

⌦ **GS-A_4413 Aktualisierung der Produktinformation**

Anbieter und Hersteller MÜSSEN bereitgestellte Informationen zu Produkten gemäß GS-A_4117 stets aktuell halten und bei Änderung den SBV informieren. ⌫

⌦ **GS-A_4118 Bekanntmachung Support-Schnittstelle**

Anbieter und Hersteller MÜSSEN dem SBV einen Link zur Support-Webseite mitteilen, der von Anwendern oder PEDs zur Information bzgl. der Störungsursachen und möglicher Lösungen genutzt werden kann. ⌫

⌦ **GS-A_4119 Benennung der Ansprechpartner**

Anbieter und Hersteller MÜSSEN im Rahmen des Knowledge Managements einen für den SBV oder Anwender bzw. PED zugänglichen Ansprechpartner bekannt machen, mit dem alle evtl. entstehenden Fragen geklärt werden können. ⌫

7.4 Obliegenheiten SBV/GBV TI

Obliegenheiten des SBV:

- Der SBV nimmt die Produktinformationen von Anbietern oder Herstellern entgegen und wertet sie aus. Diese können um weitere Produktinformationen aus eigenen Recherchen, wie Analyse von Spezifikationen und anderer Dokumentationen, ergänzt werden. Die konsolidierten Produktinformationen werden unter Angabe der Quelle in die Wissensdatenbank übernommen.
- Der SBV wird im Rahmen der Auswertung der Produktinformationen die Inhalte, bspw. durch Reviews oder Audits, regelmäßig überprüfen. Dies dient der Fehlersuche und -behebung bzw. kontinuierlichen Verbesserung der Inhalte der Wissensdatenbank.

Obliegenheiten des GBV TI:

- Durch den GBV TI wird ein übergreifendes Knowledge Management etabliert.
- Der GBV TI stellt allen Beteiligten der TI (Anwendern, PEDs, Anbietern, Herstellern sowie nach Bedarf weiteren am ITSM zu Beteiligenden – z. B. Gesellschafter der gematik einschließlich deren Landesorganisationen) eine Wissensdatenbank als Informationsinstrument und Unterstützungswerkzeug im Betrieb zur Verfügung.
- Der GBV TI trägt die redaktionelle Verantwortung für die Wissensdatenbank. Für die produktbezogenen Inhalte zur Störung, Ursache und Lösung sind die Anbieter und Hersteller verantwortlich.

8 Incident Management (INC)

Um zwischen den verschiedenen Anbietern und Herstellern sicherzustellen, dass Servicestörungen bzw. vom erwarteten Betriebsverhalten abweichende Services des TI-Plattform-Service oder eines Anwendungsservice

- gemäß ihrer Auswirkungen eine konsistent gleiche Behandlung erfahren und
- im Rahmen des Supports, der Austausch bzw. die Übergabe von Incidents zwischen den Prozessbeteiligten problemlos und nachvollziehbar gewährleistet wird,

ist durch die Anbieter und Hersteller ein übergreifendes Incident Management (INC) zu etablieren.

Die nachfolgende Abbildung veranschaulicht die Regelungen des Incident Managements im anbieter- und herstellerrelevanten Prozessausschnitt und gibt eine Zuordnung der einzelnen Prozessinhalte zu den nachfolgenden Kapiteln.

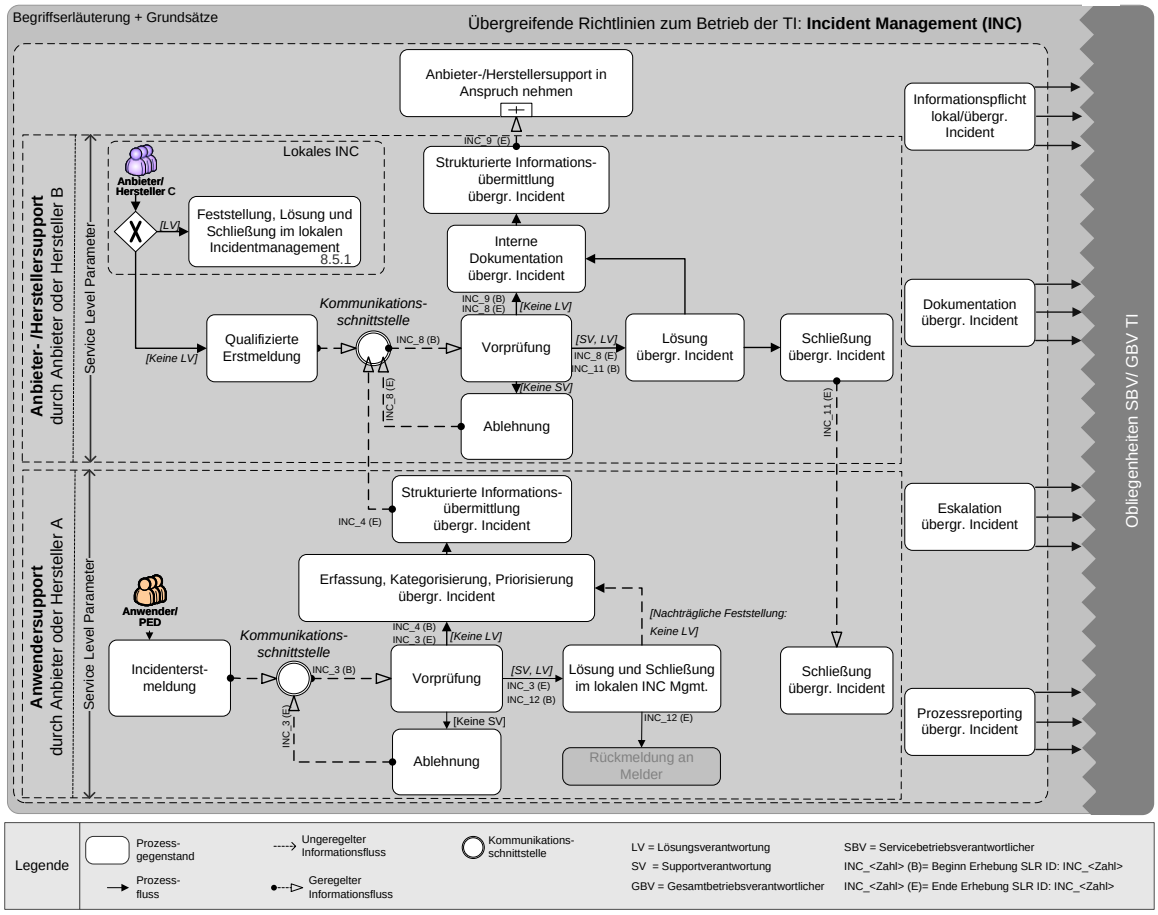


Abbildung 9: INC - Gesamtüberblick "Incident Management"

8.1 Betrachtungsgegenstand des übergreifenden INC

Fokus der nachfolgenden Incident-Management-Regelungen im übergreifenden Betrieb sind anbieter- oder herstellerübergreifende Incidents. Sofern zur Durchführung des übergreifenden INC-Prozesses notwendig, werden Prozessinhalte sowie Regelungen für die Bearbeitung von Incident-Meldungen durch Anwender oder PEDs aufgezeigt.

8.2 Begriffserläuterungen

8.2.1 Lokaler Incident

Bei einem lokalen Incident handelt es sich um eine Servicestörung bzw. um einen vom erwarteten Betriebsverhalten abweichenden Betriebszustand innerhalb des PED (Professioneller Endnutzernahe Dienstleister)/Anwendersupports sowie innerhalb des Anbieter- und Herstellersupports, für dessen Behebung der support- und lösungsverantwortliche Hersteller oder Anbieter keine anderen am Betrieb beteiligten Anbieter und Hersteller benötigt.

Ein lokaler Incident wird dabei innerhalb der lokalen INC-Prozesse des Anbieters bzw. Herstellers verarbeitet und unterliegt nur insofern Regelungen durch diese Richtlinie, wie zur Gewährleistung der Performance, Sicherheit und Stabilität der zentralen und dezentralen Produkte bzw. TI-Services notwendig ist.

Ein lokaler Incident wird durch einen Anwender bzw. PED gemeldet oder durch einen Anbieter und Hersteller im Rahmen seiner lokalen (ggf. systemischen) Störungsüberwachung festgestellt.

8.2.2 Übergreifender Incident

Um einen übergreifenden Incident handelt es sich, wenn zur Bewältigung mehrere der am Betriebsprozess beteiligten Anbieter und Hersteller involviert werden müssen, d. h. eine strukturierte Informationsübermittlung des Incidents an weitere Anbieter und Hersteller eingeleitet werden muss.

Zur Bearbeitung des übergreifenden Incidents steht es den Anbietern bzw. Herstellern frei, die Inhalte des übergreifenden Incidents in den lokalen Incident- Management-Prozess zu überführen. Dabei muss sichergestellt sein, dass an den Schnittstellen zwischen den Prozessbeteiligten weiterhin eine einheitliche Kommunikation, mittels übergreifender Incident-Dokumentation, erfolgt.

Eine Einschätzung, ob mehrere am Betriebsprozess beteiligte Anbieter und Hersteller zur Behebung (Lösung, Verifizierung, Schließen) der Störung bzw. zur Wiederherstellung des erwarteten Betriebsverhaltens der zentralen oder dezentralen Produkte notwendig sind, können - qualifiziert - ausschließlich Anbieter und Hersteller treffen. Übergreifende Incidents können daher ausschließlich durch Anbieter und Hersteller erstellt werden, jedoch nicht durch einen Anwender bzw. einen PED.

8.2.3 Anwendersupport

Der Anwendersupport hat im Gegensatz zum Anbieter-/Herstellersupport eine Kommunikationsschnittstelle in Richtung Anwender bzw. PED sowie zusätzlich eine in Richtung Anbieter und Hersteller.

Incident-Meldungen innerhalb des Anwendersupports können ausschließlich durch Anwender oder PEDs erfolgen.

Der Anwendersupport umfasst primär Regelungen zur ordnungsgemäßen Durchführung des übergreifenden Incident Managements bei Meldung eines Incidents durch einen Anwender bzw. PED.

8.2.4 Anbieter-/Herstellersupport

Der Anbieter-/Herstellersupport hat ausschließlich Kommunikationsschnittstellen in Richtung Anbieter und Hersteller, nicht jedoch gegenüber Anwendern oder PEDs.

Incident-Meldungen innerhalb des Anbieter-/Herstellersupports können ausschließlich von Anbietern oder Herstellern erfolgen (direkt oder im Rahmen einer Weiterleitung aus dem Anwendersupport heraus).

Der Anbieter-/Herstellersupport umfasst primär Regelungen zur ordnungsgemäßen Durchführung des übergreifenden Incident Managements bei Meldung eines Incident durch einen Hersteller oder Anbieter.

Anforderungen an die Dokumentation, die Information und das Reporting sind so ausgeprägt, dass sie mit Hilfe von Standard-Kommunikationswerkzeugen (bspw. E-Mail, Standard-Office-Produkte) durchgeführt werden können.

Der Einsatz bzw. die Anpassung bestehender Verfahren und Werkzeuge (bspw. der Ticketsysteme) kann die Effizienz der Incident-Bearbeitung erhöhen, ist jedoch keine Voraussetzung für das übergreifende INC.

8.2.5 Supportverantwortung

Unter dem Begriff Supportverantwortung wird die originäre Verantwortung zur Supportbereitstellung eines Anbieters bzw. Herstellers gegenüber anderen Anbietern bzw. Herstellern sowie Anwendern bzw. PEDs verstanden, der von ihm eine Dienstleistung bezieht. Die Ausgestaltung der Supportzuordnung und -inhalte ist nicht Bestandteil der Richtlinien und erfolgt in den spezifischen Betriebskonzepten.

8.2.6 Lösungsverantwortung

Ein Hersteller, Anbieter bzw. durch den Anbieter beauftragter Betreiber trägt die Lösungsverantwortung, wenn dessen Produkt für die Störungsursache verantwortlich ist. Er muss die Wiederherstellung des erwarteten Betriebsverhaltens gewährleisten.

8.3 Grundsätze des übergreifenden INC

Die nachfolgenden Grundsätze bilden die übergeordneten Regelungen des übergreifenden Incident Managements für Anbieter und Hersteller.

8.3.1 Zentrale INC-Koordinierung durch den GBV TI

Ausschließlich bei Eskalationen eines schwerwiegenden Incidents mit (produkt-) übergreifender Auswirkung kann der Gesamtbetriebsverantwortliche der TI - zur Gewährleistung der Performance, Sicherheit und Stabilität der zentralen und dezentralen Produkte - eine zentrale Koordinierung der Aktivitäten der anderen Beteiligten übernehmen.

8.3.2 Übergabe der Lösungsverantwortung

Sofern durch einen Supportverantwortlichen keine Herbeiführung einer Lösung möglich ist - bspw. weil der zu bearbeitende Incident durch eine andere Betriebsinstanz verursacht bzw. verantwortet wird - kann er die Lösungsverantwortung an andere Anbieter und Hersteller (deren Dienstleistungen er in Anspruch nimmt) mittels einer strukturierten Informationsübermittlung übergeben. D. h. innerhalb einer Supportkette (im klassischen Sinne wäre dies bspw. der 1st-, 2nd-, 3rd-Level Support) wechselt die Lösungsverantwortung jeweils zwischen den einzelnen supportleistenden Betriebsinstanzen.

8.3.3 Incident-Melder

Der Incident-Melder im übergreifenden ITSM ist immer derjenige, der eine Incident-Meldung beim nächsten aus seiner Sicht zuständigen Service Provider eröffnet. Anhand der Angabe ist es für den Incident-Empfänger vor allem im Falle von Ticketweiterleitungen möglich die strukturierte Kommunikation aufrecht zu erhalten.

Es gibt zwischen dem Incident-Melder und seinem Empfänger immer eine 1:1-Beziehung.

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

8.3.4 Incident-Bearbeiter

Der Incident-Bearbeiter ist immer derjenige, der aktuell an der Incident-Lösung arbeitet. Wird die Lösungsverantwortung von dem Weiterleitungsempfänger angenommen, wechselt der ursprüngliche Incident-Bearbeiter in die Rolle des Incident-Melders und der Weiterleitungsempfänger in die Rolle des (neuen) Incident-Bearbeiters. Lehnt er die Lösungsverantwortung ab, so bleibt der Weiterleitende der Incident-Bearbeiter.

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

8.3.5 Betroffener Anwender

Der betroffene Anwender ist der Nutzer der TI, bei dem ursprünglich eine Störung auftrat und der diese Störung an den für ihn zuständigen Service Provider gemeldet hat. Durch diesen Service Provider erfolgt die Erfassung der Störung als Incident.

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

8.4 Prozessdurchführung Anwendersupport INC

8.4.1 Incident-Erstmeldung im Anwendersupport

An die Incident Meldung eines Anwenders oder PED werden keine Anforderungen gestellt.

8.4.2 Vorprüfung im Anwendersupport

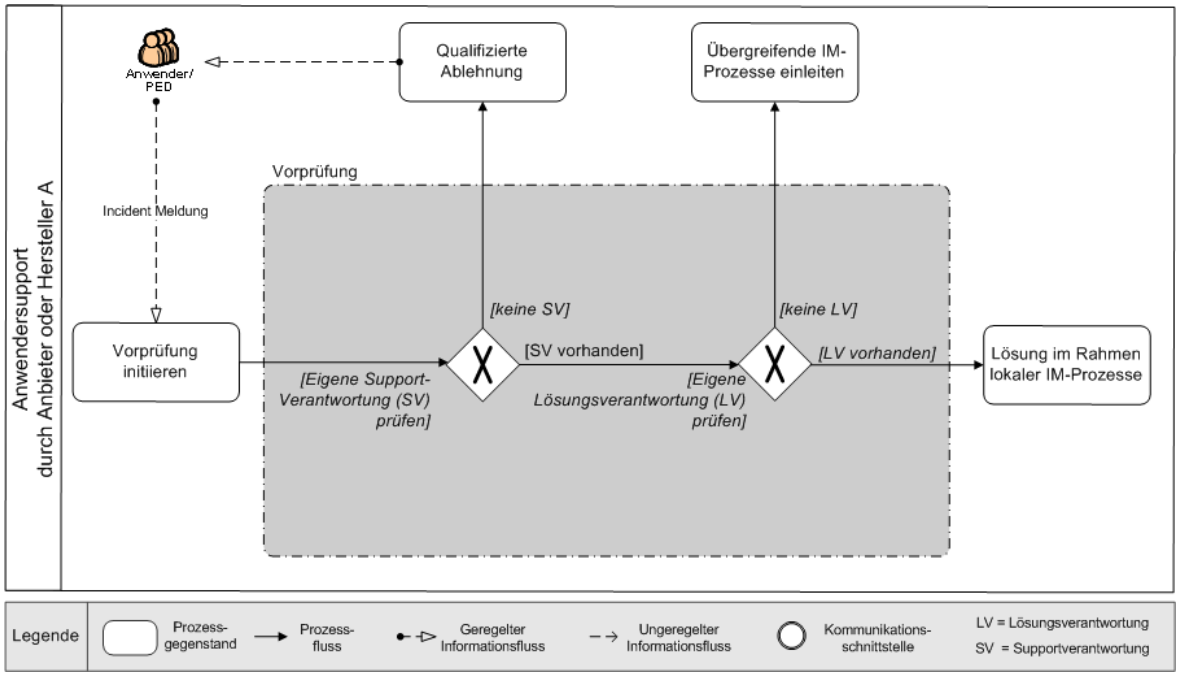


Abbildung 10: INC - Vorprüfung im Anwendersupport

GS-A_3876 Vorprüfung im Anwendersupport

Anbieter und Hersteller MÜSSEN jeden durch einen Anwender oder PED gemeldeten Incident dahingehend prüfen, ob

1. der Incident in der eigenen Supportverantwortung liegt und angenommen werden muss,
2. der Incident nicht in der eigenen Supportverantwortung liegt und qualifiziert abgelehnt werden muss,

3. der Incident in der eigenen Support- und Lösungsverantwortung liegt und es sich somit um einen lokalen Incident zur internen Bearbeitung handelt,
4. der Incident in der eigenen Supportverantwortung liegt und angenommen werden muss, dabei jedoch nicht in der eigenen Lösungsverantwortung liegt und eine Weiterleitung/Zuweisung an verantwortliche, externe Supporteinheiten notwendig ist.

Anbieter und Hersteller MÜSSEN, wenn die Prüfung in Fall eins positiv ist, eine Prüfung auf die Fälle drei und vier durchführen.

Anbieter und Hersteller MÜSSEN in Fall zwei die Ablehnung im Rahmen ihrer lokalen INC-Prozesse vornehmen.

Anbieter und Hersteller MÜSSEN in Fall drei die Bearbeitung des Incidents innerhalb der lokalen INC-Prozesse fortsetzen, da es sich um einen lokalen Incident handelt.

Anbieter und Hersteller MÜSSEN ausschließlich in Fall vier den übergreifenden Incident-Bearbeitungsprozess einleiten und eine Erstqualifizierung (gemäß GS-A_3879, GS-A_3880 , GS-A_3881, GS-A_3882 , GS-A_3883, GS-A_3884) des dann übergreifenden Incidents vornehmen. ⌫

Die Supportverantwortung gegenüber dem initial meldenden Anwender oder PED im Rahmen des Anwendersupports verbleibt grundsätzlich bei dem Hersteller oder Anbieter, welcher den Incident (im Rahmen seines Anwendersupports) entgegengenommen und eröffnet hat.

Bis zur internen Klärung, ob es sich bei dem gemeldeten Incident um einen übergreifenden Incident handelt, hat der derjenige Anbieter und Hersteller, der den Incident annimmt, zugleich die Lösungsverantwortung.

Sobald es sich um einen übergreifenden Incident handelt, muss die erstellte Dokumentation die Anforderungen an eine übergreifende Incident-Dokumentation - gemäß Kapiteln 8.4.5 „Interne Erfassung, Kategorisierung & Priorisierung übergreifender Incidents“ und 8.7 „Dokumentation“ - erfüllen und innerhalb der vorgegebenen Reaktionszeit an den zuständigen Anbieter und Hersteller strukturiert übermittelt werden. Die Supportverantwortung gegenüber dem meldenden Anwender oder PED verbleibt weiterhin bei dem Hersteller oder Anbieter, welcher die Incident-Meldung vom Anwender oder PED entgegen genommen und die initiale Incident-Dokumentation erstellt hat.

8.4.3 Ablehnung im Anwendersupport

An die Ablehnung eines durch einen Anwender oder PED gemeldeten Incidents werden keine Anforderungen gestellt. Es wird empfohlen, eine qualifizierte Ablehnung an den Meldenden zu versenden, der weiterführende Informationen (bspw. die Nennung des korrekten Ansprechpartners) zu entnehmen sind.

8.4.4 Lösung und Schließung im lokalen Incident Management

An das Verfahren zur Lösung und Schließung eines durch einen Anwender oder PED gemeldeten Incidents werden nur insofern Anforderungen gestellt, wie es zur Gewährleistung der Performance, Sicherheit und Stabilität der zentralen und dezentralen

Produkte bzw. TI-Services notwendig ist. Es wird empfohlen, stets eine qualifizierte Rückmeldung an den Meldenden zu versenden, wenn die Störung behoben ist.

Während der Bearbeitung eines lokalen Incidents kann durch den Anbieter und Hersteller festgestellt werden, dass ein TI-Service (bspw. für eine hohe Anzahl an Nutzern) gestört ist. Die Auswirkungsweite und die Dringlichkeit der produktspezifischen Ausprägung der Prioritäten (gemäß Kapitel 8.4.5 „Interne Erfassung, Kategorisierung & Priorisierung übergreifender Incidents“) sind - trotz der Bearbeitung im Rahmen der lokalen Incident-Prozesse - durch den Anbieter und Hersteller zu messen und bei Priorität 1 und 2 an den SBV zu berichten.

⌦ **GS-A_3877 Prüfung auf Erfüllung von Prioritätsanforderungen im lokalen Incident Management im Anwendersupport**

Anbieter und Hersteller MÜSSEN bei der Bearbeitung von lokalen Incidents im Rahmen ihrer lokalen INC-Management-Prozesse prüfen, ob ein Incident mit der Priorität 1 oder 2 klassifiziert werden muss.

(Für lokale Incidents der Priorität 1 und 2 gelten die Informationspflichten gemäß **GS-A_3913**) ⌫

⌦ **GS-A_3878 Nachträgliche strukturierte Informationsübermittlung von übergreifenden Incidents im Anwendersupport**

Anbieter und Hersteller, bei denen sich während der Bearbeitung im lokalen Incident Management und trotz umfangreicher Vorprüfung des durch den Anwender bzw. PED gemeldeten Incidents herausstellt, dass eine Lösung bzw. Behebung des Incidents nicht durch ihn selber möglich ist, MÜSSEN

- unverzüglich den support- und lösungsverantwortlichen Hersteller bzw. Anbieter ermitteln,
- unverzüglich den übergreifenden Incident an den richtigen support- und lösungsverantwortlichen Hersteller bzw. Anbieter strukturiert übermitteln bzw. für die Incident-Bearbeitung durch diesen, eine strukturierte Informationsübermittlung gemäß der Festlegungen für einen übergreifenden Incident durchführen.

(Zur Identifikation des richtigen support- und lösungsverantwortlichen Herstellers bzw. Anbieters werden innerhalb der spezifischen Betriebskonzepte die Leistungs- und Supportmodelle definiert. Zudem werden in der zentralen Wissensdatenbank Kontaktinformationen von Anbietern und Herstellern bereitgestellt.) ⌫

⌦ **GS-A_5086 Bearbeitung und Lösung von lokalen Incidents bei Lösungsverantwortung**

Anbieter und Hersteller, die bei der Vorprüfung feststellen, dass sie für den lokalen Incident support- und lösungsverantwortlich sind, MÜSSEN unverzüglich mit der Incident-Bearbeitung beginnen und gemäß der Priorität des Incidents und - innerhalb der vereinbarten Lösungszeiten - eine Lösung für den lokalen Incident herbeiführen und diesen beheben (lösen, verifizieren und schließen). ⌫

8.4.5 Interne Erfassung, Kategorisierung & Priorisierung übergreifender Incidents

⌦ GS-A_3879 Schriftliche Erfassung von übergreifenden Incidents

Anbieter und Hersteller MÜSSEN Incident-Meldungen von Anwendern bzw. PEDs - sobald erkennbar ist, dass es sich um einen übergreifenden Incident handelt (d. h. zur Bewältigung mehrere der am Betriebsprozess Beteiligten involviert werden müssen) - intern schriftlich erfassen, kategorisieren, priorisieren und innerhalb der vorgegebenen Qualifizierungszeit an den zuständigen Bearbeiter bzw. Anbieter und Hersteller strukturiert übermitteln. ⌫

Die Erfassung und Bearbeitung von übergreifenden Incidents muss auch nach Austausch bzw. der strukturierter Übermittlung dieser zwischen den Prozessbeteiligten problemlos und nachvollziehbar gewährleistetet sein.

Dabei darf der interne anbieter- oder herstellerspezifische Bearbeitungsprozess zur Behebung (Lösung, Verifikation, Schließen) eines Incidents nicht behindert werden. Aus diesem Grund erstellt jeder Anbieter und Hersteller eine interne Dokumentation für den übergreifenden Incident in Form eines Tickets, eines Formulars (bspw. Excel) oder einer E-Mail. Diese wird insbesondere auch für die Pflichten der Anbieter und Hersteller im Rahmen des Reportings benötigt.

Zur Gewährleistung einer übergreifenden Nachvollziehbarkeit muss jeder im übergreifenden Incident Management bearbeitete bzw. an diesen Prozess übergebene Incident - bspw. zur Verweismöglichkeit - mit einer eineindeutigen Referenznummer (Incident-ID) versehen und ordnungsgemäß kategorisiert, priorisiert sowie dokumentiert werden.

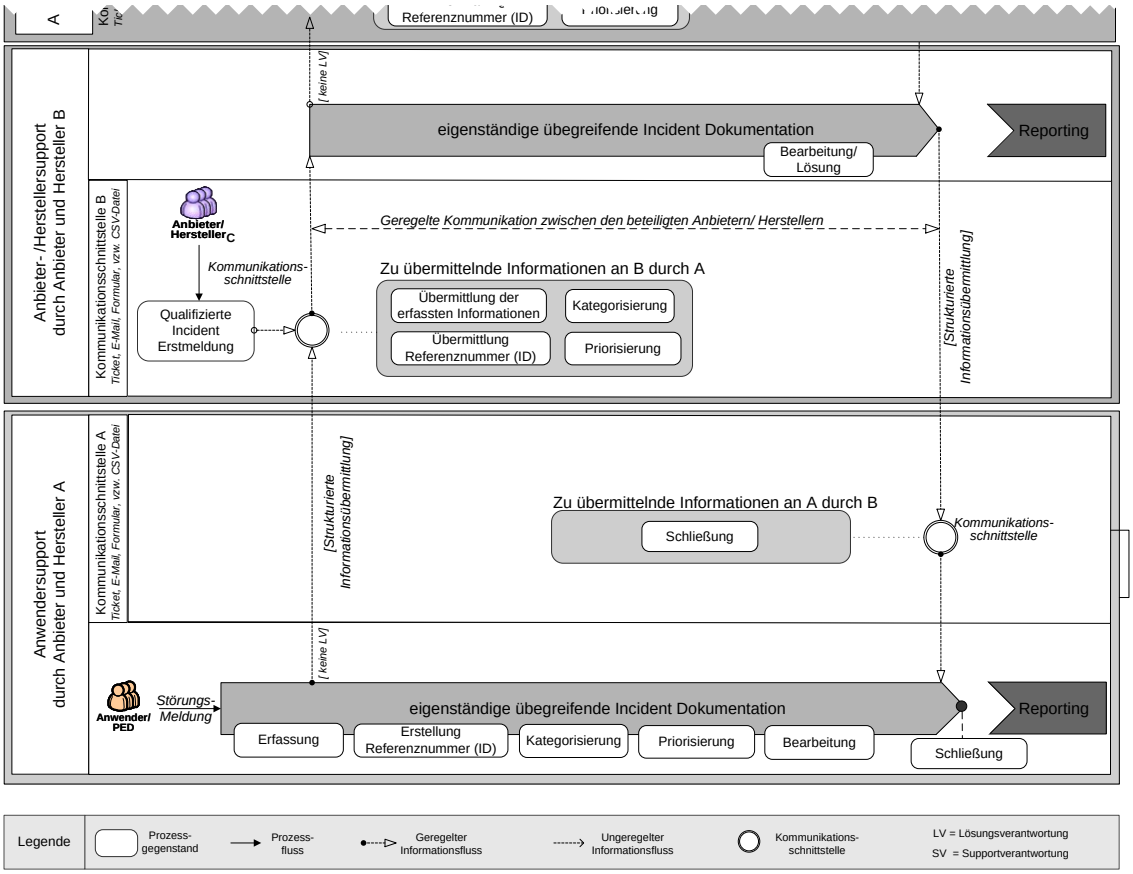


Abbildung 11: INC - Strukturierte Informationsübermittlung im übergreifenden INC

Eineindeutige Referenznummer von übergreifenden Incidents

⌦ GS-A_3880 eineindeutige Referenznummer von übergreifenden Incidents

Anbieter und Hersteller MÜSSEN bei der Erfassung eine eineindeutige Referenznummer für einen **übergreifendes** Incident nach folgendem Schema vergeben:

Die eineindeutige Referenznummer für übergreifende Incident-Dokumentation MUSS über die jeweilige Incident-ID gebildet werden, die sich aus dem aktuellem Jahr (JJJJ), der Teilnehmer-ID (TID) des Herstellers oder des Anbieters bzw. weitere Beteiligte im Betrieb der TI und einer laufenden Incident-Nummer (IN, String [4–5]) in dem Format „JJJJ-TID-IN“ (bspw. „JJJJ-ABCDE-12345“) zusammensetzt. ⌫

⌦ GS-A_3881 Eineindeutigkeit der Incident-ID

Anbieter und Hersteller MÜSSEN bei der Schnittstellenkommunikation mit anderen Anbieter und Herstellern beachten, dass sich die einmalig bei der Ersterfassung des übergreifenden Incidents aufgenommene, eindeutige Referenznummer (in Form der Incident-ID) innerhalb der gesamten Kommunikation nicht ändert, d. h. prozessdurchgängig konstant bleibt. ⌫

Kategorisierung von übergreifenden Incidents

⌦ **GS-A_3883 Kategorisierung von übergreifenden Incidents**

Anbieter und Hersteller MÜSSEN jeden im übergreifenden Incident Management bearbeiteten bzw. an diesen Prozess übergebenen Incident kategorisieren. Zur Kategorisierung MÜSSEN mindestens die im Rahmen der TI vorgegebenen Produkttypen genutzt werden. ⌫

Priorisierung von Incidents

⌦ **GS-A_3884 Priorisierung von Incidents**

Anbieter und Hersteller MÜSSEN jeden im übergreifenden Incident Management bearbeiteten bzw. an diesen Prozess übergebenen Incident gemäß nachfolgendem Schema priorisieren. Dabei ist die Anzahl der möglichen Prioritäten gemäß der Prioritätenmatrix wie folgt festgelegt:

Tabelle 15: Tab_Betr_TIP_009 INC - Prioritätenmatrix

		Auswirkung		
		Hoch	**Mittel**	**Niedrig**
Dringlichkeit	**Hoch**	1	2	3
	Mittel	2	3	4
	Niedrig	3	4	4

- Jeder im übergreifenden Incident Management bearbeitete bzw. an diesen Prozess übergebene Incident MUSS entsprechend einer vierstufigen Einteilung - wobei 1 die höchste und 4 die niedrigste Priorität ist - eingestuft werden.
  - *Priorität 1- Kritisch,*
  - *Priorität 2 - Hoch,*
  - *Priorität 3 - Mittel,*
  - *Priorität 4 - Niedrig.*

Die für einen Incident anzuwendende Priorität wird abgeleitet aus den beiden Faktoren „Auswirkung“ und „Dringlichkeit“. Folgende Festlegungen sind für eine korrekte Anwendung der beiden Faktoren zu beachten:

Tabelle 16: Tab_Betr_TIP_026 INC – Festlegung von Dringlichkeit

Dringlichkeit	Beschreibung
Hoch	• Durch die Störung stehen dem Servicenehmer die ihm bereitgestellten Leistungen (und/oder Funktionen) nicht zur Verfügung, bzw. nur so eingeschränkt, dass die Nutzung des Services für den Servicenehmer im Rahmen seiner Aufgabenerfüllung nicht zumutbar ist.

Dringlichkeit	Beschreibung
	• Die Sicherheit der TI ist nicht mehr gewährleistet • Die Störung der bereitgestellten Leistungen (und/oder Funktionen) lässt sich nicht durch eine Umgehungslösung für den Servicenehmer unmittelbar beseitigen.
Mittel	• Durch die Störung stehen dem Servicenehmer die ihm bereitgestellten Leistungen (und/oder Funktionen) erheblich eingeschränkt zur Verfügung. Die Nutzung des Services für den Servicenehmer ist im Rahmen seiner Aufgabenerfüllung jedoch möglich.
Niedrig	• Durch die Störung stehen dem Servicenehmer die ihm bereitgestellten Leistungen (und/oder Funktionen) ohne nennenswerte Auswirkungen zur Verfügung.

Tabelle 17: Tab_Betr_TIP_027 INC – Festlegung von Auswirkung

Auswirkung	Beschreibung
Hoch	• Eine Mehrheit (>50%) der Servicenehmer ist von der Störung betroffen • Der durch die Störung verursachte Schaden weitet sich schnell aus, falls nicht unmittelbar eine Lösung bereitgestellt werden kann. • Die Störung führt zu Verletzung gesetzlicher Vorschriften, wie z.B. aus Datenschutz und Informationssicherheit • Die Störung hat eine hohe Auswirkung in der öffentlichen Wahrnehmung und führt zu einem erheblichem Imageverlust der TI
Mittel	• Eine beträchtliche Anzahl (>10%) der Servicenehmer ist von der Störung betroffen • Die Störung kann zu Verletzung gesetzlicher Vorschriften führen, wie z.B. aus Datenschutz und Informationssicherheit
Niedrig	• Eine geringe Anzahl (<10%) der Servicenehmer ist von der Störung betroffen • Eine Verletzung gesetzlicher Vorschriften ist nicht gegeben

Für die Aspekte Informationssicherheit und Datenschutz gelten folgende Festlegungen:

- Jeder Incident MUSS auf die Sicherheitsrelevanz geprüft werden und bei Erfüllung der Sicherheitsrelevanz entsprechend gekennzeichnet werden (Feld 7: Sicherheitsrelevanz in „Tabelle 20: Tab_Betr_TIP_014 INC - Mindestinhalte Incident-Dokumentation“). Die Sicherheitsrelevanz ist gegeben, wenn die Vertraulichkeit bzw. Integrität eines schutzbedürftigen Informationsobjektes gefährdet ist.

- Jeder Incident MUSS auf die Datenschutzrelevanz geprüft werden und bei Erfüllung der Datenschutzrelevanz entsprechend gekennzeichnet werden (Feld 8: Datenschutzrelevanz in Tabelle 20: Tab_Betr_TIP_014 INC - Mindestinhalte Incident-Dokumentation). Datenschutzrelevanz ist gegeben, wenn personenbezogene Daten gemäß § 3 Abs. 1 [BDSG] betroffen sind. ⌫

Eine produkttypspezifische Ausprägung der Prioritätenmatrix wird in der Richtlinie nicht durchgeführt. Diese wird während der Implementierung gemeinsam mit den Anbietern und Herstellern festgelegt. Hierdurch wird eine praxisrelevante Einordnung in die Kategorien ermöglicht, unter Berücksichtigung konkreter Erfahrungswerte aus der Erprobungsphase.

8.4.6 strukturierte Informationsübermittlung übergreifender Incidents

⌦ **GS-A_3885 strukturierte Informationsübermittlung von übergreifenden Incidents im Anwendersupport**

Anbieter und Hersteller MÜSSEN einen übergreifenden Incident, nach der internen Erfassung, Priorisierung und Kategorisierung, schriftlich, innerhalb der vorgegebenen Qualifizierungszeit und auf elektronischem Weg an den zuständigen Support- bzw. Lösungsverantwortlichen strukturiert übermitteln. ⌫

Es dürfen ausschließlich vorqualifizierte (inhaltsanforderungskonforme) Incident-Fälle - gemäß Kapitel 8.4.5 „Interne Erfassung, Kategorisierung & Priorisierung übergreifender Incidents“ - übermittelt werden. Die Lösungsverantwortung, also die Verantwortung zur Behebung der Störung bzw. zur Wiederherstellung des erwarteten Betriebsverhaltens, wird mit der strukturierten Informationsübermittlung an den Anbieter und Hersteller übergeben, der den übergreifenden Incident empfängt und annimmt.

⌦ **GS-A_3886 Nutzung der Kommunikationsschnittstelle bei strukturierter Informationsübermittlung von übergreifenden Incidents**

Anbieter und Hersteller MÜSSEN zur strukturierten Informationsübermittlung von übergreifenden Incidents die ZID nutzen. ⌫

Die den übergreifenden Incident empfangenden Anbieter und Hersteller müssen eine erneute interne Erfassung durchführen oder können mit der vorhandenen Incident-Dokumentation die Bearbeitung direkt fortführen.

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

8.4.7 Schließung übergreifender Incidents

⌦ **GS-A_3887 Status eines übergreifenden Incidents während der Bearbeitung**

Anbieter und Hersteller, die für einen übergreifenden Incident lösungsverantwortlich sind, MÜSSEN den Incident als „in Bearbeitung“ markieren bis die Incident-Lösung erfolgt ist.

Anbieter und Hersteller, die für einen übergreifenden Incident nicht lösungsverantwortlich jedoch supportverantwortlich sind, MÜSSEN den Incident als "weitergeleitet" markieren bis die strukturierte Informationsübermittlung zur Schließung eintrifft. ⌫

⌦ **GS-A_3888 Verifikation vor Schließung eines übergreifenden Incidents**

Anbieter und Hersteller MÜSSEN vor der Schließung einer übergreifenden Incident-Dokumentation verifizieren, dass der Incident behoben ist.

Bei negativer Verifikation des Incidents ist kein neuer übergreifender Incident zu eröffnen. Stattdessen ist der bestehende Incident weiterzubearbeiten. Es ist der Status auf „In Bearbeitung“ zu setzen. Es beginnt keine erneute Lösungszeit.

Tickets deren Verifikation länger als sieben Tage andauert, dürfen geschlossen werden.⌫

⌦ **GS-A_3889 Schließung der übergreifenden Incident-Dokumentation, mit abschließender Bearbeitung im Anwendersupport**

Anbieter und Hersteller MÜSSEN nach der Behebung der Störung die übergreifende Incident-Dokumentation abschließend bearbeiten und schließen. Die abschließende Bearbeitung beinhaltet dabei mindestens folgende Inhalte/Schritte:

- Das Feld „Status“ MUSS auf geschlossen gesetzt werden.
- Das Feld „Kategorie verursachendes Produkt“ MUSS dem festgestellten, die Störung verursachenden, Produkttyp entsprechen.
- Das Feld „Kategorie betroffenes Produkt“ MUSS dem hauptsächlich betroffenen Produkttyp entsprechen.
- In das Feld „Incident Worklog“ MUSS die Schließung des Incidents als letzter Eintrag enthalten sein.
- Das Feld „Incident Lösung“ MUSS mindestens mit der eineindeutigen Beschreibung der Lösung und Ursache befüllt sein.
- Das Feld „Zeit Ende“ MUSS gefüllt sein. ⌫

⌦ **GS-A_3890 Information bei Schließung der übergreifenden Incident-Dokumentation im Anwendersupport**

Anbieter und Hersteller MÜSSEN an den Meldenden des übergreifenden Incidents eine Information über die Behebung des Incidents zusenden, damit dieser die Möglichkeit hat, seine - bis zur Lösung - „als weitergeleitet“ markierte Incident-Dokumentation ebenfalls zu schließen. Die strukturierte Information muss dabei mindestens die Inhalte haben, die in GS-A_3882 der „Schließung“ zugeordnet sind. ⌫

Weitere ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

8.4.8 Service Level Requirements (SLR)

⌦ **GS-A_3891 Service Requirements im Anwendersupport**

Aufbauend auf die in den jeweiligen Verträgen geregelten Servicezeiten MÜSSEN Anbieter und Hersteller im Anwendersupport mindestens folgende Service Level messen und berichten:

Tabelle 18: Tab_Betr_TIP_011 INC - SLR Anwendersupport "Prozess"

ID	Qualitäts-dimension	Beschreibung	Typ	Beispiel
INC_3	Reaktionszeit Anwendersupport	Zeitdauer während der (eingeschränkten) Servicezeit vom Eingang der Meldung bis zur Beendigung der Vorprüfung Die Messung beginnt mit dem Eintreffen (Eingang der Mail bzw. Entgegennahme am Telefon) der Meldung	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss]	
INC_4	Qualifikationszeit Anwendersupport	Zeitdauer während der (eingeschränkten) Servicezeit von Beendigung der Vorprüfung bis Übermittlung der strukturierten Information an den zuständigen Bearbeiter Die Messung beginnt mit der Übernahme der Lösungsverant-wortung (Vornahme eines entsprechenden organisatori-schen/fachlichen Eintrags im Worklog)	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss]	
INC_5	Meldezeit Bearbeitungsstatus Anwendersupport	Zeitdauer während der (eingeschränkten) Servicezeit, in der eine Erstinformation, der aktuelle Status und der Folgestatus eines übergreifenden Incidents an den SBV versendet werden müssen.	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss]	
INC_12	Lösungsdauer lokaler Incident	Zeitdauer während der (eingeschränkten) Servicezeit von Beendigung der Vorprüfung bis zur Übermittlung der Lösung an den Melder Die Messung beginnt mit der An-nahme der Lösungsverantwortung und endet mit der Übermittlung des Incidents mit dem Status „Gelöst" an den Melder Für jeweils die Priorität.	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss],	

Service Level werden in den spezifischen Betriebskonzepten produkttypspezifisch ausgeprägt. ⌫

8.5 Prozessdurchführung Anbieter-/Herstellersupport INC

8.5.1 Feststellung, Lösung und Schließung im lokalen INC

Die Ausgestaltung der Prozesse zur Bearbeitung und Lösung lokaler Incidents obliegt grundsätzlich dem Anbieter bzw. Hersteller. Der Umgang mit lokalen Störungen, die durch das interne Monitoring eines Anbieters bzw. Herstellers erkannt werden, wird durch die Produktverfügbarkeit dimensioniert. Folgende Anforderungen sind dabei zu beachten.

⌦ **GS-A_3892 Prüfung auf Erfüllung von Prioritätsanforderungen im lokalen Incident Management im Anbieter-/Herstellersupport**

Anbieter und Hersteller MÜSSEN, wenn die Anforderungen an die Priorität 1 oder 2 von lokalen Incidents erfüllt sind, innerhalb der vorgegebenen Service Level Requirements (vgl. GS-A_3891) eine Statusinformation an den SBV versenden. Darüber hinaus ist dann grundsätzlich bei jedem Statuswechsel von lokalen Incidents der Priorität 1 und 2 eine Statusinformation zu übermitteln.⌫

⌦ **GS-A_3893 nachträgliche strukturierte Informationsübermittlung von lokalen Incidents im Anbieter-/Herstellersupport**

Anbieter und Hersteller, bei denen sich während der Bearbeitung im lokalen Incident Management und trotz umfangreicher Vorprüfung des Incidents herausstellt, dass eine Lösung bzw. Behebung des Incidents nicht durch ihn selber möglich ist, MÜSSEN

- unverzüglich den richtigen support- und lösungsverantwortlichen Hersteller bzw. Anbieter ermitteln,
- unverzüglich den Incident an den richtigen support- und lösungsverantwortlichen Hersteller bzw. Anbieter strukturiert übermitteln bzw. für die Incident-Bearbeitung durch diesen, eine strukturierte Informationsübermittlung gemäß der Festlegungen für einen übergreifenden Incident durchführen.

(Zur Identifikation des richtigen support- und lösungsverantwortlichen Herstellers bzw. Anbieters werden innerhalb der spezifischen Betriebskonzepte die Leistungs- und Supportmodelle definiert. Zudem werden in der zentralen Wissensdatenbank Kontaktinformationen von Anbietern und Herstellern bereitgestellt.) ⌫

8.5.2 qualifizierte Incident-Erstmeldung im Anbieter-/Herstellersupport

Eine qualifizierte Erstmeldung ist eine Incident-Meldung durch einen Anbieter und Hersteller, bei welcher der Anbieter und Hersteller ohne Meldung durch einen Anwender oder PED eine Störung bemerkt (bspw. durch geeignete Systeme) und diese an die support- bzw. lösungsverantwortlichen Anbieter und Hersteller melden möchte.

Durch das „Anbieter/Hersteller–Anbieter/Hersteller“-Verhältnis (B2B-Kommunikation) handelt es sich bei der qualifizierten Meldung immer um einen übergreifenden Incident.

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

GS-A_3894 qualifizierte Meldung einer Störung im Anbieter-/Herstellersupport, ohne Meldung durch Anwender/PED

Anbieter und Hersteller, die eine Störung ohne Meldung durch einen Anwender oder PED feststellen und diese melden möchten, MÜSSEN dies mittels einer qualifizierten Erstmeldung des übergreifenden Incidents an den support- bzw. lösungsverantwortlichen Anbieter und Hersteller durchführen. ⌫

GS-A_3895 Erfassung und Übermittlung eines übergreifenden Incidents im Rahmen der qualifizierten Meldung im Anbieter-/Herstellersupport

Anbieter und Hersteller MÜSSEN im Rahmen der qualifizierten Meldung für die Erfassung und strukturierte Informationsübermittlung des übergreifenden Incidents, die für die übergreifende Incident-Kommunikation bereitgestellte ZID nutzen.

Anbieter und Hersteller MÜSSEN dabei die Erfassung gemäß „GS-A_3879, GS-A_3880 ,GS-A_3881, GS-A_3882 , GS-A_3883, GS-A_3884“ vornehmen. ⌫

GS-A_3896 interne Erfassung des übergreifenden Incidents im Rahmen der qualifizierten Meldung im Anbieter-/Herstellersupport

Anbieter und Hersteller, die einen Incident melden möchten, KÖNNEN (anders als im Anwendersupport, nicht Pflicht) im Rahmen der qualifizierten Erstmeldung eine interne Incident-Dokumentation erzeugen (bspw. um die interne Behebung der Störung, zu einem späteren Zeitpunkt weiter nach zu verfolgen). ⌫

8.5.3 Vorprüfung im Anbieter-/Herstellersupport

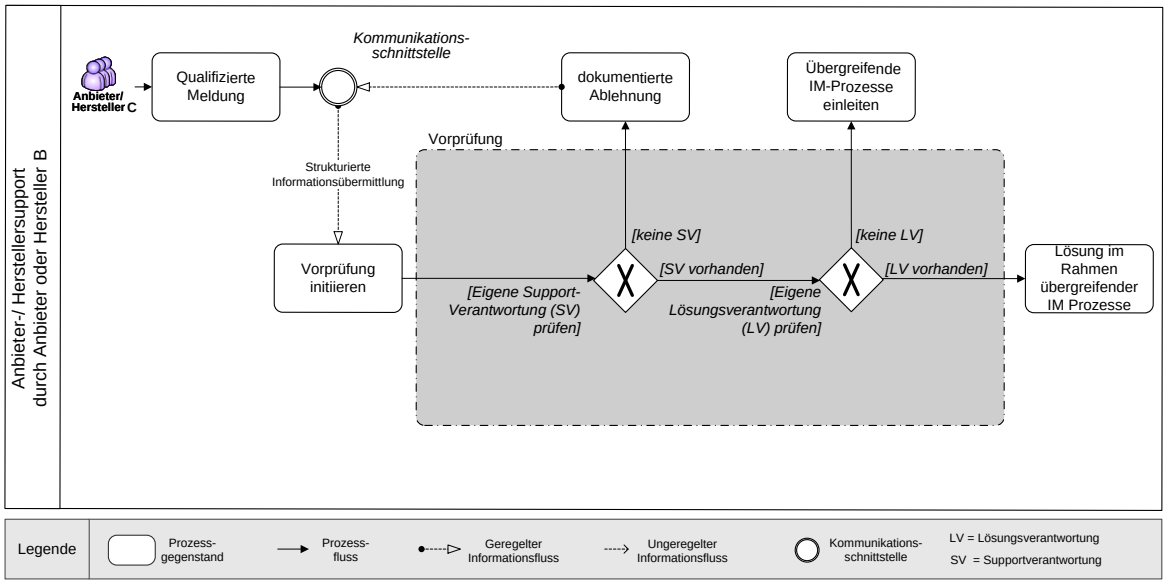


Abbildung 12: INC - Vorprüfung im Anbieter-/Herstellersupport

GS-A_3902 Vorprüfung im Anbieter-/Herstellersupport

Die Meldung erhaltende Anbieter und Hersteller MÜSSEN jeden durch einen anderen Anbieter und Hersteller gemeldeten, übergreifenden Incident dahingehend prüfen, ob

1. der Incident in der eigenen Supportverantwortung liegt und angenommen werden muss,
2. der Incident nicht in der eigenen Supportverantwortung liegt und dokumentiert abgelehnt werden muss,
3. der Incident in der eigenen Support- und Lösungsverantwortung liegt und es sich somit um einen Incident zur internen Bearbeitung handelt,
4. der Incident in der eigenen Supportverantwortung liegt und angenommen werden muss, dabei jedoch nicht in der eigenen Lösungsverantwortung liegt und eine strukturierte Informationsübermittlung an verantwortliche, externe Supporteinheiten notwendig ist.

Anbieter und Hersteller können, nach erfolgter Prüfung, einen übergreifenden Incident - gemäß GS-A_3906, GS-A_3907, GS-A_4120 - akzeptieren oder - gemäß GS-A_3905- dokumentiert ablehnen. ⌫

⌦ **GS-A_3903 Empfangsbestätigung von übergreifenden Incidents**

Der Empfang eines an einen Anbieter und Hersteller übertragenen, übergreifenden Incidents MUSS dem Versender durch den Empfänger schriftlich und in elektronischer Form bestätigt werden, womit die Supportverantwortung als zutreffend bestätigt wird.⌫

⌦ **GS-A_3904 Incident-Annahme**

Anbieter und Hersteller, die bei der Vorprüfung im Anbieter-/Herstellersupport feststellen, dass Sie eine Supportverantwortung haben, MÜSSEN den übergreifenden Incident annehmen.

Mit der Incident-Annahme geht die Annahme der Supportverantwortung gegenüber dem meldenden Anbieter und Hersteller einher. Gleichzeitig geht die Zuständigkeit für die Lösungsverantwortung auf den Anbieter und Hersteller über, der den übergreifenden Incident annimmt. ⌫

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

8.5.4 Ablehnung im Anbieter-/Herstellersupport

⌦ **GS-A_3905 Ablehnung von übergreifenden Incidents im Anbieter-/Herstellersupport**

Anbieter und Hersteller, die einen übergreifenden Incident ablehnen, MÜSSEN dieses mit einer qualifizierten Rückmeldung an den meldenden Anbieter und Hersteller des übergreifenden Incidents durchführen, aus der nachvollziehbar zu entnehmen ist, warum keine Bearbeitung erfolgen kann (bspw. dass die Bearbeitung des übergreifenden Incidents zwischen dem Meldenden und dem Anbieter und Hersteller keine bestehende Vereinbarung umfasst bzw. keine Supportverantwortung besteht).

Eine Ablehnung der Supportverantwortung erfolgt über die Nutzung der ZID.

Folgende Wege sind möglich:

1. Versand einer CSV Datei mit den folgenden Eigenschaften:
   - Der Betreff der E-Mail MUSS den CSV-Dateinamen beinhalten.
   - Die CSV-Datei einschließlich der entsprechend angepassten Felder (z.B. Incident-Bearbeiter, Status, Worklog) MUSS angehängt werden.
   - Die Begründung der Ablehnung MUSS im Worklog gepflegt sein.
   - Eine qualifizierte Rückmeldung ist ein Eintrag in den Worklog, der mit der E-Mail erhaltenen CSV-Datei.
2. Die Ablehnung der Supportverantwortung kann über die Nutzung des Webservice erfolgen:
   - Hier gelten die Vorgaben gemäß Anhang C.
   - Die Begründung der Ablehnung MUSS im Worklog gepflegt sein.
3. Nutzung des Webportals
   - Die Begründung der Ablehnung MUSS im Worklog gepflegt sein.⌫

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

8.5.5 Lösung übergreifender Incidents

⌦ **GS-A_3906 Bearbeitung von übergreifenden Incidents bei Lösungsverantwortung**

Anbieter und Hersteller, die bei der Vorprüfung feststellen, dass sie für den übergreifenden Incident support- und lösungsverantwortlich sind, MÜSSEN gemäß der Priorität (siehe auch GS-A_3884) den internen Incident-Bearbeitungs- und Lösungsprozess auslösen. ⌫

⌦ **GS-A_3907 Lösung von übergreifenden Incidents**

Der lösungsverantwortliche Anbieter und Hersteller MUSS nach erfolgter Annahme des übergreifenden Incidents unverzüglich mit der Incident-Bearbeitung beginnen und - innerhalb der vereinbarten Lösungszeiten - eine Lösung für den Incident herbeiführen und diesen beheben.

Der lösungsverantwortliche Anbieter und Hersteller MUSS bei der Incident-Bearbeitung konstant alle lösungsrelevanten Felder der übergreifenden Incident-Dokumentation weiterpflegen bzw. befüllen.

Kann eine Sofortlösung erfolgen, ist dies im Incident-Worklog so zu dokumentieren, dass nachvollziehbar ist, warum der Incident unmittelbar auf den Status „gelöst“ gesetzt wurde.⌫

⌦ **GS-A_4120 nachträgliche strukturierte Informationsübermittlung von übergreifenden Incidents im Anbieter-/Herstellersupport**

Anbieter und Hersteller, bei denen sich während der Bearbeitung des übergreifenden Incidents und trotz umfangreicher Vorprüfung des Incidents herausstellt, dass eine Lösung bzw. Behebung des Incidents nicht durch ihn selber möglich ist, MÜSSEN

- unverzüglich den richtigen support- und lösungsverantwortlichen Hersteller bzw. Anbieter ermitteln,
- unverzüglich den Incident an den richtigen support- und lösungsverantwortlichen Hersteller bzw. Anbieter strukturiert übermitteln bzw. für die Incident Bearbeitung durch diesen, eine strukturierte Informationsübermittlung gemäß der Festlegungen für einen übergreifenden Incident durchführen.

(Zur Identifikation des richtigen support- und lösungsverantwortlichen Herstellers bzw. Anbieters werden innerhalb der spezifischen Betriebskonzepte die Leistungs- und Supportmodelle definiert. Zudem werden in der zentralen Wissensdatenbank Kontaktinformationen von Anbietern und Herstellern bereitgestellt.) ⌫

8.5.6 Schließung übergreifender Incidents

⌦ **GS-A_3908 Schließung übergreifender Incident, mit abschließender Bearbeitung im Anbieter-/Herstellersupport**

Anbieter und Hersteller MÜSSEN die Schließung eines übergreifenden Incidents, mit abschließender Bearbeitung im Anbieter-/Herstellersupport analog zu GS-A_3887, GS-A_3888, GS-A_3889 im Anwendersupport durchführen.

Anbieter und Hersteller MÜSSEN bei Schließung eines übergreifenden Incidents, mit abschließender Bearbeitung im Anbieter-/Herstellersupport analog zu GS-A_3890 im Anwendersupport an den Meldenden des übergreifenden Incidents eine Information versenden. ⌫

⌦ **GS-A_5250 Lösungsverifikation vor Schließung**

Anbieter und Hersteller MÜSSEN vor der Schließung eines übergreifenden Incidents die Bestätigung des Incident-Melders über die Behebung der Störung einholen und den Incidentstatus auf „gelöst“ setzen. Die Lösungsverantwortung bleibt bis zur Schließung des Tickets die ganze Zeit beim Lösungsverantwortlichen. Mit Ablehnung der Incident-Lösung durch den Melder des übergreifenden Incidents MUSS die Messung der Lösungszeit fortgesetzt und der Status auf „in Bearbeitung“ gesetzt werden.⌫

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

8.5.7 interne Dokumentation übergreifender Incidents

⌦ **GS-A_3909 interne Dokumentation einer übergreifenden Incident-Meldung, bei nicht vorhandener Lösungsverantwortung**

Supportverantwortliche Anbieter und Hersteller, die bei der Vorprüfung eines übergreifenden Incidents feststellen, dass sie nicht lösungsverantwortlich sind, MÜSSEN bevor sie die Incident-Dokumentation an den lösungsverantwortlichen Anbieter und Hersteller übermitteln, eine interne Dokumentation des ihnen gemeldeten Incidents vornehmen.

Anbieter und Hersteller MÜSSEN dabei eine Erfassung, Kategorisierung und Priorisierung des übergreifenden Incidents analog zu GS-A_3879, GS-A_3880 , GS-A_3881,GS-A_3882 , GS-A_3883, GS-A_3884 durchführen.⌫

8.5.8 strukturierte Informationsübermittlung übergreifender Incidents

⌦ **GS-A_3910 strukturierte Informationsübermittlung von übergreifender Incidents im Anbieter/-Herstellersupport**

Anbieter und Hersteller, die eine übergreifende Incident-Dokumentation eröffnen, MÜSSEN diese - innerhalb der vorgegebenen Reaktionszeit - nach Weiterbearbeitung, an den zuständigen Support- bzw. Lösungsverantwortlichen strukturiert übermitteln.⌫

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

8.5.9 Service Level Requirements (SLR)

⌦ **GS-A_3911 Service Level Requirements Anbieter-/Herstellersupport**

Aufbauend auf die in den jeweiligen Verträgen geregelten Servicezeiten MÜSSEN Anbieter und Hersteller innerhalb des Anbieter-/Herstellersupports mindestens folgende Service Level messen und berichten:

Tabelle 19: Tab_Betr_TIP_013 INC - SLR Anbieter-/Herstellersupport „Prozess“

ID	Qualitäts-dimension	Beschreibung	Typ	Bei-spiel
INC_8	Reaktionszeit A/H Support	Zeitdauer während der (eingeschränkten) Servicezeit vom Eingang der Meldung bis zur Beendigung der Vorprüfung. Die Messung beginnt mit dem Eintreffen (Eingang der Mail bzw. Entgegennahme am Telefon) der Meldung. Für die jeweilige Priorität.	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss],	

INC_9	Qualifikationszeit A/H Support	Zeitdauer während der (eingeschränkten) Servicezeit von Beendigung der Vorprüfung bis Übermittlung der strukturierten Information an den zuständigen Bearbeiter. Die Messung beginnt mit der Übernahme der Lösungsverant-wortung (Vornahme eines ent-sprechenden organisatori-schen/fachlichen Eintrags im Worklog). Für die jeweilige Priorität.	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss],	
INC_10	Meldezeit Bearbeitungsstatu s A/H Support	Zeitdauer während der (eingeschränkten) Servicezeit, in der eine Erstinformation, der aktuelle Status und der Folgestatus eines übergreifenden Incidents an den SBV versendet werden müssen. Die Messung des Intervalls beginnt mit dem Eintreffen der Incident-Meldung. Für die jeweilige Priorität.	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss],	
INC_11	Lösungszeit übergreifender Incident	Zeitdauer während der (eingeschränkten) Servicezeit von Beendigung der Vorprüfung bis zur Übermittlung der Lösung an den Melder. Die Messung beginnt mit der An-nahme der Lösungsverantwortung und endet mit der Übermittlung des Incidents mit dem Status „Gelöst“ an den Melder. Für die jeweilige Priorität.	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss],	

Service Level werden in den spezifischen Betriebskonzepten produkttypspezifisch ausgeprägt. ⌫

Die Gesamtlösungszeit für einen übergreifenden Incident wird vorerst durch diese Richtlinie nicht weiter geregelt. Diese ergibt sich aus der Lösungszeit des übergreifenden Incidents beim Lösungsverantwortlichen sowie den Qualifizierungs- und Reaktionszeiten der zuvor am übergreifenden Incident beteiligten Anbietern und Herstellern.

Beim Wechsel der Priorität eines Incidents ergeben sich im Regelfall Änderungen der Lösungszeiten. Diese Änderungen sollen gemäß den nachfolgenden Beschreibungen und Beispielen behandelt werden:

- Bei einem Prioritätenwechsel eines Incidents von 3/4 auf 1/2 beginnt die Lösungszeit von neuem (Anpassung der SLAs). Dabei darf die Restlaufzeit des „alten“ Incidents nicht überschritten werden. Die Incident-ID bleibt gleich.

Beispiel: Ein Incident der Priorität 3 hat den SLA von 10 Stunden. Der Incident läuft bereits 8 Stunden. Der Incident wird jetzt auf Stufe 1 umpriorisiert und hat einen SLA von 3 Stunden. Die SLA-Zeit wird neu gesetzt, endet allerdings

nach 2 Stunden, da die Restlaufzeit des alten Incidents nicht überschritten werden darf.

- Bei einem Prioritätswechsel von 1/2 auf 3/4 gilt als Restlaufzeit die Laufzeit der niedrigeren Priorität abzüglich der bereits abgelaufenen Zeit des "alten" Incidents.

Beispiel: Ein Incident der Priorität 1 hat einen SLA von 3 Stunden. Der Incident läuft bereits 2 Stunden. Der Incident wird jetzt auf Stufe 3 umpriorisiert und hat einen SLA von 10 Stunden. Die SLA-Zeit wird neu gesetzt, endet allerdings nach 8 Stunden, da zwei Stunden der zulässigen Laufzeit in Priorität 3 bereits in der höheren Priorität "verbraucht" wurden.

GS-A_3912 Messung der Gesamtlösungszeit

Anbieter und Hersteller MÜSSEN, sofern durch den SBV ein Optimierungsbedarf der Gesamtlösungszeiten festgestellt wird, die Reaktions- und Qualifizierungszeit (prioritätsabhängig) und gemäß den Vorgaben des SBV umsetzen. ⌫

8.6 Informationspflichten

GS-A_3913 prioritätsabhängige Meldungen im lokalen Incident Management

Anbieter und Hersteller MÜSSEN bei lokalen Incidents, welche den Anforderungen an die Prioritäten 1 oder 2 des übergreifenden Incident Managements entsprechen, innerhalb ihres lokalen Incident Managements eine Meldung an den SBV versenden. Mindestinhalte sind dabei die unter GS-A_3882 genannten Inhalte bei Erfassung eines übergreifenden Incidents. ⌫

GS-A_3914 Statusinformation bei übergreifenden Incidents

Anbieter und Hersteller MÜSSEN bei jeder Statusänderung des Incidents eine Meldung über den aktuellen Status des übergreifenden Incidents an den SBV versenden. Bei übergreifenden Incidents erfolgt die Kommunikation über die ZID. Mindestinhalte sind dabei die unter „GS-A_3882 “ genannten Inhalte bei Erfassung eines übergreifenden Incidents. ⌫

GS-A_3915 Information bei Annahme von übergreifenden Incidents

Anbieter und Hersteller, denen bereits bei Annahme des übergreifenden Incidents ersichtlich ist, dass eine Lösung nicht innerhalb der vereinbarten Lösungszeiten herbeigeführt werden kann, MÜSSEN den SBV hierüber informieren. Bei übergreifenden Incidents erfolgt die Kommunikation über die ZID. ⌫

GS-A_3916 Informationen bei Bearbeitung von übergreifenden Incidents

Der lösungsverantwortliche Anbieter und Hersteller MUSS den SBV informieren, sobald ¾ der vereinbarten Lösungszeit für einen übergreifenden Incident verstrichen sind und nicht sichergestellt werden kann, dass in der verbleibenden Zeit eine Behebung des Incidents gewährleistet ist.

Der lösungsverantwortliche Anbieter und Hersteller MUSS den SBV über alle SLR-Verletzungen, die bei der Bearbeitung bzw. Behebung von übergreifenden

Incidents entstehen, schriftlich (per E-Mail) informieren. Bei übergreifenden Incidents erfolgt die Kommunikation über die ZID. ⌫

⌦ **GS-A_3917 Bereitstellung der Incident-Dokumentation bei Audits**

Anbieter und Hersteller MÜSSEN bei der Durchführung von Audits der betrieblichen Vorgaben dem SBV auf Verlangen die Incident-Dokumentationen bereitstellen. ⌫

8.7 Dokumentation

⌦ **GS-A_3918 Integrität der Dokumentation von übergreifenden Incidents**

Anbieter und Hersteller MÜSSEN Datensätze der Incident-Dokumentationen vor nachträglicher Veränderung mittels Zeitstempeln sichern. ⌫

Inhalte und Dokumentation von übergreifenden Incidents

⌦ **GS-A_3882 Mindestinhalte von übergreifenden Incidents**

Anbieter und Hersteller MÜSSEN jede im übergreifenden Incident Management bearbeitete bzw. an diesen Prozess übergebene Incident-Dokumentation gemäß Tabelle 20: Tab_Betr_TIP_014 INC - Mindestinhalte Incident-Dokumentation erstellen.

Die an die Webservice-Schnittstelle der ZID zu sendenden Daten entsprechen dieser Beschreibung. Die Felder sind im Anhang C beschrieben.

Zeichenerklärung in der Spalte Befüllungszeitpunkt/Befüllungsstatus

X	entspricht	muss befüllt bzw. geändert werden
O	entspricht	kann befüllt bzw. geändert werden
-	entspricht	darf nicht geändert werden

Tabelle 20: Tab_Betr_TIP_014 INC - Mindestinhalte Incident-Dokumentation

#	Feldname	Inhalt	Typ	Beispiel	Befüllungszeitpunkt(e) / Befüllungsstatus						
					Erfassung	Qual. Erstmeldung	Int. Dokumentation	Strukt.Informations.	Lösung	Schließung	Eskalation
1	Incident ID	Incident-ID gemäß GS-A_3880 bei Eröffnung. (Die Vergabe ist ausschließlich durch den Ticketowner (Anbieter und Hersteller der die übergreifende Incident-Dokumentation eröffnet) möglich.)	[String]		X	-	-	-	-	-	-
2	Incident Status	Aktueller Status des Incidents. Bei Dokumentations-erstellung ist dieser immer „In Bearbeitung“.	[Auswahlfeld], (In Bearbeitung), (Weitergeleitet), (Gelöst), (Geschlossen)		X	O	O	O	X	X	-
3	Priorität	Priorität des Incidents gemäß GS-A_3884	[Integer]		X	O	O	O	O	O	-
4	Kategorie betroffenes Produkt	Kategorie des betroffenen Produktes zum Berichtszeitpunkt. (Hauptsächliche Auswirkung der Störung auf Produkttyp gemäß Spalte „ID“ der Tab_gemSpec_Perf_Produkttypen) Ist kein Produkttyp vergeben oder möglicherweise mehrere Produkttypen betroffen, kann auch „SONST“ eingetragen werden. Das betroffene Produkt muss dann im Worklog eindeutig benannt	[String]		X	O	O	O	O	O	-

#	Feldname	Inhalt	Typ	Beispiel	Befüllungszeitpunkt(e) / Befüllungsstatus						
					Erfassung	Qual. Erstmeldung	Int. Dokumentation	Strukt.Informations.	Lösung	Schließung	Eskalation
		werden									
5	Kategorie verursachendes Produkt	Kategorie des verursachenden Produktes zum Berichtszeitpunkt. Bis zur Lösung ist dies die vermutete Ursache. Mit erfolgter Lösung muss dieses die Produkttyp-ID des verursachenden Produkttypen enthalten. (Verursachender Produkttyp der Störung gemäß Spalte „ID“ der Tab_gemSpec_Perf_Produkttypen) Ist kein Produkttyp vergeben oder möglicherweise mehrere Produkttypen betroffen, kann auch „SONST“ eingetragen werden. Das betroffene Produkt muss dann im Worklog eindeutig benannt werden	[String]		X	O	O	O	O	O	O
6	Betroffene Betriebsumgebung	Nennung der Betriebsumgebung, in welcher die Störung aufgetreten ist. Mögliche Einträge: RU (Referenz) TU (Test) PU (Produktiv)	[Auswahlfeld], (RU), (TU), (PU)		X	O	O	O	O	O	-
7	Sicherheitsrelevanz	Kennzeichnung der Sicherheitsrelevanz Mögliche Einträge Ja; Nein	[Auswahlfeld], (Ja), (Nein)		X	O	O	O	O	O	-

#	Feldname	Inhalt	Typ	Beispiel	Befüllungszeitpunkt(e) / Befüllungsstatus						
					Erfassung	Qual. Erstmeldung	Int. Dokumentation	Strukt.Informations.	Lösung	Schließung	Eskalation
8	Datenschutzrelevanz	Einstufung der Datenschutzrelevanz Mögliche Einträge Ja; Nein	[Auswahlfeld], (Ja), (Nein)		X	O	O	O	O	O	-
9	Eskalation	Auswahlfeld, ob sich der Incident in einer Eskalation befindet/befand und an wen eskaliert wurde. (Level 1= SBV, Level 2 = GBV). Nach Entscheidung über die Eskalation durch den GBV bzw. SBV ist das Auswahlfeld wieder auf ‚Nein' zu setzen. Mögliche Einträge Nein; L1; L2	[Auswahlfeld], (Nein), (L1), (L2)		X	O	O	O	O	O	O
10	TI Notfall	Auswahlfeld, ob es sich um einen TI Notfall (gemäß Kap. 10 handelt.) Mögliche Einträge Ja; Nein	[Auswahlfeld], (Ja), (Nein)		X	O	O	O	O	O	-
11	Zeit Erfassung	Datum und Uhrzeit bei Erfassung des Incidents.	[Date]		X	-	-	O	-	-	-
12	Zeit Weiterleitung	Datum und Uhrzeit bei Weiterleitung bzw. Zuweisung des Incidents an den zuständigen Bearbeiter bzw. Hersteller oder Anbieter.	[Date]		-	-	-	X	-	-	-
13	Incident	ID die einen Anbieter und Hersteller	[String]		X	X	-	-	-	-	-

#	Feldname	Inhalt	Typ	Beispiel	Befüllungszeitpunkt(e) / Befüllungsstatus						
					Erfassung	Qual. Erstmeldung	Int. Dokumentation	Strukt.Informations.	Lösung	Schließung	Eskalation
	Melder	eineindeutig identifiziert. (im Herstellersupport) Oder „PED“ bzw. „Anwender“ (im Anwendersupport)									
14	Incident Bearbeiter	ID die einen Anbieter und Hersteller eineindeutig identifiziert (derjenige Anbieter und Hersteller, der die aktuelle Incident Dokumentation erstellt).	[String]					O	X	-	-
15	Incident Beschreibung	Strukturierte Beschreibung der Störung inklusive textuelle Beschreibung der Auswirkungen sowie der Dringlichkeit. Hier kann jederzeit eine nachträgliche Veränderung im Sinne einer Schärfung und Klarstellung erfolgen.	[String]		X	O	O	O	O	-	-
16	Incident Worklog	Qualifizierte Beschreibung aller bislang erfolgten Prüfungen, Aktionen/Eskalationen und Schritte mit Nennung der jeweils und aktuell verantwortlich Handelnden. Fortlaufend ergänzter [String] (neueste Einträge zuerst) <tr><Zeitstempel>#<Tätigkeiten/Freitext></tr>	<tr>[date]#[String]</tr> Maximale Größe des Feldes: 15000 Zeichen	<tr>2015-02-23T01:47:36+01#qualifizierte Beschreibung der Tätigkeit</tr>	X	O	X	O	X	X	X
17	Incident	Zieltermin für den	[Date]	2015-02-	X	O	-	-	-	-	-

#	Feldname	Inhalt	Typ	Beispiel	Befüllungszeitpunkt(e) / Befüllungsstatus						
					Erfassung	Qual. Erstmeldung	Int. Dokumentation	Strukt.Informations.	Lösung	Schließung	Eskalation
	Zieltermin	Abschluss der Störung (in Abhängigkeit von der Auswirkung und Dringlichkeit (Priorität)) sowie für die aktuell in Arbeit befindliche Aktion.		23T01:47:36+01							
18	Zeit Lösung	Datum und Uhrzeit der Lösung des Incidents.	[Date]	2015-02-23T01:47:36+01					X	-	-
19	Incident Lösung	Eineindeutige Beschreibung der Ursache des übergreifenden Incidents (bspw. ID des störungs-verursachenden Produkttypen) und - falls möglich - Benennung des Verursachers des Incidents (bspw. Teilnehmer-ID des Diensteanbieters und dazugehöriger Dienst) sowie der Lösung.	[String]						X	-	-
20	Zeit Ende	Datum und Uhrzeit bei Schließen des Incidents.	[Date]	2015-02-23T01:47:36+01						X	-
21	Meldungstyp	Art der Meldung: „WE“: Weiterleitung im Sinne der funktionalen Eskalation mit Übergang der Lösungsverantwortung „ES“: Eskalation an den SBV „SI“: Statusinformation an den SBV	[Auswahlfeld], (WE), (NI), (AN), (AL), (ES), (SI)		O	O	O	X	O	O	X

#	Feldname	Inhalt	Typ	Beispiel	Befüllungszeitpunkt(e) / Befüllungsstatus						
					Erfassung	Qual. Erstmeldung	Int. Dokumentation	Strukt.Informations.	Lösung	Schließung	Eskalation
		„NI“ - Nachreichen von Informationen zum übergreifenden Incident / Problem „AN“ - Annahmen des übergreifende Incidents gemäß GS-A_3904 „AL“ – Ablehnen des übergreifen Incidents gemäß GS-A_3905									

⌫

8.8 Eskalationen

⌦ **GS-A_3919 Bereitstellung Eskalationsschnittstelle**

Anbieter und Hersteller MÜSSEN eine Kommunikationsschnittstelle (bspw. E-Mail, Telefon) für den Eskalationsfall bereitstellen und den SBV über die Inhalte (bspw. E-Mail-Adresse, Telefonnummer) in Kenntnis setzen.

Anbieter und Hersteller MÜSSEN dem SBV mitteilen, wenn die Inhalte (bspw. E-Mail-Adresse, Telefonnummer) der Kommunikationsschnittstelle für Eskalationen verändert werden. ⌫

⌦ **GS-A_3920 Eskalationseinleitung durch den Anbieter und Hersteller im INC**

Anbieter und Hersteller KÖNNEN bei (produkt-) übergreifenden Incidents eine hierarchische Eskalation an den SBV einleiten, wenn

- keine Einigung über die Support- bzw. Lösungsverantwortung für den übergreifenden Incident mit anderen Herstellern bzw. Anbietern erzielt werden kann (bspw. wenn ein übergreifender Incident undokumentiert oder unausreichend dokumentiert abgelehnt wurde und kein Lösungsverantwortlicher benannt werden kann),
- nach seinem Verständnis zur Bewältigung bei Vorfällen - zur Gewährleistung der Performance, Sicherheit und Stabilität der zentralen und dezentralen Produkte - eine übergeordnete Koordination notwendig ist,

- er keinen support- bzw. lösungsverantwortlichen Hersteller bzw. Anbieter ermitteln kann,
- die Bearbeitung durch einen anderen Anbieter und Hersteller zu lange dauert oder sich als schwierig erweist. ⌫

⌦ **GS-A_3921 Eskalationsinhalte im INC**

Anbieter und Hersteller MÜSSEN bei jeder Eskalationsmeldung an einen SBV im übergreifenden Incident Management folgende Inhalte übermitteln:

- aktuelle Incident-Dokumentation gemäß GS-A_3882
- Das Worklog der Incident-Dokumentation muss um folgende Informationen ergänzt werden:
  - Eskalationsbeschreibung: qualifizierte Beschreibung aller bislang erfolgten Prüfungen, Aktionen/Eskalationen und Schritte, Eskalationsgrund und Dringlichkeit sowie konkret angefragter Unterstützungsbedarf.
  - Eskalationsmelder sowie Kontaktdaten, inklusive Telefonnummer und E-Mail-Adresse für eventuelle Rückfragen.

Die Eskalationsmeldung muss strukturiert über die ZID erfolgen. ⌫

Ergänzende Erläuterungen zum konkreten Vorgehen und der Austausch der festgelegten Kommunikationsschnittstellen (z.B. Kontaktinformationen, E-Mail-Adressen) werden im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

Bei Incidents mit (produkt-)übergreifender Auswirkung kann der Gesamtbetriebsverantwortliche der TI - zur Gewährleistung der Performance, Sicherheit und Stabilität der zentralen und dezentralen Produkte – eine Taskforce zur Behebung der Störung bilden. Diese wird aus mehreren der am Betriebsprozess beteiligten Anbietern bzw. Herstellern zusammengesetzt.

⌦ **GS-A_3922 Mitwirkung bei serviceübergreifenden Taskforces im Eskalationsfall**

Anbieter und Hersteller MÜSSEN, wenn sie zur Teilnahme bei einer Taskforce zur Behebung von übergreifenden Incidents mit der Priorität 1 oder 2 aufgefordert werden, der Taskforce beitreten und die Lösungsfindung unterstützen.

Anbieter und Hersteller MÜSSEN nach der Lösung des übergreifenden Incidents mit der Priorität 1 oder 2 innerhalb einer Taskforce im Anschluss die Erstellung des Abschlussberichtes bzw. die Durchführung des Audits unterstützen. ⌫

8.9 Prozessreporting (Vorgangsdaten) INC

⌦ **GS-A_3923 Zusendung von Reports an den Servicebetriebsverantwortlichen**

Anbieter und Hersteller MÜSSEN, zur Sicherstellung und Optimierung der Prozessqualität, Reports - gemäß den produkttypabhängigen Frequenzen (siehe spezifische Betriebskonzepte) - an den SBV versenden. ⌫

⌦ **GS-A_3924 Bereitstellung von Vorgangsdaten aus dem übergreifenden Incident Management**

Anbieter und Hersteller MÜSSEN die an den SBV zu versendenden Reports im .CSV-Format übermitteln.

Anbieter und Hersteller MÜSSEN bei den an den SBV zu versendenden Reports die AFO GS-A_5248 beachten.⌫

⌦ **GS-A_3925 Reportinhalte von Vorgangsdaten aus dem übergreifenden Incident Management**

Anbieter und Hersteller MÜSSEN Vorgangsdatenreports nach der in „GS-A_3882 " genannten Struktur (die Reihenfolge ist ebenfalls verbindlich) erstellen. Alle Felder der Tabelle 20: Tab_Betr_TIP_014 INC - Mindestinhalte Incident-Dokumentation sind für Reports relevant. ⌫

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

8.10 Obliegenheiten SBV/GBV TI

Obliegenheiten des SBV:

- Der jeweilige SBV nimmt Eskalationsmeldungen entgegen und entscheidet, ob eine Meldung an den GBV TI durchzuführen ist.
- Der jeweilige SBV nimmt übergreifende Incidents mit der Priorität 1 und 2 entgegen und entscheidet, ob eine Meldung an den GBV TI durchzuführen ist.
- Der jeweilige SBV wird sich bei übergreifenden Incidents der Priorität 1 oder 2 selbständig über den jeweils aktuellen Stand der Bearbeitung durch den betreffenden Anbieter und Hersteller informieren, so dass er gegenüber dem GBV TI jederzeit auskunftsfähig ist.

Obliegenheiten der GBV TI:

- Bei Incidents mit (produkt-)übergreifender Auswirkung kann der Gesamtbetriebsverantwortliche der TI - zur Gewährleistung der Performance, Sicherheit und Stabilität der zentralen und dezentralen Produkte - eine zentrale Koordinierung der Aktivitäten der anderen Prozessbeteiligten übernehmen.
- Bei Incidents mit (produkt-)übergreifender Auswirkung kann der Gesamtbetriebsverantwortliche der TI - zur Gewährleistung der Performance, Sicherheit und Stabilität der zentralen und dezentralen Produkte - eine Taskforce zur Behebung der Störung bilden. Diese wird aus mehreren der am Betriebsprozess beteiligten Anbietern bzw. Herstellern durch den GBV TI zusammengesetzt.
- Nach Bildung einer Taskforce und Lösung des Incidents kann der GBV TI ein Abschlussbericht oder ein Audit durchführen.

9 Problem Management (PRO)

Um zwischen den verschiedenen Anbietern bzw. durch den Anbieter beauftragten Betreibern und Herstellern der TI sicherzustellen, dass

- Probleme gemäß ihrer Auswirkungen eine konsistent gleiche Behandlung erfahren,
- im Rahmen der Unterstützung der Problembearbeitung, sofern mehrere Anbieter und Hersteller involviert werden müssen, die Übergabe von Problemen untereinander reibungslos und nachvollziehbar gewährleistet wird,
- eine zuverlässige Lösung von aufgetretenen Problemen anbieterübergreifend gewährleistet ist,

ist durch Anbieter und Hersteller ein übergreifendes Problem Management (PRO) zu etablieren

Die nachfolgende Abbildung veranschaulicht die Regelungen des übergreifenden Problem Managements im anbieter- und herstellerrelevanten Prozessausschnitt und gibt eine Zuordnung der einzelnen Prozessinhalte zu den nachfolgenden Kapiteln.

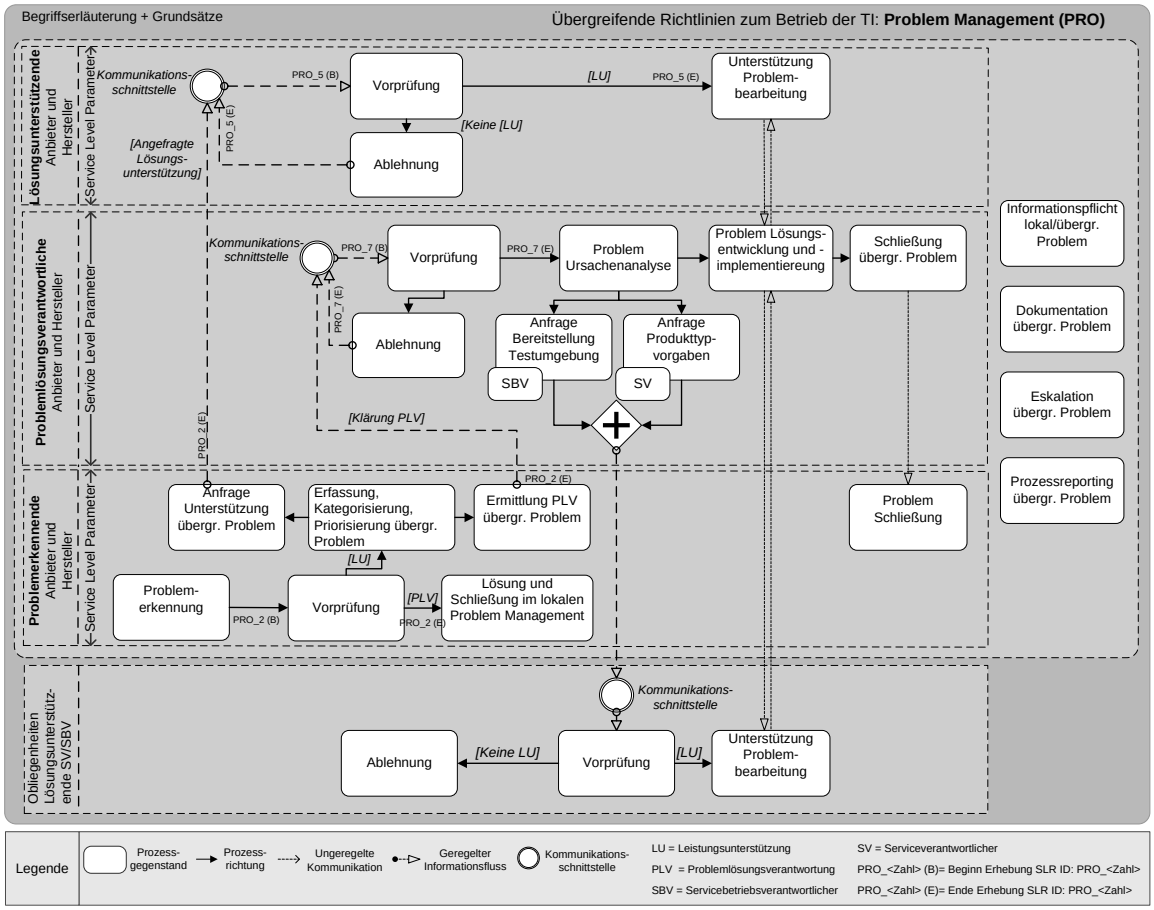


Abbildung 13: PRO - Gesamtüberblick "Problem Management“

9.1 Betrachtungsgegenstand des übergreifenden PRO

Im Fokus der nachfolgenden Problem-Management-Grundsätze im übergreifenden Betrieb stehen anbieter- oder herstellerübergreifende Probleme.

Eine Anfrage zur übergreifenden Lösungsunterstützung und Klärung der Problemlösungsverantwortlichkeit zwischen Anbietern oder Herstellern erfolgt nach dem any-to-any-Prinzip, d. h. jeder Anbieter und Hersteller bietet prinzipiell jedem Anbieter und Hersteller Problemlösungssupport in zumutbaren Umfang an.

Anforderungen an die Dokumentation, die Information und das Reporting sind so ausgeprägt, dass sie mit Hilfe von Standard-Kommunikationswerkzeugen (bspw. E-Mail, Standard-Office-Produkte) durchgeführt werden können.

Der Einsatz bzw. die Anpassung bestehender Verfahren und Werkzeuge (bspw. der Ticketsysteme) kann die Effizienz der Problembearbeitung erhöhen, ist jedoch keine Voraussetzung für das übergreifende PRO.

9.2 Begriffserläuterungen

9.2.1 Problem

Bei einem Problem handelt es sich um die unbekannte Ursache einer eingetretenen oder einer möglichen Störung (Incident). Die Problemlösung vollzieht sich in 2 Phasen:

1. Durchführen einer Ursachenanalyse und
2. Entwickeln und implementieren einer Lösung. Diese wirkt nachhaltig und verhindert das erneute Auftreten von wiederkehrenden Störungen, die durch das Problem bedingt verursacht wurden.

9.2.2 Lokales Problem

Ein lokales Problem liegt vor, wenn zu seiner Ursachenanalyse und Lösung der problemlösungsverantwortliche Hersteller keine anderen am Betrieb beteiligten Anbieter und Hersteller benötigt.

Ein lokales Problem wird dabei innerhalb der lokalen Problem-Management-Prozesse des Anbieters bzw. Herstellers verarbeitet und unterliegt nur insofern Regelungen durch diese Richtlinie, wie sie zur Wahrnehmung der Gesamtbetriebsverantwortung, insbesondere zur Gewährleistung der Performance, Sicherheit und Stabilität der TI-Services und der zentralen und dezentralen Produkte notwendig ist.

9.2.3 Übergreifendes Problem

Ein übergreifendes Problem liegt vor, wenn zu seiner Ursachenanalyse und Lösung mehrere der am Betriebsprozess beteiligten Anbieter und Hersteller involviert werden müssen.

9.2.4 Problemerkennender

Ein Anbieter und Hersteller, der ein Problem identifiziert hat, jedoch für die Problembehebung nicht zuständig ist, ist als Problemerkennender zu bezeichnen. Die gematik in ihrer Rolle als SBV darf ein identifiziertes Problem an den aus ihrer Sicht verantwortlichen Anbieter oder Hersteller als Problemverantwortlichen übergeben. Im Rahmen der übergreifenden Problemursachenanalyse kann ein Problemerkennender die Rolle eines Problemlösungsverantwortlichen übernehmen. In diesem Fall muss er beide Rollen (Problemerkennender und Problemlösungsverantwortlicher) einnehmen.

9.2.5 Problemlösungsverantwortlicher

Ein Problemlösungsverantwortlicher ist ein Anbieter und Hersteller, dessen Produkt für die Störung verantwortlich ist. Der Problemlösungsverantwortliche hat nach erfolgter Ursachenanalyse die Lösungsverantwortung bis zur Problembehebung.

9.2.6 Lösungsunterstützender

Ein vom Anbieter und Hersteller zur Problemlösungsunterstützung angefragter Anbieter und Hersteller ist als lösungsunterstützender Anbieter und Hersteller zu bezeichnen. Der lösungsunterstützende Anbieter und Hersteller hat den Problemlösungsverantwortlichen in seiner Problemlösung zu unterstützen.

9.3 Grundsätze des übergreifenden Problem Managements

An die bestehenden Problemlösungsverfahren der Anbieter und Hersteller werden keine Anforderungen gestellt, eine Regelung der Verfahren erfolgt ausschließlich im Rahmen der übergreifenden Problembearbeitung.

Die nachfolgenden Grundsätze bilden die übergeordneten Regelungen des übergreifenden Problem Managements für Anbieter und Hersteller.

9.3.1 Zentrale PRO Koordinierung durch den SBV TI

Bei Eskalationen eines Problems mit (produkt-)übergreifender Auswirkung kann der jeweils zuständige SBV - zur Gewährleistung der Performance, Sicherheit und Stabilität der zentralen und dezentralen Produkte - eine zentrale Koordinierung der Aktivitäten der anderen Beteiligten übernehmen.

Die Koordination der Problemlösung erfolgt durch die betroffenen Anbieter und Hersteller in Eigenverantwortung. Falls eine wirksame Kooperation zur Problemlösung nicht zustande kommt, hat der jeweils zuständige SBV koordinierend einzugreifen.

Der jeweils zuständige SBV kann innerhalb des übergreifenden Problem Managements für eine Koordination im Rahmen der Nachstellung von Fehlerzuständen in TI-Testumgebungen einbezogen werden.

9.4 Prozessdurchführung problemerkennende Anbieter und Hersteller

9.4.1 Problemerkennung

⌦ **GS-A_3958 Problemerkennung durch Anbieter und Hersteller**

Anbieter und Hersteller MÜSSEN geeignete Maßnahmen implementieren, um proaktiv und reaktiv eine Problemerkennung zu ermöglichen.

(Bei einer Problemerkennung handelt es sich um eine Problemfeststellung im Betrieb der Anbieter und Hersteller.) ⌫

9.4.2 Vorprüfung

Ziel der Vorprüfung ist die Identifizierung von Problemen mit produktübergreifender Ursache oder Auswirkung.

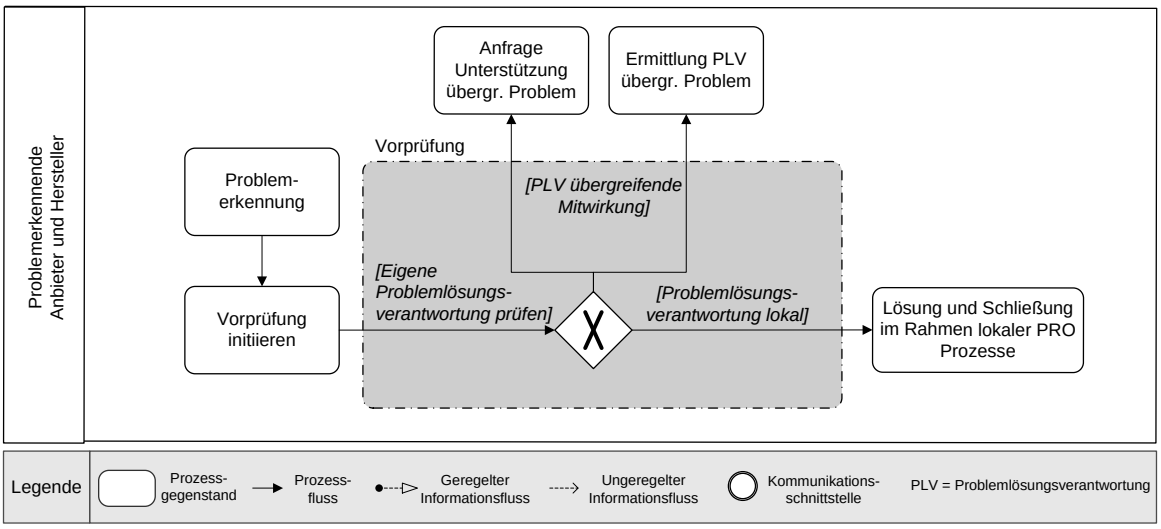


Abbildung 14: PRO - Vorprüfung problemerkennende Anbieter und Hersteller

⌦ GS-A_3959 Vorprüfung als Problemerkennender

Die problemerkennenden Anbieter und Hersteller MÜSSEN jedes identifizierte Problem dahingehend prüfen, ob

1. es sich um ein Problem zur lokalen Bearbeitung handelt,
2. es sich um ein übergreifendes Problem handelt, für welches zur Problemlösung die problemlösungsverantwortlichen und lösungsunterstützenden Anbieter und Hersteller sowie der SV oder der SBV herangezogen werden sollen.

Problemerkennende Anbieter und Hersteller MÜSSEN in Fall eins die Ursachenanalyse und Lösungsentwicklung des Problems eigenverantwortlich innerhalb der lokalen PRO-Prozesse fortsetzen, da es sich um ein lokales Problem handelt.

Problemerkennende Anbieter und Hersteller MÜSSEN in Fall zwei den übergreifenden Problem-Bearbeitungsprozess einleiten und zur Ursachenanalyse und Lösungsentwicklung des Problems die problemlösungsverantwortlichen und lösungsunterstützenden Anbieter und Hersteller sowie den SV oder den SBV anfragen. ⌫

9.4.3 Lösung und Schließung im lokalen Problem Management

Die Ausgestaltung des Prozesses zur Lösung und Schließung lokaler Problem obliegt dem jeweiligen Anbieter bzw. Hersteller. Folgende Anforderungen sind dabei zu berücksichtigen:

⌦ GS-A_3960 Statusinformation an SBV für lokale Problems

Anbieter und Hersteller MÜSSEN den SBV über den Status lokaler Probleme informieren, wenn das lokale Problem die Schwellwerte für die Priorität 1 oder 2 erfüllt. Es gelten die Service Level Requirements für Statusinformation an den SBV gemäß GS-A_3972. ⌫

9.4.4 Erfassung, Kategorisierung & Priorisierung übergreifender Probleme

Das Ziel der Erfassung, Kategorisierung & Priorisierung ist die Festlegung einer einheitlich gestalteten, an den lösungsunterstützenden Anbieter und Hersteller gestellten Anfrage zur Unterstützung des übergreifenden Problems sowie die Nutzung einer einheitlichen Dokumentation für die Kommunikation mit allen beteiligten Anbietern und Herstellern sowie SV oder SBV, insbesondere für das Reporting.

eineindeutige Referenznummer von übergreifenden Problemen

⌦ **GS-A_3961 eineindeutige Referenznummer von übergreifenden Problemen**

Problemerkennende Anbieter und Hersteller MÜSSEN bei der Erfassung eine eineindeutige Referenznummer für ein **übergreifendes** Problemen nach folgendem Schema vergeben:

Die eineindeutige Referenznummer für übergreifende Problemdokumentation MUSS über die jeweilige Problem-ID gebildet werden, die sich aus dem aktuellem Jahr (JJJJ), der Teilnehmer-ID (TID) und einer laufenden Problemnummer (PN, Integer [5]) in dem Format „JJJJ-TID-PN“ (bspw. „JJJJ-K234A-12345“) zusammensetzt. ⌫

⌦ **GS-A_3962 Eineindeutigkeit der Problem ID**

Anbieter und Hersteller MÜSSEN bei der Schnittstellenkommunikation mit anderen Anbieter und Herstellern beachten, dass sich die einmalig bei der Ersterfassung des übergreifenden Problems aufgenommene, eindeutige Referenznummer (in Form der Problem-ID) innerhalb der gesamten Kommunikation nicht ändert, d.h. prozessdurchgängig konstant bleibt. ⌫

Kategorisierung von übergreifenden Problemen

⌦ **GS-A_3963 Kategorisierung von übergreifenden Problemen**

Problemerkennender Anbieter und Hersteller MÜSSEN jedes identifizierte übergreifende Problem kategorisieren. Zur Kategorisierung MÜSSEN mindestens die im Rahmen der TI vorgegebenen Produkttypen genutzt werden. ⌫

Priorisierung von übergreifenden Problemen

⌦ **GS-A_3964 Priorisierung von übergreifenden Problemen**

Anbieter und Hersteller MÜSSEN jedes identifizierte übergreifende Problem gemäß nachfolgendem Schema priorisieren. Dabei ist die Anzahl der möglichen Prioritäten gemäß der in GS-A_3884 aufgeführten Prioritätenmatrix wie folgt festgelegt:

Jedes im übergreifenden Problem Management identifizierte bzw. an diesen Prozess übergebene **Problem** MUSS entsprechend einer vierstufigen Einteilung - wobei 1 die höchste und 4 die niedrigste Priorität ist - eingestuft werden.

- *Priorität 1- Kritisch,*
- *Priorität 2 - Hoch,*
- *Priorität 3 - Mittel,*
- *Priorität 4 - Niedrig.*

(Anhand der Priorisierung müssen die in Service Level Requirements ernannte Qualitätsdimensionen (siehe GS-A_3972) eingehalten werden, wobei die Festlegung von Service Level Requirements für Prioritäten im spezifischen Betriebskonzept stattfindet.) ⌫

Die Anwendung der Prioritätenmatrix wird in der Richtlinie nicht beschrieben und wird während der Implementierung gemeinsam mit den Anbietern und Herstellern festgelegt. Hierdurch wird eine Praxisrelevante Einordnung in die Kategorien ermöglicht, in die auch konkrete Erfahrungswerte aus der Erprobungsphase einfließen können.

9.4.5 Anfrage zur Unterstützung übergreifender Probleme

⌦ **GS-A_3965 Anfrage zur Unterstützung von übergreifenden Problemen bei lösungsunterstützenden Anbietern oder Herstellern**

Problemerkennende Anbieter und Hersteller MÜSSEN in der Anfrage an die lösungsunterstützenden Anbieter und Hersteller eine qualifizierte Beschreibung der benötigten Unterstützungsleistung vornehmen. ⌫

⌦ **GS-A_3966 Zusendung der Anfrage zur Unterstützung von übergreifenden Problemen**

Anbieter und Hersteller MÜSSEN eine übergreifende Problemanfrage zur Unterstützung mit Informationen gemäß GS-A_3961, GS-A_3962 , GS-A_3963, GS-A_3964 und GS-A_4000, schriftlich, innerhalb der vorgegebenen Qualifizierungszeit „Start Problembearbeitung durch Problemerkennenden“ (gemäß GS-A_3972) und auf elektronischem Weg an den lösungsunterstützenden Anbieter und Hersteller senden. ⌫

⌦ **GS-A_3967 Nutzung der Kommunikationsschnittstelle bei Anfrage zur Unterstützung von übergreifenden Problemen**

Anbieter und Hersteller MÜSSEN bei einer Anfrage zur Lösungsunterstützung von übergreifenden Problemen die ZID. ⌫

9.4.6 Ermittlung der Problemlösungsverantwortung bei übergreifenden Problemen

Der problemerkennende Anbieter und Hersteller kann während der Ermittlung der Problemlösungsverantwortung die Wissensdatenbank als Informationsquelle nutzen.

⌦ **GS-A_3968 Anfrage zur Ermittlung der Problemlösungsverantwortung von übergreifenden Problemen**

Problemerkennende Anbieter und Hersteller MÜSSEN in der Anfrage zur Ermittlung der Problemlösungsverantwortung von übergreifenden Problemen an die (aus ihrer Sicht) problemlösungsverantwortlichen Anbieter und Hersteller eine qualifizierte Beschreibung zur Klärung der Problemlösungsverantwortung vornehmen. ⌫

⌦ **GS-A_3969 Zusendung der Anfrage zur Ermittlung der Problemlösungsverantwortung von übergreifenden Problemen**

Anbieter und Hersteller MÜSSEN eine Anfrage zur Ermittlung der Problemlösungsverantwortung mit Informationen gemäß GS-A_3961, GS-A_3962 , GS-A_3963, GS-A_3964, GS-A_4000 und GS-A_5200 schriftlich, innerhalb der vorgegebenen Qualifizierungszeit „Start Problembearbeitung durch Problemerkennenden“ (GS-A_3972) und auf elektronischem Weg an den problemlösungsverantwortlichen Anbieter und Hersteller senden. ⌫

⌦ **GS-A_3970 Nutzung der Kommunikationsschnittstelle bei Anfrage zur Ermittlung der Problemlösungsverantwortung von übergreifenden Problemen**

Anbieter und Hersteller MÜSSEN bei einer Anfrage zur Ermittlung der Problemlösungsverantwortung von übergreifenden Problemen die ZID nutzen.⌫

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

9.4.7 Problemschließung

⌦ **GS-A_3971 Problem nach Verifizierung schließen**

Problemerkennende Anbieter und Hersteller MÜSSEN die Problemschließung der problemlösungsverantwortlichen Anbieter und Hersteller verifizieren sowie bei vollständiger Problemlösungsentwicklung lokal schließen. Problemerkennender Anbieter und Hersteller MÜSSEN bei nicht vollständiger Problemlösungsentwicklung den problemlösungsverantwortlichen Anbieter und Hersteller solange mit der Nacharbeit beauftragen, bis die Problemlösung erfolgt ist und anschließend das Problem lokal schließen. ⌫

Weitere ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

9.4.8 Service Level Requirements (SLR)

⌦ **GS-A_3972 Service Level Requirements problemerkennende Anbieter und Hersteller**

Aufbauend auf die in den jeweiligen Verträgen geregelten Servicezeiten MÜSSEN problemerkennende Anbieter und Hersteller mindestens folgende Service Level messen und berichten:

Tabelle 21: Tab_Betr_TIP_016 PRO - SLR Problemerkennende A/H „Prozess”

ID	Qualitätsdimension	Beschreibung	Typ	Beispiel
PRO_2	Qualifikationszeit Problemerkennende A/H	Zeitdauer während der Servicezeit zwischen der Problemerkennung und der Übermittlung der „Anfrage Unterstützung übergr. Problem“ bzw. der „Ermittlung PLV übergr. Problem“	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss],	

ID	Qualitätsdimension	Beschreibung	Typ	Beispiel
PRO_3	Meldezeit Bearbeitungsstatus Problemerkennende A/H	Zeitdauer während der Servicezeit in der eine Information (qualifizierte Aussage zu Erfassung, Kategorisierung und Priorisierung), der aktuelle Status und der Folgestatus eines übergreifenden Problems an den SBV versendet werden müssen. Statusinfo auch nach Anfrage zur Unterstützung und Ermittlung Problemlösungsverantwortlichkeit. Die Messung des Intervalls beginnt mit dem Eintreffen der Problem-Meldung. Für jede Priorität	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss],	

Service Level werden in den spezifischen Betriebskonzepten produkttypspezifisch definiert. ⌫

9.5 Prozessdurchführung lösungsunterstützende Anbieter und Hersteller

9.5.1 Vorprüfung

Das Ziel der Vorprüfung ist die Feststellung der Lösungsunterstützung der Anbieter und Hersteller im Rahmen des übergreifenden PRO.

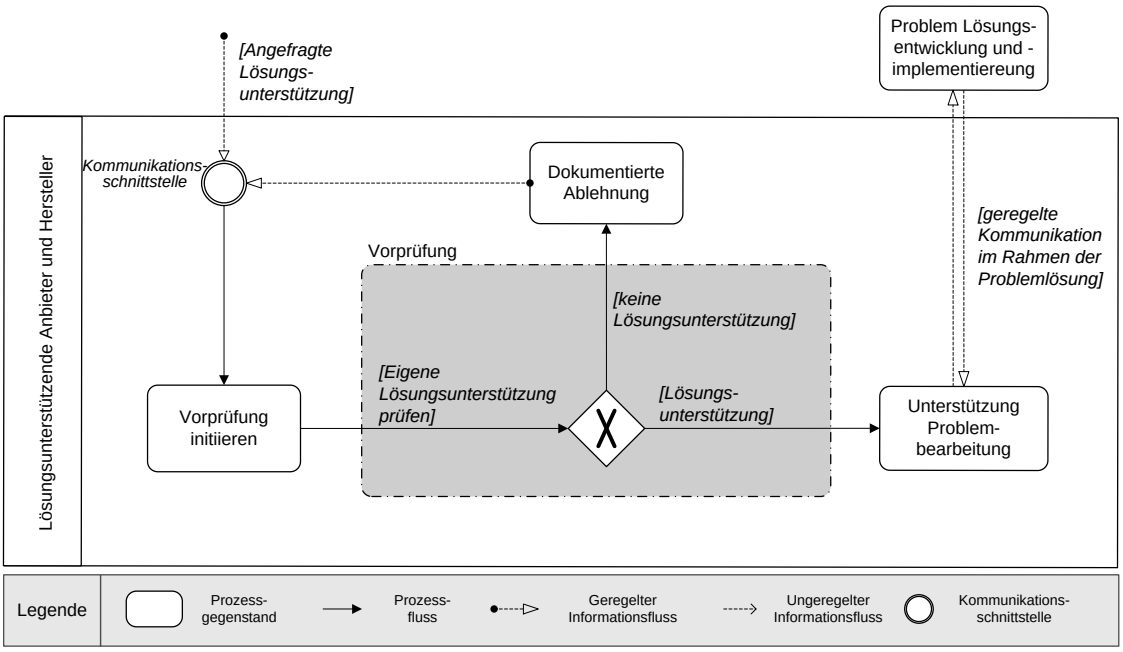


Abbildung 15: PRO - Vorprüfung lösungsunterstützende Anbieter und Hersteller

⌦ **GS-A_3975 Vorprüfung lösungsunterstützende Anbieter und Hersteller**

Anbieter und Hersteller MÜSSEN jedes von dem problemerkennenden oder problemverantwortlichen Anbieter und Hersteller zur Lösungsunterstützung angefragte übergreifende Problem dahingehend prüfen, ob

1. das übergreifende Problem in der eigenen Lösungsunterstützung liegt und angenommen werden muss,
2. das übergreifende Problem nicht in der eigenen Lösungsunterstützung liegt und dokumentiert abgelehnt werden muss. ⌫

9.5.2 Ablehnung

⌦ **GS-A_3976 Ablehnung von übergreifenden Problemen bei lösungsunterstützenden A/H**

Anbieter und Hersteller, die ein übergreifendes Problem ablehnen, MÜSSEN dieses mit einer qualifizierten Rückmeldung an den anfragenden Anbieter und Hersteller des übergreifenden Problems durchführen, aus der nachvollziehbar zu entnehmen ist, warum keine Lösungsunterstützung erfolgen kann. ⌫

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

9.5.3 Unterstützung Problembearbeitung

Bei Unterstützung Problembearbeitung handelt es sich um die unterstützenden Leistungen der Anbieter und Hersteller bei der Analyse bzw. Lösung der übergreifenden Probleme der problemerkennenden oder problemlösungsverantwortliche Anbieter und Hersteller.

⌦ **GS-A_3977 Unterstützung bei übergreifenden Problemen**

Lösungsunterstützende Anbieter und Hersteller, die ein übergreifendes Problem angenommen haben, MÜSSEN bei der Bearbeitung von übergreifenden Problemen im erforderlichen Umfang Unterstützung leisten. ⌫

9.5.4 Service Level Requirements (SLR)

⌦ **GS-A_3978 Service Level Requirements für lösungsunterstützende Anbieter und Hersteller**

Aufbauend auf die in den jeweiligen Verträgen geregelten Servicezeiten MÜSSEN lösungsunterstützende Anbieter und Hersteller mindestens folgende Service Level messen und berichten:

Tabelle 22: Tab_Betr_TIP_018 PRO - SLR Lösungsunterstützende A/H „Prozess"

ID	Qualitätsdimension	Beschreibung	Typ	Beispiel
PRO_5	Qualifikationszeit	Zeitdauer während der	1␣[hhhh:mm:ss],	

ID	Qualitätsdimension	Beschreibung	Typ	Beispiel
	Lösungsunterstützende A/H	Servicezeit zwischen Eingang der Anfrage zur Lösungsunterstützung und Start „Unterstützung Problembearbeitung“ bzw. „Ablehnung“ . Die Messung beginnt mit dem Eintreffen (Eingang der Mail bzw. Entgegennahme am Telefon) der Meldung.	2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss],	

Service Level werden ggf. im spezifischen Betriebskonzept produkttypspezifisch definiert. ⌫

9.6 Prozessdurchführung problemlösungsverantwortlicher Anbieter und Hersteller

9.6.1 Vorprüfung

Ziel der Vorprüfung ist die Feststellung der Problemlösungsverantwortlichkeit bei Problemen mit produktübergreifender Ursache oder Auswirkung.

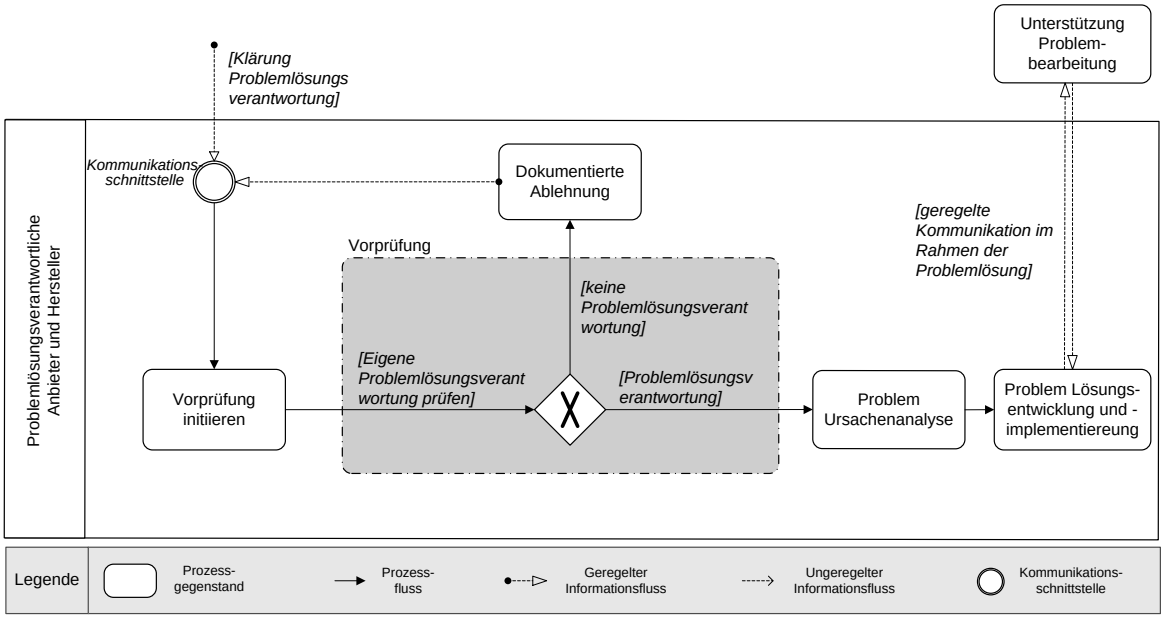


Abbildung 16: PRO - Vorprüfung problemlösungsverantwortlicher Anbieter und Hersteller

⌦ **GS-A_3981 Problembearbeitung von übergreifenden Problemen**

Problemlösungsverantwortliche Anbieter und Hersteller, welche das übergreifende Problem identifiziert sowie dokumentiert haben, MÜSSEN unverzügliche den

Problem-Bearbeitungsprozess entsprechend der festgestellten Problempriorität auslösen.⌫

9.6.2 Ablehnung

⌦ **GS-A_3982 Ablehnung von übergreifenden Problemen bei problemlösungsverantwortlichen A/H**

Anbieter und Hersteller, die ein übergreifendes Problem ablehnen, MÜSSEN dieses mit einer qualifizierten Rückmeldung an den anfragenden Anbieter und Hersteller des übergreifenden Problems durchführen, aus der nachvollziehbar zu entnehmen ist, warum keine Problemlösungsverantwortung übernommen werden kann. ⌫

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt.

9.6.3 Problem Ursachenanalyse

⌦ **GS-A_3983 Ursachenanalyse von übergreifenden Problemen durch Problemlösungsverantwortlichen**

Die Ursachenanalyse der Problemlösung MUSS durch den problemlösungsverantwortlichen Anbietern und Herstellern erfolgen. ⌫

Der problemlösungsverantwortliche Anbieter und Hersteller kann während der Bearbeitung die Wissensdatenbank zur Ursachenanalyse als Informationsquelle nutzen.

9.6.4 Anfrage zur Bereitstellung der Testumgebung bei SBV

⌦ **GS-A_3984 Anfrage zur Bereitstellung der TI-Testumgebung**

Anbieter und Hersteller, die für die Lösung des übergreifenden Problems eine TI-Testumgebung benötigen, MÜSSEN die Nutzung vorab beim SBV anfragen.

Anbieter und Hersteller MÜSSEN in der an einen SBV zu meldenden Anfrage beschreiben, welche Art der Unterstützung, zu welchem Zeitpunkt und im welchen Umfang benötigt wird. ⌫

Problemlösungsverantwortliche Anbieter und Hersteller müssen die von dem SV oder SBV zur Verfügung gestellte Kommunikationsschnittstelle nutzen.

9.6.5 Anfrage zu Produkttypvorgaben

⌦ **GS-A_3985 Anfrage Produkttypvorgaben**

Problemlösungsverantwortliche Anbieter und Hersteller KÖNNEN bei Fragen zu den spezifischen Produkttypvorgaben, mittels der vom SV bereitgestellten Kommunikationsschnittstelle, beim zuständigen SV Unterstützung und Klärungen anfordern. ⌫

9.6.6 Problem Lösungsentwicklung und -implementierung

Die Lösungsentwicklung erfolgt durch den problemlösungsverantwortlichen Anbieter und Hersteller. Dabei wird er von anderen am Prozess beteiligten Anbietern und Herstellern sowie von SBV und SV unterstützt.

⌦ **GS-A_3986 problemlösungsverantwortliche Koordination von übergreifenden Problems**

Die Koordination zwischen allen erforderlichen Lösungsbeteiligten im Rahmen der Problemlösungsentwicklung MUSS durch den problemlösungsverantwortlichen Anbieter und Hersteller erfolgen. ⌫

⌦ **GS-A_3987 Lösung von übergreifenden Problemen**

Der problemlösungsverantwortliche Anbieter und Hersteller MUSS unverzüglich mit der Problembearbeitung beginnen und innerhalb der vorgegebenen Problemlösungszeit eine Lösungsentwicklung für das Problem herbeiführen und dieses beheben.

Der problemlösungsverantwortliche Anbieter und Hersteller MUSS eine Dokumentation der Problemlösungsentwicklung vornehmen. Diese MUSS im qualifizierten Umfang bereitgestellt werden, aus dem hervorgeht, welche Problembehebungsmaßnahmen für das übergreifende Problem getroffen wurden.

Der problemlösungsverantwortliche Anbieter und Hersteller MUSS während der Problemlösungsentwicklung einen Change initiieren, in dem die Durchführung von Autorisierung, Entwicklung, Test und Implementierung der Lösung dokumentiert wird.

Der problemlösungsverantwortliche Anbieter und Hersteller MUSS im Rahmen der Problembehebung mit daraus hervorgehender Änderung an dem Produkt einen Verweis auf die RfC-ID (Request for Change ID) in die Dokumentation gemäß „GS-A_4000“ aufnehmen.

Anbieter und Hersteller MÜSSEN im Change-Management-Verweis der Dokumentation die zur Problemlösung notwendigen Maßnahmen und die durchgeführten Produkttypänderungen inkludieren. ⌫

9.6.7 Schließung übergreifendes Problem

Nach der Problemlösung wird die Lösung dem problemerkennenden Anbieter und Hersteller zur Verifizierung vorgelegt. Nach erfolgreicher Verifizierung erfolgt die vollständige Problemschließung durch den problemlösungsverantwortlichen Anbieter und Hersteller. Anschließend erfasst er die notwendige Dokumentation über die Problembehebung in der Wissensdatenbank.

Eine Problemlösung kann auch sein, dass die Problembearbeitung nicht weiterverfolgt wird, wobei das Problem in diesem Fall den abschließenden Status „Storniert“ erhält. Über dieses Vorgehen entscheidet der Problemerkennende bzw. Problemlösungsverantwortliche aber grundsätzlich niemals selbst, sondern darf den Status „Storniert“ immer nur mit Zustimmung des SBV oder GBV setzen. Die entsprechende Abstimmung und Begründung der Entscheidung ist vom Bearbeiter im Problem zu dokumentieren.

Ergänzende Erläuterungen sind im Rahmen des Knowledge Managements innerhalb der Wissensdatenbank dargestellt

⌦ **GS-A_3988 Versendung Verifizierung vor Schließung eines übergreifenden Problems**

Problemlösungsverantwortliche Anbieter und Hersteller MÜSSEN vor Schließung eines übergreifenden Problems die Lösung des Problems durch den problemerkennenden Anbieter und Hersteller verifizieren lassen. Bei negativer Verifikation des Problems ist kein neues übergreifendes Problem zu eröffnen. Stattdessen ist das bestehende Problem weiterzubearbeiten. Es ist erneut der Status auf „In Bearbeitung“ zu setzen, außerdem wird die Lösungszeit fortgeschrieben. Dabei bestimmt der entsprechend im Problem gesetzte problemerkennende Anbieter und Hersteller den Zeitpunkt der Verifikation. Dies gilt sinngemäß auch für den Zeitpunkt der Bestätigung und Schließung. ⌫

⌦ **GS-A_3989 Nacharbeitung vor Schließung eines übergreifenden Problems**

Problemlösungsverantwortliche Anbieter und Hersteller MÜSSEN die von problemerkennenden Anbietern und Herstellern beauftragte Nacharbeit überprüfen und bei nicht vollständiger Lösungsentwicklung die Mängel beseitigen. ⌫

⌦ **GS-A_3990 Schließung nach Verifizierung des Problemerkennenden**

Problemlösungsverantwortliche Anbieter und Hersteller MÜSSEN nach der erfolgreichen Verifizierung eines übergreifenden Problems durch problemerkennende Anbieter und Hersteller dieses abschließend dokumentieren und schließen. ⌫

⌦ **GS-A_3991 WDB Aktualisierung nach Schließung der übergreifenden Problemmeldungen**

Problemlösungsverantwortliche Anbieter und Hersteller MÜSSEN nach der Behebung eines übergreifenden Problems die Wissensdatenbank um die relevanten Problemlösungsinformationen aktualisieren. ⌫

9.6.8 Service Level Requirements (SLR)

⌦ **GS-A_3992 Service Level Requirements problemlösungsverantwortliche Anbieter und Hersteller**

Aufbauend auf die in den jeweiligen Verträgen geregelten Servicezeiten MÜSSEN problemlösungsverantwortliche Anbieter und Hersteller mindestens folgende Service Level messen und berichten:

Tabelle 23: Tab_Betr_TIP_020 PRO - SLR PLVe A/H „Prozess“

ID	Qualitätsdimension	Beschreibung	Typ	Bei-spiel
PRO_7	Qualifikationszeit problemlösungs-verantwortliche A/H	Zeitdauer während der Servicezeit zwischen Eingang der Anfrage zur „Klärung PLV“ und Start der „Problem Ursachenanalyse“ bzw. „Ablehnung. Die Messung beginnt mit dem Ein-treffen (Eingang der Mail bzw. Ent-gegennahme am Telefon) der Meldung	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss],	
PRO_8	Meldezeit Bearbeitungsstatus problemlösungs-verantwortliche A/H	Zeitdauer während der Servicezeit in der eine Erstinformation bzw. aktuelle Status eines übergreifenden Problems an den SBV gesendet werden muss.	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss],	
PRO_9	Zeitdauer für Problemlösung durch problemlösungs-verantwortliche A/H	Zeitdauer in der mit der Problemlösungsanalyse begonnen und eine Problemlösung bereitgestellt bzw. implementiert werden muss.	1␣[hhhh:mm:ss], 2␣[hhhh:mm:ss], 3␣[hhhh:mm:ss], 4␣[hhhh:mm:ss],	

Service Level werden in den spezifischen Betriebskonzepten produkttypspezifisch definiert. ⌫

9.7 Informationspflichten

Für die ordnungsgemäße Wahrnehmung und Umsetzung der Informationspflichten sind problemerkennende sowie problemlösungsverantwortliche Anbieter und Hersteller verant-wortlich.

⌦ **GS-A_3993 Information bei Feststellung von Problemen im lokalen und übergreifenden Problem Management**

Problemerkennende sowie problemlösungsverantwortliche Anbieter und Hersteller MÜSSEN bei der Feststellung eines produkttypspezifischen Problems (siehe GS-A_3972 für Problemerkennende und GS-A_3992 Problemlösungsverantwortliche) mit hoher Kritikalität, d.h. Prioritäten „1. Kritisch“ und „2. Hoch“ unter Beachtung der Mindestinhalte bei Erfassung eines Problems (siehe GS-A_4000), den SBV informieren. Im übergreifenden Problem Management erfolgt die Kommunikation über die ZID. ⌫

⌦ **GS-A_3994 Statusinformation bei lokalen und übergreifenden Problemen**

Problemerkennende sowie problemlösungsverantwortliche Anbieter und Hersteller MÜSSEN gemäß den zeitlichen Vorgaben der Service Level Requirements (siehe GS-A_3972 für Problemerkennende und GS-A_3992 Problemlösungsverantwortliche) eine Meldung über den aktuellen Status des produkttypspezifischen Problems mit hoher Kritikalität, d.h. Prioritäten „1. Kritisch“ und „2. Hoch“ unter Beachtung der Mindestinhalte bei Erfassung eines Problems (siehe GS-A_4000), an den SBV versenden. Darüber hinaus ist grundsätzlich, unabhängig von der Priorität, bei jedem Statuswechsel eines Problems eine Statusinformation zu übermitteln.

Im übergreifenden Problem Management erfolgt die Kommunikation über die ZID.⌫

9.8 Dokumentation

Die Dokumentation der Problembearbeitung erfolgt durch die problemerkennenden und problemlösungsverantwortlichen Anbieter und Hersteller und ist durch diese zu unterschiedlichen Zeitpunkten zu befüllen.

⌦ **GS-A_4000 Mindestinhalte Dokumentation von übergreifenden Problemen**

Anbieter und Hersteller MÜSSEN jedes im übergreifenden PRO zu erfassende Problem nach folgendem Schema dokumentieren, wobei die Felder durch die problemerkennenden (PE) und problemlösungsverantwortlichen (PLV) Anbieter und Hersteller zu unterschiedlichen Zeitpunkten zu befüllen sind:

Die an die Webservice-Schnittstelle der ZID zu sendenden Daten entsprechen dieser Beschreibung und sind im Anhang C beschrieben.

Zeichenerklärung in der Spalte Befüllungszeitpunkt / Befüllungsstatus

X	entspricht	muss befüllt bzw. geändert werden
O	entspricht	kann befüllt bzw. geändert werden
-	entspricht	darf nicht geändert werden

Tabelle 24: Tab_Betr_TIP_021 PRO - Mindestinhalte Problemdokumentation

#	Feldname	Inhalt	Typ	Bespiel	Befüllungszeitpunkt(e)								
					Erfassung	Anfrage Unterstützung	PLV Ermittlung	Unterstütz. Prob. Bearb.	Ursachenanalyse	Lösungsentw.&Implement.	Verifizierung Schließung	Schließung	Eskalation
1	Problem ID	Problem-ID. (Die Vergabe ist ausschließlich durch den Problemerkennenden (Anbieter und Hersteller, der das übergreifende Problem identifiziert hat) möglich, entsprechend GS-A_3961 und GS-A_3962)	[String]		X	-	-	-	-	-	-	-	-
2	Problemerkennender ID	Eindeutige TID des problemerkennenden Anbieters und Herstellers	[String]	ATOSO	X	-	-	-	-	-	-	-	-
3	Problemlösungsverantwortlicher ID	Eindeutige TID des problemlösungsverant-wortlichen Anbieters und Herstellers	[String]	ATOSO					X	-	-	-	-
4	Problem Status	Aktueller Status der Problemmeldung. Bei Eröffnung der Problemmeldung ist dieser immer in „Bearbeitung“.	[Auswahlfeld], (In Bearbeitung), (PLV ermittelt) ,(Ursache erkannt), (Lösung bekannt), (Lösung implementiert), (Verifizierung), (Geschlossen), (Storniert)		X	-	O	O	O	O	O	O	-
5	Priorität	Priorität des Problems (siehe GS-A_3964).	[Integer]	2	X	O	O	O	O	O	O	O	-

#	Feldname	Inhalt	Typ	Bespiel	Befüllungszeitpunkt(e)								
					Erfassung	Anfrage Unterstützung	PLV Ermittlung	Unterstütz. Prob. Bearb.	Ursachenanalyse	Lösungsentw.&Implement.	Verifizierung Schließung	Schließung	Eskalation
6	Kategorie	Kategorie (GS-A_3963) zum Berichtszeitpunkt, bei gelösten Problemen ist dies die abschließende Kategorisierung, die der Produkttypversion entsprechen muss. Ist kein Produkttyp vergeben oder möglicherweise mehrere Produkttypen betroffen, kann auch „SONST“ eingetragen werden. Das betroffene Produkt muss dann im Worklog eindeutig benannt werden	[String]		X	O	O	O	O	O	O	O	-
7	Zeit Erfassung	Datum und Uhrzeit der Problem-Ersterfassung.	[Date]		X	-	-	-	-	-	-	-	-
8	Betroffene Betriebsumgebung	Nennung der Betriebsumgebung, in welcher das Problem aufgetreten ist	[Auswahlfeld], (RU), (TU), (PU)		X	O	O	O	O	O	O	O	-
9	Sicherheitsrelevanz	Einstufung der Sicherheitsrelevanz	[Auswahlfeld], (Ja), (Nein)		X	O	O	O	O	O	O	O	-
10	Eskalation	Auswahlfeld, ob sich das Problem in einer Eskalation befindet/befand und an wen eskaliert wurde. (Level 1= SBV, Level 2 = GBV TI) Nach Entscheidung über die Eskalation durch den GBV TI bzw. SBV ist das Auswahlfeld wieder auf	[Auswahlfeld], (Nein), (L1), (L2)		X	O	O	O	O	O	O	O	O

#	Feldname	Inhalt	Typ	Bespiel	Befüllungszeitpunkt(e)								
					Erfassung	Anfrage Unterstützung	PLV Ermittlung	Unterstütz. Prob. Bearb.	Ursachenanalyse	Lösungsentw.&Implement.	Verifizierung Schließung	Schließung	Eskalation
		‚Nein' zu setzen.											
11	Problem Beschreibung	strukturierte Beschreibung der Störung inklusive textuelle Beschreibung der Auswirkungen, Dringlichkeit und ggf. Querverweis auf Incidents. Hier kann jederzeit eine nachträgliche Veränderung im Sinne einer Schärfung und Klarstellung erfolgen.	[String]		X	O	O	O	O	O	O	O	-
12	Problem Worklog	Beschreibung der durchgeführten Aktivitäten Fortlaufend ergänzter [String], (neueste Einträge zuerst): <tr><Zeitstempel>#<Tätigkeiten/Freitext></tr>	<tr>[date]#[String]</tr> Maximale Größe des Feldes: 15000 Zeichen	<tr>2015-02-23T01:47:36+01#qualifizierte Beschreibung der Tätigkeit</tr>	X	X	X	X	O	O	X	X	X
13	Problem Lösung	Eineindeutige Beschreibung der Lösung des übergreifenden Problems.	[String]							X	O	O	-
14	RfC ID	Aufzählung der Request for Change IDs, mit der das Problem gelöst wurde.	Strukturierte Aufzählung [String] mit # getrennt							X	-	-	-
15	Zeitpunkt Lösung	Datum und Uhrzeit der Lösung des Problems.	[Date]	2015-02-23T01:47:36+01						X	-	-	-
16	Zeitpunkt	Datum und Uhrzeit der Verifizierung vor	[Date]	2015-02-23T01:4							X	-	-

#	Feldname	Inhalt	Typ	Bespiel	Befüllungszeitpunkt(e)								
					Erfassung	Anfrage Unterstützung	PLV Ermittlung	Unterstütz. Prob. Bearb.	Ursachenanalyse	Lösungsentw.&Implement.	Verifizierung Schließung	Schließung	Eskalation
	Verifizierung	Schließung durch den Problemerkennenden.		7:36+01									
17	Zeit Ende	Datum und Uhrzeit bei Schließen des Problems. (Der PLV schließt das Ticket nach positiver Verifikation (durch den PE, fallweise) und gibt dann an den Problem-melder eine Schlie-ßungsbestätigung mit dem entsprechenden Zeitstempel).	[Date]	2015-02-23T01:47:36+01								X	-
18	Meldungstyp	Art der Meldung: „WE“: Weiterleitung „RQ“: Anfrage ohne Übergang der Lösungsverantwortung „ES“: Eskalation an den SBV „SI“: Statusinformation an den SBV NI“ - Nachreichen von Informationen zum übergreifenden Problem „AN“ - Annahme des übergreifenden Problems „AL“ – Ablehnen des übergreifenden Problems	[Auswahlfeld], (WE), (NI), (AN), (AL), (ES), (SI)		X	O	O	O	O	O	O	O	X

⌫

9.9 Eskalationen

⌦ **GS-A_3995 Eskalationseinleitung durch den Anbieter und Hersteller im PRO**

Anbieter und Hersteller KÖNNEN bei übergreifenden Problemen mit Prioritäten „1. Kritisch“ und „2. Hoch“ oder bei sicherheitsrelevanten Problemen eine hierarchische Eskalation an den SBV einleiten, wenn:

- er keinen lösungsunterstützenden Hersteller bzw. Anbieter ermitteln kann,
- er keine Einigung über die Lösungsunterstützung für das übergreifende Problem mit anderen Herstellern bzw. Anbietern erreicht werden kann,
- nach seinem Verständnis zur Bewältigung der Probleme mit Prioritäten „1. Kritisch“ und „2. Hoch“ eine übergeordnete Koordination notwendig ist,
- die Bearbeitungsdauer eines anderen Anbieter und Hersteller die Service Level Requirements für die Bearbeitung des Problems (mit der gegebenen Priorität) zu verletzen droht bzw. die eigene Serviceerbringung gefährdet. ⌫

⌦ **GS-A_3996 Eskalationsinhalte im PRO**

Anbieter und Hersteller MÜSSEN bei jeder Eskalationsmeldung an einen SBV im übergreifenden Problem Management folgende Inhalte erfassen:

- aktuelle Problemdokumentation gemäß GS-A_4000.
- Das Worklog der Problem-Dokumentation muss um folgende Informationen ergänzt werden:
    - Eskalationsbeschreibung: qualifizierte Beschreibung aller bislang erfolgten Prüfungen, Aktionen/Eskalationen und Schritte, Eskalationsgrund und Dringlichkeit sowie konkret angefragter Unterstützungsbedarf.
    - Eskalationsmelder ID, sowie Kontaktdaten, inklusive Telefonnummer und E-Mail-Adresse für eventuelle Rückfragen.

Die Eskalationsmeldung muss strukturiert über die ZID erfolgen. ⌫

Bei Problemen mit Prioritäten „1. Kritisch“ und „2. Hoch“ sowie bei sicherheitsrelevanten Problemen kann der SBV der TI - zur Gewährleistung der Performance, Sicherheit und Stabilität der zentralen und dezentralen Produkte - eine Taskforce zur Problembehebung bilden. Diese wird aus mehreren der am Betriebsprozess beteiligten Anbietern bzw. Herstellern durch den SBV TI zusammengesetzt.

⌦ **GS-A_3997 Mitwirkung bei Taskforces im Eskalationsfall**

Anbieter und Hersteller MÜSSEN bei Aufforderung durch den SBV an einer Taskforce zur Behebung von übergreifenden Problemen mit der Priorität 1 oder 2 teilzunehmen, der Taskforce beitreten und die Lösungsfindung unterstützen.

Anbieter und Hersteller MÜSSEN nach der Lösung des übergreifenden Problems mit der Priorität 1 oder 2 innerhalb einer Taskforce im Anschluss die Erstellung des Abschlussberichtes bzw. die Durchführung des Audits unterstützen. ⌫

9.10 Obliegenheiten SBV/GBV TI

Obliegenheiten des SBV:

- Der jeweilige SBV nimmt Eskalationsmeldungen entgegen und entscheidet, ob eine Meldung an den GBV TI durchzuführen ist.
- Der jeweilige SBV nimmt übergreifende Problems mit der Priorität 1 und 2 entgegen und entscheidet, ob eine Meldung an den GBV TI durchzuführen ist.
- Der jeweilige SBV wird sich bei übergreifenden Problems der Priorität 1 oder 2 selbständig über den jeweils aktuellen Stand der Bearbeitung durch den betreffenden Anbieter und Hersteller informieren, so dass er ggü. dem GBV TI jederzeit auskunftsfähig ist.

Obliegenheiten der GBV TI:

- Bei Problems mit (produkt-)übergreifender Auswirkung kann der GBV TI - zur Gewährleistung der Performance, Sicherheit und Stabilität der zentralen und dezentralen Produkte - eine zentrale Koordinierung der Aktivitäten der anderen Prozessbeteiligten übernehmen.

9.11 Prozessreporting (Vorgangsdaten) PRO

Das Prozessreporting der Problemursache und -lösung dient der geordneten Aufbewahrung von bereits behobenen Problemen. Durch diese ist es zu einem späteren Zeitpunkt möglich, ein möglicherweise ähnliches Problem so früh wie möglich zu identifizieren oder mit Hilfe von einer Problem- oder Lösungsbeschreibung anhand der übergreifenden Zusammenhänge zu analysieren.

Für die ordnungsgemäße Wahrnehmung und Umsetzung des Prozessreportings ist ausschließlich der problemlösungsverantwortliche Anbieter und Hersteller verantwortlich.

⌦ **GS-A_3998 Bereitstellung von Problemdokumentationen aus dem übergreifenden Problem Management**

Problemlösungsverantwortliche Anbieter und Hersteller MÜSSEN die an den SBV zu versendenden Reports im .CSV-Format übermitteln.

Anbieter und Hersteller MÜSSEN bei den an den SBV zu versendenden Reports die AFO GS-A_5248 beachten. ⌫

⌦ **GS-A_3999 Reportinhalte von Vorgangsdaten aus dem übergreifenden Problem Management**

Problemlösungsverantwortliche Anbieter und Hersteller MÜSSEN Vorgangsdatenreports nach der in GS-A_3961, GS-A_3962 , GS-A_3963, GS-A_3964 und GS-A_4000 vorgegebenen Struktur erstellen. ⌫

Im Rahmen der Fehleranalyse und zu Auswertungszwecken sind durch Anbieter und Hersteller Systemprotokolle und Fehlerlogs, sowie Incidentdokumentationen an den SBV zu übermitteln, welche nicht Bestandteil des regelmäßigen Reportings sind.

⌦ **GS-A_5251 Übermittlung von Fehlerlogs, Systemprotokollen der Produktinstanzen und lokalen Incidents**

Anbieter und Hersteller MÜSSEN die vom SBV bei Bedarf angeforderten Systemprotokolle und Fehlerlogs der Produktinstanzen sowie Dokumentationen der lokalen Incidents, unverzüglich in elektronischer Form und in einem weiter bearbeitbaren und auswertbaren Format an den SBV oder den durch den SBV benannten Empfänger übermitteln.⌫

9.12 Obliegenheiten lösungsunterstützende SV/SBV

Lösungsunterstützende SV und SBV unterstützen, koordinieren und stellen sicher, dass die am spezifischen Service beteiligten Anbieter und Hersteller aufgetretene Probleme lösen und dass sie die Service Qualität und Performance nicht nachhaltig beeinträchtigen. Dies wird durch strikte Befolgung der Service Level Requirements, wie z.B. Reaktionszeiten in Abhängigkeit von Problem-Prioritäten, erreicht.

9.12.1 Vorprüfung

Die die Meldung erhaltenden lösungsunterstützenden SV oder SBV werden die von Anbieter und Hersteller gemeldeten, übergreifenden Problemen innerhalb einer angemessenen Zeitspanne beantworten.

9.12.2 Ablehnung

SV oder SBV, die ein übergreifendes Problem ablehnen, werden dieses mit einer Rückmeldung an den meldenden Anbieter und Hersteller des übergreifenden Problems durchführen.

9.12.3 Unterstützung Problembearbeitung

Problemlösungsverantwortliche Anbieter und Hersteller, die ein übergreifendes Problem gemeldet haben, werden entsprechende Unterstützung bei der Problemanalyse von SV oder SBV erhalten. Problemlösungsverantwortliche Anbieter und Hersteller werden entsprechende Unterstützung bei der Koordinierung der Aktivitäten für die relevante Testumgebung und bei der Klärung der wesentlichen Produkttypvorgaben vom SV oder SBV erhalten.

Der SBV unterstützt und koordiniert bei Bedarf die Kooperation zwischen problemlösungsverantwortlichen und lösungsunterstützenden Anbietern und Herstellern.

10 Notfallmanagement

Um zwischen den verschiedenen Anbietern bzw. durch den Anbieter beauftragten Anbietern und Herstellern der TI sicherzustellen, dass

- die entsprechenden Vorkehrungen zur Bewältigung von TI-Notfällen getroffen werden bzw. die Umsetzung der in der TI-Notfallvorsorge geplanten Maßnahmen erfolgt ist,
- dass eine zuverlässige Notfallkoordination bzw. -unterstützung von aufgetretenen Schadensereignissen produkt- sowie serviceübergreifend gewährleistet ist,

ist durch Anbieter und Hersteller ein Notfallmanagement zu etablieren.

Die nachfolgende Abbildung veranschaulicht hierzu die Regelungen von TI-Notfällen im anbieter- und herstellerrelevanten Prozessausschnitt und gibt eine Zuordnung der einzelnen Prozessinhalte zu den nachfolgenden Kapiteln.

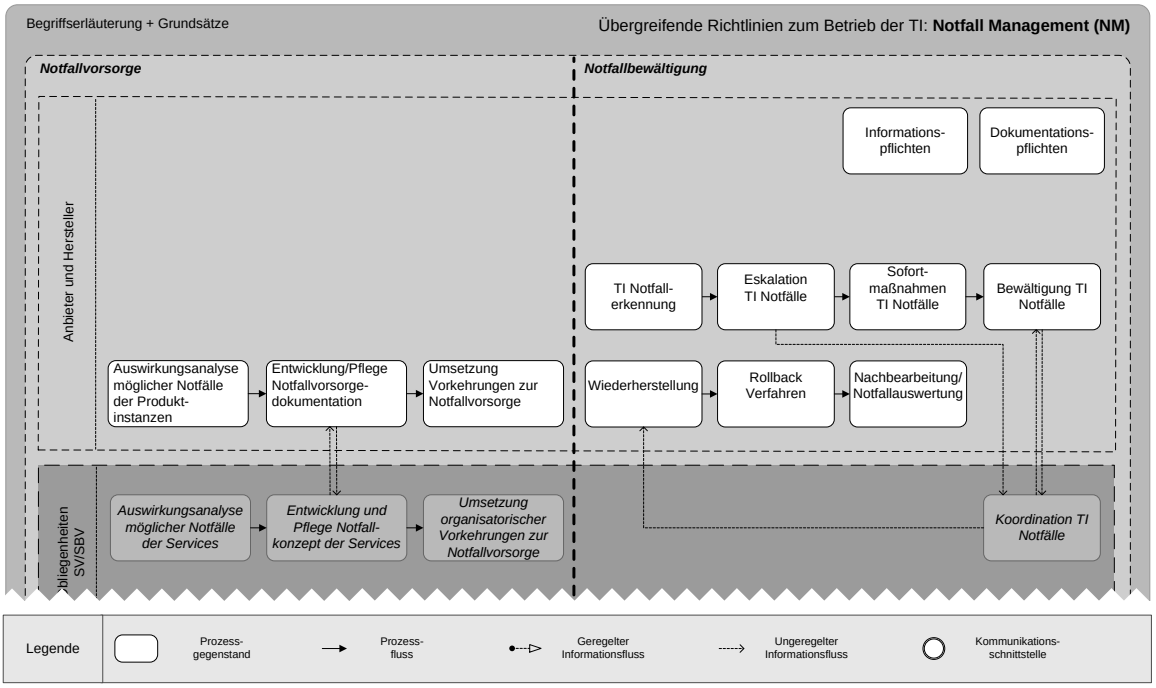


Abbildung 17: Notfallmanagement - Gesamtprozessschaubild "Notfallmanagement“

10.1 Betrachtungsgegenstand des übergreifenden Notfallmanagement

Der primäre Fokus der Richtlinie liegt in Ausprägung der Vorsorge und Bewältigung von TI-Notfällen durch Anbieter und Hersteller.

Art und Umfang der Notfallvorsorge und -bewältigung von lokalen Notfällen durch Anbieter und Hersteller sind nicht Gegenstand dieser Richtlinie. Ein lokales

Notfallmanagement wird vorausgesetzt. Anforderungen an das lokale Notfallmanagement sind [gemSpec_SiBetrUmg] zu entnehmen.

Die operative Behebung von TI-Notfällen obliegt grundsätzlich den Anbietern und Herstellern, wobei der SBV eine zentrale koordinierende Rolle im Rahmen der Bewältigung einnehmen kann. Dazu etabliert er ein Lösungsteam und das EMC, welches die Anbieter und Hersteller unterstützt.

10.2 Begriffserläuterungen

10.2.1 Notfall

Gemäß dem [BSI 100-4] wird unter Notfall ein länger andauernder Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden verstanden. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer geforderten Zeit nicht wieder hergestellt werden. Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallbewältigungsorganisation.

10.2.2 lokaler Notfall

Ein lokaler Notfall beschreibt ein Schadensereignis der Produkte mit lokal ausgeprägten Auswirkungen. Lokale Notfälle werden durch Anbieter und Hersteller bewältigt und erfordern i.d.R. keine Koordination durch SBV.

10.2.3 TI-Notfall

Ein TI-Notfall beschreibt ein Schadensereignis, welches nicht allein durch die lokale Notfallorganisation von betroffenen Anbietern und Herstellern zu bewältigen ist (also der Koordination durch SBV bedarf) und sich insbesondere dadurch hervorhebt, dass die TI bzw. ein TI-Service in ihrer ganzheitlichen Funktion (auch im Kontext der Sicherheit) gestört oder gefährdet ist.

10.2.4 TI-Notfallvorsorge

Gemäß dem [BSI 100-4] zählen zur TI-Notfallvorsorge alle organisatorischen und konzeptionellen Aspekte sowie alle proaktiven Maßnahmen und Tätigkeiten des Notfallmanagements. Dazu zählen:

- vorbeugende Maßnahmen, die den Schaden oder die Eintrittswahrscheinlichkeit von Risiken reduzieren und die Widerstandsfähigkeit der Institution durch Anheben der Krisenschwelle erhöhen, wie auch
- proaktive Maßnahmen, um ein schnelles und sinnvolles Reagieren auf einen Vorfall zu ermöglichen.

Die Ausgestaltung der Vorsorgemaßnahmen sollte sich an der Kritikalität des Dienstes orientieren.

10.2.5 TI-Notfallmaßnahme

Als TI-Notfallmaßnahme gilt jede Handlung, welche die Auswirkung eines TI-Notfalls eindämmen, schmälern oder aufheben kann. Die Maßnahme bietet in der Regel keine nachhaltige Beseitigung der Ursache des TI-Notfalls, kann aber einen Notbetrieb ermöglichen bzw. in Art und Ausprägung die TI-Notfallbewältigung erleichtern oder ermöglichen.

10.2.6 Notbetrieb

Als Notbetrieb wird der Betriebszustand bezeichnet, welcher durch eine erfolgreiche Maßnahme innerhalb der TI-Notfallbewältigung die Grundfunktionen des Dienstes zwar aufrechterhält, diese jedoch entweder noch nicht nachhaltig stabilisiert sind und/oder noch nicht in der gewünschten Güte geleistet werden können (bspw. längere Antwortzeiten, Fehlen einer Redundanz, Verzicht auf einzelne Features etc.). Wichtigstes Merkmal des Notbetriebes ist dabei, dass betroffene Produkte keine schädigenden Wechselwirkungen mit anderen TI-Produkten mehr verursachen. Mit der erfolgreichen Aufnahme des Notbetriebs beginnt die Wiederherstellung.

10.2.7 TI-Notfallbewältigung

Bei der der TI-Notfallbewältigung handelt es sich um das operative Agieren innerhalb des in der TI-Notfallvorsorge festgelegten Rahmens. Das Ziel der TI-Notfallbewältigung ist das Fortführen des vom TI-Notfall betroffenen Services, gegebenenfalls auch mit Einschränkungen sowie die vollständige Wiederherstellung des Services im vorgegebenen Leistungsumfang und Sicherheitsmerkmalen.

10.2.8 Emergency Management Committee (EMC)

Das Emergency Management Committee (EMC) ist das Führungsinstrument im TI-Notfall. Es wird zeitlich befristet eingesetzt und ist für die Koordination der TI-Notfallbewältigung verantwortlich.

Das EMC ist im Rahmen der geltenden betrieblichen und rechtlichen Regelungen gegenüber allen Rollen der Notfallorganisation im Rahmen der TI-Notfallbewältigung weisungsbefugt. Es befasst sich ausschließlich mit dem vorliegenden TI-Notfall und den davon betroffenen Bereichen.

Das EMC umfasst:

- einen Vertreter der Leitungsebene des GBV TI,
- einen Vertreter der Leitungsebene der SBVs der TI-Services,
- den Koordinator Informationssicherheit- und Datenschutz TI (GBV TI).

Diese Zusammensetzung kann fallspezifisch um die Vertreter der relevanten Experten sowie Anbieter und Hersteller erweitert werden.

10.2.9 Lösungsteam

Das Lösungsteam ist ein durch das EMC einberufenes Team von Fachexperten der durch den TI-Notfall unmittelbar betroffenen oder gefährdeten Dienste der TI. Aufgabe des Lösungsteams ist das Identifizieren und Bewerten, sowie (nach erfolgter Freigabe durch das EMC) das Durchführen von Maßnahmen der TI-Notfallbewältigung. Das Lösungsteam kann jederzeit während der TI-Notfallbewältigung hinsichtlich der Anforderungen umbesetzt werden und wird spätestens mit der Deeskalation des TI-Notfalls aufgelöst.

10.3 Grundsätze des übergreifenden Notfallmanagements

Die nachfolgenden Grundsätze bilden die Regelungen des übergreifenden Notfallmanagements für Anbieter und Hersteller sowie SBV.

10.3.1 Kommunikation des übergreifenden Notfallmanagements

Die Kommunikation zwischen den Prozessbeteiligten hat auf Basis der Kommunikationsschnittstellen für Incident Management zu erfolgen und wird im Notfallmanagement nicht weiter ausgeprägt. Ein TI-Notfall wird insofern als höchste Eskalationsstufe einer Störung bezeichnet.

Die Kommunikation innerhalb der Notfallorganisation hat in allen Informations- und Eskalationsrichtungen (funktional, hierarchisch) sachlich, ruhig und umgehend zu erfolgen.

Die Kommunikation während des TI-Notfalls mit außenstehenden Dritten (Öffentlichkeit; nicht betroffene oder unbeteiligte Anbieter und Hersteller) muss ausschließlich in vorheriger Abstimmung mit, oder durch das EMC erfolgen.

10.3.2 zentrale Koordination von TI-Notfällen durch das EMC

Notfälle mit Auswirkung auf die TI-Services werden durch das EMC koordiniert. Das EMC wird durch den SBV einberufen.

10.4 Prozessdurchführung Notfallvorsorge

10.4.1 Analyse der Auswirkungen möglicher Notfälle der Produktinstanzen

Der SV wird ein Notfallvorsorgekonzept erstellen. Das Ziel des Notfallvorsorgekonzepts ist, die TI-Notfälle in ihrer Auswirkung auf die Erbringung der TI-Services zu analysieren und vorbeugend proaktive Maßnahmen zu entwickeln. Im Rahmen der Analyse von möglichen (lokalen) Schadensereignissen und im Rahmen der Bereitstellung bzw. dem Betrieb von Produkten wird der SV durch die jeweiligen Anbieter und Hersteller unterstützt.

⌦ **GS-A_4121 Analyse Auswirkungen möglicher Schadensereignisse auf Sicherheit und Funktion der TI-Services**

Anbieter und Hersteller MÜSSEN die Auswirkungen möglicher Schadensereignisse der Produkte auf Sicherheit und Funktion der TI-Services analysieren und bewerten. Die Auswirkungsanalyse MUSS mit mindestens folgenden Vorgaben erstellt werden:

- angenommener Ausfall einer tatsächlichen Funktionalität bzw. Eigenschaft des Produkts (Notfallszenario),
- Beschreibung der Auswirkung möglicher Wechselwirkung mit anderen Produkten bzw. auf den TI-Service,
- Risikobewertung des Notfallszenarios. ⌫

⌦ **GS-A_4122 Unterstützung TI-Notfallvorsorge**

Anbieter und Hersteller MÜSSEN, zur Gewährleistung der Sicherheit und Funktionalitäten der TI-Services, andere Anbieter und Hersteller bei der Auswirkungsanalyse der TI-Notfallvorsorgemaßnahmen im Rahmen der TI-Notfallvorsorge unterstützen. ⌫

10.4.2 Entwicklung und Pflege der Notfallvorsorgedokumentation

⌦ **GS-A_4123 Entwicklung und Pflege der TI-Notfallvorsorgedokumentation**

Anbieter und Hersteller MÜSSEN eine TI-Notfallvorsorgedokumentation, welche die Ergebnisse der Auswirkungsanalyse sowie Vorkehrungen zur TI-Notfallvorsorge des SV enthält, entwickeln und pflegen. In der TI-Notfallvorsorgedokumentation sind die Aktivitäten festgelegt, die bei Eintritt eines TI-Notfalls durchführen sind. ⌫

10.4.3 Umsetzung Vorkehrungen zur Notfallvorsorge

⌦ **GS-A_4124 Umsetzung Vorkehrungen zur TI-Notfallvorsorge**

Anbieter und Hersteller MÜSSEN die erarbeiteten Vorkehrungen zur TI-Notfallvorsorge umsetzen. ⌫

10.5 Prozessdurchführung TI-Notfallbewältigung

Die nachfolgende Abbildung zeigt einen generischen, idealtypischen Ablauf der TI-Notfallbewältigung, an dessen Beispiel die einzelnen Aktivitäten im Folgenden beschrieben werden.

Diese Abbildung stellt keinen Prozessablauf dar und erhebt keinen Anspruch auf vollständige Abdeckung sämtlicher Szenarien. Sie soll mit Hilfe der nachfolgend textuell beschriebenen Arbeitsschritte einen Rahmen für die Mitwirkungsverpflichtungen der Anbieter und Hersteller bei der Bewältigung von TI-Notfällen definieren.

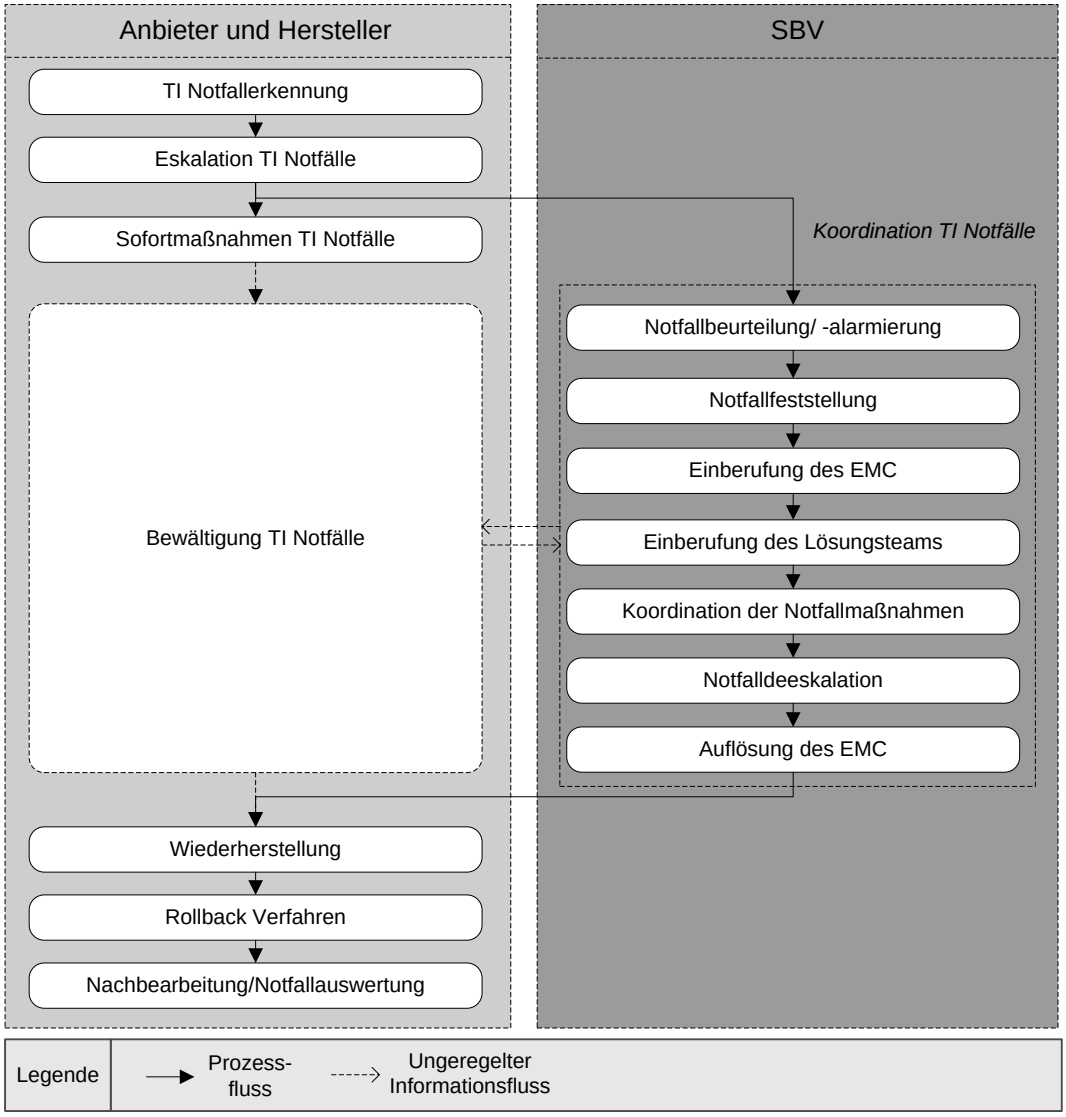


Abbildung 18: Notfallmanagement - Idealtypischer Ablauf TI-Notfallbewältigung

TI-Notfallerkennung

Die TI-Notfallerkennung ist eine operative Aufgabe des Incident Managements. Sie stellt sicher, dass Vorfälle erkannt werden und eine schnelle und angemessene Reaktion erfolgen kann.

⌦ **GS-A_4125 TI-Notfallerkennung**

Anbieter und Hersteller MÜSSEN TI-Notfälle im operativen Betrieb im Rahmen des Incident Managements feststellen. TI-Notfälle werden als Incidents der Priorität 1 mit Kennzeichnung „TI-Notfall“ klassifiziert. ⌫

Im Folgenden werden weitergehende Regelungen für Eskalation, Koordination sowie Informations- und Dokumentationspflichten für die Bewältigung von TI-Notfällen festgelegt.

10.5.1 Eskalation TI-Notfälle

⌦ **GS-A_4126 Eskalation TI-Notfälle**

Anbieter und Hersteller MÜSSEN erkannte TI-Notfälle, unverzüglich an den für sie zuständigen SBV eskalieren. Eine Meldung an den SBV MUSS im Sinne einer umgehenden und persönlichen Benachrichtigung erfolgen.⌫

10.5.2 Sofortmaßnahmen TI-Notfälle

⌦ **GS-A_4127 Sofortmaßnahmen TI-Notfälle**

Anbieter und Hersteller, die von einem TI-Notfall betroffen sind, MÜSSEN entsprechende Maßnahmen einleiten, mit dem Ziel die Auswirkungen der TI-Notfälle eigenständig zu reduzieren oder einzuschränken. ⌫

10.5.3 Bewältigung TI-Notfälle

⌦ **GS-A_4128 Bewältigung der TI-Notfälle**

Anbieter und Hersteller MÜSSEN vom EMC autorisierte TI-Notfallmaßnahmen zur Bewältigung von TI-Notfällen im eigenen Verantwortungsbereich umsetzen. ⌫

⌦ **GS-A_4129 Unterstützung bei TI-Notfällen**

Anbieter und Hersteller MÜSSEN bei der Bewältigung sowie Koordination der TI-Notfälle den SBV oder andere Anbietern und Herstellern im erforderlichen Umfang unterstützen. ⌫

10.5.4 Koordination der TI-Notfallbewältigung durch SBV

Notfallbeurteilung/-alarmierung

Nach dem die Anbieter und Hersteller einen möglichen TI-Notfall erkannt und an den SBV gemeldet haben, wird der SBV die durch das Incident Management vorgenommene Beurteilung und die zu erwartende Auswirkung des TI-Notfalls anhand des Schadenbeurteilungsplans überprüfen.

Im Falle einer negativen Notfallbewertung (keine zu erwartende Auswirkung, Notfallkriterien sind zwischenzeitlich nicht mehr erfüllt etc.) wird die Zurückweisung des TI-Notfalls entsprechend dem regulären Betriebsprozess in der Incident-Dokumentation festgehalten.

Im Falle einer positiven Notfallbewertung wird der GBV TI durch den SBV über die Art und Ausprägung sowie zu erwartende Auswirkungen des vorliegenden TI-Notfalls alarmiert.

Notfallfeststellung

Der SBV wird ggf. in Abstimmung mit dem GBV TI im Falle eines TI-Notfalls die vorgenommene Notfallbewertung bestätigen und einen formellen Ausruf des TI-Notfalls durchführen.

Einberufung des EMC

Nach der Notfallbestätigung beruft der SBV das EMC ein. Die Zusammensetzung des EMC wird auf Basis des vorliegenden TI-Notfalls beschlossen und wird entsprechend des Schwierigkeitsgrades der eingetretenen oder zu erwartenden Auswirkungen fallspezifisch erweitert.

Im Laufe der TI-Notfallbewältigung kann das EMC seine Zusammensetzung erweitern.

⌦ **GS-A_4130 Festlegung der Räumlichkeiten für EMC**

Prozessbeteiligte Anbieter und Hersteller MÜSSEN die von SBV bereitgestellten Räumlichkeiten im Rahmen der Einberufung des EMC wahrnehmen. ⌫

⌦ **GS-A_4131 Bereitstellung der Ansprechpartner und Teilnehmer für EMC**

Anbieter und Hersteller MÜSSEN entsprechend den Anforderungen des SBV Ansprechpartner und Teilnehmer für das EMC mit entsprechenden Fach- und/oder Entscheidungskompetenzen bereitstellen. ⌫

⌦ **GS-A_4893 Kommunikationsschnittstellen im Rahmen von TI-Notfällen**

Anbieter und Hersteller MÜSSEN für die Kommunikation im Rahmen von TI-Notfällen Kommunikationsschnittstellen per E-Mail und Telefon bereithalten. ⌫

Zusammenstellung des Lösungsteams

Das Lösungsteam wird durch das EMC eingesetzt. Die Zusammensetzung des Lösungsteams kann im Laufe der TI-Notfallbewältigung durch das EMC verändert werden.

Durchführung der Notfallmaßnahmen

Das Lösungsteam wird die geeigneten TI-Notfallmaßnahmen identifizieren, diese zusammen mit dem EMC hinsichtlich Aufwand, Durchführbarkeit und Wirkung bewerten und sie dem EMC zur Freigabe vorlegen. Die Freigabe erfolgt durch die Mitglieder des EMC.

Die freigegebenen Maßnahmen werden durchgeführt und deren Erfolg geprüft.

Notfalldeeskalation

Nach erfolgreich durchgeführten TI-Notfallmaßnahmen wird der SBV die Beseitigung des TI-Notfalls bzw. die Erreichung des Notbetriebs bestätigen und den TI-Notfall formell deeskalieren.

Auflösung des EMC

Nach der Deeskalation des TI-Notfalls wird der SBV das EMC auflösen. Mit der Auflösung des EMC endet die Dokumentation in Form des TI-Notfall-Logbuchs. Das TI-Notfall-Logbuch wird direkt im Anschluss an die Auflösung in elektronischer Form an die Teilnehmer des EMC und des Lösungsteams verteilt.

10.5.5 Wiederherstellung

Der SBV wird im Anschluss der EMC Auflösung, die Wiederherstellung veranlassen. Die Wiederherstellung hat zum Ziel, den Betriebszustand zu erreichen, welcher vor Eintreten

des TI-Notfalls bestand. Die erfolgreiche Wiederherstellung wird in Form eines Wiederherstellungsberichtes an die Teilnehmer des EMC und des Lösungsteams gemeldet.

⌦ **GS-A_4132 Durchführung der Wiederherstellung und TI-Notfällen**

Anbieter und Hersteller MÜSSEN alle Aktivitäten, welche der Erreichung und Stabilisierung des Leistungsumfangs im eigenen Verantwortungsbereich dienen, durchführen und dokumentieren. ⌫

10.5.6 Rollback-Verfahren

Der SBV wird kurz darauf das Rollback-Verfahren veranlassen. Das erfolgreiche Rollback-Verfahren wird in Form eines Rollback-Berichtes an die Teilnehmer des EMC und des Lösungsteams gemeldet.

⌦ **GS-A_4133 Rollback-Verfahren nach TI-Notfällen**

Anbieter und Hersteller MÜSSEN die interimistischen und im Zuge der Sofortmaßnahmen installierten Notfallhandlungen zurücknehmen und dokumentieren. ⌫

10.5.7 Nachbearbeitung/Notfallauswertung

⌦ **GS-A_4134 Auswertungen von TI-Notfällen**

Anbieter und Hersteller MÜSSEN nach Abschluss der TI-Notfallbewältigung den TI-Notfall hinsichtlich seiner Ursache, Auswirkung, Dauer, Wahrscheinlichkeit eines erneuten Eintritts und der Angemessenheit der ergriffenen Maßnahmen zur TI-Notfallbewältigung auswerten. Die Auswertungsergebnisse sind zusammen mit TI-Notfall-Logbuch, Widerherstellungsbericht, Rollback-Bericht an den zuständigen SBV zu übergeben. ⌫

Notfallauswertung

Der SBV wird nach Bewältigung der in seinem Verantwortungsbereich eingetretenen TI-Notfälle eine Auswertung vornehmen. Der SBV wird dabei untersuchen, ob die im Rahmen der Notfallplanung festgelegten Abläufe und Maßnahmen für die Bewältigung des TI-Notfalls geeignet und ausreichend und ob weitere von ihm getroffenen Entscheidungen und Maßnahmen angemessen für eine effiziente TI-Notfallbewältigung waren. Mit erfolgter Notfallauswertung sind die Notfallvorsorgemaßnahmen/Notfallplan zu validieren und bei erkanntem Bedarf zu optimieren.

10.5.8 Service Level Requirements (SLR)

⌦ **GS-A_4135 Service Level Requirements Anbieter und Hersteller**

Anbieter und Hersteller MÜSSEN mindestens folgende Service Level messen und berichten:

Tabelle 25: Tab_Betr_TIP_022 Notfallmanagement - SLR A/H „Serviceerbringung"

ID	Qualitäts-dimension	Beschreibung	Typ	Beispiel
NM_1	Rufbereitschaft	Feststellung, Prüfung und Bearbeitung von TI-Notfällen anhand der schwerwiegenden, übergreifenden Incidents mit den Prioritäten 1-2 außerhalb der Servicezeiten.	MO [hh:mm] – [hh:mm], DI [hh:mm] – [hh:mm], MI [hh:mm] – [hh:mm], DO [hh:mm] – [hh:mm], FR [hh:mm] – [hh:mm], SA [hh:mm] – [hh:mm], SO [hh:mm] – [hh:mm]	MO 00:00 -24:00

Service Level werden in den spezifischen Betriebskonzepten produkttypspezifisch definiert. ⌫

10.6 Informationspflichten

⌦ **GS-A_4136 Statusinformation bei TI-Notfällen**

Anbieter und Hersteller, die von einem TI-Notfall betroffen sind, MÜSSEN im Rahmen der TI-Notfallbewältigung den SBV ständig über den aktuellen Status der Durchführung der TI-Notfallmaßnahmen informieren. Sie haben gegenüber SBV eine ständige Informationspflicht.⌫

Anbieter und Hersteller werden im Rahmen der Teilnahme am EMC mit den notwendigen Informationen zur TI-Notfallbewältigung versorgt**.**

10.7 Dokumentation

TI-Notfall-Logbuch

⌦ **GS-A_4137 Dokumentation im TI-Notfall-Logbuch**

Anbieter und Hersteller MÜSSEN zu jedem TI-Notfall ein TI-Notfall-Logbuch erstellen.

Anbieter und Hersteller MÜSSEN im Rahmen der TI-Notfallbewältigung im eigenen Verantwortungsbereich folgende Angaben im TI-Notfall-Logbuch dokumentieren:

- Zeit (Wann?),
- Verantwortung (Wer?),
- Durchführung (Was, Wie?) und
- Ergebnis einer Maßnahme.

Anbieter und Hersteller MÜSSEN dabei das TI-Notfall-Logbuch in Phasen von Notfallbekanntwerden bis -deeskalation ständig aktualisieren. ⌫

Wiederherstellungsbericht

⌦ **GS-A_4138 Erstellung des Wiederherstellungsberichts nach TI-Notfällen**

Anbieter und Hersteller MÜSSEN zu jeder Wiederherstellung in der TI-Notfallbewältigung einen Wiederherstellungsbericht erstellen.

Anbieter und Hersteller MÜSSEN einen Wiederherstellungsbericht mit allen durchgeführten Aktionen und Änderungen sowie Angaben zu Erfolg und Misserfolg jeder einzelnen Aktivität im eigenen Verantwortungsbereich, welche im Rahmen der Wiederherstellung durchgeführt wurden, erstellen. ⌫

Rollback-Bericht

⌦ **GS-A_4139 Rollback-Bericht nach TI-Notfällen**

Anbieter und Hersteller MÜSSEN zu jedem Rollback in der TI-Notfallbewältigung einen Wiederherstellungsbericht erstellen.

Anbieter und Hersteller MÜSSEN einen Rollback-Bericht mit allen durchgeführten Aktionen und Änderungen sowie Angaben zu Erfolg und Misserfolg jeder einzelnen Aktivität im eigenen Verantwortungsbereich, welche im Verlauf des Rollback-Verfahrens durchgeführt wurden, erstellen. ⌫

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
A/H	Anbieter und Hersteller
CAB	Change Advisory Board
CHG	Change Management
CI	Configuration Item
CM	Configuration Management
CSV	Comma-Separated Values
EMC	Emergency Management Committee
FSC	Forward Schedule of Change
GBV TI	Gesamtbetriebsverantwortlicher der Telematikinfrastruktur
ID	Identifikationsnummer
INC	Incident Management
ITIL	IT Infrastructure Library
ITSM	IT-Service-Management
PE	Problemerkennender
PED	Professionelle Endnutzernahe Dienstleister
PERF	Performance Management
PLV	Problemlösungsverantwortlicher
PRO	Problem Management
RFC	Request for Change
RLM	Release Management
SBV	Servicebetriebsverantwortlicher
SLK	Service Level Katalog
SLM	Service Level Management
SLR	Service Level Requirements
SPOC	Single Point of Contact
SV	Serviceverantwortlicher
TI	Telematikinfrastruktur
UML	Unified Modeling Language
WDB	Wissensdatenbank
ZID	Zentrale Informationsdrehscheibe

A2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

Abbildung 1: SLM - Prozessausschnitt „Service Level Management“.....26
Abbildung 2: PERF - Gesamtüberblick „Performance Management“.....31
Abbildung 3: CHG & RM - Gesamtkontext "Change & Release Management".....34
Abbildung 4: CHG - Gesamtüberblick „Change Management der Produkte“.....37
Abbildung 5: CM - Beziehung TI-Konfigurations-DB & lokal. Konfigurationssys. der A/H 49
Abbildung 6: CM - Gesamtüberblick "Configuration Management“.....50
Abbildung 7: CM - A/H-relevanter Ausschnitt TI-Konfigurationsdatenbank.....52
Abbildung 8: KM - Gesamtüberblick "Knowledge Management“ 56
Abbildung 9: INC - Gesamtüberblick "Incident Management".....59
Abbildung 10: INC - Vorprüfung im Anwendersupport.....63
Abbildung 11: INC - Strukturierte Informationsübermittlung im übergreifenden INC.....67
Abbildung 12: INC - Vorprüfung im Anbieter-/Herstellersupport 74
Abbildung 13: PRO - Gesamtüberblick "Problem Management“ 91
Abbildung 14: PRO - Vorprüfung problemerkennende Anbieter und Hersteller 94
Abbildung 15: PRO - Vorprüfung lösungsunterstützende Anbieter und Hersteller.....98
Abbildung 16: PRO - Vorprüfung problemlösungsverantwortlicher Anbieter und Hersteller 100
Abbildung 17: Notfallmanagement - Gesamtprozessschaubild "Notfallmanagement“ ...113
Abbildung 18: Notfallmanagement - Idealtypischer Ablauf TI-Notfallbewältigung 118

A4 – Tabellenverzeichnis

Tabelle 1: Tab_Betr_TIP_025 Bestandteile des konsolidierten Reportings 16
Tabelle 2: Tab_Betr_TIP_028 Übersicht Meldungstypen – Incident Management 21
Tabelle 3: Tab_Betr_TIP_029 Übersicht Meldungstypen – Problem Management.....21
Tabelle 4: Tab_Betr_TIP_026 reservierte Zeichen Ersetzungstabelle.....24
Tabelle 5: Tab_Betr_TIP_030 Basisfeldtypen von csv-Dateien.....24
Tabelle 6: Tab_Betr_TIP_023 SLM - Service Level "Performance".....27
Tabelle 7: Tab_Betr_TIP_002 SLM - Reportinhalte Service Level Report.....29
Tabelle 8: Tab_Betr_TIP_003 PERF - Reportinhalte von Performance Messungen 32

Tabelle 9: Tab_Betr_TIP_004 PERF-Performance-Messungen Anb. „Serviceerbringung” 33
Tabelle 10: Tab_Betr_TIP_024 CHG - Vorprüfung lokal./genehmig. Produktänderungsbedarf 39
Tabelle 11: Tab_Betr_TIP_005 CHG - Change Management - SLP "Prozess" 45
Tabelle 12: Tab_Betr_TIP_006 CHG - Reportinginhalte des CHG-Prozessreportings 47
Tabelle 13: Tab_Betr_TIP_007 CM - CI „Produktverantwortliche Organisation“.....52
Tabelle 14: Tab_Betr_TIP_008 CM - „CI Produkt“ 53
Tabelle 15: Tab_Betr_TIP_009 INC - Prioritätenmatrix 68
Tabelle 16: Tab_Betr_TIP_026 INC – Festlegung von Dringlichkeit.....68
Tabelle 17: Tab_Betr_TIP_027 INC – Festlegung von Auswirkung.....69
Tabelle 18: Tab_Betr_TIP_011 INC - SLR Anwendersupport “Prozess” 72
Tabelle 19: Tab_Betr_TIP_013 INC - SLR Anbieter-/Herstellersupport „Prozess“.....78
Tabelle 20: Tab_Betr_TIP_014 INC - Mindestinhalte Incident-Dokumentation.....82
Tabelle 21: Tab_Betr_TIP_016 PRO - SLR Problemerkennende A/H „Prozess”.....97
Tabelle 22: Tab_Betr_TIP_018 PRO - SLR Lösungsunterstützende A/H „Prozess”.....99
Tabelle 23: Tab_Betr_TIP_020 PRO - SLR PLVe A/H „Prozess“.....104
Tabelle 24: Tab_Betr_TIP_021 PRO - Mindestinhalte Problemdokumentation 106
Tabelle 25: Tab_Betr_TIP_022 Notfallmanagement - SLR A/H „Serviceerbringung”.....122
Tabelle 26: Tab_Betr_TIP_041 - Allgemeine Festlegungen zur WebService Schnittstelle 132
Tabelle 27: Tab_Betr_TIP_042 - Operation AddObject.....133
Tabelle 28: Tab_Betr_TIP_043 - Operation GetObjectList.....135
Tabelle 29: Tab_Betr_TIP_040 - Attribute der Objekttypen Incident und Problem.....137

A5 - Referenzierte Dokumente

A5.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Test_ORS1]	gematik: Testkonzept Online-Rollout (Stufe 1)
[gemSpec_DSM]	gematik: Koordinierendes Datenschutzmanagement der Telematikinfrastruktur
[gemSpec_ISM]	gematik: Koordinierendes Informationssicherheitsmanagement der Telematikinfrastruktur
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_Perf]	gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform
[gemSpec_SiBetrUmg]	gematik: Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI 100-4]	BSI-Standardreihe zur Informationssicherheit: 100-4 Notfallmanagement Version 1.0 (2008) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109
[BDSG]	Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (20.12.1990 (neugefasst durch Bek. 14.01.2003, Letzte Änderung vom 14.08.2009): Bundesdatenschutzgesetz
[ISO 8601]	ISO 8601:2000: Data elements and interchange formats – Information interchange – Representation of dates and times
[OMNI WSDL]	omnitracker.wsdl Version 10.3.200 (build 6408) Namespace http://www.omninet.de/OtWebSvc/v1
[OMNI MANUAL]	OMNITRACKER Web Service Manual, The OMNINET Problem and Request Tracking System Version 10.3 (build 6408)
[RFC2617]	RFC 2617 (Juni 1999): HTTP Authentication: Basic and Digest Access Authentication http://tools.ietf.org/html/rfc2617
[RFC2616]	RFC 2616 (Juni 1999): Hypertext Transfer Protocol -- HTTP/1.1 http://tools.ietf.org/html/rfc2616
[BSI TR-02102]	BSI TR-02102-2 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS)" https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.html

Anhang B – Management der Test- und Referenzumgebung im ORS1

Organisation des anbieter- und herstellerübergreifenden Betriebes der Test- und Referenzumgebung in der Erprobungsphase (ORS1)

Die benötigten Produkte für die im ORS1 definierten Anwendungs- und Basisservices werden in der Produktivumgebung betrieben und erprobt.

Parallel wird eine Referenzumgebung (RU) und eine Testumgebung (TU) während der Erprobungsphase benötigt, um Testungen und Zulassungen von Änderungen an Produkten im Rahmen der Entwicklung, Fehlerbehebung, Optimierung und Erweiterung der definierten Basis- und Anwendungsservices durchzuführen.

Die Service Provider der Erprobungsphase stellen dazu Instanzen ihrer Produkte für die Referenzumgebung und die Testumgebung bereit und betreiben diese.

Nutzer der **Referenzumgebung** in der Erprobungsphase sind die am ORS1 teilnehmenden Service Provider bzw. deren beauftragten Anbieter und Hersteller sowie weitere durch die gematik autorisierte Industrieunternehmen mit berechtigtem Interesse zur Nutzung.

Die Organisation des Betriebes der Referenzumgebung wird gemäß Testkonzept [gemKPT_Test_ORS1] vom Testbetriebsverantwortlichen (TBV)[1] verantwortet. Mit der Wahrnehmung der Rolle TBV für die Referenzumgebung wird der Service Provider zentrale Plattformdienste (Los 3) beauftragt werden. Der TBV koordiniert die Bereitstellung der Referenzumgebung im Auftrag der gematik.

Nutzer der **Testumgebung** ist die gematik als testdurchführende Instanz[2]. Die Organisation des Betriebes der Testumgebung wird gemäß Testkonzept [gemKPT_Test_ORS1] vom TBV verantwortet. Mit der Wahrnehmung der Rolle TBV für die Testumgebung wird der Service Provider Zentrale Plattformdienste (Los 3) beauftragt. Der TBV koordiniert die Bereitstellung der Testumgebung im Auftrag der gematik.

Der Betrieb der Produkte in der Referenz- und Testumgebung erfolgt analog zur Produktivumgebung im Rahmen der Erbringung der Anwendungs- und Basisservices für die Anwender in der Erprobungsphase. Es bestehen dieselben Leistungsbeziehungen zwischen den beteiligten Service Providern im Rahmen der Bereitstellung der Serviceeinheiten.

Die übergreifende Richtlinie zum Betrieb der TI [gemRL_Betr_TI] gilt sinngemäß für den Betrieb der Referenz- und Testumgebung im Rahmen der Erprobungsphase. Im Folgenden werden Hinweise zur Anwendbarkeit der übergreifenden Richtlinie zum Betrieb der TI für das Management der Referenz- und Testumgebung aufgeführt.

---

[1] Zur Definition der Rolle Testbetriebsverantwortlicher (TBV) siehe Testkonzept [gemKPT_Test_ORS1]

[2] Zur Definition der Rolle Testdurchführende Instanz siehe Testkonzept [gemKPT_Test_ORS1]

Hinweise zur Anwendung der übergreifenden Richtlinien zum Betrieb der TI für das Management der Referenz- und Testumgebung

Scope der IT-Service-Management-Prozesse im Rahmen des Betriebs der Referenz- und Testumgebung ist die Koordination der zeit- und bedarfsgerechten Bereitstellung der notwendigen Konfiguration der Referenz- und Testumgebung für und der ordnungsgemäße Betrieb der Referenz- und Testumgebung während der Testdurchführung.

Bezüglich der Durchführung der IT-Service-Management-Prozesse sind folgende Hinweise und Abweichungen zu beachten:

Service Level Management

Getroffene Regelungen des Service Level Managements gelten uneingeschränkt im Betrieb der Referenz- und Testumgebung.

Performance Management

Getroffene Regelungen des Performance Managements gelten uneingeschränkt im Betrieb der Referenz- und Testumgebung.

Change & Release Management

Getroffene Regelungen des Change & Release Managements gelten sinngemäß im Betrieb der Referenz- und Testumgebung. Betrachtungsgegenstand im Management der Referenz- und Testumgebung sind Änderungsanforderungen der gematik (bzw. des von ihr beauftragten TBV) zur Umsetzung in der Referenz- und Testumgebung, die Regelungen der Richtlinie sind sinngemäß anzuwenden.

Changekoordinator ist der TBV. Der TBV ist gegenüber der gematik verantwortlich für die zeitgerechte Bereitstellung der Referenz- und Testumgebung zur Durchführung von Testaktivitäten. Nutzer der Testumgebung ist die gematik, Nutzer der Referenzumgebung sind die am ORS1 teilnehmenden Service Provider bzw. deren beauftragten Anbieter und Hersteller sowie weitere durch die gematik autorisierte Industrieunternehmen mit berechtigtem Interesse.

Für die Testumgebung werden im Rahmen des Aufbaus und der Erprobung Standard Changes zwischen gematik (bzw. des von ihr beauftragten TBV) und den Service Providern definiert. Ziel ist eine zeitgerechte Bereitstellung von bekannten Testumgebungskonfigurationen (Baseline) durch die Service Provider um eine zügige Testbereitschaft in der Testumgebung herzustellen.

„Non Standard“ Changes (unbekannte Konfigurationen) müssen gemäß dem regulären Change Prozess durchgeführt werden.

Der TBV richtet eine Kommunikationsschnittstelle zur Kommunikation mit den Service Providern und der gematik ein.

Für die Bearbeitung von Änderungsanfragen durch den TBV gelten die vereinbarten Servicezeiten

Configuration Management

Getroffene Regelungen zum Configuration Management gelten uneingeschränkt im Betrieb der Referenz- und Testumgebung.

Gegebenenfalls werden im Rahmen des Aufbaus und der Erprobung testspezifische Ergänzungen an den zu übermittelnden Produktdaten vorgenommen.

Knowledge Management

Die Regelungen zum Wissensmanagement sind auf Erbringung der Anwendungs- und Basisservices gegenüber dem Leistungserbringer als Anwender ausgelegt und müssen für den Betrieb der Referenz- und Testumgebung durch die Anbieter und Hersteller sinngemäß angewendet werden.

Incident Management

Getroffene Regelungen zum Incident Management gelten sinngemäß im Betrieb der Referenz- und Testumgebung.

Die Incident-Management-Prozesse sind in den Richtlinien für die Bearbeitung von Störungen ausgeprägt, die eine anbieter- bzw. herstellerübergreifende Kommunikation im Rahmen der Incident Bearbeitung bedürfen. Es wird dabei unterschieden, ob es sich um den Support von Anwendern als (unqualifizierter) Melder oder einen Anbieter bzw. Hersteller als (qualifizierten) Melder handelt. Nutzer der Testumgebung ist ausschließlich die gematik als testdurchführende Instanz. Nutzer der Referenzumgebung sind die am ORS1 teilnehmenden Service Provider bzw. deren beauftragten Anbieter und Hersteller sowie weitere durch die gematik autorisierte Industrieunternehmen mit berechtigtem Interesse. Anwender (LE) und Versicherte sind keine Nutzer der Referenz- und Testumgebung. Ein UHD wird nicht bereitgestellt. Regelungen zum Anwendersupport sind gegenstandslos.

Die gematik als Nutzer der Testumgebung wendet sich bei einer Störung in der Bereitstellung der Testumgebung an den TBV. Der TBV koordiniert die Behebung der Störung durch den jeweiligen lösungsverantwortlichen Service Provider. Es gelten die Regelungen zum Anbieter und Herstellersupport.

Fehler am Testobjekt, welche sich im Rahmen der Durchführung von Testfällen ergeben, werden nicht als Störung behandelt, sondern über die von der testdurchführenden Instanz bereitgestellten Verfahren zum Fehlermanagement verwaltet.

Für die Behebung von Störungen in der TU/RU durch den TBV gelten die vereinbarten Servicezeiten.

Eine allgemeine Rufbereitschaft für Service Provider und den TBV wird nicht definiert. Diese wird -für den Fall von Testaktivitäten außerhalb der Servicezeiten- fallweise vereinbart. Der Servicelevel „INC_7: Rufbereitschaft“ entfällt.

Problem Management

Getroffene Regelungen Problem Management gelten sinngemäß im Betrieb der Referenz- und Testumgebung.

Der TBV tritt hier in der Rolle des „problemerkennenden“ Anbieter und Herstellers auf.

Notfall Management

Getroffene Regelungen zur TI-Notfallvorsorge und -bewältigung gelten sinngemäß im Betrieb der Referenz- und Testumgebung.

Die Bereitstellung der Testumgebung hat Geschäftskritikalität in Bezug auf die Durchführung von Zulassungstest und Fehlerbehebung in der Produktivumgebung.

Anbieter und Hersteller haben etwaige Notfallvorsorgemaßnahmen auf Relevanz und Anwendbarkeit für die Referenz- und Testumgebung zu prüfen und ggf. anzuwenden. Umgebungsspezifische Notfallszenarien sind im Rahmen der TI-Notfallvorsorge zu prüfen.

Die Bereitstellung der Referenzumgebung ist nicht geschäftskritisch. Notfallvorsorgemaßnahmen für die Bereitstellung der Services der Referenzumgebung haben – nach Relevanzprüfung wie oben beschrieben - dem aktuellen Stand der Technik zu entsprechen.

Reporting

Getroffene Regelungen zum konsolidierten Reporting gelten uneingeschränkt für den Betrieb der Referenz- und Testumgebung.

Anhang C – Webservice-Schnittstelle

Im Folgenden wird die Webservice-Schnittstelle zum Webservice-basierten Austausch von Incidents und Problems definiert.

Die Definition erfolgt in drei Stufen:

1. Allgemeine Festlegungen für die einzelnen Ebenen der Schnittstelle mittels Tabelle Tab_Betr_TIP_041.
2. Festlegungen zu den verwendeten Operationen
   a. AddObject mittels Tabelle Tab_Betr_TIP_042
   b. GetObjectList mittels Tabelle Tab_Betr_TIP_043
3. Mapping der in den Operationen verwendeten Feldnamen auf die Schnittstellenübergreifend definierten Feldnamen in Kapitel 8 und 9 mittels Tabelle Tab_Betr_TIP_040.

Tabelle 26: Tab_Betr_TIP_041 - Allgemeine Festlegungen zur WebService Schnittstelle

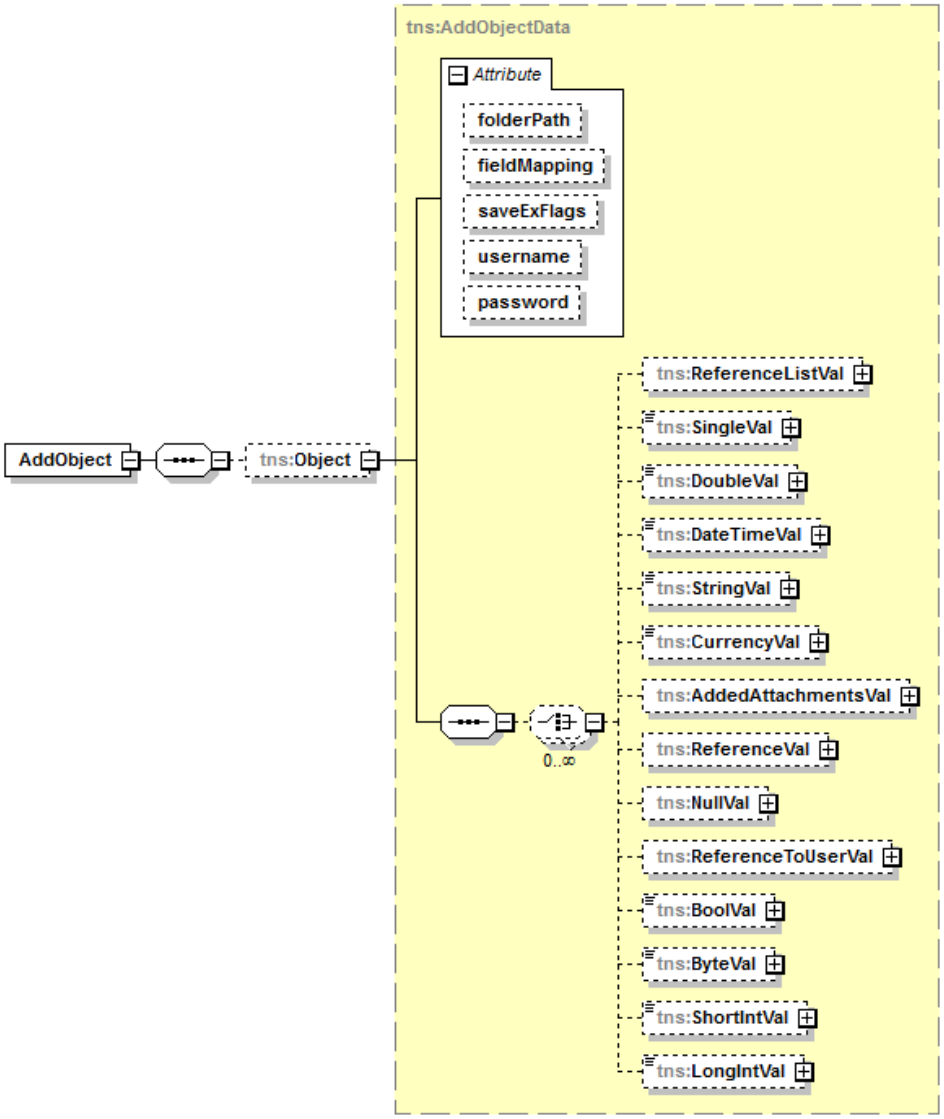
Aspekt	Festlegung
Client-Authentisierung	Per Basic Access Authentication gemäß [RFC2617], d.h. unter Verwendung von Username und Passwort.
Operationen	Von den in der WSDL aufgeführten Operationen • AddObject • ModifyObject • RemoveObject • InvokeScript • GetObjectList werden die Operationen • AddObject • GetObjectList verwendet. Ein Aufruf der Operationen per Input-Message • ModifyObject • RemoveObject • InvokeScript wird mit der in der WSDL definierten zugehörigen Output-Message mit dem Attribut „success“ gleich „false“ beantwortet.
WSDL	[OMNI WSDL]

Aspekt	Festlegung
SOAP	Versionen 1.1 und 1.2 werden wie in WSDL definiert vom Server unterstützt. Der Client hat die Wahl, mit welcher SOAP-Version er Aufrufe erzeugt.
http-Protokoll	Version 1.1 gemäß [RFC2616]
TLS	Serverseitige Authentisierung (eine Orientierung bieten die Vorgaben aus [BSI TR-02102].

Die Webservice-Schnittstelle des Produkts OMNITRACKER wird im Produkthandbuch [OMNI MANUAL] beschrieben.

Tabelle 27: Tab_Betr_TIP_042 - Operation AddObject

Name	`AddObject`
Beschreibung	Legt ein einzelnes Incident- oder Problem-Objekt an oder ändert Attribute für ein bestehendes Incident- oder Problem-Objekt. Bei Änderung eines bestehenden Objekts wird dieses über die `Referenznummer_T` adressiert. Die zu schreibenden Attribute für ein neues oder zu änderndes Objekt werden als Parameter übergeben. Die Unterscheidung nach Problem und Incident erfolgt über das Attribut „ITSM_Prozess_T“. Welche Attribute für einen Incident relevant sind und wie die innere Struktur der Attribute ist, definiert Kapitel 8, siehe Tab_Betr_TIP_014 INC - Mindestinhalte Incident-Dokumentation. Welche Attribute für ein Problem relevant sind und wie die innere Struktur der Attribute ist, definiert Kapitel 9, siehe Tab_Betr_TIP_021 PRO - Mindestinhalte Problemdokumentation. Zusätzlich ist bei jedem neu anzulegenden Incident bzw. Problem das Attribut „Zeitstempel“ mitzugeben. Die jeweils relevanten Attribute aus Tab_Betr_TIP_014 und Tab_Betr_TIP_021, sind als Parameter als Kindelemente unter tns:Object einzufügen, wobei Name und Typ aus „Tab_Betr_TIP_040 - Attribute der Objekttypen Incident und Problem“ zu verwenden sind. Der Typ bestimmt den XML-Elementtypen, etwa „tns:StringVal“, während der Name den Wert des Attributs „name“ vorgibt.

Name	AddObject
Aufruf-parameter	

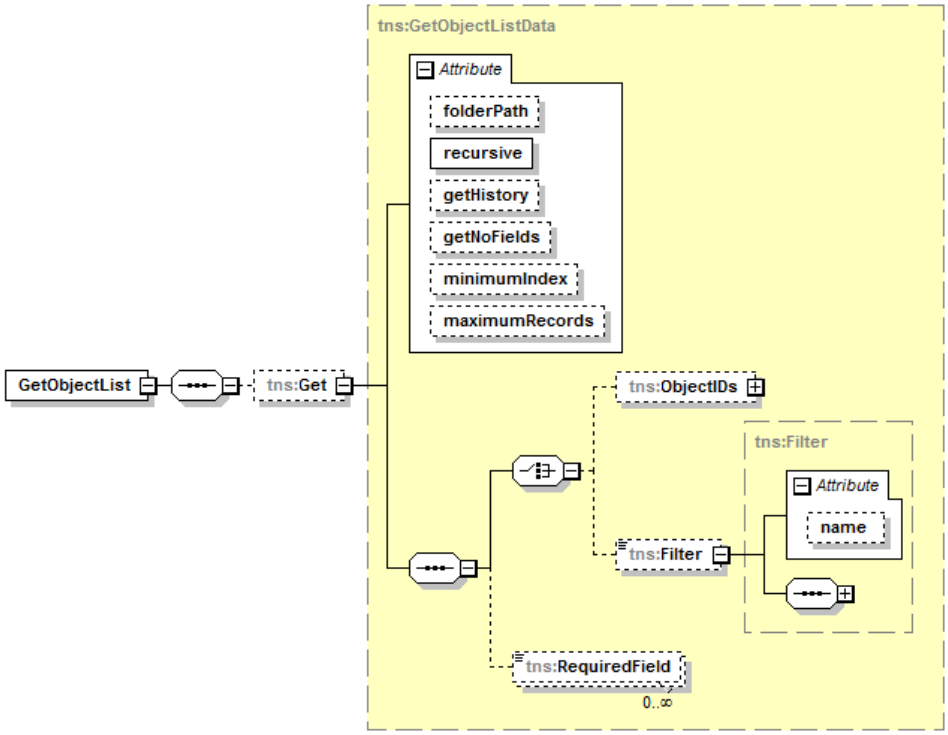
Name	Beschreibung
`folderPath`	“FLD_ZID\FLD_ZID_Kommunikation”
`fieldMapping`	nicht zu füllen
`saveExFlags`	nicht zu füllen
`username`	nicht zu füllen Hinweis: username/password wird im Rahmen der http basic authentication über den http-header übergeben
`password`	nicht zu füllen
`<tns:StringVal name="ITSM_Prozess_T">INC</tns:StringVal>`	Falls Incident

	`<tns:StringVal name="ITSM_Prozess_T">PRO</tns:StringVal>`	Falls Problem
	`<tns:StringVal name="Referenznummer_T">%ID%</tns:StringVal>`	Falls ein bestehender Incident bzw. Problem geändert werden soll, muss seine %ID% als Referenznummer_T mitgegeben werden.
Rückgabe		

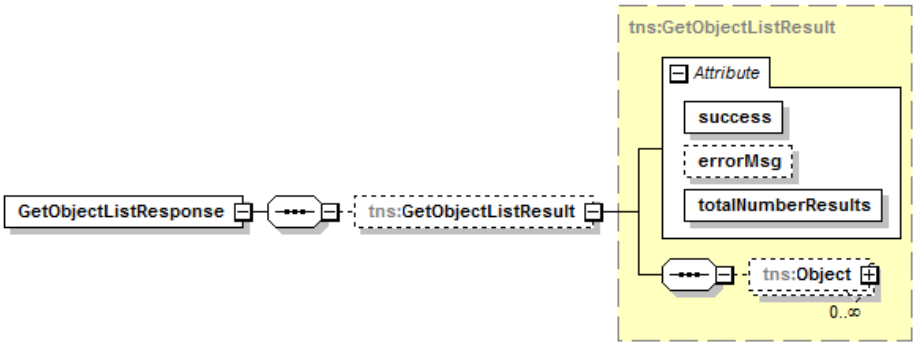
Name	Beschreibung
`success`	- true, wenn erfolgreich, und - false, wenn nicht erfolgreich
`objectId`	Enthält die OMNITRACKER interne ID des neu angelegten Incident bzw. Problem
`errorMsg`	Enthält eine Fehlernachricht, wenn success = false

Tabelle 28: Tab_Betr_TIP_043 - Operation GetObjectList

Name	**GetObjectList**
Beschreibung	Ruft die Liste aller für den Benutzer (identifiziert über Username/Passwort im Rahmen der http basic authentication) verfügbaren Problems oder Indidents auf. Alternativ kann ein spezielles Problem oder ein spezieller Incident per ID abgerufen werden. Andere Abrufe sind nicht möglich (z. B. mehrere IDs abzurufen).

Name	GetObjectList
Aufruf-parameter	

Name	Beschreibung
`folderPath`	Im Fall eines Incidents: “ServiceDesk\Incidents“ Im Fall eines Problems: „ServiceDesk\Problems“
`recursive`	Im Fall true werden auch abgeschlossene Tickets zurückgeben, im Fall false nur offene Tickets
`getHistory`	nicht zu füllen
`getNoFields`	nicht zu füllen
`minimumIndex`	nicht zu füllen
`MaximumRecords`	nicht zu füllen
`tns:Filter`	Um einen speziellen Incident bzw. Problem mit der ID %ID% abzurufen, ist das Element wie folgt zu füllen: `<tns:Filter>ZID<tns:StringVal name="Referenznummer_T">%ID%</tns:StringVal></tns:Filter>` Um alle für den Benutzer sichtbaren Incidents bzw. Problems abzurufen, ist das Element `tns:Filter` wegzulassen.
`tns:RequiredField`	Jedes Feld, das ausgelesen werden soll, ist über `tns:RequiredField` anzugeben. (Es werden nicht automatisch alle Felder eines Incidents bzw. Problems ausgelesen.)

Name	GetObjectList
Rückgabe	

Name	Beschreibung
`success`	- true, wenn erfolgreich, und - false, wenn nicht erfolgreich
`errorMsg`	Enthält eine Fehlernachricht, wenn success = false
`totalNumberResults`	die Anzahl der zurückgelieferten Results
`tns:Object`	Es werden die angefragten Problems bzw. Incidents jeweils als einzelne Objects mit den angefragten Attributen zurückgegeben.

Tabelle 29: Tab_Betr_TIP_040 - Attribute der Objekttypen Incident und Problem

Incident	Problem	Name	Typ
Incident Bearbeiter	Problemlösungsverantwortlicher ID	Bearbeiter_T	StringVal
Incident Beschreibung	Problem Beschreibung	Beschreibung_T	StringVal
Betroffene Betriebsumgebung	Betroffene Betriebsumgebung	Betroffene_BU_T	StringVal
Datenschutzrelevanz		Datenschutzrel_T	StringVal
Eskalation	Eskalation	Eskalation_T	StringVal
ITSM-Prozess	ITSM-Prozess	ITSM_Prozess_T	StringVal
Kategorie betroffenes Produkt	Kategorie	Kat_Betr_Produkt_T	StringVal
Kategorie verursachendes Produkt		Kat_Verurs_Produkt_T	StringVal
Incident Lösung	Problem Lösung	Loesung_T	StringVal
Incident Melder	Problemerkennender ID	Melder_T	StringVal
Meldungstyp	Meldungstyp	Meldungstyp_T	StringVal
Priorität	Priorität	Prioritaet_T	StringVal
Incident ID	Problem ID	Referenznummer_T	StringVal

Incident	Problem	Name	Typ
Sicherheitsrelevanz	Sicherheitsrelevanz	Sicherheitsrel_T	StringVal
Incident Status	Problem Status	Status_T	StringVal
TI Notfall		TI_Notfall_T	StringVal
Incident Worklog	Problem Worklog	Worklog_T	StringVal
Zeit Ende	Zeit Ende	Zeit_Ende_T	StringVal
Zeit Erfassung	Zeit Erfassung	Zeit_Erfassung_T	StringVal
Zeit Lösung	Zeitpunkt Lösung	Zeit_Loesung_T	StringVal
Zeit Weiterleitung		Zeit_Weiterleitung_T	StringVal
Zeitstempel	Zeitstempel	Zeitstempel_T	StringVal
Incident Zieltermin		Zieltermin_T	StringVal
	RfC ID	RFC_ID_T	StringVal
	Zeitpunkt Verifizierung	Zeit_Verifizierung_T	StringVal

Bei jeder Informationsübermittlung per Webservice-Schnittstelle sind unabhängig vom Meldungstyp die in der GS-A_5200 definierten Daten sowie die TID des Empfängers des Kommunikationsvorganges zu übermitteln.

Die Übermittlung eines neuen Incidents oder Problems (d. h. die Referenz-ID ist neu und der ZID bisher noch nicht mitgeteilt worden) kann nur mit dem Meldungstyp „WE“ (Weiterleitung) erfolgen.

Bei den in der obigen Tabelle aufgeführten Zeitfeldern handelt es sich durchgängig um Zeitpunkte und **nicht** um Zeiträume.

Zur Erreichbarkeit der Webservice-Schnittstelle werden die benötigten Adressen (URLs) in der Wissensdatenbank bekannt gegeben (getrennt nach SOAP 1.1 und SOAP 1.2 und getrennt nach Test- und Produktivumgebung).