gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation

Service Monitoring

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

ENTWURF

Version:	1.0.0 CC
Revision:	\main\rel_opb1\rel_ors2\14
Stand:	16.02.2018
Status:	Entwurf
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	[gemSpec_ServiceMon]

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
	31.01.18		initiale Erstellung	gematik
1.0.0 CC	16.02.18		zur Abstimmung freigegeben	gematik

ENTWURF

Inhaltsverzeichnis

Dokumentinformationen **2**

Inhaltsverzeichnis **3**

1 Einordnung des Dokumentes **5**

1.1 Zielsetzung **5**

1.2 Zielgruppe **5**

1.3 Geltungsbereich **5**

1.4 Abgrenzungen **5**

1.5 Methodik **6**

2 Systemüberblick **7**

3 Zerlegung des Produkttyps **10**

4 Übergreifende Festlegungen **12**

4.1 Implementierung des Service Monitorings **12**

4.1.1 Verwendung von Standardprodukten 12

4.1.2 Administration und Konfiguration 12

4.1.3 Nutzeroberfläche 15

4.1.4 Dokumentation 15

4.2 Betrieb des Service Monitorings **15**

4.2.1 Verfügbarkeits- und Durchsatzanforderungen 15

4.2.2 Speicherungsdauer der übermittelten Daten 16

4.3 Zugriffs- und Berechtigungskonzept **16**

4.3.1 Zugriffskonzept 16

4.3.2 Berechtigungskonzept 16

5 Funktionsmerkmale **20**

5.1 Schnittstelle I_View_Service_Monitoring **20**

5.1.1 Darstellung der Monitoring-Daten 20

5.1.2 Schnittstelle View Service Monitoring API Web Service 21

5.1.3 Umsetzung 23

5.2 Schnittstelle I_Monitoring_Update **23**

5.2.1 Schnittstellendefinition 23

5.2.2 Umsetzung 25

5.2.3 Nutzung 26

5.3 Technische Use Cases – TUCs **29**

5.4 Probes **31**

ENTWURF

5.4.1 DNS Name Resolution 34
5.4.2 Konnektorregistrierung 35
5.4.3 VPN_Tunnel 37
5.4.4 VPN_Tunnel SIS 39
5.4.5 Zeitinformation_TI 40
5.4.6 Zeitinformation_VPN_Zugangsdienst 41
5.4.7 CRL Download 41
5.4.8 TSL Download 42
5.4.9 TSL Download mit Prüfung 43
5.4.10 TSL Download IPsecTunnel TI 44
5.4.11 TSL Download Internet 44
5.4.12 BNetzA_VL Download 45
5.4.13 BNetzA Download IPsecTunnel TI 46
5.4.14 OCSP 46
5.4.15 OCSP IPsecTunnel TI 47
5.4.16 Fachdienste VSDM 48
5.4.16.1 Fachdienst VSDM UFS 48
5.4.16.2 Fachdienst VSDM_VSDD_CMS 49
5.4.17 Intermediär VSDM 51
5.4.18 VSDM- Intermediär VSDM IPsecTunnel TI 52
5.4.19 VSDM-Intermediär VSDM Erreichbarkeit 53
5.4.20 KSRS Upload 53
5.4.21 KSRS Download 54
5.4.22 KSRS Download IPsecTunnel TI 55
5.4.23 KSRS Download Bestandsnetze 56
5.4.24 KSRS Download Bestandsnetze IPsecTunnel TI 57
5.4.25 Verzeichnisdienst Query 57
5.4.26 Verzeichnisdienst Query IPsecTunnel TI 58
5.4.27 Verzeichnisdienst Application_Maintenance 59
5.4.28 Erfassung von Service Monitoring-Daten in Probes 60

5.5 Performance-Kenngrößen 62

Anhang A – Verzeichnisse 63

A1 – Abkürzungen 63

A2 – Glossar 63

A3 – Abbildungsverzeichnis 63

A4 – Tabellenverzeichnis 63

A5 – Referenzierte Dokumente 64
A5.1 – Dokumente der gematik 64
A5.2 – Weitere Dokumente 65

A6 – Fehlercodes 65

ENTWURF

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps Service Monitoring.

Das Service Monitoring überwacht ausgewählte Parameter, um den Betriebszustand der Telematikinfrastruktur und der Anwendungen der Gesundheitstelematik darzustellen. Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Service Monitorings.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter des Service Monitorings sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Leistungsbeschreibung) festgelegt und bekanntgegeben.

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 Abgrenzungen

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang A5).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps Service Monitoring verzeichnet.

ENTWURF

Detailspezifikationen zu den Monitoringdaten, d. h. zu den Ziel- und Messwerten für z. B. den Durchsatz, die Verfügbarkeit sowie für die Bearbeitungszeit sind in diesem Dokument nicht weiter dargestellt und der [gemSpec_Perf] für die TI-Plattform und für die Fachdienste zu entnehmen.

Weitergehende betriebliche Festlegungen sowie Details zu dem in diesem Dokument verwendeten Begriff „Serviceeinheiten“ sind [gemKPT_Betr] zu entnehmen.

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:

⌦ **gemxxxxxx_AFO_0000 <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

ENTWURF

2 Systemüberblick

Die folgende Abbildung zeigt die logischen Komponenten und die Außensicht des Service Monitorings.

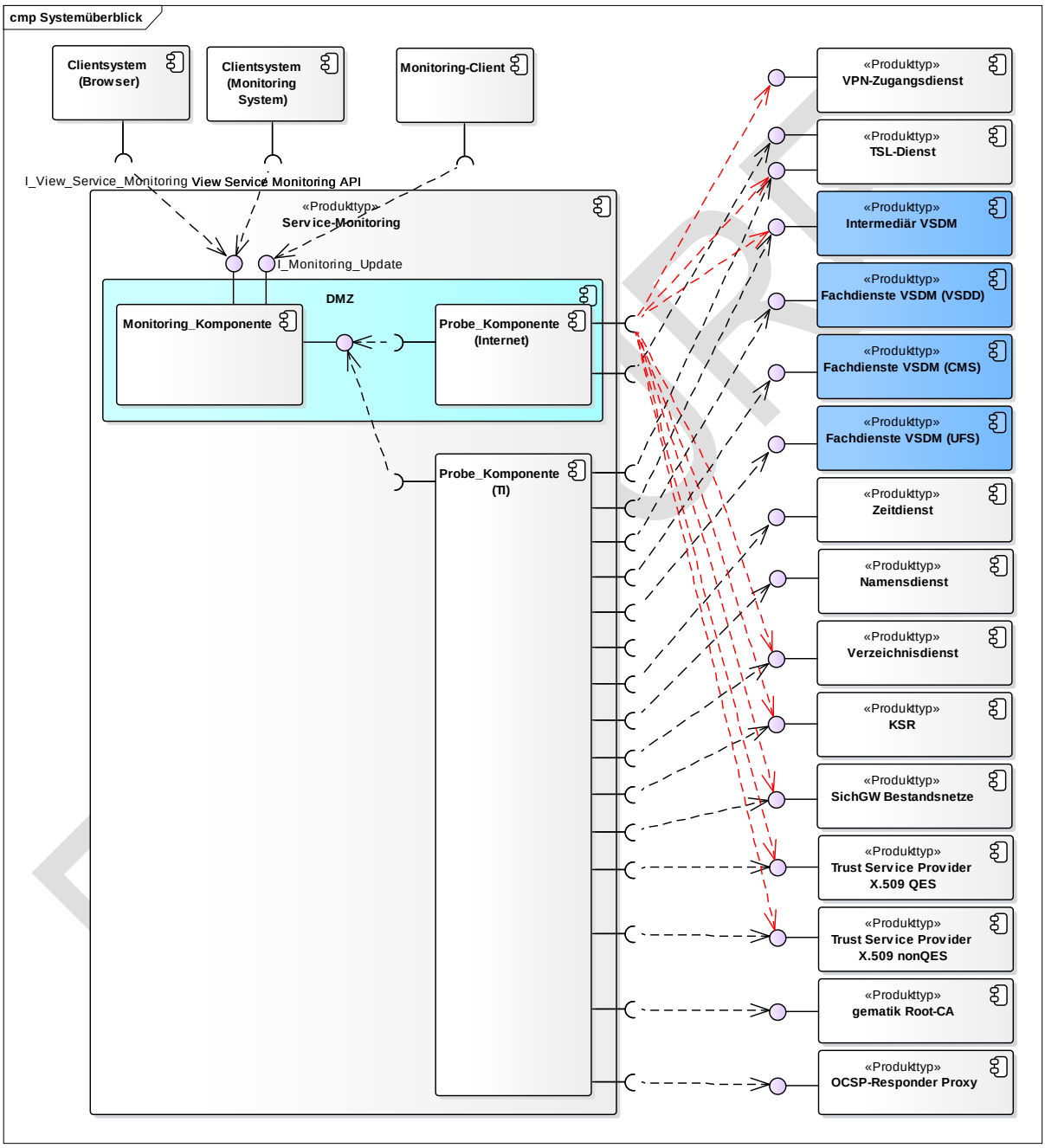

Abbildung 1: ABB_ServMon_301 Komponenten und Außensicht des Service Monitorings

Das Service Monitoring besteht logisch aus den Systemen Monitoring_Komponente, Probe_Komponente (Internet) und Probe_Komponente (TI).

Über die Probe_Komponenten wird die Verfügbarkeit der Dienste der TI im zentralen Netz der TI und im Internet mittels Probes überwacht. Die in Rot dargestellten Kommunikationsbeziehungen benötigen einen bestehenden IPsec-Tunnel der TI.

Die Ergebnisse der Probes-Messungen werden über eine interne Schnittstelle an die Monitoring_Komponente zur Weiterverarbeitung übertragen.

Die folgende Abbildung zeigt zum besseren Verständnis des Dokuments beispielhaft verschiedene Daten-Ebenen (es wird aber keine Anzahl von konkreten Ebenen vorgegeben) des Service Monitorings und die entsprechenden Aggregationen/Korrelationen und die Quellen der Daten:

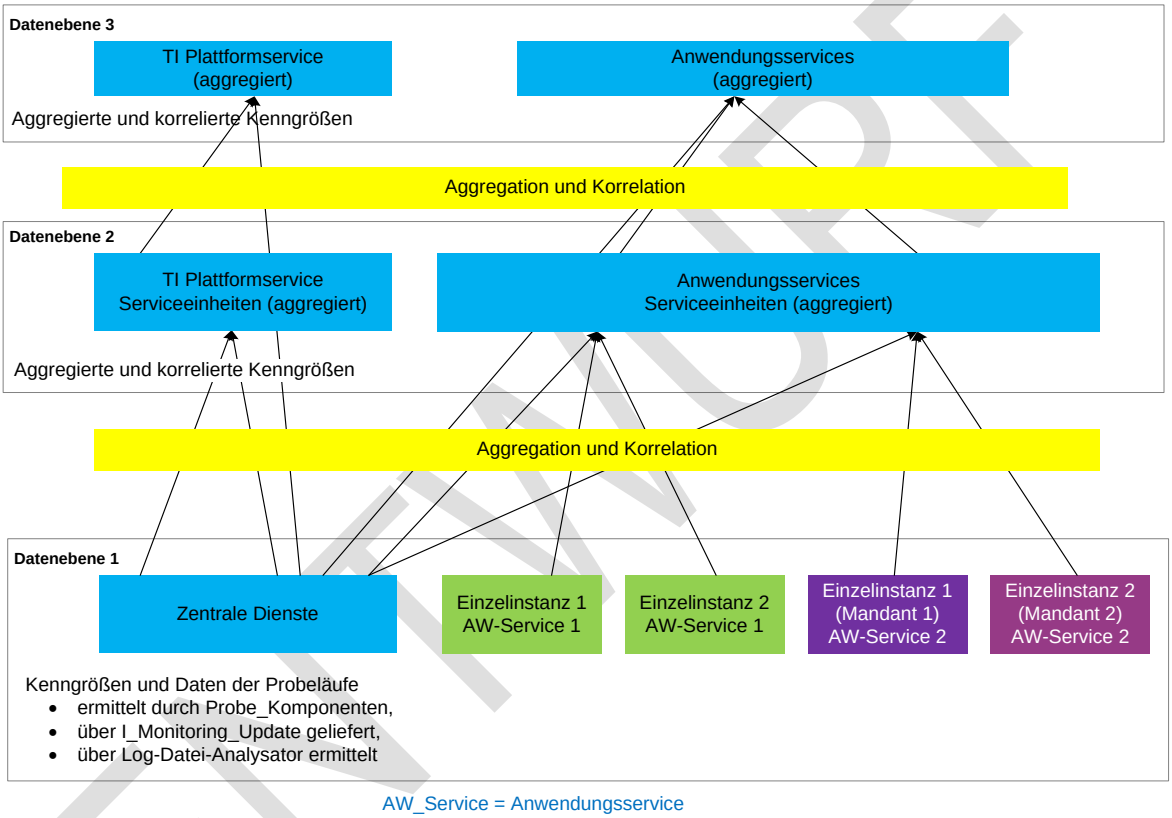

Abbildung 2: ABB_ServMon_303 Datenfluss Service Monitoring

Kenngrößen auf Datenebene 1 stammen aus verschiedenen Quellen:

- Probes ermitteln Kenngrößen und erzeugen Daten über den Probe-Lauf (z.B. Zeitpunkt und Erfolg).
- Über I_Monitoring_Update werden Kenngrößen von den Anwendungs-services/Diensten geliefert.
- Der Log-Datei-Analysator kann aus Log-Dateien Kennwerte extrahieren.

Kenngrößen auf höheren Datenebenen werden durch Aggregation bzw. Korrelation aus vorliegenden Kenngrößen erzeugt. Basis für die Aggregation bzw. Korrelation können vorliegende Kenngrößen und Probe-Lauf Daten auf verschiedenen Ebenen sein. Die

EINWURF

Aggregation bzw. Korrelation erfolgt Anwendungsservice- bzw. Plattformgrenzen übergreifend.

ENTWURF

3 Zerlegung des Produkttyps

Im Folgenden wird die Zerlegung des Service Monitorings dargestellt, welche für die Übersicht der funktionalen Leistungsmerkmale in vorliegender Spezifikation nötig ist.

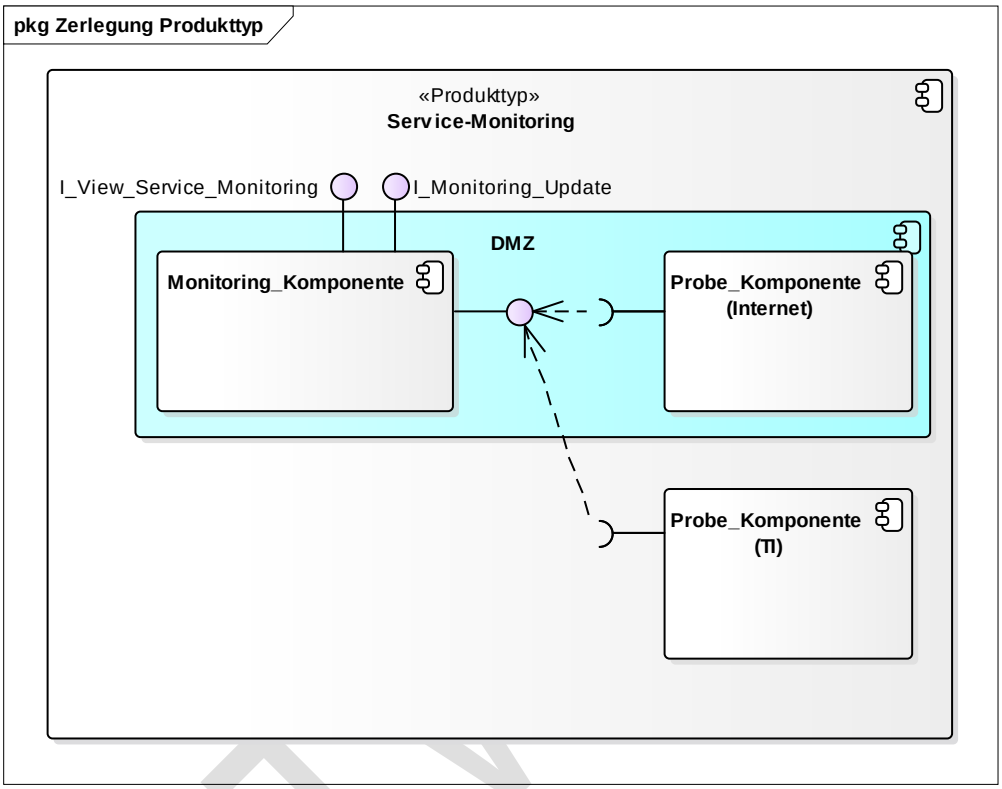

Abbildung 3: ABB_ServMon_300 – Komponentendiagramm des Service Monitorings

In Abbildung 3 werden die Komponenten des Service Monitorings dargestellt.

Die Probes greifen auf die überwachten Schnittstellen analog zu den normalen Clients dieser Schnittstellen aus dem Internet und aus der TI zu. Dafür werden zwei Probe-Komponenten vorgesehen:

- Probe_Komponente (Internet) und

  Alle Probes mit Zugriff aus dem Internet auf TI Schnittstellen.

- Probe_Komponente (TI).

  Alle Probes mit Zugriff aus der TI auf TI Schnittstellen.

Die Monitoring-Komponente stellt folgende Funktionalitäten bereit:

- Anzeige der aggregierten Monitoring-Daten in Webbrowsern (I_View_Service_Monitoring)
- Erlaubt übergeordneten Monitoring-Systemen den Zugriff auf Monitoring-Daten (I_View_Service_Monitoring)

- Entgegennahme von Performance-Daten von Anbietern (I_Monitoring_Update)
- Aggregation der Rohdaten (aus Probes und von den Diensten geliefert)
- Konfiguration des Service Monitorings (Aggregationsregeln, Darstellung der Daten, Benutzerverwaltung)

Die Probe-Komponenten stellen folgende Funktionalitäten bereit:

- Integration der einzelnen Probes in das Service Monitoring
- Ansteuerung der Probes und Entgegennahme der Probe-Ergebnisse
- Übertragung der Probe-Daten an die Monitoring-Komponente

Die Architektur des Service Monitorings sieht die Erweiterbarkeit um neue Funktionalitäten (z. B. Aufruf zusätzlicher Probes) vor, indem die bestehenden Schnittstellen im Komponentenmodell erweitert oder neue Schnittstellen zu den Komponenten hinzugefügt werden.

ENTWURF

4 Übergreifende Festlegungen

4.1 Implementierung des Service Monitorings

⌦ **TIP1-A_6739 Service Monitoring, Festlegung der bereitzustellenden Schnittstellen**

Das Service Monitoring MUSS die Schnittstellen I_View_Service_Monitoring und I_Monitoring_Update implementieren und bereitstellen.

⌫

Diese Schnittstellen werden in Kap. 5.1 und Kap. 5.2 näher definiert.

⌦ **TIP1-A_6740 Erreichbarkeit des Service Monitorings**

Das Service Monitoring MUSS die Schnittstellen I_Monitoring_Update in der TI und I_View_Service_Monitoring im Internet und der TI für Nutzer mit entsprechenden Rechten anbieten.⌫

4.1.1 Verwendung von Standardprodukten

⌦ **TIP1-A_6743 Verwendung von Standardprodukten**

Der Anbieter des Service Monitorings SOLL IT-Monitoring-Standardprodukte für das Service Monitoring verwenden. ⌫

4.1.2 Administration und Konfiguration

⌦ **TIP1-A_6745 Service Monitoring, Konfigurierbarkeit**

Das Service Monitoring MUSS so implementiert werden, dass Administratoren Berechtigungen, Schwellwerte, Aggregationsregeln und Probes konfigurieren können.

Die Konfigurationsdaten des Service Monitorings MÜSSEN persistent gespeichert werden sowie exportierbar und importierbar sein. ⌫

⌦ **TIP1-A_6746 Service Monitoring, Schwellwerte**

Das Service Monitoring MUSS die Konfiguration sowie den Export und Import von Schwellwerten für jede einzelne Performance-Kenngrößen erlauben. Die Über- bzw. Unterschreitung dieser Schwellwerte durch die Daten der dazugehörenden Performance-Kenngröße MUSS zur Markierung (z.B. in Grün, Gelb und Rot) der entsprechenden Werte in der Darstellung führen. Für jede Performance-Kenngröße MUSS die Angabe mehrerer Schwellwerte mit dazugehörender Kritikalität/Darstellungsfarbe möglich sein. ⌫

⌦ **TIP1-A_6747 Service Monitoring, Aggregationsregeln**

ENTWURF

Das Service Monitoring MUSS mindestens folgende Aggregationsregeln für alle Kenngrößen (also übergreifend für alle Dienste, Mandanten und aus allen Quellen ermittelte) unterstützen:

- Aggregation (z.B. Summe, Mittelwerte, Quantile, Maximal- und Minimalwerte) der Werte einer Kenngröße (inkrementelle Kennwerte und Gauges (Kennwerte, welche nicht inkrementell verarbeitet werden wie z.B. Temperatur oder Füllstand einer Queue)) für einen definierbaren Zeitraum.
- Aggregation mehrerer Kenngrößen und Daten von Probe-Lauf-Daten (z.B. Zuordnung von Kenngrößen zu Probe-Lauf-Ausführungen), welche im Zusammenhang stehen für einen definierbaren Zeitraum. Beispiele für solche Kenngrößen sind Ausführungszeiten von Teiloperationen, welche zusammengerechnet und deren Ergebnisse aggregiert werden müssen. Dabei MÜSSEN Kenngrößen aus verschiedenen Quellen (z.B. Probes, Schnittstelle I_Monitoring_Update und Kenngrößen, welche durch Aggregation im Service Monitoring ermittelt wurden) übergreifend verarbeitet werden können.
- Aggregation der Nicht-Verfügbarkeiten, welche durch Probes ermittelt werden mit Ausfallszeiten, welche vom Dienst gemeldet werden, und dem Wartungskalender.

Die Ergebnisse der Aggregation MÜSSEN als Kenngrößen in den aggregierten Service Monitoring Daten gespeichert werden und wie alle anderen aggregierten Daten darstellbar und auswertbar sein. ⌫

Für das Monitoring von komplexen Anwendungsfällen ist die direkte Ermittlung von Kenngrößen für den gesamten Anwendungsfall nicht immer direkt möglich. Deshalb besteht die Notwendigkeit der Aggregation und Darstellung von Teilschritt-Kenngrößen auf Anwendungsfallniveau.

⌦ **TIP1-A_7084 Service Monitoring, Konfiguration komplexer Anwendungsfälle**

Das Service Monitoring MUSS für komplexe Anwendungsfälle die folgenden Konfigurationen durch berechtigte Nutzer unterstützen:

- Definition der – zum Anwendungsfall gehörenden – Kenngrößen inklusive ihrer Aggregationsregeln
  - Kenngrößen mit Zeitangaben oder Anzahl können summiert sowie Mittelwerte und Abweichungen berechnet werden.
  - Verfügbarkeiten: Wenn eine Kenngröße Nichtverfügbarkeit anzeigt, ist der gesamte Anwendungsfall nicht verfügbar.
- Definition einer geeigneten Darstellung des Anwendungsfalls im GUI. Auf Nutzerwunsch MUSS:
  - der Anwendungsfall mit seinen aggregierten Daten als Ganzes sichtbar sein,
  - die Bestandteile des Anwendungsfalls mit ihren einzelnen aggregierten Daten sichtbar sein,

ENTWURF

- der Anwendungsfall nur sichtbar sein, wenn er nicht verfügbar ist bzw. ein oder mehrere Schwellwerte über- oder unterschritten werden.

⌫

⌦ **TIP1-A_7353 Service Monitoring, Konfiguration Dashboard**

Das Service Monitoring MUSS jedem Nutzer die Konfiguration eines eigenen Dashboards ermöglichen. Ein konfiguriertes Dashboard eines Nutzers MUSS von anderen Nutzern übernommen werden können. ⌫

⌦ **TIP1-A_7085 Service Monitoring, Wartungskalender**

Das Service Monitoring MUSS für jede Dienstinstanz einen Wartungskalender unterstützen. Der Wartungskalender MUSS das Eintragen von Wartungszeiträumen erlauben. Die Wartungszeiträume MÜSSEN bei der Berechnung und Darstellung der Verfügbarkeit dieser Dienstinstanz bzw. von übergreifenden Anwendungsfällen berücksichtigt werden. ⌫

⌦ **TIP1-A_7086 Service Monitoring, Alarmierung**

Das Service Monitoring MUSS eine konfigurierbare Alarmierung bei Störungen (Ausfall/Nichtverfügbarkeit, Über-/Unterschreitung von Schwellwerten) pro Kenngröße unterstützen. Als Alarmierungsziel MÜSSEN pro Kombination aus Kenngröße, Dienstinstanz und Mandant (falls der Dienst mandantenfähig ist) mindestens unterstützt werden:

- E-Mail Adressen
- SMS

Die Alarmierungsziele (Gruppen von E-Mail Adressen und/oder SMS Nummern) MÜSSEN in Abhängigkeit von Tageszeit und Wochentag/Feiertag gewählt werden können.

Die Alarmierung MUSS eine Eskalation beinhalten, wenn der Alarmierte die Bearbeitung nicht nach einer konfigurierbaren Zeit bestätigt.

Die Alarmierung MUSS wiederholte Alarmierungen zur gleichen Ursache (z.B. Ausfall eines Dienstes wird alle 5 Minuten gemeldet) unterdrücken können (nur eine Alarmierung wenn der Alarmierungszustand eintritt und (optional) wenn er endet).

Die Alarmierung MUSS eine Übersicht über die ausgelösten Alarmierungen und den Status der Alarmierung (offen, vom Bearbeiter bestätigt, …) darstellen können. ⌫

⌦ **TIP1-A_7087 Service Monitoring, Log-Datei-Analysator**

Das Service Monitoring MUSS einen Log-Datei-Analysator bereitstellen. Dieser Log-Datei-Analysator MUSS Log-Dateien von Diensten importieren, aus ihnen konfigurierbar Daten extrahieren und in den Service Monitoring-Datenbestand als Kenngrößen übernehmen können. Die Konfiguration für konkrete Log-Dateien MUSS für Administratoren möglich sein. ⌫

⌦ **TIP1-A_7088 Service Monitoring, Rechte der Nutzer gemäß Rolle**

Das Service Monitoring MUSS sicherstellen, dass ein Nutzer nur die Funktionen nutzen kann, die ihm gemäß seiner Rolle zugeteilt sind.⌫

ENTWURF

4.1.3 Nutzeroberfläche

⌦ **TIP1-A_7089 Nutzeroberfläche des Service Monitorings: Nutzeroberfläche**

Das Service Monitoring MUSS den Nutzern des Service Monitorings eine Nutzeroberfläche (I_View_Service_Monitoring) zur Verfügung stellen, welche den Zugriff auf die Betriebsstatusinformationen ermöglicht. ⌫

⌦ **TIP1-A_7091 Service Monitoring: Nutzerauthentifizierung für Konfigurationsaufgaben**

Das Service Monitoring MUSS mittels einer Authentifizierung sicherstellen, dass nur Nutzer mit entsprechenden Rechten die Konfiguration des Service Monitorings ändern können. ⌫

⌦ **TIP1-A_7092 Service Monitoring: Beschreibung Administrationsoberfläche**

Der Anbieter des Service Monitorings MUSS die Inhalte und Funktionen der Administrationsoberflächen sowie deren Nutzung beschreiben. ⌫

4.1.4 Dokumentation

⌦ **TIP1-A_7094 Protokollierung Nutzerzugriffe**

Das Service Monitoring MUSS alle durch die autorisierten Nutzer (inklusive der Administratoren) erfolgten übergreifenden (persönliche Einstellungen für z.B. eigene Dashboards fallen nicht darunter) Daten-, Konfigurations- und Einstellungsänderungen chronologisch in Form eines Auditlogs protokollieren und auswertbar zur Verfügung stellen.⌫

⌦ **TIP1-A_7095 Protokollierung Zugriffe durch autorisierte übergeordnete Monitoring Systeme**

Das Service Monitoring MUSS alle durch die autorisierten übergeordneten Monitoring-Systeme (I_View_Service_Monitoring) erfolgten Zugriffe und Einstellungsänderungen chronologisch in Form eines Auditlogs protokollieren und auswertbar zur Verfügung stellen. Der Zugriff auf die „Auditlogs“ MUSS rollenbasiert erfolgen.⌫

4.2 Betrieb des Service Monitorings

4.2.1 Verfügbarkeits- und Durchsatzanforderungen

Verfügbarkeits- und Durchsatzanforderungen für den Betrieb des Service Monitorings sind in der [gemSpec_Perf] vorgegeben.

⌦ **TIP1-A_6742 Monitoring des Service Monitorings**

Der Betreiber des Service Monitorings MUSS die Verfügbarkeit des Service Monitorings über ein eigenes IT-Monitoring-System erfassen und die Einhaltung der entsprechenden Anforderungen nachweisen.⌫

ENTWURF

4.2.2 Speicherungsdauer der übermittelten Daten

⌦ **TIP1-A_7096 Speicherungsdauer von übermittelten Daten an das Service Monitoring**

Das Service Monitoring MUSS ermöglichen, dass die Speicherungsdauer für an das Service Monitoring gelieferte Daten pro Dienst einstellbar ist.

Das Service Monitoring MUSS als Ausgangswert für die Speicherungsdauer ein Jahr für aggregierte Daten und 2 Monate für Rohdaten (über Schnittstelle I_Monitoring_Update gelieferte Daten) als Standardwert setzen und die Verkürzung und Verlängerung der Speicherungsdauer ermöglichen.

Die Verkürzung und Verlängerung der Speicherungsdauer MUSS möglich sein.⌫

Die Werte für die Speicherungsdauer werden vom GTI (Gesamtverantwortlicher TI) nach Bedarf festgelegt.

4.3 Zugriffs- und Berechtigungskonzept

4.3.1 Zugriffskonzept

⌦ **TIP1-A_7097 Zugriffsschutz gemäß Schutzbedarf**

Der Anbieter des Service Monitorings MUSS entsprechend des Schutzbedarfes der im Service Monitoring dargestellten und verarbeiteten Daten entsprechende Mechanismen zum Schutz vor unberechtigtem Zugriff umsetzen.⌫

4.3.2 Berechtigungskonzept

⌦ **TIP1-A_7352 Service Monitoring, Konfiguration Berechtigungen**

Das Service Monitoring MUSS Administratoren die Verwaltung von Nutzer erlauben und – auf Anfrage des GTI – eine Auflistung aller Nutzerkonten liefern können. ⌫

⌦ **TIP1-A_7098 Service Monitoring, Erteilung Einzel-Zugriffsberechtigungen**

Das Service Monitoring MUSS ein nachvollziehbares Zugriffskonzept vorsehen, über das zu jeder Zeit für Administratoren erkenn- und verwaltbar ist, welcher Nutzer welche Zugriffsberechtigungen hat. Dabei MUSS es mindestens folgende Zugriffsberechtigungen für Nutzer geben:

- Einsehen von Daten/Kenngrößen.
- Einsehen von Teilmengen von Daten. Die Einschränkungen der Daten MUSS mindestens für Instanzen von Diensten und – wenn der Dienst mandantenfähig ist – auf Mandanten der Dienste möglich sein.
- Konfiguration des Service Monitorings (z. B. Ausführungszeitpunkte von Probes, Konfiguration der Probes inklusive der benötigten Zertifikate und des Truststores).

⌫

ENTWURF

⌦ **TIP1-A_7111 Service Monitoring, Erteilung Einzel-Zugriffsberechtigungen**

Das Service Monitoring MUSS für Clients der Service Monitoring-Schnittstellen (z.B. I_View_Service_Monitoring API Web Service) ebenfalls die Definition von Zugriffsberechtigungen erlauben. Dabei entfallen die Rechte zur Konfiguration des Service Monitoring GUIs (Dashboards, …). Diese Zugriffsberechtigungen MÜSSEN auf die eigenen Daten des nutzenden Systems und die Daten aller für die Serviceerbringung nötigen Dienste beschränkbar sein.⌫

⌦ **TIP1-A_7099 Service Monitoring, Verbot Gruppenberechtigungen**

Das Service Monitoring DARF Gruppenberechtigungen NICHT vorsehen oder implementieren.

Es ist nicht zulässig, dass mehrere Nutzer eine Nutzerkennung verwenden. ⌫

⌦ **TIP1-A_6741 Service Monitoring, Zugriff gemäß Berechtigungs- und Rollenkonzept**

Das Service Monitoring MUSS die Rechte der Nutzer (Akteure) gemäß Tab_Service_Monitoring_Akteure_und_Rollen beschränken. ⌫

Tabelle 1: Tab_Service_Monitoring_Akteure_und_Rollen

Schnittstelle	Akteur	Basis-Rolle	Berechtigung / Beschreibung
I_Monitoring_Update (aus dem zentralen Netz der TI erreichbar)	FA_spez_Dienst, Zentraler_Dienst_TI_Plattform	Keine Rolle	Der Nutzer sendet Monitoringdaten an die Störungsampel. Es erfolgt keine Authentisierung des Nutzers.
View Service Monitoring API (aus dem zentralen Netz der TI und aus dem Internet erreichbar)	ZIS und Monitoring Systeme (z.B. der Fachdienstbetreiber)	SM-MonRead	Der Nutzer hat lesenden Zugriff (Sichtbar sind seine eigenen Daten sowie die – für seine Diensterbringung nötigen – TI-Plattformservices) auf Kenngrößen, Schwellwerte und Daten der Probe-Läufe.
I_View_Service_Monitoring (im Internet und in der TI erreichbar)	Registrierter Nutzer (ohne Zusatzberechtigungen Anwendungsservices)	SM-TI-User	Der Nutzer hat lesenden Zugriff (Sichtbar sind die Daten der TI-Plattformservices) auf Kenngrößen, Schwellwerte und Daten der Probe-Läufe.
	Registrierter Nutzer (mit Zusatzberechtigungen für einzelne Anwendungsservices)	SM-AS-User	Wie SM-TI-User Zusätzlich hat der Nutzer lesenden Zugriff auf die Daten (Kenngrößen, Schwellwerte und Daten der Probe-Läufe) der berechtigten Anwendungsservices. Diese Zugriff wird eingeschränkt auf die Daten eines Mandanten des Anwendungsservices falls der Nutzer einem Mandanten zugeordnet ist.

ENTWURF

Schnittstelle	Akteur	Basis-Rolle	Berechtigung / Beschreibung
			Falls der Nutzer keinem Mandanten zugeordnet ist und der Anwendungsservice Mandanten unterstützt, darf er die Daten aller Mandanten sehen (z.B. der Betreiber des Anwendungsservices darf die Daten aller Mandanten sehen).
	Registrierter Nutzer (mit Administrations-berechtigungen)	SM-Admin	Wie SM-AS-User Zusätzlich hat der Administrator schreibenden und lesenden Zugriff auf die Konfigurationsdaten des Service Monitorings und der Probes.
	Registrierter Nutzer (mit Nutzerverwaltungs-berechtigungen)	SM-UserAdmin	Der Administrator kann • die Nutzer des Service Monitorings verwalten (anlegen, ändern, löschen, Anwendungsservices und Mandanten zuordnen), • Auditlogs einsehen, • Kenngrößen zu Anwendungsservices und Mandanten oder TI-Plattformservices zuordnen.

⌦ **TIP1-A_7090 Service Monitoring, Nutzeroberfläche, Nutzerauthentifizierung**

Das Service Monitoring MUSS ermöglichen, dass Nutzer eine User-ID, ein initiales Passwort und die zur Zwei-Faktor-Authentifizierung nötigen Mittel zur Nutzung der Schnittstellen I_View_Service_Monitoring beantragen können.

Das Passwort muss durch den Anwender änderbar sein.

Die Schnittstelle darf nur nach erfolgreicher Authentisierung (d.h. nach Nutzen von User-ID, Passwort, Zwei-Faktor-Authentifizierung) genutzt werden können.

Jedem Nutzer muss eine Rolle gemäß Tab_Service_Monitoring_Akteure_und_Rollen zugewiesen werden.

Für Nutzer mit der Rolle SM-AS-User muss der berechtigte Anwendungsservice und Mandant (falls vom Anwendungsservice unterstützt) festgelegt werden. ⌫

Die folgende Abbildung zeigt beispielhaft verschiedene Ebenen des Service Monitorings und die entsprechenden Berechtigungen von Nutzern der verschiedenen Rollen und Anwendungsservice -Zugehörigkeiten:

ENTWURF

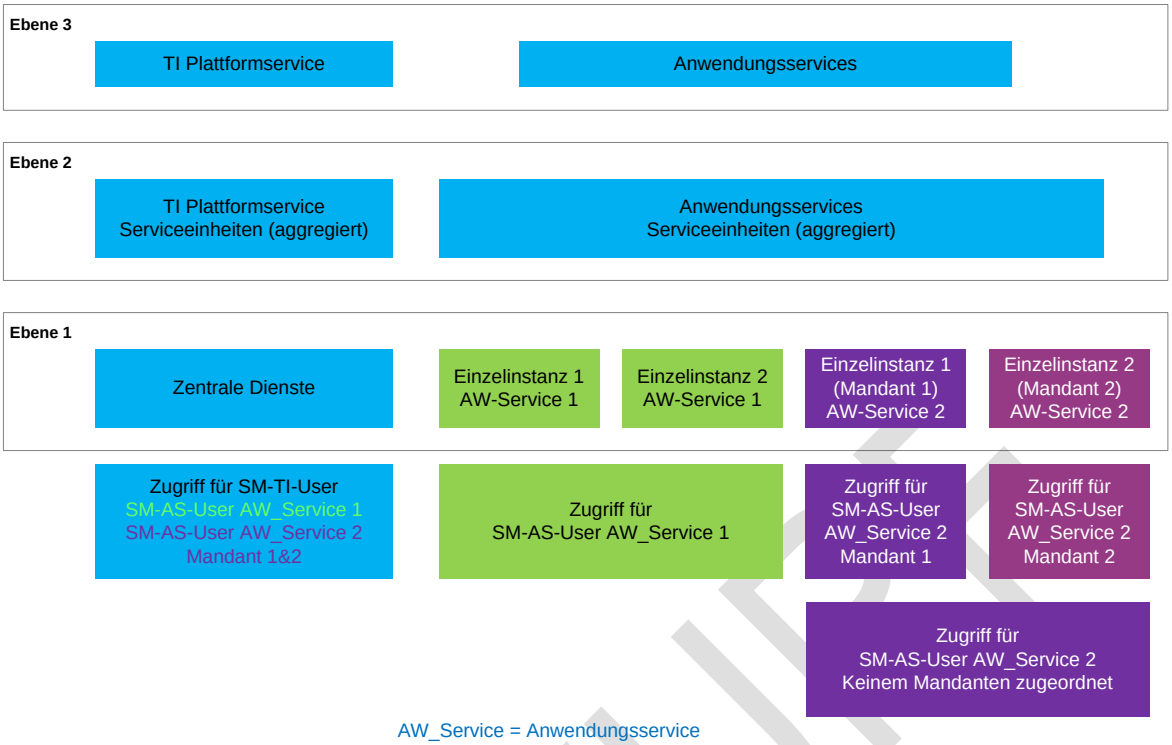

Abbildung 4: ABB_ServMon_302 Berechtigungskonzept

ENTWURF

5 Funktionsmerkmale

5.1 Schnittstelle I_View_Service_Monitoring

⌦ **TIP1-A_7100 Service Monitoring, I_View_Service_Monitoring, Zugriff gemäß Berechtigungs- und Rollenkonzept**

Das Service Monitoring MUSS eine Benutzer- und Rollenverwaltung unterstützen und die Rechte der Nutzer für den Zugriff sowohl in der grafischen Darstellung wie auch bei dem Zugriff durch andere Monitoring-Systeme (Schnittstelle View Service Monitoring API) auf bestimmte Informationen gemäß ihrer Rolle beschränken.⌫

⌦ **TIP1-A_7101 Service Monitoring, I_View_Service_Monitoring, Mandantenfähigkeit**

Das Service Monitoring MUSS eine Benutzer- und Rollenverwaltung unterstützen:

- Nutzer, welche keinem Mandanten zugeordnet sind, können auf alle – für sie durch das Berechtigungs- und Rollenkonzept freigegebenen – Daten (Verfügbarkeit, Performance, Auslastung) unabhängig von den darin enthaltenen Mandanteninformationen zugreifen.
- Nutzer, welche einem Mandanten zugeordnet sind, können auf alle – für sie durch das Berechtigungs- und Rollenkonzept freigegebenen – Daten (Verfügbarkeit, Performance, Auslastung) zugreifen wenn
  - die Daten (Verfügbarkeit, Performance, Auslastung) enthaltenen Mandanteninformationen mit den Mandanteninformationen des Nutzers übereinstimmen,
  - die Daten (Verfügbarkeit, Performance, Auslastung) keine Mandanteninformationen enthalten.

⌫

5.1.1 Darstellung der Monitoring-Daten

⌦ **TIP1-A_7102 Service Monitoring, Darstellung, GUI**

Das Service Monitoring MUSS über die Schnittstelle I_View_Service_Monitoring eine grafische Darstellung der Monitoring-Daten bereitstellen.⌫

⌦ **TIP1-A_7103 Service Monitoring, GUI, Dashboard**

Das Service Monitoring MUSS in der grafischen Darstellung ein Dashboard zur Darstellung des Status der überwachten Dienste bereitstellen.⌫

⌦ **TIP1-A_7104 Service Monitoring, GUI, Browser**

Das Service Monitoring MUSS die aktuellen und historischen Ereignisse des Service Monitorings wie z. B. Statusmessungen der Probes oder empfangene

ENTWURF

Performance- und Auslastungsdaten grafisch über marktübliche Browser (mindestens Firefox in der aktuellen Version) darstellen können. ⌫

⌦ **TIP1-A_7105 Service Monitoring, GUI, Performance-, Auslastungs- und Verfügbarkeitsdaten**

Das Service Monitoring MUSS in der grafischen Darstellung die Performance-, Auslastungs- und Verfügbarkeitsdaten mit konfigurierbaren Zeiträumen anzeigen. Reports mit den Performance-, Auslastungs- und Verfügbarkeitsdaten mit konfigurierbaren Zeiträumen MÜSSEN über das GUI als File exportierbar sein. Das Service Monitoring MUSS eine Beschreibung von dem File-Format bereitstellen, welche auch über das GUI abgerufen werden kann. ⌫

⌦ **TIP1-A_7106 Service Monitoring, GUI, Störungs-Dashboard**

Das Service Monitoring MUSS in der grafischen Darstellung die Konfiguration eines Dashboards zur Darstellung der Störungen der überwachten Dienste bereitstellen. Unter Störungen fallen Ausfall/Nichtverfügbarkeit und Über-/Unterschreitung von Schwellwerten. Das Störungs-Dashboard zeigt nur die Dienste mit Störungen und keine Dienste ohne Störungen. ⌫

⌦ **TIP1-A_7107 Service Monitoring, GUI, Dokumentation**

Das Service Monitoring MUSS für die grafische Darstellung eine Dokumentation bereitstellen (z. B. Bedeutung der Statusfarben, Bedingungen für Status-änderungen). Die Dokumentation MUSS für die Nutzer einsehbar sein.⌫

⌦ **TIP1-A_7108 Service Monitoring, GUI, Details zu den Probe-Messungen**

Die grafische Darstellung SOLL Details zu den Probe-Messungen (unter anderem den Mitschnitt der Prüfkommunikation) für eine konfigurierbare Anzahl der letzten Messungen speichern und anzeigen können.⌫

⌦ **TIP1-A_7109 Service Monitoring, Darstellung, Tabellen und Metriken**

Die Darstellung der Monitoring Daten SOLL – konfigurierbar für jede Kenngröße – in Tabellen und Metriken anzeigt werden können.⌫

⌦ **TIP1-A_7110 Service Monitoring, Darstellung, Zeitachse mit verschiedenen Kenngrößen**

Die Darstellung der Monitoring-Daten SOLL einen zeitlichen Bezug zwischen auswählbaren Kenngrößen darstellen können.⌫

5.1.2 Schnittstelle View Service Monitoring API Web Service

Als Bestandteil der I_View_Service_Monitoring bietet der View Service Monitoring API Web Service die Möglichkeit der automatisierten Abfrage über HTTP-GET-Requests, die als Antwort wahlweise Performance-Daten im XML- oder JSON-Format zurückgeben.

⌦ **TIP1-A_7112 Service Monitoring, View Service Monitoring API**

Das Service Monitoring MUSS die Schnittstelle View Service Monitoring API unter einer URL im Internet und in der TI bereitstellen. ⌫

ENTWURF

⌦ **TIP1-A_7113 Service Monitoring, I_View_Service_Monitoring, View Service Monitoring API, Dokumentation**

Das Service Monitoring MUSS für das View Service Monitoring API

- ein etabliertes Standard-Authentifizierungsverfahren nutzen und dokumentieren. Die Beschreibung MUSS auch alle organisatorischen Prozesse umfassen (z.B. Beantragung des Zugangs, Ausgabe/Erneuerung von Credentials).
- ein Benutzer-/Programmierhandbuch bereitstellen, welches mit der gematik abzustimmen ist. Das Benutzer-/Programmierhandbuch MUSS auch im Service Monitoring I_View_Service_Monitoring GUI verfügbar sein. ⌫

⌦ **TIP1-A_7349 Service Monitoring, View Service Monitoring API, Parameter**

Das Service Monitoring MUSS die HTTP GET-Anfragen in der Schnittstelle View Service Monitoring API entsprechend von Parametern in der Anfrage beantworten:

- Das Format der Rückgabedatei (xml oder json) MUSS über einen Parameter steuerbar sein. Das Encoding der Rückgabedatei ist in beiden Fällen UTF-8. Das XML-Format MUSS über ein XML-Schema definiert werden. Das json-Format MUSS gemäß [RFC7159] gleich zum XML-Format sein.
- Über eine Liste von Parametern gemäß Tabelle Tab_Service Monitoring_ViewServiceMonitoringAPI_Parameters MUSS der Umfang der Rückgabedaten steuerbar sein. Sämtliche Daten, die über Probes gemessen wurden, als auch sämtliche Daten, die über die Schnittstelle I_Monitoring_Update hochgeladen wurden MÜSSEN lieferbar sein.
- Die Aggregationsstufe der Daten MUSS über einen Parameter wählbar sein. Dabei MÜSSEN mindestens folgende Aggregationsstufen unterstützt werden:
  - „kein“ = keine Aggregation

    (z.B. durch Probes ermittelte Daten)
  - „fein“ = 5 Minuten
  - „stunde“ = 1 Stunde
  - „tag“ = 1 Tag
  - „woche“ = 1 Woche
  - „monat“ = 1 Monat

⌫

⌦ **TIP1-A_7350 Service Monitoring, View Service Monitoring API, Probe Kenngrößen**

Das Service Monitoring MUSS in der Schnittstelle View Service Monitoring API für die – über Probes ermittelten – Daten eine Zuordnung zum Probe-Lauf ermöglichen. ⌫

ENTWURF

⌦ **TIP1-A_7351 Service Monitoring, View Service Monitoring API, Kenngrößen**

Das Service Monitoring MUSS über die Schnittstelle View Service Monitoring API einen Report mit den Kenngrößen und ihren Schwellwerten bereitstellen. ⌫

⌦ **TIP1-A_7348 Service Monitoring, I_View_Service_Monitoring, View Service Monitoring API, Authentifizierung**

Das Service Monitoring MUSS den Aufrufer authentifizieren und den Zugriff auf Service Monitoring-Daten entsprechend seinen Zugriffsrechten beschränken. ⌫

5.1.3 Umsetzung

⌦ **TIP1-A_7114 Service Monitoring, I_View_Service_Monitoring, TLS-gesicherte Verbindung**

Das Service Monitoring MUSS die Schnittstelle I_View_Service_Monitoring durch Verwendung von TLS mit serverseitiger Authentisierung sichern.⌫

5.2 Schnittstelle I_Monitoring_Update

Diese Schnittstelle wird aus Kompatibilität zur Schnittstelle der Störungsampel [gemSpec_St_Ampel] unverändert übernommen. Dies erleichtert die Migration von Diensten, welche bereits die I_Monitoring_Update-Schnittstelle der Störungsampel nutzen.

5.2.1 Schnittstellendefinition

Diese Schnittstelle ermöglicht das Senden von Monitoringdaten der fachanwendungsspezifischen Dienste und der zentralen Dienste der TI-Plattform an das Service Monitoring.

Die zu sendenden Daten sind in [gemSpec_Perf#Tab_gemSpec_Perf_Performance-Kenngroessen] festgelegt.

⌦ **TIP1-A_7116 Service Monitoring, Schnittstelle I_Monitoring_Update**

Das Service Monitoring MUSS die Schnittstelle I_Monitoring_Update gemäß Tabelle Tab_Service_Monitoring_I_Monitoring_Update anbieten.

Tabelle 2: Tab_Service_Monitoring_I_Monitoring_Update

Name	I_Monitoring_Update	
Version	Webservice: v1.1	
Webservice Operationen	Name	Kurzbeschreibung
	update	Die Operation ermöglicht das Senden von Monitoringdaten an das Service Monitoring.
WSDL	I_Monitoring_Update10.wsdl Version: 1.1.0 TargetNamespace: http://ws.gematik.de/tel/stoerungsampel/wsdl/v1.1	

ENTWURF

Schema	I_Monitoring_Update10.xsd Version: 1.1.0 TargetNamespace: http://ws.gematik.de/tel/stoerungsampel/v1.1 ProductInformation.xsd Version: 1.1.0 TargetNamespace: http://ws.gematik.de/tel/version/ProductInformation/v1.1 TelematikError.xsd Version: 2.0.0 TargetNamespace: http://ws.gematik.de/tel/error/v2.0
Webservice Zugangspunkt	https://monitoring-update.stampel.telematik:8443/I_Monitoring_Update10

⌫

⌦ **TIP1-A_7117 Service Monitoring und Client, I_Monitoring_Update, WebService**

Das Service Monitoring und die Clients MÜSSEN die Schnittstelle I_Monitoring_Update in ihrer jeweiligen Rolle Client bzw. Server als SOAP-Webservice über HTTPS implementieren. Der Webservice wird durch die Dokumente I_Monitoring_Update10.wsdl und I_Monitoring_Update10.xsd sowie Tab_Service_Monitoring_SOAP-Request und Tab_Service_Monitoring_SOAP-Response definiert.⌫

⌦ **TIP1-A_7118 Service Monitoring und Client, I_Monitoring_Update, eindeutige Zuordnung**

Der Anbieter des Service Monitorings MUSS dem Anbieter des Clients der Schnittstelle I_Monitoring_Update eine eindeutige SystemID (zur Zuordnung der Monitoringdaten zur Instanz des Produkttyps) zuweisen, die in den SOAP-Requests (tns:systemid) verwenden MUSS.⌫

⌦ **TIP1-A_7119 Service Monitoring und Client, I_Monitoring_Update, Servicepunkte und IP-Adressen**

Der Anbieter des Clients der Schnittstelle I_Monitoring_Update MUSS dem Anbieter des Service Monitorings die IP-Adressen mitteilen, von denen Daten an das Service Monitoring gesendet werden.

Der Anbieter des Clients MUSS mit dem Anbieter des Service Monitorings die gültigen Servicepunkte (Host, Port und URL) verifizieren.⌫

In einer Nachricht können mehrere Performancewerte oder Auslastungswerte übertragen werden.

⌦ **TIP1-A_7120 Service Monitoring und Client, I_Monitoring_Update, maximale Zeitabweichung zwischen Berichtszeitraum und Nachrichtenübermittelung**

Der Client der Schnittstelle I_Monitoring_Update MUSS die in [gemSpec_Perf] geforderten Monitoringdaten innerhalb von 120 Sekunden nach Ablauf eines Reportzeitraumes an das Service Monitoring übertragen haben. Eine Kennzeichnung des Report-Zeitraumes erfolgt durch eine Zeitbereichsangabe (Startzeit und Endzeit) in der übermittelten Nachricht.⌫

ENTWURF

⌦ **TIP1-A_7125 Service Monitoring, I_Monitoring_Update, keine Daten für Berichtszeitraum**

Das Service Monitoring MUSS Berichtszeiträume – für die nach der maximalen Zeitabweichung zwischen Berichtszeitraum und Nachrichtenübermittelung keine Monitoringdaten über die Schnittstelle I_Monitoring_Update geliefert wurden – im GUI bzw. Dashboard hervorheben.⌫

⌦ **TIP1-A_6744 Service Monitoring, I_Monitoring_Update, Datenverarbeitung**

Das Service Monitoring MUSS über die Schnittstelle I_Monitoring_Update gelieferte Daten in den Service Monitoring-Datenbestand als Kenngrößen entsprechend [gemSpec_Perf] übernehmen. Diese Kenngrößen MÜSSEN analog zu den durch Probes ermittelten Kenngrößen und den im Service Monitoring durch Aggregation/Korrelation ermittelten Kenngrößen

- im GUI/Dashboard anzeigbar (Schnittstelle I_View_Service_Monitoring) sein,
- übergreifend mit allen anderen Kenngrößen auswertbar (Aggregation, Korrelation (z.B. gemeldete Ausfallzeiten mit Nichterreichbarkeit durch Probes)) sein und
- maschinell abrufbar (Schnittstelle View Service Monitoring API) sein. ⌫

5.2.2 Umsetzung

Die Schnittstelle ist aus dem zentralen Netz der TI-Plattform erreichbar.

⌦ **TIP1-A_7121 Service Monitoring, I_Monitoring_Update, TLS-gesicherte Verbindung**

Das Service Monitoring MUSS die Schnittstelle I_Monitoring_Update durch Verwendung von TLS mit serverseitiger Authentisierung sichern.

Das Service Monitoring MUSS sich mit der Identität ID.ZD.TLS-S und der enthaltenen Admission-OID „oid_stamp“ gegenüber den nutzenden Systemen authentisieren.⌫

⌦ **TIP1-A_7122 Service Monitoring, Datenerhebung**

Der Anbieter des Service Monitorings MUSS die Voraussetzungen dafür schaffen, dass die in der [gemSpec_Perf] unter GS-A_4147 Performance - Störungsampel - Performance Daten festgelegten Daten und Informationen an das Service Monitoring übermittelt werden können.

Hierfür sind durch den Anbieter des Service Monitorings mindestens zu leisten:

- Nutzung des zentralen Netzwerks der TI zur Übertragung der Daten,
- Sicherstellung, dass alle Anbieter von monitoring-pflichtigen TI-Komponenten an das Service Monitoring angebunden werden können.⌫

⌦ **TIP1-A_7123 Service Monitoring, I_Monitoring_Update, Fehlermeldungen**

Das Service Monitoring MUSS fehlerhafte Zugriffe auf die Webservice-Schnittstelle I_Monitoring_Update

ENTWURF

- auf HTTP-Ebene mit den protokolleigenen HTTP-Fehlercodes
- auf SOAP-Ebene mit gematik-SOAP-Fault gemäß [gemSpec_OM]

beantworten.⌫

⌦ **TIP1-A_7124 Service Monitoring, I_Monitoring_Update, Rückmeldung der Nachrichten-ID**

Das Service Monitoring MUSS jeden akzeptierten SOAP-Request mit einem SOAP-Reply beantworten, der eine eindeutige Nachrichten-ID enthält, die als Referenz für Rückfragen beim Anbieter des Service Monitorings genutzt werden kann.⌫

5.2.3 Nutzung

⌦ **TIP1-A_7126 Nutzer des Service Monitorings I_Monitoring_Update, Zeitstempel bei Ausfall/Wiederherstellung**

Der Nutzer der Schnittstelle I_Monitoring_Update MUSS beim Versenden von Verfügbarkeitsdaten im Alarm-Nachrichtenelement/Nachrichtenobjekt einen Zeitstempel übermitteln, der die Startzeit oder Endzeit des Alarms angibt.⌫

⌦ **TIP1-A_7127 Nutzer des Service Monitorings I_Monitoring_Update, eindeutige Zuordnung des Messwertes**

Der Nutzer der Schnittstelle I_Monitoring_Update MUSS durch die Verwendung von Attributen gemäß der Tabelle Tab_Service_Monitoring_Attribute jede übermittelte Performance-Kenngröße und jeden übermittelten Alarm-Status-Wert eindeutig kennzeichnen.

Optionale Attribute dürfen nur verwendet werden, wenn sie zur eindeutigen Zuordnung benötigt werden.⌫

Tabelle 3: Tab_Service_Monitoring_Attribute

Attribut / Objekt	Beschreibung
pdt	Produkttyp-ID lt. [gemSpec_Perf]
perftype	Performance-Kenngrößen-ID lt. [gemSpec_Perf]
interface	Schnittstellenoperationen-ID lt. [gemSpec_Perf]
certtype	Zertifkats-Typen-ID lt. [gemSpec_Perf]
querysource	Aufrufquellen-ID lt. [gemSpec_Perf]
connect	Eindeutige ID zur Identifikation bei Ende-zu-Ende-Messungen im Netzwerk-Bereich

Für die Übermittlung von Monitoringdaten wird der SOAP-Request der Operation „update“ verwendet.

Die folgende Abbildung zeigt die Datenstruktur des SOAP-Requests.

ENTWURF

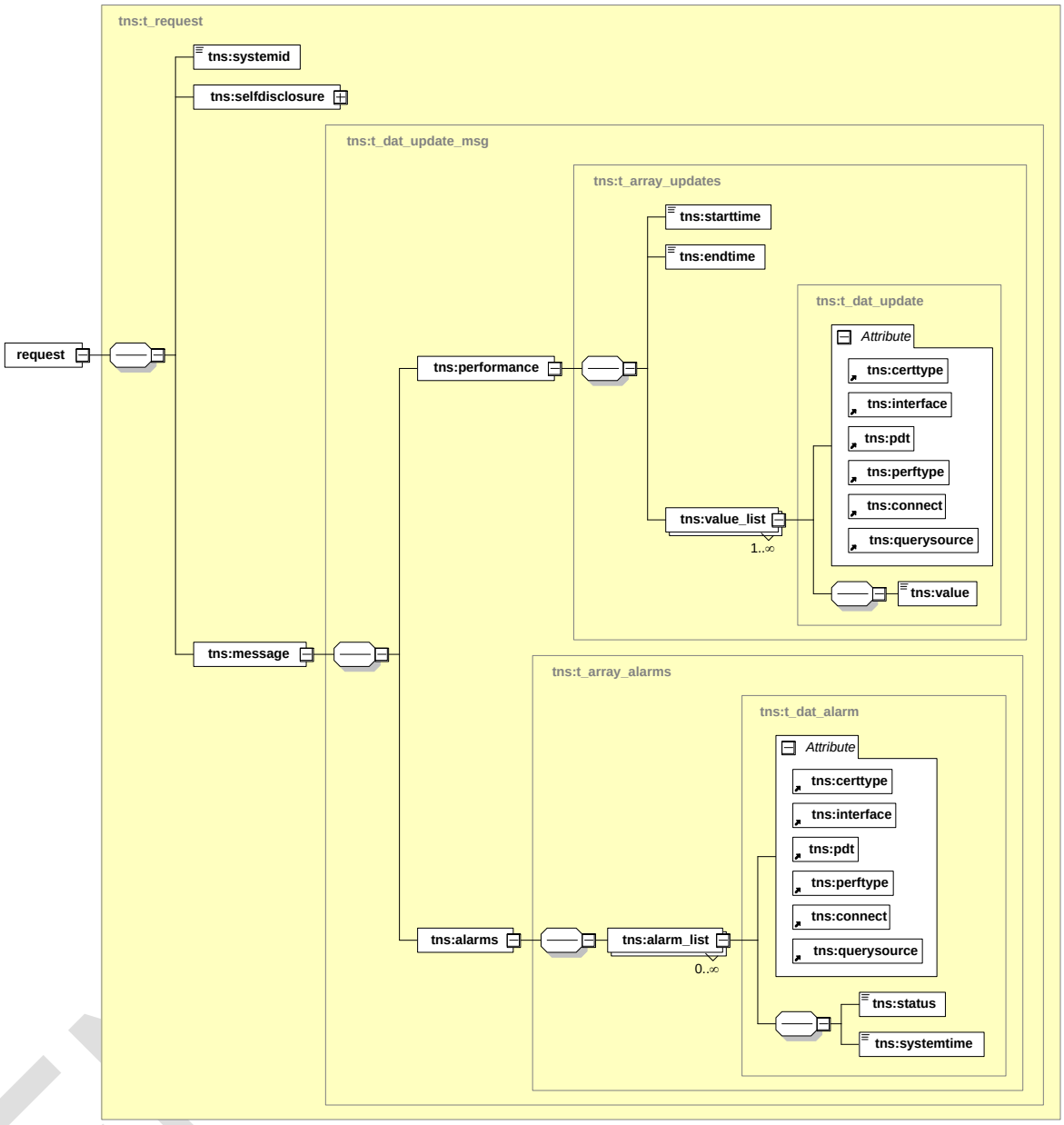

Abbildung 5: Abb_Service_Monitoring_SOAP-Request

Tabelle 4: Tab_Service_Monitoring_SOAP-Request, Beschreibung der Elemente

Element	Beschreibung
tns:request	definiert den SOAP-Request, der über die Operation update an das Service Monitoring gesendet wird.
tns:systemid	ermöglicht eine eindeutige Identifikation des sendenden Systems/Dienstes. Diese ID MUSS eindeutig sein und deren Vergabe erfolgt in Abstimmung zwischen dem Anbieter Service Monitoring und dem Dienstanbieter.
tns:selfdisclosure	enthält Informationen zur Selbstauskunft eines meldenden Systems, siehe [gemSpec_OM].
tns:message	beinhaltet die in [gemSpec_Perf] für den Dienst geforderten Verfügbarkeits-, Performance- und Auslastungsdaten.
tns:performance	beinhaltet die in [gemSpec_Perf] für den Dienst geforderten Performance- und Auslastungsdaten.

tns:alarms	beinhaltet die in [gemSpec_Perf] für den Dienst geforderten Verfügbarkeitsdaten.
tns:starttime, tns:endtime	definieren das zugrundeliegende Zeitintervall für Performance- und Auslastungswerte.
tns:value_list	enthält die Liste der Performance-Kenngrößen vom Typ t_dat_update. Dieses Element muss die folgenden Attribute enthalten. tns:interface: Schnittstellenoperationen-ID lt. [gemSpec_Perf] tns:pdt: Produkttyp-ID lt. [gemSpec_Perf] tns:perftype: Performance-Kenngrößen-ID lt. [gemSpec_Perf] Dieses Element kann die folgenden Attribute enthalten. tns:certtype: Zertifkats-Typen-ID lt. [gemSpec_Perf] tns:connect: Eindeutige ID zur Identifikation bei Ende-zu-Ende-Messungen im Netzwerk-Bereich tns:querysource: Aufrufquellen-ID lt. [gemSpec_Perf] Mit einer SOAP-Nachricht können mehrere Werte für gleiche Zeitintervalle übergeben werden.
tns:value	Wert der Performance-Kenngröße
tns:alarm_list	enthält die Alarmstatus-Informationen. Dieses Element muss die folgenden Attribute enthalten. tns:interface: Schnittstellenoperationen-ID lt. [gemSpec_Perf] tns:pdt: Produkttyp-ID lt. [gemSpec_Perf] tns:perftype: Performance-Kenngrößen-ID lt. [gemSpec_Perf] Dieses Element kann die folgenden Attribute enthalten. tns:certtype: Zertifkats-Typen-ID lt. [gemSpec_Perf] tns:connect: Eindeutige ID zur Identifikation bei Ende-zu-Ende-Messungen im Netzwerk-Bereich tns:querysource: Aufrufquellen-ID lt. [gemSpec_Perf]
tns:status	enthält den Alarm-Status. open: Alarmstatus gesetzt close: Alarmstatus gelöscht warn: nicht benutzt grace: nicht genutzt
tns:systemtime	Alarmzeit des sendenden Systems zur Erkennung von Inkonsistenzen (z.B. Alarme aus historischen Daten).

Die Rückgabe enthält die Elemente gemäß der Tabelle Tab_Service_Monitoring_SOAP-Response.

Tabelle 5: Tab_Service_Monitoring_SOAP-Response, Beschreibung der Elemente

Element	Beschreibung
tns:request	definiert die SOAP-Response, die als Antwort auf den SOAP-Request an den Nutzer gesendet wird.
tns:result	beinhaltet Abnahmebestätigung der Nachricht. true | 1: Die Nachricht wurde vom Service Monitoring angenommen und zur Analyse der Messwerte weitergeleitet. false | 0: Die Nachricht konnte nicht an das Auswertesystem weitergeleitet werden.
tns:id	ermöglicht eine eindeutige Quittungs-ID für gesendete Nachricht (relevant für Fehleranalyse).
tns:selfdisclosure	enthält Informationen zur Selbstauskunft des Service Monitorings, siehe [gemSpec_OM].

Für den Fehlerfall ist das Nachrichtenelement err:Error (gematik-SOAP-Fault, definiert in Schemadatei TelematikError.xsd gemäß [gemSpec_OM]) verfügbar.

EINWURF

⌦ **TIP1-A_7128 Nutzer des Service Monitorings I_Monitoring_Update, maximale HTTP-Nachrichtenlänge**

Der Nutzer der Schnittstelle I_Monitoring_Update MUSS beachten, dass bei Monitoringnachrichten die maximale HTTP-Nachrichtenlänge (Headerinformationen und Daten) von 16.000 Bytes nicht überschritten wird. Größere Nachrichten werden verworfen.⌫

Nachrichten mit fehlenden oder inkonsistenten Informationen werden akzeptiert, der Dateninhalt jedoch verworfen.

Das sendende System erhält als Rückmeldung eine Nachrichten-ID, die für Rückfragen beim Anbieter des Service Monitorings als Referenz genutzt werden kann. Eine Referenzierung von übermittelten Nachrichten ist nur im Rahmen der genutzten Datenaufbewahrungsrichtlinie möglich.

⌦ **TIP1-A_7129 Nutzer des Service Monitorings I_Monitoring_Update, Selbstauskunft als Bestandteil jeder SOAP-Nachricht**

Der Nutzer der Schnittstelle I_Monitoring_Update MUSS in jeder SOAP-Nachricht das Element selfdisclosure (Selbstauskunft) befüllen. Die Selbstauskunft basiert auf dem Schema [ProductInformation.xsd] gemäß [gemSpec_OM]. ⌫

5.3 Technische Use Cases – TUCs

Die hier beschriebenen TUCs werden in Probes für wiederkehrende Abläufe genutzt.

⌦ **TIP1-A_7147 Service Monitoring, TUC_SM_001_DNS_Name_Resolution**

Das Service Monitoring MUSS TUC_SM_001_DNS_Name_Resolution entsprechend Tab_Service_Monitoring_TUC_SM_001_DNS_Name_Resolution bereitstellen. Dieser TUC MUSS in allen Probes zur DNS-Namensauflösung genutzt werden.

Tabelle 6: Tab_Service_Monitoring_TUC_SM_001_DNS_Name_Resolution

Name	TUC_SM_001_DNS_Name_Resolution	
Beschreibung	Dieser TUC führt die Auflösung eines FQDN in eine IP-Adresse durch.	
Vorbedingungen	• Keine	
Eingangsdaten	• IP-Adresse Namensdienst • Aufzulösender FQDN • Bisher ermittelte Service Monitoring Daten	
Komponenten	• Service Monitoring Probe, DNS-Nameserver	
Ausgangsdaten	• Aufgelöste IP-Adresse • Ermittelte Service Monitoring Daten für die DNS Namensauflösung	
Standardablauf	**Aktion**	**Beschreibung**
	IP-Adresse der Schnittstelle ermitteln	Durch eine DNS-Anfrage (I_DNS_Name_Resolution:: get_IP_Address.) wird der FQDN in eine IP-Adresse aufgelöst.
	Falls bei der	Prüfung der Erreichbarkeit des DNS-Nameserver über

ENTWURF

	DNS-Anfrage keine Antwort (und kein DNS-Fehler) ermittelt werden konnte	TUC_SM_002_Erreichbarkeitsprüfung. Der Service Monitoring Datensatz für die DNS-Namensauflösung wird in diesem Fall in TUC_SM_002_Erreichbarkeitsprüfung erstellt.
	Falls bei der DNS-Anfrage eine Antwort oder ein DNS-Fehler ermittelt werden konnte	Die Service Monitoring-Daten (aus den Eingangsdaten) werden entsprechend der durchgeführten Aktionen, Tab_Service_Monitoring_Probe_Daten und um die Performance-Kenngröße „Bearbeitungszeit“ ergänzt. Dabei wird das „Probe-Ergebnis“ dieses Datensatzes • auf OK gesetzt, falls der FQDN in eine IP-Adresse aufgelöst wurde. • auf 7102 gesetzt, falls der DNS-Server mit einem Fehler geantwortet hat.
	Rückgabe der Daten	Rückgabe der Ausgangsdaten

⌫

⌦ **TIP1-A_7148 Service Monitoring, TUC_SM_002_Erreichbarkeitsprüfung**

Das Service Monitoring MUSS TUC_SM_002_Erreichbarkeitsprüfung entsprechend Tab_Service_Monitoring_TUC_SM_002_Erreichbarkeitsprüfung bereitstellen. Dieser TUC MUSS in Probes genutzt werden wenn

- die Erreichbarkeit von Diensten geprüft wird und
- wenn der Dienst keine erwartete Antwort und keine Fehlermeldung liefert. In diesem Fall wird festgestellt, ob der Dienst noch erreichbar ist, obwohl er auf fachlicher Ebene nicht mehr antwortet.

Tabelle 7: Tab_Service_Monitoring_TUC_SM_002_Erreichbarkeitsprüfung

Name	TUC_SM_002_Erreichbarkeitsprüfung	
Beschreibung	Dieser TUC prüft die Erreichbarkeit einer Schnittstelle/Dienstes.	
Vorbedingungen	• Keine	
Eingangsdaten	• IP-Adresse • Port(s) • TCP/UDP (soll ein TCP oder UDP Scan durchgeführt werden) • Bisher ermittelte Service Monitoring-Daten	
Komponenten	Service Monitoring Probe, jeweiliger Dienst	
Ausgangsdaten	• Ermittelte Kenngröße „Verfügbarkeit“	
Standardablauf	**Aktion**	**Beschreibung**
	Prüfung ob Port(s) offen sind	Für die übergebenen Ports/IP-Adresse wird je nach Eingangsparametern ein TCP-SYN-Scan oder ein UDP-Scan durchgeführt.

ENTWURF

	Ergänzen der Service Monitoring-Daten	Die Service Monitoring-Daten (aus den Eingangsdaten) werden entsprechend der durchgeführten Aktionen bzw. deren Ergebnis ergänzt. Falls • alle Ports geöffnet sind (für alle Ports wurde ein Datenpaket mit SYN/ACK Flags empfangen), wird das „Probe-Ergebnis“ dieses Datensatzes auf OK gesetzt. • mindestens ein Port aus den Eingangsdaten geschlossen ist (für den Port wurde ein Datenpaket mit RST-Flag empfangen), wird das „Probe-Ergebnis“ dieses Datensatzes auf 7101 gesetzt. • beim Port-Scan keine Antwort empfangen wurde, wird das „Probe-Ergebnis“ dieses Datensatzes auf 7100 gesetzt.
	Rückgabe der Daten	Rückgabe der Ausgangsdaten

⌫

5.4 Probes

⌦ **TIP1-A_7130 Service Monitoring, Probes, Installation**

Das Service Monitoring MUSS Administratoren das Einbringen/Installieren von Probes in das laufende Service Monitoring-System erlauben. ⌫

⌦ **TIP1-A_7131 Service Monitoring, Probes, Entwicklung eigener Probes**

Das Service Monitoring MUSS die Entwicklung eigener Probes erlauben. Falls für die Probe Entwicklung Tools vorgegeben sind, MÜSSEN diese benannt werden. Nötige Randbedingungen (z.B. Schnittstelle zwischen Probes und dem Service Monitoring System) MÜSSEN dokumentiert werden. ⌫

⌦ **TIP1-A_7132 Service Monitoring, Monitoring der Verfügbarkeit mittels Probes**

Das Service Monitoring MUSS die Verfügbarkeit der Schnittstellen der fachanwendungsspezifischen Dienste und der zentralen Dienste der TI-Plattform sowie der Dienste sicherer Übermittlungsverfahren (sowohl im zentralen Netz der TI als auch im Internet) durch Abfrage der Schnittstellen mit Systemen, die das Verhalten der echten Nutzer der Schnittstellen simulieren (den sogenannten Probes) ermitteln.

Die Probes senden Abfragen – welche den Abfragen der echten Nutzer möglichst nahekommen – an die Schnittstellen und vergleichen die Antworten mit dem erwarteten Ergebnis. Wenn die Antwort dem erwarteten Ergebnis entspricht, wird die Schnittstelle als verfügbar gewertet. Bei Abweichungen vom erwarteten Ergebnis MUSS die Schnittstelle – optional in Abhängigkeit von Regeln – als nicht verfügbar gewertet werden. ⌫

ENTWURF

⌦ **TIP1-A_7115 Service Monitoring, Monitoring der Verfügbarkeit, mehrere Probe-Läufe**

Das Service Monitoring MUSS für das Monitoring der Verfügbarkeit die Ergebnisse verschiedener Probe-Läufe (z.B. bei redundanten Knoten oder wenn die Verfügbarkeit eines Anwendungsfalls aus der Verfügbarkeit von beteiligten Diensten abgeleitet wird) kombinieren können.⌫

⌦ **TIP1-A_7133 Service Monitoring, Probes, Ursachen-Analyse**

Das Service Monitoring MUSS die Probes so implementieren, dass im Falle einer negativen Verfügbarkeitsmessung weitere Daten geliefert werden, um die Ursache der Nicht-Verfügbarkeit genauer zu bestimmen.

Die Aktionen zur Ermittlung der weiteren Daten MÜSSEN vom Anbieter des Service Monitorings mit den Betreibern der überwachten Dienste im Rahmen der gematik-Vorgaben abgestimmt werden. ⌫

⌦ **TIP1-A_7134 Service Monitoring, Probes, Abstimmung**

Die von den Probes ausgeführten Operationen und das Ausführungsintervall MÜSSEN vom Anbieter des Service Monitorings mit den Betreibern der überwachten Dienste im Rahmen der gematik-Vorgaben abgestimmt werden. ⌫

⌦ **TIP1-A_7135 Service Monitoring, keine Beeinträchtigung der Dienste durch Probes**

Das Service Monitoring DARF die mittels Probes überwachten Dienste NICHT negativ beeinflussen.⌫

⌦ **TIP1-A_7136 Service Monitoring, Probes, Konfigurationsdatensätze**

Das Service Monitoring MUSS berechtigten Nutzern die Eingabe bzw. Änderung von Konfigurationsdaten von Probes erlauben. Für jede Probe MÜSSEN mehrere Konfigurationsdatensätze unterstützt werden. ⌫

⌦ **TIP1-A_7137 Service Monitoring, Probes, Konfiguration von erwarteten Ergebnissen**

Das Service Monitoring MUSS in Probes die Konfiguration der erwarteten Antworten von aufgerufenen Operationen erlauben. Es MUSS möglich sein – neben der normalen fachlichen Antwort – die Fehlermeldung oder ausbleibende Antwort einer Operation als positives Probe-Ergebnis zu werten. ⌫

⌦ **TIP1-A_7138 Service Monitoring, Probes, Konfiguration von Kenngrößen**

Das Service Monitoring MUSS in Probes die Konfiguration von Kenngrößen für die ermittelten Werte (z. B. Bearbeitungszeit von aufgerufenen Operationen) erlauben. Diese Kenngrößen und die über die Schnittstelle I_Monitoring_Update gelieferten Performance-Kenngrößen sowie alle anderen vorhandenen Kenngrößen im Service Monitoring (z.B. durch den Log-Datei-Analysator importierte Kenngrößen) MÜSSEN in den Aggregationsregeln und Schnittstelle I_View_Service_Monitoring (Darstellung und View Service Monitoring API Web Service) verwendet werden können. ⌫

⌦ **TIP1-A_7328 Service Monitoring, Probes, Konfigurationsvariante**

ENTWURF

Das Service Monitoring MUSS in Probes die Konfiguration der Konfigurationsvariante erlauben. Die Konfigurationsvariante identifiziert den Satz von Konfigurationsdaten, welche für diesen Probe-Lauf genutzt werden. Die Konfigurationsvariante MUSS für jeden Probe-Lauf in dem Service Monitoring-Datensatz abgelegt werden. Die Konfigurationsvariante MUSS zusammen mit den dazugehörigen Konfigurationsdaten bei der Darstellung der Probe im GUI einsehbar sein. ⌫

⌦ **TIP1-A_7139 Service Monitoring, Probes, Ausführungszeitpunkt**

Das Service Monitoring MUSS berechtigten Nutzern die vorhandenen Probes anzeigen und für jede Probe in Kombination mit einem Konfigurationsdatensatz den Ausführungszeitpunkt wählen lassen:

- Periodisch, ab einem bestimmten Start-Zeitpunkt mit Angabe des Intervalls
- Zu einem bestimmten Zeitpunkt
- Sofortige (manuelle) Ausführung

Jede Probe MUSS mehrfach mit unterschiedlichen Konfigurationsdatensätzen zum gleichen und zu verschiedenen Ausführungszeitpunkt(en) ausführbar sein. ⌫

⌦ **TIP1-A_7140 Service Monitoring, Probes, parallele Ausführung**

Das Service Monitoring MUSS die parallele Ausführung von Probes erlauben. Auch eine einzelne Probe MUSS mehrfach parallel (z.B. für verschiedene Dienstinstanzen) ausführbar sein. ⌫

⌦ **TIP1-A_7141 Service Monitoring, Probes, Übersicht über active Probes**

Das Service Monitoring MUSS berechtigten Nutzern eine Übersicht über die aktiven Probes mit ihren Ausführungszeitpunkten anzeigen können. Aktive Probes sind Probes mit Ausführungszeitpunkten in der Zukunft.

Das Service Monitoring MUSS den berechtigten Nutzern die Änderung und Stornierung der Ausführungszeitpunkte der Probes erlauben. ⌫

⌦ **TIP1-A_7142 Service Monitoring, Probes, Details zu den Probe-Messungen**

Das Service Monitoring MUSS für alle Probe Ausführungen folgende Daten erfassen

- Die Ausführung der Probe inklusive der in der Probe Beschreibung definierten Daten.
- Den Mitschnitt der Kommunikation (gesendete und empfangene Daten) für eine konfigurierbare Anzahl der letzten Messungen.
- Das Ergebnis der Probe Messung (Entspricht das Ergebnis der Probe dem erwarteten Ergebnis?)
- Falls die Probe für einen Mandanten eines Dienstes ausgeführt wurde, muss die Mandanteninformation in jedem relevanten Service Monitoring-Datensatz erfasst werden.

ENTWURF

Die durch Probes erfassten Daten MÜSSEN von den durch Betreiber gelieferten Daten im Service Monitoring unterscheidbar (bei der Aggregation und in der Darstellung) sein. ⌫

⌦ **TIP1-A_7143 Service Monitoring, Probes, Ergebnis bei komplexen Probes**

Das Service Monitoring MUSS für Probes, welche sich aus Aufrufen mehrerer Operationen zusammensetzen, das Probe-Ergebnis folgendermaßen bilden:

Probe-Ergebnis der gesamten Probe:

- OK – Falls alle aufgerufenen Operationen ohne Fehler beendet wurden.
- 7107 „In der Probe ist ein Fehler aufgetreten“ – falls ein oder mehrere Operationen mit Fehlern beendet wurden. ⌫

⌦ **TIP1-A_7144 Service Monitoring, Probes, Unabhängige parallele Ausführung von mehreren Probes**

Das Service Monitoring MUSS die parallele Ausführung von mehreren Probes unterstützen. Die gegenseitige Beeinflussung von Probes MUSS vermieden werden (ist eine Probe blockiert oder verlangsamt, dürfen andere Probes nicht davon beeinflusst sein). ⌫

⌦ **TIP1-A_7145 Service Monitoring, Probes, Timeouts**

Das Service Monitoring MUSS in Probes die Konfiguration von Timeouts für aufgerufene Operationen erlauben. Für das Timeout MUSS die Angabe eines Probe-Ergebnisses, einer Aktion oder eines alternativen Pfades im Probe-Ablauf möglich sein. ⌫

⌦ **TIP1-A_7146 Service Monitoring, Probes, Mandantenfähigkeit**

Das Service Monitoring MUSS in Probes die Konfiguration von Mandanten für aufgerufene Operationen erlauben, falls für die Operation Mandanten unterstützt werden. Der Mandant muss in den relevanten Service Monitoring-Datensätzen abgelegt werden. ⌫

⌦ **TIP1-A_7093 Service Monitoring, Probes, Kartenterminals**

Das Service Monitoring MUSS für Probes den Einsatz von Smartcards ermöglichen und dafür Kartenterminals vorsehen. ⌫

In vorliegender Spezifikation betrifft das alle Probes, die mit SMC-B-Zertifikaten (OSIG und AUT) arbeiten.

5.4.1 DNS Name Resolution

⌦ **TIP1-A_7149 Service Monitoring, Probe DNS_Name_Resolution**

Das Service Monitoring MUSS die Probe DNS_Name_Resolution entsprechend Tab_Service_Monitoring_Probes_DNS_Name_Resolution bereitstellen.

Tabelle 8: Tab_Service_Monitoring_Probes_DNS_Name_Resolution

ENTWURF

Element	Beschreibung
Benennung der Probe	DNS_Name_Resolution
Dienst	Namensdienst
Schnittstelle	I_DNS_Name_Resolution
Operation	get_IP_Address
Netzwerk	Internet zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für • die autoritativen Nameserver des Namensdienstes • alle Bestandsnetze (implizit I_Secure_Access_Bestandsnetz)
Vorbedingung	Die DNS-Nameserver und die aufzulösenden FQDN müssen in der Probe konfigurierbar sein.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jeden DNS-Nameserver verfügbar sein.
Standardablauf	1. Die Probe ruft für jeden DNS-Nameserver TUC_SM_001_DNS_Name_Resolution mit der FQDN und den Service Monitoring Daten für diese Operation auf.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.

⌫

5.4.2 Konnektorregistrierung

⌦ **TIP1-A_7150 Service Monitoring, Probe Konnektorregistrierung**

Das Service Monitoring MUSS die Probe Konnektorregistrierung entsprechend Tab_Service_Monitoring_Probes_Konnektorregistrierung bereitstellen.

Tabelle 9: Tab_Service_Monitoring_Probes_Konnektorregistrierung

Element	Beschreibung
Benennung der Probe	Konnektorregistrierung
Dienst	Registrierungsserver
Schnittstelle	I_Registration_Service
Operation	registerKonnektor deregisterKonnektor
Netzwerk	Internet
Beschreibung	Diese Probe wird ausgeführt für alle Standorte des VPN-ZugD, inkl. der Schnittstelle I_DNS_Name_Resolution (implizit für Namensraum Internet). Es wird ein Konnektor registriert und gleich wieder deregistriert. Dieser Konnektor bzw. die ContractID wird nur für diese Probe genutzt. In anderen Probes benötigte VPN-Kanäle werden mit separaten Konnektorregistrierungen/ContractIDs realisiert.

ENTWURF

Element	Beschreibung
Vorbedingung	Der Betreiber des Registrierungsservers muss informiert sein, dass für eine festgelegte Contract-ID durch die Probes häufig eine Registrierung und Deregistrierung erfolgt. Der Konnektor (den die Probe simuliert) muss für alle VPN-Zugangsdienste registriert sein. In der Probe müssen für jeden VPN-Zugangsdienstanbieter folgende Daten konfigurierbar sein: - DNS_SERVERS_INT (DNS-Server im Internet) - DNS_DOMAIN_VPN_ZUGD_INT (alle DNS-Domainnamen für die Service Discovery der VPN-Konzentratoren) - ContractID Das Zertifikat ID.NK.VPN (SMC-K) muss vorliegen (für die Erstellung des registerKonnektor Requests nötig). Sie SMC-B muss für die Signatur des Registrierungsrequests freigeschaltet sein.
Nachbedingung	Im Service Monitoring müssen die definierten Daten für jeden VPN-Konzentrator des entsprechenden VPN-Zugangsdienstes verfügbar sein: • für die Teilschritte des Standardablaufs der Probe (wie im Standardablauf definiert) • für jeden gesamten Probe Lauf für einen VPN-Konzentrator
Standardablauf	1. Ermittlung der URI aller Registrierungsservers für alle DNS-Domänen (siehe auch TIP1-A_4825 [gemSpec_Kon]). • Falls der DNS-Namensdienst keine erwartete Antwort und keine Fehlermeldung liefert, wird die Erreichbarkeit des DNS-Namensdienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit Punkt 3 und „Probe-Ergebnis“ o 7100 Namensdienst nicht erreichbar oder o 7101 Ports vom Namensdienst geschlossen oder o 7103 Aufruf mit Fehler beendet beendet. • Falls der DNS-Namensdienst eine valide Antwort ohne Informationen über die Registrierungsserver oder eine Fehlermeldung liefert wird die Probe mit Punkt 3 („Probe-Ergebnis“ = 7104) beendet.
	2. Für jeden ermittelten Registrierungsservers:
	2.1. Erstellung eines registerKonnektor-Requests inklusive Signatur durch SM-B / ID.HCI.OSIG mit passender ContractID für die DNS Domäne (siehe auch TIP1-A_4390 [gemSpec_VPN_ZugD] bzw. TIP1-A_4825 [gemSpec_Kon]).
	2.2. Aufruf Operation I_Registration_Service::registerKonnektor (siehe auch TIP1-A_4390 [gemSpec_VPN_ZugD] bzw. TIP1-A_4825 [gemSpec_Kon]).
	2.3. Ermittlung der Service Monitoring-Daten für Operation registerKonnektor entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2.4. Auf- und Abbau eines TI-/SIS-Tunnels entsprechend Probe „ VPN Tunnel“ als Nachweis, dass der gerade registrierte Konnektor bzw. seine Zertifikate durch das ZugD-Netz korrekt propagiert wurden, und für die TI-Verbindungen verwendet werden können.
	2.5. Erstellung einer deRegisterKonnektorRequest-Struktur inklusive Signatur durch SM-B / ID.HCI.OSIG (siehe auch TIP1-A_4391 [gemSpec_VPN_ZugD] bzw. TIP1-A_4827 [gemSpec_Kon])

ENTWURF

Element	Beschreibung
	2.6. Aufruf Operation I_Registration_Service::deRegisterKonnektor (siehe auch TIP1-A_4827 [gemSpec_Kon]) mit der URI des Registrierungsservers. Auch wenn die Operation registerKonnektor fehlschlägt, weil der Konnektor schon registriert ist, muss die Operation deRegisterKonnektor ausgeführt werden (um wieder den Ausgangszustand für die Probe herzustellen).
	2.7. Ermittlung der Service Monitoring-Daten für Operation deRegisterKonnektor entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2.8. Ermittlung der Service Monitoring-Daten für den gesamten Probe-Lauf entsprechend Tab_Service_Monitoring_Probe_Daten.
	3. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Registrierungsservers Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten Registrierungsserver fortgesetzt werden. Das „Probe-Ergebnis“ für den Aufruf dieses Registrierungsservers wird auf o 7100 Registrierungsserver nicht erreichbar oder o 7101 Ports vom Registrierungsserver geschlossen oder o 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.3 VPN_Tunnel

⌦ **TIP1-A_7151 Service Monitoring, Probe VPN Tunnel**

Das Service Monitoring MUSS die Probe VPN-Tunnel entsprechend Tab_Service_Monitoring_Probes_VPN_Tunnel bereitstellen.

Tabelle 10: Tab_Service_Monitoring_Probes_VPN_Tunnel

Element	Beschreibung
Benennung der Probe	VPN Tunnel
Dienst	VPN-Zugangsdienst
Schnittstelle	I_Secure_Channel_Tunnel I_IP_Transport
Operation	I_Secure_Channel_Tunnel::connect I_Secure_Channel_Tunnel::send_secure_IP_Packet I_Secure_Channel_Tunnel::disconnect
Netzwerk	Internet

ENTWURF

Element	Beschreibung
Beschreibung	Diese Probe wird ausgeführt für alle VPN-Konzentratoren aller Standorte des VPN-ZugD, inkl. der Schnittstelle I_DNS_Name_Resolution (implizit für Namensraum Internet und TI). Die Probe wird für jeden VPN-Konzentrator ausgeführt. Es wird ein VPN-Tunnel auf- und – nach Senden von Datenpaketen – wieder abgebaut.
Vorbedingung	Der Konnektor (den die Probe simuliert) muss für alle VPN-Zugangsdienste registriert sein. Die Probe muss für jeden VPN-Zugangsdienstanbieter mit folgenden Daten konfigurierbar sein: • DNS_SERVERS_INT (DNS Server im Internet) • DNS_DOMAIN_VPN_ZUGD_INT (alle DNS-Domainnamen für die Service Discovery der VPN-Konzentratoren) • ContractID • Dauer der IPSec-Verbindung
Nachbedingung	Im Service Monitoring müssen die definierten Daten den VPN-Konzentrator verfügbar sein: • für die Teilschritte des Standardablaufs der Probe (wie im Standardablauf definiert) • für jeden gesamten Probe Lauf für einen VPN-Konzentrator
Standardablauf	1. Liste der VPN-Konzentratoren über DNS-SRV ermitteln (siehe auch TIP1-A_4373 [gemSpec_VPN_ZugD]). • Falls der DNS-Namensdienst keine erwartete Antwort und keine Fehlermeldung liefert, wird die Erreichbarkeit des DNS-Namensdienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit Punkt 3 und „Probe-Ergebnis“ o 7100 Namensdienst nicht erreichbar oder o 7101 Ports vom Namensdienst geschlossen oder o 7103 Aufruf mit Fehler beendet beendet. • Falls der DNS-Namensdienst eine valide Antwort ohne Informationen über die Registrierungsserver oder eine Fehlermeldung liefert, wird die Probe mit Punkt 3 („Probe-Ergebnis“ = 7104) beendet.
	2. Für jeden ermittelten VPN-Konzentrator muss die Probe mit den folgenden Unterpunkten einen Tunnelaufbau-Test durchführen.
	2.1. Aufbau einer Verbindung zum VPN-Konzentrator (siehe auch TUC_VPN-ZD_0001 [gemSpec_VPN_ZugD] bzw. TIP1-A_4783 [gemSpec_Kon]).
	2.2. Ermittlung der Service Monitoring-Daten für den Verbindungsaufbau entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2.3. Senden eines Datenpakets über den VPN Tunnel und Empfang eines Antwortpakets (siehe auch [gemSpec_VPN_ZugD#5.1.3]). Das kann z.B. ein Ping (ICMP-„Echo-Request“) zu einem zentralen Dienst der TI sein. Das Senden des Datenpakets muss mit dem Betreiber des zentralen Dienstes abgestimmt sein.
	2.4. Ermittlung der Service Monitoring-Daten für die Übertragung des Datenpakets entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.

ENTWURF

Element	Beschreibung
	2.5. Abbau der Verbindung zum VPN-Konzentrator (siehe auch TIP1-A_4389 [gemSpec_VPN_ZugD]) nach der konfigurierten Zeit (Dauer der IPSec-Verbindung). Falls die Verbindung vor der konfigurierten Zeit abbricht, MUSS dies in den Service Monitoring-Daten erfasst werden. Auch wenn der Verbindungsaufbau zum VPN-Konzentrator fehlgeschlagen ist, weil der Konnektor bzw. die Probe schon eine Verbindung aufgebaut hat, muss die Operation I_Secure_Channel_Tunnel::disconnect ausgeführt werden (um wieder den Ausgangszustand für die Probe herzustellen).
	2.6. Ermittlung der Service Monitoring-Daten für den Verbindungsabbau entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2.7. Ermittlung der Service Monitoring-Daten für den gesamten Probe-Lauf entsprechend Tab_Service_Monitoring_Probe_Daten.
	3. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des VPN-Konzentrators Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung (TCP Ports 500 und 4500) geprüft und die Probe mit dem nächsten VPN-Konzentrator fortgesetzt werden. Das „Probe-Ergebnis“ für diesen VPN-Konzentrator wird auf o 7100 VPN-Konzentrator nicht erreichbar oder o 7101 Ports vom VPN-Konzentrator geschlossen oder o 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.4 VPN_Tunnel SIS

⌦ **TIP1-A_7152 Service Monitoring, Probe VPN Tunnel SIS**

Das Service Monitoring MUSS die Probe VPN Tunnel SIS entsprechend Tab_Service_Monitoring_Probes_VPN_Tunnel mit folgenden Änderungen für den VPN-Konzentrator SIS realisieren:

- Benennung der Probe: VPN Tunnel SIS
- Dienst: VPN-Zugangsdienst SIS
- Schnittstelle: I_Secure_Internet_Tunnel
- Operation: I_Secure_Internet_Tunnel::connect
  I_Secure_Internet_Tunnel::send_secure_IP_Packet
  I_Secure_Internet_Tunnel::disconnect
- Vorbedingung:
  Zusätzlich muss mit der genutzten ContractID ein VPN Tunnel aufgebaut sein.

ENTWURF

- Standardablauf Punkt 2.3: Folgende Prüfungen werden durchgeführt:
  - DNS-Abfrage zum SIS-zugehörigen DNS-Server.
  - ICMP Request auf drei Server z.B. heise.de, google.de, Bertelsmann.de und Auswertung der Response (Laufzeit und Erhalt werden erfasst)
  - HTTPS GET auf drei Server z.B. https://www.heise.de/, https://www.google.de/, https://www.commerzbank.de/ und Auswertung der Response (Erhalt, TCP Connect Time, TTFB)
- Für diese Probe sind die Anforderungen zur Schnittstelle I_Secure_Channel_Tunnel [gemSpec_VPN_ZugD] relevant.

⌫

5.4.5 Zeitinformation_TI

⌦ **TIP1-A_7153 Service Monitoring, Probe Zeitinformation TI**

Das Service Monitoring MUSS die Probe Zeitinformation TI entsprechend Tab_Service_Monitoring_Probes_Zeitinformation_TI bereitstellen.

Tabelle 11: Tab_Service_Monitoring_Probes_Zeitinformation_TI

Element	Beschreibung
Benennung der Probe	Zeitinformation TI
Dienst	Zeitdienst
Schnittstelle	I_NTP_Time_Information
Operation	sync_Time
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle Stratum-1-NTP-Server der TI.
Vorbedingung	Die NTP-Server der TI müssen für die Probe konfigurierbar sein.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jeden NTP-Server verfügbar sein.
Standardablauf	1. Die Probe führt für jeden NTP-Server die folgenden Schritte durch:
	1.1. Ermittlung der IP-Adresse des NTP-Servers durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	1.2. Die Probe ermittelt von dem NTP-Server die Zeit über das NTPv4 Protokoll (siehe auch GS-A_3934 [gemSpec_Net]).
	1.3. Ermittlung der Service Monitoring-Daten für den NTP-Server entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“

ENTWURF

Element	Beschreibung
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des NTP-Servers Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten NTP-Server fortgesetzt werden. Das „Probe-Ergebnis“ für diesen NTP-Server wird auf o 7100 NTP-Servers nicht erreichbar oder o 7101 Ports vom NTP-Servers geschlossen oder o 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.6 Zeitinformation_VPN_Zugangsdienst

⌦ **TIP1-A_7154 Service Monitoring, Probe Zeitinformation VPN Zugangsdienst**

Das Service Monitoring MUSS die Probe Zeitinformation VPN-Zugangsdienst entsprechend Tab_Service_Monitoring_Probes_Zeitinformation_TI für die Stratum-2-NTP-Server mit folgenden Änderungen für die Zeitinformation VPN-Zugangsdienst realisieren:

- Benennung der Probe: Zeitinformation VPN-Zugangsdienst
- Netzwerk: Internet
- Beschreibung:

  Diese Probe wird ausgeführt für alle Stratum-2-NTP-Server aller VPN Zugangsdienste.
- Vorbedingung:
  - Die Stratum-2-NTP-Server der TI MÜSSEN für die Probe konfigurierbar sein.
  - VPN-Tunnel zu allen VPN Zugangsdiensten sind aufgebaut.

⌫

5.4.7 CRL Download

⌦ **TIP1-A_7155 Service Monitoring, Probe CRL Download**

Das Service Monitoring MUSS die Probe CRL Download entsprechend Tab_Service_Monitoring_Probes_CRL_Download bereitstellen.

Tabelle 12: Tab_Service_Monitoring_Probes_CRL_Download

Element	Beschreibung

ENTWURF

Element	Beschreibung
Benennung der Probe	CRL Download
Dienst	Trust Service Provider X.509 nonQES
Schnittstelle	I_CRL_Download
Operation	download_CRL
Netzwerk	Internet
Beschreibung	Diese Probe wird ausgeführt für alle CRL Distribution Points (CDP).
Vorbedingung	Die CRL Distribution Points (CDP) müssen für die Probe konfigurierbar sein.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jeden CRL Distribution Point (CDP) verfügbar sein.
Standardablauf	1. Die Probe führt für jeden CRL Distribution Point (CDP) die folgenden Schritte durch:
	1.1. Ermittlung der IP-Adresse des CRL Distribution Points durch TUC_SM_001_DNS_Name_Resolution.
	1.2. Die Probe lädt die CRL vom CRL Distribution Point (siehe auch TIP1-A_4248 [gemSpec_X.509_TSP]). Falls die CRL nicht auf dem CRL Distribution Point vorliegt wird der gelieferte Fehlercode in den Service Monitoring Daten erfasst.
	1.3. Ermittlung der Service Monitoring-Daten für den CRL Distribution Point entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf beim Laden der CRL Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten CRL Distribution Point fortgesetzt werden. Das „Probe-Ergebnis“ für diesen CRL Distribution Point wird auf o 7100 CRL Distribution Point nicht erreichbar oder o 7101 Ports vom CRL Distribution Point geschlossen oder o 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.8 TSL Download

⌦ **TIP1-A_7156 Service Monitoring, Probe TSL Download**

Das Service Monitoring MUSS die Probe TSL Download entsprechend Tab_Service_Monitoring_Probes_TSL_Download bereitstellen.

Tabelle 13: Tab_Service_Monitoring_Probes_TSL_Download

Element	Beschreibung

ENTWURF

Element	Beschreibung
Benennung der Probe	TSL Download
Dienst	TSL-Dienst
Schnittstelle	I_TSL_Download
Operation	download_TSL
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für den TSL Dienst.
Vorbedingung	Die URL(s) für den Download der TSL vom TSL-Dienst muss für die Probe konfigurierbar sein.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für den TSL Dienst verfügbar sein.
Standardablauf	1. Die Probe führt für jede TSL-Download-Adresse die folgenden Schritte durch:
	1.1. Ermittlung der IP-Adresse des TSL-Dienstes durch TUC_SM_001_DNS_Name_Resolution.
	1.2. Die Probe lädt die TSL (siehe auch [gemSpec_TSL#6.3.1]).
	1.3. Ermittlung der Service Monitoring-Daten für den Download entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf beim Laden der TSL Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit der nächsten TSL-Download-Adresse fortgesetzt werden. Das „Probe-Ergebnis“ wird für diesen TSL Download-Punkt auf o 7100 TSL Download-Punkt nicht erreichbar oder o 7101 Ports vom TSL Download-Punkt geschlossen oder o 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.9 TSL Download mit Prüfung

⌦ **TIP1-A_7157 Service Monitoring, Probe TSL Download mit Prüfung**

Das Service Monitoring MUSS die Probe TSL Download mit Prüfung entsprechend Tab_Service_Monitoring_Probes_TSL_Download bereitstellen.

Folgende Abweichungen von Tab_Service_Monitoring_Probes_TSL_Download MÜSSEN beachtet werden:

- Benennung der Probe: TSL-Download mit Prüfung
- Standardablauf:

ENTWURF

- Nach dem Laden der TSL erfolgt die Prüfung der TSL entsprechend TUC_PKI_019 [gemSpec_PKI].
- Stellt die TSL-Prüfung einen Fehler in der TSL fest wird das „Probe-Ergebnis“ auf 7106 gesetzt.

⌫

5.4.10 TSL Download IPsecTunnel TI

⌦ **TIP1-A_7158 Service Monitoring, Probe TSL Download IPsecTunnel TI**

Das Service Monitoring MUSS die Probe TSL Download IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_TSL_Download bereitstellen. Die Probe TSL Download IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI einen IPsecTunnel nutzen.

Folgende Abweichungen von Tab_Service_Monitoring_Probes_TSL_Download MÜSSEN beachtet werden:

- Benennung der Probe: TSL Download IPsecTunnel TI
- Netzwerk: IPsec Tunnel TI
- Vorbedingung:
  - Zusätzlich wird für den Aufbau des IPsec-Tunnels das SMC-K Zertifikat ID.NK.VPN benötigt.
  - Der der IPsec-Tunnel zur TI MUSS aufgebaut sein.

⌫

5.4.11 TSL Download Internet

⌦ **TIP1-A_7159 Service Monitoring, Probe TSL Download Internet**

Das Service Monitoring MUSS die Probe TSL Download Internet entsprechend Tab_Service_Monitoring_Probes_TSL_Download bereitstellen. Die Probe TSL Download Internet MUSS die TSL vom TSL-Dienst im Internet laden.

Folgende Abweichungen von Tab_Service_Monitoring_Probes_TSL_Download MÜSSEN beachtet werden:

- Benennung der Probe: TSL Download Internet
- Netzwerk: Internet
- Vorbedingung: Die Internet-TSL-Dienst-URL wird für die Probe konfiguriert.

⌫

ENTWURF

5.4.12 BNetzA_VL Download

⌦ **TIP1-A_7160 Service Monitoring, Probe BNetzA Download**

Das Service Monitoring MUSS die Probe BNetzA Download entsprechend Tab_Service_Monitoring_Probes_BNetzA_Download bereitstellen.

Tabelle 14: Tab_Service_Monitoring_Probes_BNetzA_Download

Element	Beschreibung
Benennung der Probe	BNetzA Download
Dienst	TSL-Dienst
Schnittstelle	I_BNetzA_VL_Download
Operation	download_VL
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle ServiceSupplyPoints für die BNetzA-VL.
Vorbedingung	Die Download-Adressen der BNetzA-VL müssen konfigurierbar sein.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Die Probe führt für jede Download-Adresse der BNetzA-VL die folgenden Schritte durch:
	1.1. Ermittlung der IP-Adresse der BNetzA-VL Download-Adresse durch TUC_SM_001_DNS_Name_Resolution.
	1.2. Die Probe lädt die BNetzA-VL vom Download-Adresse (siehe auch TIP1-A_4248 [gemSpec_PKI]).
	1.3. Ermittlung der Service Monitoring-Daten für den BNetzA-VL Download entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf beim Laden der BNetzA-VL Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit der nächsten BNetzA-VL Adresse fortgesetzt werden. Das „Probe-Ergebnis“ wird für diese Download-Punkt der BNetzA-VL auf • 7100 Download-Punkt der BNetzA-VL nicht erreichbar oder • 7101 Ports vom Download-Punkt der BNetzA-VL geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

⌫

ENTWURF

5.4.13 BNetzA Download IPsecTunnel TI

⌦ **TIP1-A_7310 Service Monitoring, Probe BNetzA Download IPsecTunnel TI**

Das Service Monitoring MUSS die Probe BNetzA Download IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_BNetzA_Download bereitstellen. Die Probe BNetzA Download IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI einen IPsec-Tunnel nutzen.

Folgende Abweichungen von Tab_Service_Monitoring_Probes_BNetzA_Download sind zu beachteten:

- Benennung der Probe: BNetzA Download IPsecTunnel TI
- Netzwerk: IPsec Tunnel TI
- Vorbedingung:
  - Zusätzlich wird für den Aufbau des IPsec-Tunnels das SMC-K Zertifikat ID.NK.VPN benötigt.
  - Der IPsec Tunnel zur TI ist aufgebaut.

⌫

5.4.14 OCSP

⌦ **TIP1-A_7311 Service Monitoring, Probe OCSP**

Das Service Monitoring MUSS die Probe OCSP entsprechend Tab_Service_Monitoring_Probes_OCSP bereitstellen.

Tabelle 15: Tab_Service_Monitoring_Probes_OCSP

Element	Beschreibung
Benennung der Probe	OCSP
Dienst	TSL-Dienst
Schnittstelle	I_OCSP_Status_Information
Operation	check_Revocation_Status
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle ServiceSupplyPoints in der TSL (inkl. alle ServiceSupplyPoints in der VL über den OCSP-Responder Proxy).
Vorbedingung	In der Probe müssen folgende Daten konfigurierbar sein: • OCSP-Responder Adressen • Für jeden OCSP-Responder müssen Zertifikatsdaten für die OCSP-Abfrage konfigurierbar sein Die OCSP-Responder Adressen können optional auch aus der TSL ermittelt werden. Die manuelle Konfiguration der OCSP-Adressen muss auch in diesem Fall alternativ möglich sein.

ENTWURF

Element	Beschreibung
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Die Probe führt für jeden OCSP-Responder die folgenden Schritte durch:
	1.1. Ermittlung der IP-Adresse des OCSP-Responder ServiceSupplyPoints durch TUC_SM_001_DNS_Name_Resolution.
	1.2. Die Probe führt eine OCSP-Abfrage entsprechend GS-A_4657 TUC_PKI_006 [gemSpec_PKI] durch.
	1.3. Ermittlung der Service Monitoring-Daten für die OCSP-Abfrage entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den OCSP Abfragen Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten OCSP-Responder fortgesetzt werden. Das „Probe-Ergebnis“ wird für diesen OCSP auf • 7100 OCSP nicht erreichbar oder • 7101 Ports vom OCSP geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.15 OCSP IPsecTunnel TI

⌦ **TIP1-A_7312 Service Monitoring, Probe OCSP IPsecTunnel TI**

Das Service Monitoring MUSS die Probe OCSP IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_OCSP bereitstellen. Die Probe BNetzA Download IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI einen IPsecTunnel nutzen.

Folgende Abweichungen von Tab_Service_Monitoring_Probes_OCSP sind zu beachteten:

- Benennung der Probe: OCSP IPsecTunnel TI
- Netzwerk: IPsec Tunnel TI
- Beschreibung:

  Diese Probe wird ausgeführt für jeden VPN-Zugangsdienst und jeden Standort eines VPN-Zugangsdienstes (für alle ServiceSupplyPoints in der TSL über den http-Forwarder)
- Standardablauf:

  Die OCSP-Abfrage wird über den http-Forwarder ausgeführt
- Vorbedingung:

ENTWURF

- Zusätzlich wird für den Aufbau des IPsec Tunnels das SMC-K Zertifikat ID.NK.VPN benötigt.
- Der der IPsec Tunnel zur TI muss aufgebaut sein.

⌫

5.4.16 Fachdienste VSDM

⌦ **TIP1-A_7313 Service Monitoring, Probe Fachdienste VSDM**

Das Service Monitoring MUSS die Konfiguration der Fachdienste VSDM Probes mit jedem Fachdienstbetreiber abstimmen und individuell für jeden Fachdienst konfigurieren.⌫

5.4.16.1 Fachdienst VSDM UFS

⌦ **TIP1-A_7314 Service Monitoring, Probe UFS**

Das Service Monitoring MUSS die Probe UFS entsprechend Tab_Service_Monitoring_Probes_UFS bereitstellen.

Tabelle 16: Tab_Service Monitoring_Probes_UFS

Element	Beschreibung
Benennung der Probe	UFS
Dienst	Update Flag Service
Schnittstelle	I_UFS
Operation	GetUpdateFlags
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle UFS-Fachdienste.
Vorbedingung	Die Daten für alle UFS-Fachdienste – welche durch die Probe aufgerufen werden – müssen konfigurierbar sein. Für den Aufruf von Operation I_UFS::GetUpdateFlags müssen folgende Werte in der Probe für den jeweiligen UFS konfigurierbar sein: • URL des Fachdienstes UFS • ServiceType (UFS) • ICCSN • Provider ID • Erwartete Fachdienstantwort/Fehlercode Die Probe muss sowohl eine korrekte Fachdienst-Antwort (mit UpdateID oder ServiceReceipt) wie auch einen SOAP-Fehler mit Fehlercode (z.B. 11101) als erwartete Antwort akzeptieren können. Die Probe muss über ein TLS-Client-Zertifikat (C.FD.TLS-C) für den Verbindungsaufbau zum UFS verfügen.
Nachbedingung	Im Service Monitoring müssen für die gesamte Probe und für die Teilschritte des Probe-Ablaufs die dort definierten Daten für den UFS verfügbar sein. Falls der Fachdienst UFS eine UpdateID liefert, muss sie in einem folgenden Aufruf des VSDD- oder CMS-Fachdienstes als Eingangsparameter nutzbar sein.

ENTWURF

Element	Beschreibung
Standardablauf	1. Für jeden Fachdienst:
	1.1. Ermittlung der IP-Adresse des UFS durch eine DNS-Anfrage (DNS-SRV Fachdienst) mit TUC_SM_001_DNS_Name_Resolution.
	1.2. Verbindungsaufbau zum UFS unter Nutzung des TLS-Client-Zertifikats.
	1.3. Senden des GetUpdateFlags Requests zum UFS unter Nutzung der Konfigurationsparameter ICCSN und Provider ID [gemSpec_SST_FD_VSDM#3.1].
	1.4. Das vom Fachdienst gelieferte Ergebnis wird mit der erwarteten Fachdienstantwort/Fehlercode verglichen. Das Fachdienstergebnis ist von den Konfigurationsparametern ProviderId und ICCSN abhängig. Für eine nicht existierende ICCSN wird als Ergebnis ein Gematik SOAP Fault mit Fehlercode 11101 (für die eGK mit der angegebenen ICCSN ist der aufgerufene Dienst nicht zuständig) erwartet. Für eine existierende ICCSN wird eine korrekte Fachdienst Antwort (mit UpdateID oder ServiceReceipt) erwartet.
	1.5. Ermittlung der Service Monitoring-Daten für Operation GetUpdateFlags entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Ermittlung der Service Monitoring-Daten für die gesamte Probe und Rückgabe aller Datensätze an das Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Fachdienstes Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten Fachdienst fortgesetzt werden. Das „Probe-Ergebnis“ wird für diesen Fachdienst auf • 7100 Fachdienst nicht erreichbar oder • 7101 Ports vom Fachdienst geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.16.2 Fachdienst VSDM_VSDD_CMS

⌦ **TIP1-A_7315 Service Monitoring, Probe VSDD_CMS**

Das Service Monitoring MUSS die Probe VSDD_CMS entsprechend Tab_Service_Monitoring_Probes_VSDD_CMS bereitstellen.

Tabelle 17: Tab_Service_Monitoring_Probes_VSDD_CMS

Element	Beschreibung
Benennung der Probe	VSDD_CMS
Dienst	VSDD- und CMS-Fachdienste
Schnittstelle	I_CCS
Operation	PerformUpdates

ENTWURF

Element	Beschreibung
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle VSDD- und CMS-Fachdienste.
Vorbedingung	Die Daten für alle VSDD- und CMS-Fachdienste – welche durch die Probe aufgerufen werden – müssen konfigurierbar sein. Für den Aufruf der Operationen PerformUpdates müssen folgende Werte in der Probe individuell für den jeweiligen Fachdienst konfigurierbar sein: • URL des Fachdienstes • ICCSN • ServiceType (VSD | CMS) • Provider ID • UpdateID Die UpdateID muss konfigurierbar und aus der vorangehenden Operation GetUpdateFlags übernehmbar sein. • Der kartenindividuelle symmetrische Schlüssel für die ICCSN muss optionaler konfigurierbar sein. • Update Flag verbrauchen (ja/nein) • Erwartete Fachdienstantwort/Fehlercode Die Probe muss sowohl korrekte Fachdienst-Antworten wie auch einen SOAP-Fehler mit Fehlercode (z.B. 12101) oder den Abbruch der Kommunikation beim Aufbau des sicheren Kanals vom Fachdienst zur eGK als erwartete Antwort akzeptieren. Die Probe muss über ein TLS-Client-Zertifikat (C.FD.TLS-C) für den Verbindungsaufbau zum Fachdienst verfügen.
Nachbedingung	Im Service Monitoring müssen für die gesamte Probe und für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Für jeden Fachdienst:
	1.1. Ermittlung der IP-Adresse des Fachdienstes durch eine DNS-Anfrage (DNS-SRV-Fachdienst) mit TUC_SM_001_DNS_Name_Resolution.
	1.2. Verbindungsaufbau zum Fachdienst unter Nutzung des TLS-Client-Zertifikats.
	1.3 Durchführung einer komplette Aktualisierung der eGK mit den SOAP-Requests PerformUpdates und GetNextCommandPackage gemäß [gemSpec_SST_FD_VSDM#4] unter Nutzung der Konfigurationsparameter. Abhängig von den Konfigurationsparametern kann der Fachdienst mit einem SOAP-Fehler antworten wenn z.B. keine „echte“ ICCSN genutzt wird oder kein Update vorliegt. Falls der kartenindividuelle symmetrische Schlüssel für die ICCSN nicht vorliegt, wird nach Senden des PerformUpdates an den Fachdienst der Probe-Lauf für diesen Fachdienst mit einem Fehler beendet. Falls Konfigurationsparameter „Update Flag verbrauchen“ auf „nein“ gesetzt ist, muss die Aktualisierung bei dem letzten GetNextCommandPackage mittels dem Element Abort abgebrochen werden, so dass das Update-Flag nach dem Aktualisierungsversuch nicht im Fachdienst UFS gelöscht wird und erneut für eine Aktualisierung verwendet werden kann.
	1.4. Das vom Fachdienst gelieferte Ergebnis wird mit der erwarteten Fachdienstantwort/Fehlercode verglichen. Das Fachdienstergebnis ist von den Konfigurationsparametern ServiceType, ProviderId, UpdateId und ICCSN abhängig. Die Probe prüft, ob die Fachdienstantwort den Erwartungen (siehe Vorbedingungen) entspricht. Falls die Fachdienstantwort von dem erwarteten Ergebnis abweicht, wird das in den Daten für das Service Monitoring erfasst.

ENTWURF

Element	Beschreibung
	Zum Beispiel wird für eine nicht existierende ICCSN und UpdateId als Ergebnis ein Gematik SOAP Fault mit Fehlercode 12101 (Für die angegebene Kombination aus ICCSN und Update-Identifier liegt kein Update vor) erwartet.
	1.5. Ermittlung der Service Monitoring-Daten für Operation PerformUpdates entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Ermittlung der Service Monitoring-Daten für die gesamte Probe und Rückgabe aller Datensätze an das Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Fachdienstes Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten Fachdienst fortgesetzt werden. Das „Probe-Ergebnis“ wird für diesen Fachdienst auf • 7100 Fachdienst nicht erreichbar oder • 7101 Ports vom Fachdienst geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.17 Intermediär VSDM

⌦ **TIP1-A_7316 Service Monitoring, Probe Intermediär VSDM**

Das Service Monitoring MUSS die Probe Intermediär VSDM entsprechend Tab_Service Monitoring_Probes_Intermediär_VSDM bereitstellen.

Tabelle 18: Tab_Service_Monitoring_Probes_ Intermediär_VSDM

Element	Beschreibung
Benennung der Probe	Intermediär VSDM
Dienst	Intermediär VSDM
Schnittstelle	I_TLS Intermediär
Operation	GetUpdateFlags via Intermediär
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für jeden Intermediär.
Vorbedingung	Für den Aufruf von Operation I_UFS::GetUpdateFlags via Intermediär müssen folgende Werte in der Probe für den jeden Intermediär individuell konfigurierbar sein. • URL des Intermediär • ServiceType (UFS) • Schnittstellen-Version UFS (2.0) • ICCSN • Provider ID Die Probe muss über eine SM-B-Prüfkarte (bzw. das AUT-Zertifikat dieser Karte entsprechend [gemSpec_SST_VSDM#2.4.1]) für den Verbindungsaufbau zum Intermediär verfügen.

ENTWURF

Element	Beschreibung
	Die SM-B muss freigeschaltet sein. Weiterhin muss für die Probe mit einem Fachdienstbetreiber die Verwendung von einem Fachdienst UFS abgesprochen sein.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Für jeden Intermediär:
	1.1. Ermittlung der IP-Adresse des Intermediär VSDM durch eine DNS-Anfrage (DNS-SRV Intermediär) mit TUC_SM_001_DNS_Name_Resolution.
	1.2. Verbindungsaufbau zum Intermediär VSDM unter Nutzung des TLS-Client-Zertifikats (SM-B AUT Zertifikat).
	1.3. Senden des GetUpdateFlags Requests zum Intermediär VSDM unter Nutzung der Konfigurationsparameter [gemSpec_SST_FD_VSDM#3.1].
	1.4. Als Ergebnis wird ein Gematik SOAP Fault mit Fehlercode 11101 (Für die eGK mit der angegebenen ICCSN ist der aufgerufene Dienst nicht zuständig) erwartet.
	1.5. Ermittlung der Service Monitoring-Daten für Operation GetUpdateFlags entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Ermittlung der Service Monitoring-Daten für die gesamte Probe und Rückgabe aller Datensätze an das Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Intermediärs Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten Intermediär fortgesetzt werden. Das „Probe-Ergebnis“ wird für diesen Intermediär auf • 7100 Intermediär nicht erreichbar oder • 7101 Ports vom Intermediär geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.18 VSDM- Intermediär VSDM IPsecTunnel TI

⌦ **TIP1-A_7317 Service Monitoring, Probe Intermediär VSDM IPsecTunnel TI**

Das Service Monitoring MUSS die Probe Intermediär VSDM IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_Intermediär_VSDM bereitstellen. Die Probe Intermediär VSDM IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI/Intermediär VSDM einen IPsecTunnel zum VPN-ZugD nutzen.

Folgende Abweichungen von Tab_Service_Monitoring_Probes_Intermediär_VSDM müssen beachtet werden:

- Benennung der Probe: Intermediär VSDM IPsecTunnel TI
- Netzwerk: IPsec Tunnel TI
- Vorbedingung:

ENTWURF

- Zusätzlich wird für den Aufbau des IPsec Tunnels das SMC-K Zertifikat ID.NK.VPN benötigt.
- Der der IPsec-Tunnel zur TI muss aufgebaut sein.

⌫

5.4.19 VSDM-Intermediär VSDM Erreichbarkeit

⌦ **TIP1-A_7318 Service Monitoring, Probe Intermediär VSDM Erreichbarkeit**

Das Service Monitoring MUSS die Probe Intermediär Erreichbarkeit entsprechend Tab_Service_Monitoring_Probes_Intermediär_VSDM bereitstellen. Mit dieser Probe wird die Erreichbarkeit des Intermediär VSDM geprüft. Mit einer fehlerhaften „Provider ID“ wird die Weiterleitung der UFS Anfrage an den Fachdienst verhindert.

Folgende Abweichungen von Tab_Service_Monitoring_Probes_Intermediär_VSDM MÜSSEN beachtet werden:

- Benennung der Probe: Intermediär VSDM Erreichbarkeit
- Vorbedingung:

  Es wird für „Provider ID“ eine nicht vorhandene Provider ID genutzt. Damit schlägt die Lokalisierung des Fachdienstes im Intermediär fehl. Der Intermediär liefert einen Fehlercode 502 [gemSpec_Intermediär_VSDM#3.5] an den Client.

  Ein Fachdienst UFS wird für diese Probe nicht benötigt.
- Standardablauf:

  Als Ergebnis wird vom Intermediär VSDM ein HTTP-Fehlercode 502 (Adresse des Fachdienstes nicht ermittelbar) erwartet.

⌫

5.4.20 KSRS Upload

⌦ **TIP1-A_7319 Service Monitoring, Probe KSRS Upload**

Das Service Monitoring MUSS die Probe KSRS Upload entsprechend Tab_Service_Monitoring_Probes_KSRS_Upload bereitstellen.

Tabelle 19: Tab_Service Monitoring_Probes_KSRS_Upload

Element	Beschreibung
Benennung der Probe	KSRS Upload
Dienst	KSR
Schnittstelle	P_KSRS_Upload
Operation	Erreichbarkeit KSRS-Upload-Schnittstelle

ENTWURF

Element	Beschreibung
Netzwerk	Internet
Beschreibung	Diese Probe wird ausgeführt für den KSR.
Vorbedingung	Für die Prüfung der Erreichbarkeit der KSRS-Upload-Schnittstelle müssen folgende Werte in der Probe konfigurierbar sein. • URL der KSRS-Upload-Schnittstelle
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Ermittlung der IP-Adresse der KSRS-Upload-Schnittstelle durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	2. Prüfung ob die KSRS-Upload-Webseite erreichbar ist. Die Prüfung kann z.B. mit einem HTTP HEAD Request [RFC 7231#4.3.2] auf die URL der KSRS-Upload-Schnittstelle erfolgen.
	3. Falls die KSRS-Upload-Webseite nicht erreichbar ist: Prüfung der Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung.
	5. Rückgabe der ermittelten Daten für die Erreichbarkeit der KSRS-Upload-Schnittstelle an das Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Kenngröße „Verfügbarkeit“.

⌫

5.4.21 KSRS Download

⌦ **TIP1-A_7320 Service Monitoring, Probe KSRS Download**

Das Service Monitoring MUSS die Probe KSRS Download entsprechend Tab_Service_Monitoring_Probes_KSRS_Download bereitstellen.

Tabelle 20: Tab_Service_Monitoring_Probes_KSRS_Download

Element	Beschreibung
Benennung der Probe	KSRS Download
Dienst	KSR
Schnittstelle	I_KSRS_Download
Operation	I_KSRS_Download::list_Updates I_KSRS_Download::get_Updates
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für den KSR.
Vorbedingung	Für die Operationen von Schnittstelle I_KSRS_Download müssen folgende Werte in der Probe konfigurierbar sein. • URL der KSRS-Download-Schnittstelle • ProductVendorID • ProductCode • Hardware Version (HWVersion) • Firmware Version (FMVersion)
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.

ENTWURF

Element	Beschreibung
Standardablauf	1. Ermittlung der IP-Adresse der KSRS-Download-Schnittstelle durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	2. TLS Verbindungsaufbau zum Konfigurationsdienst.
	3. Senden von Request I_KSRS_Download::listUpdates gemäß [gemSpec_KSR] an den Konfigurationsdienst
	4. Auswerten des Response gemäß I_KSRS_Download::get_Updates und Ermittlung der Service Monitoring-Daten für diese Operation entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	5. Download des Files „Bestandsnetze.xml“ mit I_KSRS_Download::get_Updates gemäß [gemSpec_KSR] vom Konfigurationsdienst. Dieses File wird hier verwendet, weil es immer auf dem KSR vorhanden ist und über die gleiche unterliegende Operation [gemSpec_KSR#TUC_KSR_001] bereitgestellt wird. Siehe I_KSRS_Download::get_Ext_Net_Config [gemSpec_KSR] für den Download dieses Files.
	6. Auswerten des Downloads gemäß I_KSRS_Download::get_Updates und Ermittlung der Service Monitoring-Daten für diese Operation entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	7. Speicherung der ermittelten Daten für die KSRS-Download-Schnittstelle im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des KSR Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft werden. Das „Probe-Ergebnis“ wird für die jeweilige KSR Operation auf • 7100 KSR nicht erreichbar oder • 7101 Ports vom KSR geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.22 KSRS Download IPsecTunnel TI

⌦ **TIP1-A_7321 Service Monitoring, Probe KSRS Download IPsecTunnel TI**

Das Service Monitoring MUSS die Probe KSRS Download IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_KSRS_Download bereitstellen. Die Probe KSRS Download IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI/Intermediär einen IPsecTunnel nutzen.

Folgende Abweichungen von Tab_Service_Monitoring_Probes_KSRS_Download sind zu beachten:

- Benennung der Probe: KSRS Download IPsecTunnel TI
- Beschreibung:

  Diese Probe wird ausgeführt für jeden VPN-Zugangsdienst Standort.

ENTWURF

- Vorbedingung:
  - Zusätzlich wird für den Aufbau des IPsec-Tunnels das SMC-K-Zertifikat ID.NK.VPN benötigt.
  - Zu jedem VPN-Zugangsdienst-Standort wird ein aufgebauter IPsec-Tunnel zur TI benötigt.
- Standardablauf:
  - Die Schritte des Standardablaufs in Tab_Service_Monitoring_Probes_KSRS_Download werden für jeden VPN-Zugangsdienst-Standort mit dem jeweiligen VPN-Kanal durchgeführt. Am Ende der Probe wird ein Service Monitoring-Datensatz für den gesamten Probe-Lauf erzeugt.

⌫

5.4.23 KSRS Download Bestandsnetze

⌦ **TIP1-A_7322 Service Monitoring, Probe KSRS Download Bestandsnetze**

Das Service Monitoring MUSS die Probe KSRS Download Bestandsnetze entsprechend Tab_Service_Monitoring_Probes_KSRS_Download_Bestandsnetze bereitstellen.

Tabelle 21: Tab_Service_Monitoring_Probes_KSRS_Download_Bestandsnetze

Element	Beschreibung
Benennung der Probe	KSRS Download Bestandsnetze
Dienst	KSR
Schnittstelle	I_KSRS_Net_Config
Operation	I_KSRS_Net_Config::get_Ext_Net_Config
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für den KSR.
Vorbedingung	Für die Operationen von Schnittstelle I_KSRS_Net_Config müssen folgende Werte in der Probe konfigurierbar sein: • URL der KSRS-Download-Schnittstelle
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Ermittlung der IP-Adresse der KSRS-Download-Schnittstelle durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	2. TLS Verbindungsaufbau zum Konfigurationsdienst.
	3. Download des Files „Bestandsnetze.xml“ mit I_KSRS_Net_Config::get_Ext_Net_Config Updates gemäß [gemSpec_KSR] vom Konfigurationsdienst.

ENTWURF

Element	Beschreibung
	4. Auswerten des Downloads gemäß I_KSRS_Net_Config::get_Ext_Net_Config und Ermittlung der Service Monitoring-Daten für diese Operation entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	5. Speicherung der ermittelten Daten für die KSRS-Download-Schnittstelle im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des KSR Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft werden. Das „Probe-Ergebnis“ wird auf • 7100 KSR nicht erreichbar oder • 7101 Ports vom KSR geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.24 KSRS Download Bestandsnetze IPsecTunnel TI

⌦ **TIP1-A_7323 Service Monitoring, Probe KSRS Download Bestandsnetze IPsecTunnel TI**

Das Service Monitoring MUSS die Probe KSRS Download Bestandsnetze IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_KSRS_Download_Bestandsnetze bereitstellen. Die Probe KSRS Download IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI/Intermediär einen IPsecTunnel nutzen.

Folgende Abweichungen von Tab_Service_Monitoring_Probes_KSRS_Download_Bestandsnetze MÜSSEN beachtet werden:

- Benennung der Probe: KSRS Download Bestandsnetze IPsecTunnel TI
- Vorbedingung:
  - Zusätzlich wird für den Aufbau des IPsec-Tunnels das SMC-K-Zertifikat ID.NK.VPN benötigt.
  - Der der IPsec-Tunnel zur TI ist aufgebaut.

⌫

5.4.25 Verzeichnisdienst Query

⌦ **TIP1-A_7324 Service Monitoring, Probe Verzeichnisdienst Query**

Das Service Monitoring MUSS die Probe Verzeichnisdienst Query entsprechend Tab_Service_Monitoring_Probes_Verzeichnisdienst_Query bereitstellen.

Tabelle 22: Tab_Service_Monitoring_Probes_Verzeichnisdienst_Query

ENTWURF

Element	Beschreibung
Benennung der Probe	Verzeichnisdienst Query
Dienst	Verzeichnisdienst
Schnittstelle	I_Directory_Query
Operation	I_Directory_Query::search_Directory
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für den Verzeichnisdienst.
Vorbedingung	Für die Operation I_Directory_Query::search_Directory müssen folgende Werte in der Probe konfigurierbar sein: • Suchkriterien für die LDAP Verzeichnisdienstabfrage
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Ermittlung FQDN und Port des Verzeichnisdienstes analog zu TIP1-A_5517 [gemSpec_Kon#4.1.12.4.1] entsprechend Tab_Service_Monitoring_Probes_DNS_Name_Resolution.
	2. LDAPS-Verbindungsaufbau zum Verzeichnisdienst (analog zu A_5517 [gemSpec_Kon#4.1.12.4.1]).
	3. Abfrage des Verzeichnisdienstes mit den konfigurierten Eingangsdaten analog zu TIP1-A_5518 [gemSpec_Kon#4.1.12.4.2].
	4. Auswerten der Verzeichnisdienst-Antwort und Ermittlung der Service Monitoring-Daten für diese Operation entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	5. Die Probe beendet die Verbindung zum Verzeichnisdienst (analog zu A_5519 [gemSpec_Kon#4.1.12.4.3]).
	6. Speicherung der ermittelten Daten für die Verzeichnisdienst I_Directory_Query Schnittstelle im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Verzeichnisdienstes Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft werden. Das „Probe-Ergebnis“ wird für diese Verzeichnisdienst Operation auf • 7100 Verzeichnisdienst nicht erreichbar oder • 7101 Ports vom Verzeichnisdienst geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.26 Verzeichnisdienst Query IPsecTunnel TI

⌦ **TIP1-A_7325 Service Monitoring, Probe Verzeichnisdienst Query IPsecTunnel TI**

Das Service Monitoring MUSS die Probe Verzeichnisdienst Query IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_Verzeichnisdienst_Query

bereitstellen. Die Probe Verzeichnisdienst Query IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI/-Verzeichnisdienst einen IPsecTunnel nutzen.

Folgende Abweichungen von Tab_Service_Monitoring_Probes_Verzeichnisdienst_Query MÜSSEN beachtet werden:

- Benennung der Probe: Verzeichnisdienst Query IPsecTunnel TI
- Vorbedingung:
  - Zusätzlich wird für den Aufbau des IPsec Tunnels das SMC-K-Zertifikat ID.NK.VPN benötigt.
  - Der der IPsec-Tunnel zur TI ist aufgebaut.

⌫

5.4.27 Verzeichnisdienst Application_Maintenance

⌦ **TIP1-A_7326 Service Monitoring, Probe Verzeichnisdienst Application Maintenance**

Das Service Monitoring MUSS die Probe Verzeichnisdienst Application Maintenance entsprechend Tab_Service_Monitoring_Probes_Verzeichnisdienst_Application_Maintenance bereitstellen.

Tabelle 23: Tab_Service_Monitoring_Probes_Verzeichnisdienst_Application_Maintenance

Element	Beschreibung
Benennung der Probe	Verzeichnisdienst Application Maintenance
Dienst	Verzeichnisdienst
Schnittstelle	I_Directory_Application_Maintenance
Operation	I_Directory_Application_Maintenance::add_Directory_FA-Attributes
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für den Verzeichnisdienst. Es wird die Webservice (SOAP) Ausprägung der Operationen genutzt.
Vorbedingung	Die Probe muss beim Verzeichnisdienst für die Nutzung der Schnittstelle registriert sein (TIP1-A_5604 [gemSpec_VZD]). Für den Aufbau einer TLS Verbindung muss die Probe über ein C.FD.TLS-C Zertifikat verfügen (TIP1-A_5585 [gemSpec_VZD]). Für diese Probe muss im Verzeichnisdienst ein Basisdatensatz verfügbar sein, dem ein Fachdatensatz hinzugefügt (bzw. ein existierender Fachdatensatz überschrieben) wird. Der Basisdatensatz muss mit dem Verzeichnisdienst-Betreiber abgestimmt sein. Für diese Probe müssen folgende Werte konfigurierbar sein: • Telematik-ID • fachdienstspezifische Attribute, welche mit dem SOAP-Request dem

ENTWURF

Element	Beschreibung
	Verzeichniseintrag hinzugefügt (bzw. überschrieben) werden
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Ermittlung FQDN und Port der Schnittstelle I_Directory_Application_Maintenance vom Verzeichnisdienst entsprechend Tab_Service_Monitoring_Probes_DNS_Name_Resolution.
	2. Ermittlung der IP-Adresse des Verzeichnisdienstes durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	3. TLS-Verbindungsaufbau zum Verzeichnisdienst. Die Probe muss sich mit dem Client Zertifikat C.FD.TLS-C authentisieren (TIP1-A_5585 [gemSpec_VZD]).
	4. Senden des add_Directory_FA-Attributes Requests an den Verzeichnisdienst mit den konfigurierten Eingangsdaten.
	5. Auswerten der Verzeichnisdienst Antwort und Ermittlung der Service Monitoring-Daten für diese Operation entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	6. Die Probe beendet die TLS-Verbindung zum Verzeichnisdienst.
	7. Speicherung der ermittelten Daten für die Verzeichnisdienst Schnittstelle _Directory_Application_Maintenance im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Verzeichnisdienstes Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft werden. Das „Probe-Ergebnis“ wird für diese Verzeichnisdienst Operation auf • 7100 Verzeichnisdienst nicht erreichbar oder • 7101 Ports vom Verzeichnisdienst geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

⌫

5.4.28 Erfassung von Service Monitoring-Daten in Probes

⌦ **TIP1-A_7327 Service Monitoring, Probes, Datenerfassung**

Das Service Monitoring MUSS die in Probes ermittelten Daten im Service Monitoring ablegen. Im Service Monitoring MÜSSEN für

- den gesamten Probe-Lauf ein Datensatz mit den Daten des Probe-Laufs und
- für jede aufgerufene Operation von überwachten Diensten einen Datensatz mit den ermittelten Kenngrößen und dem Ergebnis

erfasst werden.

In den internen Service Monitoring Daten MUSS die Zugehörigkeit aller geschriebenen Datensätze zu Probe-Läufen erfasst und für Aggregationsregeln auswertbar sein.⌫

ENTWURF

Tabelle 24: Tab_Service_Monitoring_Probe_Daten

Monitoring Daten	Datensatz	Einheit	Erläuterung
ProbeID	P & O		Identifikation der Probe Wird bei Erstellung der Probe vergeben und muss eindeutig sein. Probe-Datensatz: Dient der Identifikation der Probe Operation-Datensatz: Zeigt, durch welche Probe die Daten ermittelt wurden. Falls nicht vorhanden, wurden die Daten nicht durch eine Probe ermittelt.
ProbeBeschreibung			Beschreibung der Probe Wird bei Erstellung der Probe erstellt. Ist im GUI anzeigbar.
Betriebsumgebung	P & O		RU/TU/PU Die Umgebung muss nicht in jedem Datensatz enthalten sein. Die Datensätze müssen aber der Umgebung zuordenbar sein.
TeilnehmerID	O		ID des Teilnehmers wie in TI-ITSM für den diese Operation aufgerufen wurde
Dienstinstanz	O		Operation-Datensatz: Instanz des Dienstes für den die Operation ausgeführt wird.
ProductType	O		ID zu Eintrag aus Tab_gemSpec_Perf_Produkttypen
Schnittstelle	O		ID zu Eintrag aus Tab_gemSpec_Perf_Schnittstellenoperationen
Zertifikatstyp	O		ID zu Eintrag aus Tab_gemSpec_Perf_Zertifikatstypen
AnfrageQuelle	O		Angabe, ob die Schnittstelle, zu der reportet wird, in der TI oder im Internet bereitgestellt wird. Werte aus Tab_gemSpec_Perf_Aufrufquelle
Mandant	O		Identifikation des Mandanten (falls für die Operation ein Mandant genutzt wird). Wird ein „Probe“-Mandant genutzt, bleibt dieser Wert leer. Damit sehen alle Mandanten des Dienstes die Daten des „Probe“-Mandanten.
Zeitstempel	P & O	ms	Probe-Datensatz: Zeitpunkt des Probe-Laufs Operation-Datensatz: Zeigt zusammen mit der ProbeID durch welchen Probe-Lauf die Daten ermittelt wurden
Bearbeitungszeit	P & O	ms	Probe Datensatz: Ausführungsdauer der Probe Operation-Datensatz: Ausführungsdauer der Operation. Wird als Performance-Kenngröße erfasst.
Ergebnis	P & O		Probe-Datensatz: Ergebnis des Probe-Laufs Operation Datensatz: Ergebnis der Operation Das Ergebnis kann auch „Erfolgreich“ sein, wenn das erwartete Ergebnis einer Einzeloperation ein Fehler war.
Mitschnitt der Kommunikation	P		Aufzeichnung der gesamten Kommunikation der Probe mit den Diensten für den Probe-Lauf, im Fehlerfall auch für die Ursachen-Analyse. Die Operation-Datensätze enthalten keinen Mitschnitt der Kommunikation, verweise aber auf

ENTWURF

Monitoring Daten	Datensatz	Einheit	Erläuterung
			den aufrufenden Probe-Lauf (wo diese Daten zu finden sind).

Legende:

- Datensatz
  - P – im Probe Datensatz enthalten
  - O – im Operation Datensatz enthalten

5.5 Performance-Kenngrößen

Performance-Kenngrößen werden

- über Schnittstelle I_Monitoring_Update von den Diensten gemeldet,
- durch den Log-Datei-Analysator aus gelieferten Logdaten ermittelt,
- durch Probes ermittelt,
- durch Aggregation aus Performance-Kenngrößen ermittelt.

⌦ **TIP1-A_7329 Service Monitoring, Performance-Kenngrößen**

Das Service Monitoring MUSS Performance-Kenngrößen anhand einer eindeutigen Identifikation (ID im XML-Schema) identifizieren. Für gleiche Performance-Kenngrößen (z.B. Bearbeitungszeit) MUSS der gleiche Identifikator über Produkttypgrenzen hinaus nutzbar sein. Eindeutig identifiziert wird ein Wert über

- Produkttyp
- Schnittstelle
- Identifikator (ID)
- Zertifikatstyp (optional)
- Anfragequelle (optional)⌫

Die Identifikatoren für Performance-Kenngrößen werden in [gemSpec_Perf] definiert. Bei Notwendigkeit werden in [gemSpec_Perf] neue Performance-Kenngrößen Identifikatoren aufgenommen.

ENTWURF

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
eGK	elektronische Gesundheitskarte
FQDN	Fully Qualified Domain Name
GTI	Gesamtverantwortlicher TI
HBA	Heilberufsausweis
GUI	Graphical User Interface - Grafische Benutzeroberfläche
SMC-B	Security Module Card Typ B,
TI	Telematikinfrastruktur
TLS	Transport Layer Security
VSDM	Versichertenstammdatenmanagement

A2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

Abbildung 1: ABB_ServMon_301 Komponenten und Außensicht des Service Monitorings7
Abbildung 2: ABB_ServMon_303 Datenfluss Service Monitoring 8
Abbildung 3: ABB_ServMon_300 – Komponentendiagramm des Service Monitorings.....10
Abbildung 4: ABB_ServMon_302 Berechtigungskonzept 19
Abbildung 5: Abb_Service_Monitoring_SOAP-Request 27

A4 – Tabellenverzeichnis

Tabelle 1: Tab_Service_Monitoring_Akteure_und_Rollen 17
Tabelle 2: Tab_Service_Monitoring_I_Monitoring_Update 23
Tabelle 3: Tab_Service_Monitoring_Attribute 26
Tabelle 4: Tab_Service_Monitoring_SOAP-Request, Beschreibung der Elemente 27
Tabelle 5: Tab_Service_Monitoring_SOAP-Response, Beschreibung der Elemente 28
Tabelle 6: Tab_Service_Monitoring_TUC_SM_001_DNS_Name_Resolution 29
Tabelle 7: Tab_Service_Monitoring_TUC_SM_002_Erreichbarkeitsprüfung 30

ENTWURF

Tabelle 8: Tab_Service_Monitoring_Probes_DNS_Name_Resolution 34
Tabelle 9: Tab_Service_Monitoring_Probes_Konnektorregistrierung.....35
Tabelle 10: Tab_Service_Monitoring_Probes_VPN_Tunnel.....37
Tabelle 11: Tab_Service_Monitoring_Probes_Zeitinformation_TI 40
Tabelle 12: Tab_Service_Monitoring_Probes_CRL_Download.....41
Tabelle 13: Tab_Service_Monitoring_Probes_TSL_Download 42
Tabelle 14: Tab_Service_Monitoring_Probes_BNetzA_Download.....45
Tabelle 15: Tab_Service_Monitoring_Probes_OCSP.....46
Tabelle 16: Tab_Service Monitoring_Probes_UFS 48
Tabelle 17: Tab_Service_Monitoring_Probes_VSDD_CMS.....49
Tabelle 18: Tab_Service_Monitoring_Probes_ Intermediär_VSDM.....51
Tabelle 19: Tab_Service Monitoring_Probes_KSRS_Upload.....53
Tabelle 20: Tab_Service_Monitoring_Probes_KSRS_Download 54
Tabelle 21: Tab_Service_Monitoring_Probes_KSRS_Download_Bestandsnetze 56
Tabelle 22: Tab_Service_Monitoring_Probes_Verzeichnisdienst_Query 57
Tabelle 23: Tab_Service_Monitoring_Probes_Verzeichnisdienst_Application_Maintenance 59
Tabelle 24: Tab_Service_Monitoring_Probe_Daten.....61
Tabelle 25 - Tab_Service_Monitoring_Fehlercodes 65

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: Einführung der Gesundheitskarte - Glossar
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemSpec_OM]	gematik: Übergreifenden Spezifikation Operations und Maintenance
[gemSpec_Perf]	gematik: Performancespezifikation TI-Plattform
[gemSpec_Net]	gematik: Übergreifenden Spezifikation Netzwerk
[gemKPT_Betr]	gematik: Spezifisches Betriebskonzept

ENTWURF

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner http://tools.ietf.org/html/rfc2119

A6 – Fehlercodes

Tabelle 25 - Tab_Service_Monitoring_Fehlercodes

Fehlercode	ErrorType	Severity	Fehlertext
7100	Technical	Fatal	Dienst ist nicht erreichbar
7101	Technical	Fatal	Ein oder mehrere Port(s) vom Dienst sind geschlossen
7102	Technical	Fatal	Zu einem DNS Namen konnte keine IP-Adresse gefunden werden
7103	Technical	Fatal	Aufruf mit Fehler beendet
7104	Technical	Fatal	Werte können nicht über DNS Service Discovery ermittelt werden
7105	Technical	Fatal	Fehler beim Aufruf des Registrierungsservers
7106	Technical	Fatal	TSL nicht valide
7107	Technical	Fatal	In der Probe ist ein Fehler aufgetreten

ENTWURF