

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation Service Monitoring

Version: 1.1.0  
Revision: 58261  
Stand: 26.10.2018  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemSpec\_ServiceMon

---

## Dokumentinformationen

---

### Änderungen zur Vorversion

Einarbeitung P15.9.

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	14.05.18		freigegeben	gematik
			Einarbeitung P15.9	
1.1.0	26.10.18		freigegeben	gematik

## Inhaltsverzeichnis

<b>1</b>	<b>Einordnung des Dokumentes .....</b>	<b>5</b>
1.1	Zielsetzung .....	5
1.2	Zielgruppe .....	5
1.3	Geltungsbereich .....	5
1.4	Abgrenzungen .....	5
1.5	Methodik.....	6
<b>2</b>	<b>Systemüberblick .....</b>	<b>7</b>
<b>3</b>	<b>Zerlegung des Produkttyps .....</b>	<b>10</b>
<b>4</b>	<b>Übergreifende Festlegungen .....</b>	<b>12</b>
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 .....	16
4.2	Betrieb des Service Monitorings .....	16
4.2.1	Verfügbarkeits- und Durchsatzanforderungen.....	16
4.2.2	Speicherungsdauer der übermittelten Daten.....	16
4.3	Zugriffs- und Berechtigungskonzept .....	17
4.3.1	Zugriffskonzept .....	17
4.3.2	Berechtigungskonzept .....	17
<b>5</b>	<b>Funktionsmerkmale .....</b>	<b>20</b>
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 .....	22
5.2	Schnittstelle I_Monitoring_Update .....	22
5.2.1	Schnittstellendefinition .....	22
5.2.2	Umsetzung .....	24
5.2.3	Nutzung .....	25
5.3	Technische Use Cases – TUCs.....	28
5.4	Probes .....	30
5.4.1	DNS Name Resolution.....	34
5.4.2	Konnektorregistrierung* .....	34
5.4.3	VPN_Tunnel* .....	37
5.4.4	VPN_Tunnel SIS* .....	39
5.4.5	Zeitinformation_Tl.....	40

5.4.6	Zeitinformation_VPN_Zugangsdienst .....	41
5.4.7	CRL Download .....	41
5.4.8	TSL Download .....	43
5.4.9	TSL Download mit Prüfung .....	44
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	Ablauf von Server-Zertifikaten (TI) .....	60
5.4.29	Ablauf von Server Zertifikaten (Internet) .....	63
5.4.30	Erfassung von Service Monitoring-Daten in Probes .....	63
<b>5.5</b>	<b>Performance-Kenngrößen .....</b>	<b>65</b>
<b>6</b>	<b>Anhang A – Verzeichnisse .....</b>	<b>66</b>
6.1	Abkürzungen .....	66
6.2	Glossar .....	66
6.3	Abbildungsverzeichnis .....	66
6.4	Tabellenverzeichnis .....	67
6.5	Referenzierte Dokumente .....	68
6.5.1	Dokumente der gematik .....	68
6.5.2	Weitere Dokumente .....	69
6.6	Fehlercodes .....	69
6.7	Offene Punkte / Klärungsbedarf .....	70

---

## 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.

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:

**<AFO-ID> - <Titel der Afo>**

Text / Beschreibung

[<=]

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

## 2 Systemüberblick

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

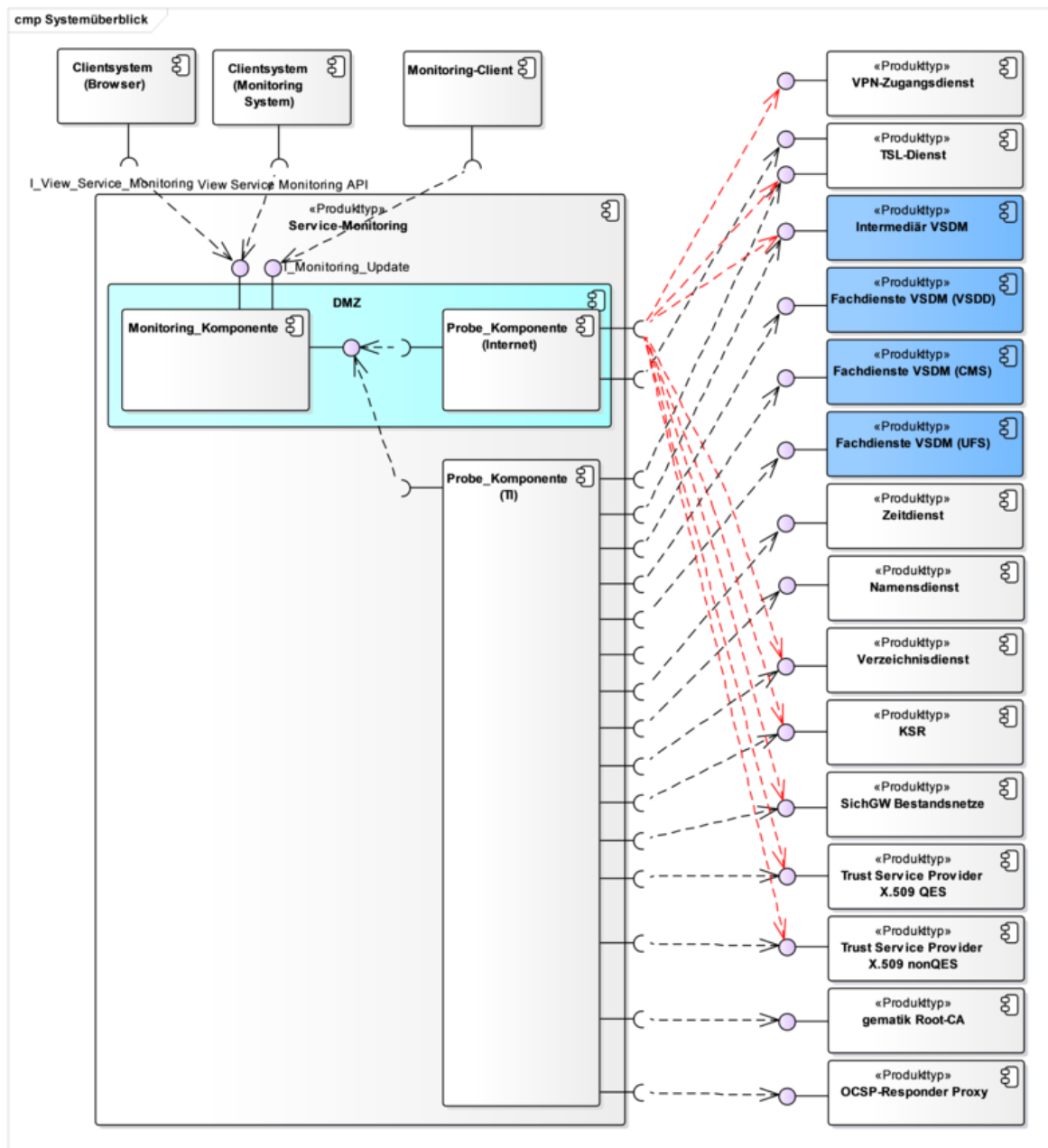


Abbildung 1: ABB\_ServMon\_301 Komponenten und Außensicht des Service Monitorings

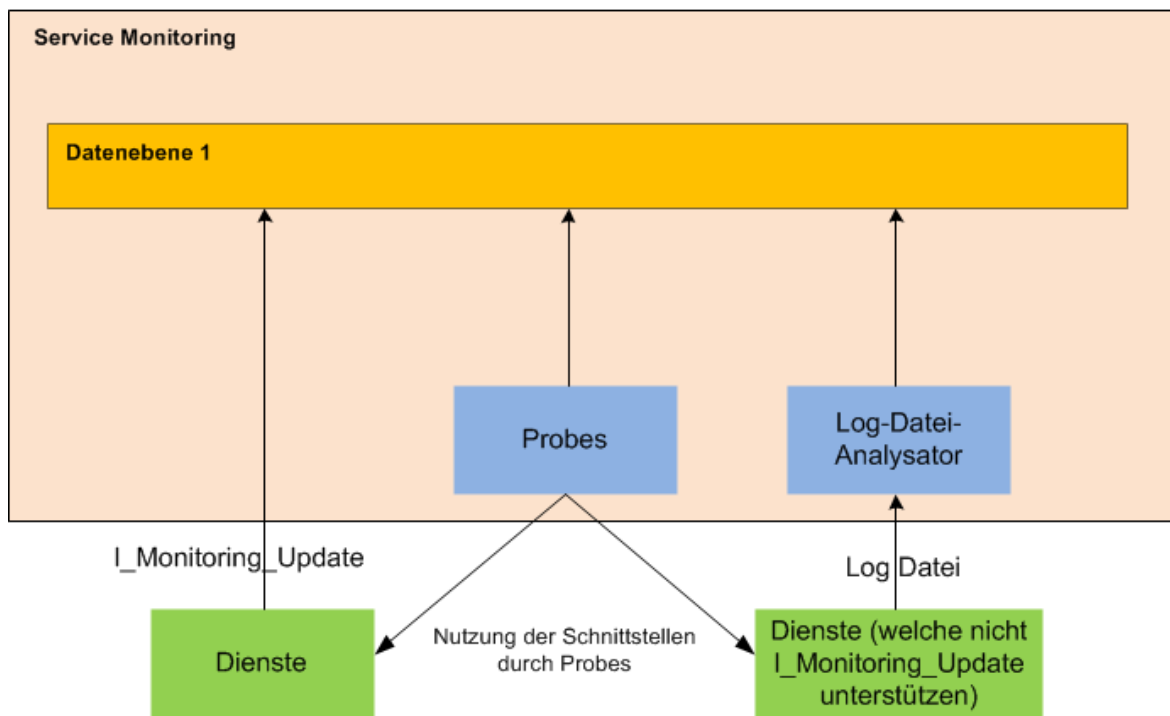
Das Service Monitoring besteht logisch aus den Systemen Monitoring\_Komponente, Probe\_Komponente (Internet) und Probe\_Komponente (TI).

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.

Hinweis: ABB\_ServMon\_301 bildet den Stand für das Release 2.1.2 ab und kann bei künftigen Releases Erweiterungen erfahren.

ABB\_ServMon\_304 zeigt eine Übersicht über die Datenquellen des Service Monitorings.



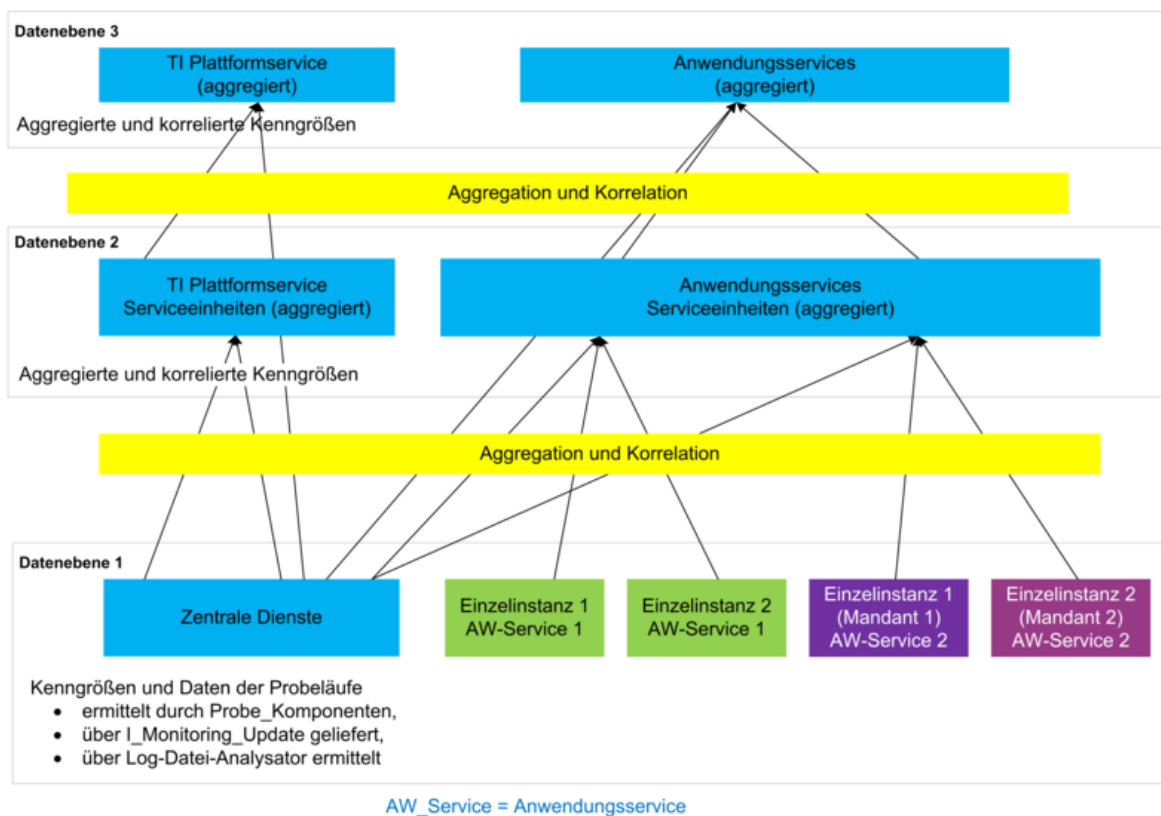
**Abbildung 2: ABB\_ServMon\_304 Übersicht Service Monitoring-Datenquellen**

Kenngößen auf Datenebene 1 des Service Monitorings stammen aus folgenden Quellen:

- Probes ermitteln Kenngößen und erzeugen Daten über die Probe-Ausführung (z.B. Zeitpunkt und Erfolg).
- Über `I_Monitoring_Update` werden Kenngößen von den Anwendungsservices/Diensten geliefert.
- Der Log-Datei-Analysator kann aus Log-Dateien Kennwerte extrahieren.

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 3: ABB\_ServMon\_303 Datenfluss Service Monitoring**

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

Der Log-Datei-Analysator wird für zukünftige Fachdienste genutzt, welche noch nicht das I\_Monitoring\_Update Interface nutzen.

### 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.

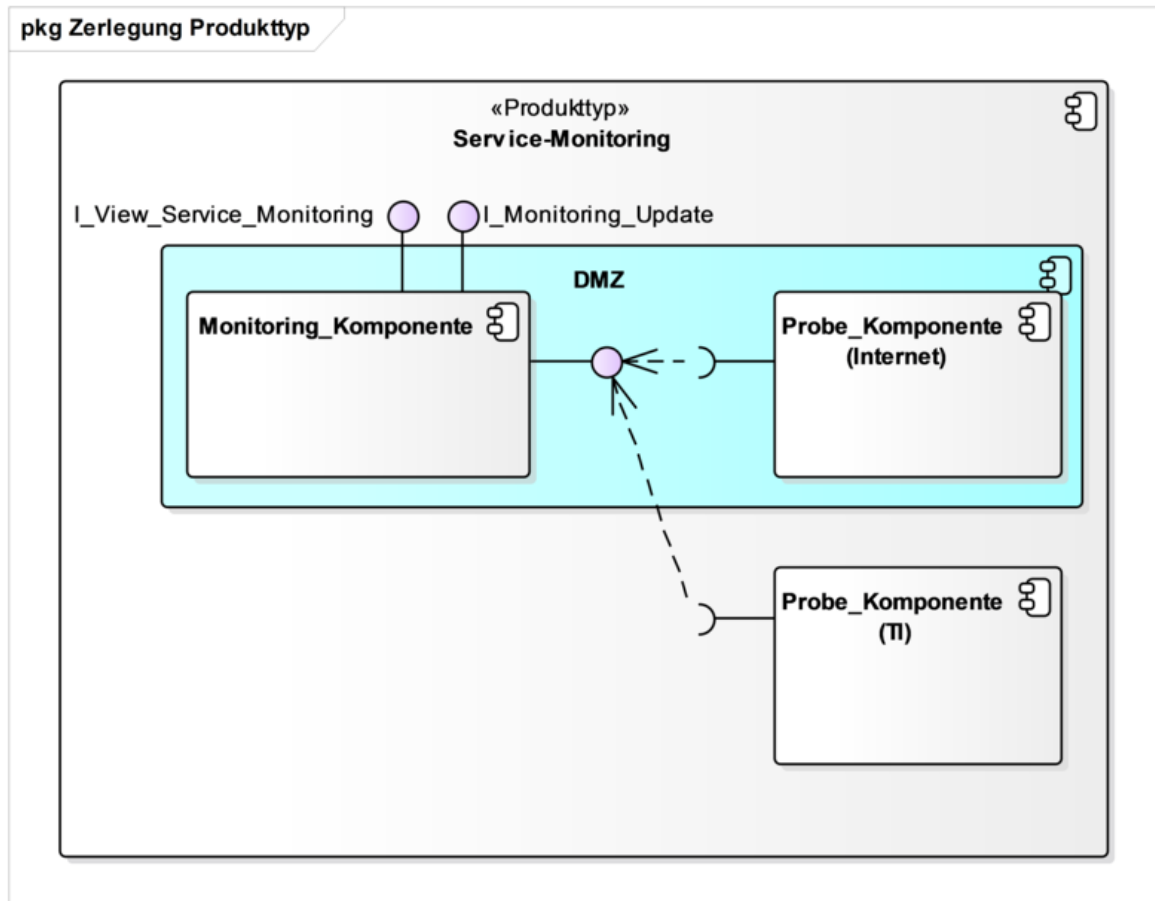


Abbildung 4: ABB\_ServMon\_300 – Komponentendiagramm des Service Monitorings

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.

---

## 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.[<=]

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

### 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.

[<=]

#### **A\_13498 - Service Monitoring, Speicherung Konfigurationsdaten**

Das Service Monitoring MUSS die Konfigurationsdaten persistent speichern sowie deren Export und Import unterstützen.

[<=]

#### **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 dazugehöriger Kritikalität/Darstellungsfarbe möglich sein.

[<=]

#### **TIP1-A\_6747 - Service Monitoring, Aggregationsregeln**

Das Service Monitoring MUSS mindestens folgende Aggregationsregeln für alle Kenngrößen (übergreifend für alle Dienste und Dienstinstanzen) 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-Ausführungen (z.B. Zuordnung von Kenngrößen zu Probe-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,
  - 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.

[<=]

#### **A\_13501 - Service Monitoring, Öffentliche Dashboards**

Das Service Monitoring MUSS dem Nutzer die Veröffentlichung eines eigenen Dashboards ermöglichen. Ein öffentliches Dashboard MUSS von allen 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.

[<=]

#### **A\_13502 - Service Monitoring, Wartungskalender, Berechtigungen**

Das Service Monitoring MUSS allen Nutzern mit Berechtigungen für eine Dienstinstanz die Anzeige des Wartungskalenders dieser Dienstinstanz ermöglichen. Die Änderung des Wartungskalenders MUSS für alle Nutzer mit der Zusatzberechtigung "Wartungskalender ändern" möglich sein.

[<=]

#### **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 und Dienstinstanz 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 berechtigten Nutzern eine Übersicht über die ausgelösten Alarmierungen und den Status der Alarmierung (offen, vom Bearbeiter bestätigt, ...) in der Nutzeroberfläche darstellen können.

Die Alarmierung MUSS eine Kurzbeschreibung der auslösenden Ursache enthalten.

Die Kurzbeschreibung MUSS konfigurierbar für jede Alarmierung aus mindestens folgenden Quellen wählbar sein:

- Durch die Probe ausgeworfene Fehlerbeschreibung.
- Konfigurierbarer Text (z.B. für auslösende Bedingungen welche keine nutzbare Beschreibung liefern).
- Name des Schwellwerts mit aktuellem Wert.

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 berechtigten Nutzern eine Übersicht über die ausgelösten

Alarmierungen und den Status der Alarmierung (offen, vom Bearbeiter bestätigt, ...) in der Nutzeroberfläche darstellen können.

[<=]

Die Alarmierung dient der Benachrichtigung von Service Monitoring-Nutzern über Störungen. Zu den Nutzern gehören auch Betreiber von (Fach-) Diensten, für welche die Alarmierungsziele durch einen Administrator entsprechend eingerichtet werden 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.

[<=]

### **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.

[<=]

#### **A\_13479 - Service Monitoring: Nutzeroberfläche Gebrauchstauglichkeit**

Der Anbieter des Service Monitorings SOLL die Gebrauchstauglichkeit der Webanwendung durch Beachtung der Leitsätze gemäß [DIN EN ISO 9241#Teil11] sicherstellen.

[<=]

#### **A\_13480 - Service Monitoring: Nutzeroberfläche Dialoggestaltung**

Der Anbieter des Service Monitorings SOLL die Dialoggestaltung der Webanwendung durch die Beachtung der Grundsätze der Dialoggestaltung gemäß [DIN EN ISO 9241#Teil110] sicherstellen.

[<=]

#### **A\_13481 - Service Monitoring: Nutzeroberfläche Interaktion**

Der Anbieter des Service Monitorings SOLL bei Verwendung von Formulardialogen in der Webanwendung die Anforderungen und Empfehlungen gemäß [DIN EN ISO 9241-



143:2012-06] beachten.  
[<=]

#### 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.[<=]

##### **A\_13499 - Service Monitoring: Zugriff auf die „Auditlogs“**

Das Service Monitoring MUSS den Zugriff auf die „Auditlogs“ rollenbasiert gestalten.

[<=]

## 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.

[<=]

### 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, Übersicht 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 möglich sein.
- Konfiguration des Service Monitorings (z. B. Ausführungszeitpunkte von Probes, Konfiguration der Probes inklusive der benötigten Zertifikate und des Truststores).

[<=]

#### **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.

[<=]

#### **A\_13574 - Service Monitoring, Zugriffsberechtigungen, Probe Ausführung**

Das Service Monitoring MUSS die Zuordnung von Zugriffsberechtigungen für einzelne - über ihre ProbeID identifizierte - Probes für alle registrierten Nutzer mit folgenden Randbedingungen erlauben:

- Der Nutzer darf die Probes - für die er Zugriffsberechtigungen hat - über das I\_View\_Service\_Monitoring GUI ausführen.
- Die Probes dürfen nicht über Schnittstelle View Service Monitoring API ausführbar sein.
- Der Nutzer darf die Konfigurationsdaten der Probe nicht ändern.
- Der Nutzer darf das Ergebnis der Probe Ausführung einsehen.

[<=]

**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.[<=]

Hinweis: Als Gruppenberechtigung wird gewertet, wenn mehrere Nutzer die gleiche Login/Passwort-Kombination benutzen. Das Rollenkonzept erlaubt die Zuordnung gleicher Rechte für verschiedene Nutzer (mit verschiedenen Logins).

**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 das Service Monitoring. 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-MonReald	Der Nutzer hat lesenden Zugriff (Sichtbar sind seine eigenen Daten sowie die – für seine Dienstleistung 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. Dieser Zugriff wird eingeschränkt auf die Daten von Dienstinstanzen des Anwendungsservices, welche dem Nutzer zugeordnet sind.
	Registrierter Nutzer (mit Administrationsberechtigung)	SM-Admin	Wie SM-AS-User Zusätzlich hat der Administrator schreibenden und lesenden Zugriff auf die Konfigurationsdaten des Service

			Monitorings und der Probes. Weiterhin kann er Kenngrößen zu Anwendungsservices oder TI-Platformservices zuordnen.
	Registrierter Nutzer (mit Nutzerverwaltungsberechtigungen)	SM-UserAdmin	Der Administrator kann <ul style="list-style-type: none"> <li>• die Nutzer des Service Monitorings verwalten (anlegen, ändern, löschen, Anwendungsservices und Dienstinstanzen zuordnen),</li> <li>• dem Nutzer zusätzliche Berechtigungen zuweisen. Das beinhaltet mindestens:             <ul style="list-style-type: none"> <li>• Übersicht über Alarmierungen anzeigen</li> <li>• Wartungskalender ändern</li> <li>• Probe Ausführung im GUI</li> </ul> </li> <li>• Auditlogs einsehen.</li> </ul>

**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 festgelegt werden.

[<=]

---

## 5 Funktionsmerkmale

---

### 5.1 Schnittstelle I\_View\_Service\_Monitoring

#### 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 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 Statusänderungen). 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 angezeigt 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.

[<=]

#### **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 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:
- keine Aggregation (z.B. durch Probes ermittelte Daten)
- Vielfache von 5 Minuten
- 1 Stunde
- 1 Tag
- 1 Woche
- 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 zur Probe-Ausführung ermöglichen.

[<=]

**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-Kenngrößen] 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: <a href="http://ws.gematik.de/tel/stoerungsampel/wSDL/v1.1">http://ws.gematik.de/tel/stoerungsampel/wSDL/v1.1</a>	
Schema	I_Monitoring_Update10.xsd Version: 1.1.0 TargetNamespace: <a href="http://ws.gematik.de/tel/stoerungsampel/v1.1">http://ws.gematik.de/tel/stoerungsampel/v1.1</a>	
	ProductInformation.xsd Version: 1.1.0 TargetNamespace: <a href="http://ws.gematik.de/tel/version/ProductInformation/v1.1">http://ws.gematik.de/tel/version/ProductInformation/v1.1</a>	
	TelematikError.xsd Version: 2.0.0 TargetNamespace: <a href="http://ws.gematik.de/tel/error/v2.0">http://ws.gematik.de/tel/error/v2.0</a>	
Webservice Zugangspunkt	<a href="https://monitoring-update.stampel.telematik:8443/I_Monitoring_Update10">https://monitoring-update.stampel.telematik:8443/I_Monitoring_Update10</a>	

[<=]

**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 der Anbieter des Clients 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 Nachrichtenübermittlung**

Der Client der Schnittstelle I\_Monitoring\_Update MUSS die Übertragung der in [gemSpec\_Perf] geforderten Monitoringdaten innerhalb von 120 Sekunden nach Ablauf eines Reportzeitraumes an das Service Monitoring beginnen. Eine Kennzeichnung des Report-Zeitraumes erfolgt durch eine Zeitbereichsangabe (Startzeit und Endzeit) in der übermittelten Nachricht.

[<=]

**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 Nachrichtenübermittlung 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 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

- 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	Zertifikats-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.

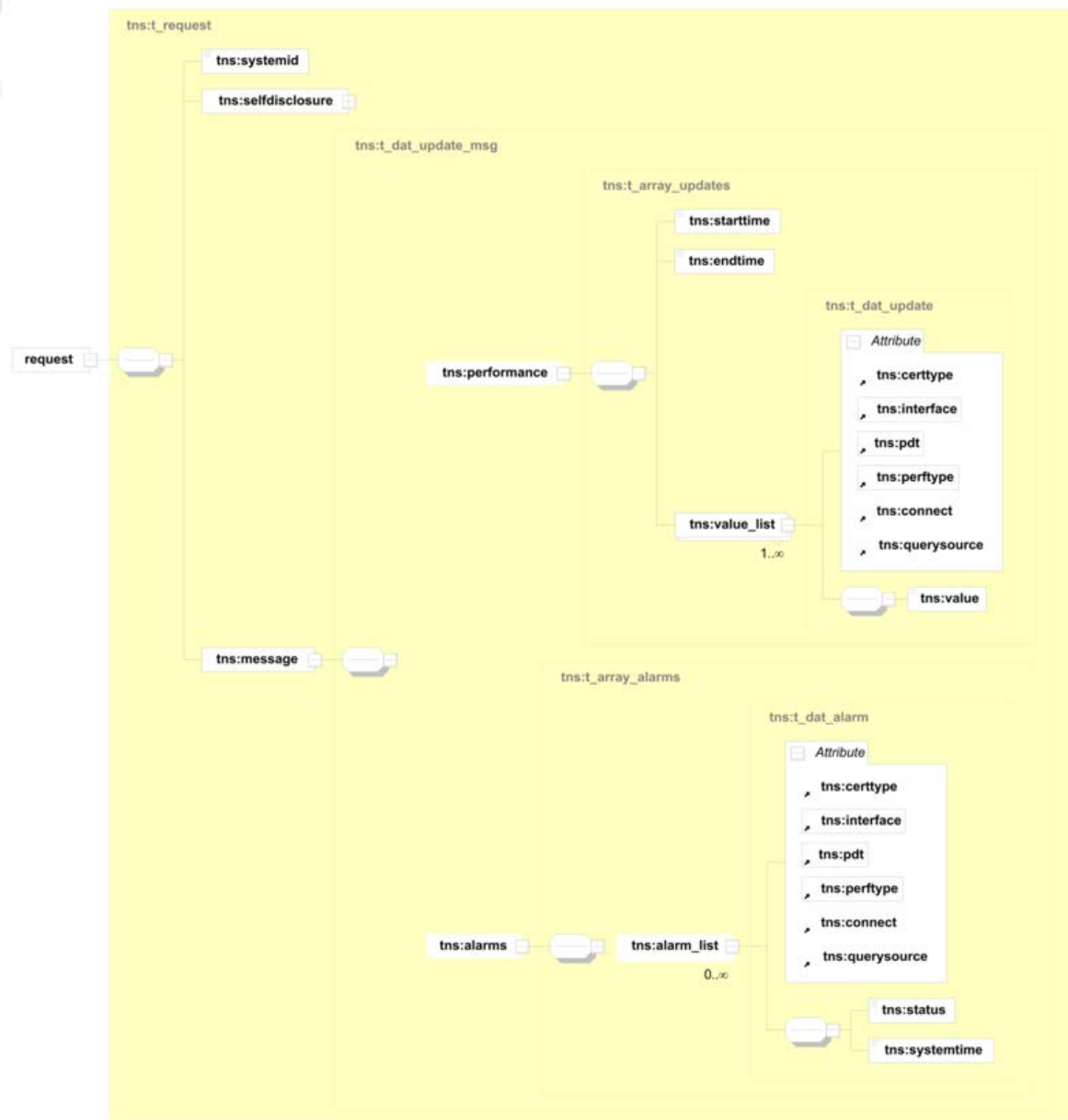


Abbildung 5: Abb\_Service\_Monitoring\_SOAP-Request

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	<p>enthält die Liste der Performance-Kenngrößen vom Typ t_dat_update.</p> <p>Dieses Element muss die folgenden Attribute enthalten.            tns:interface: Schnittstellenoperationen-ID lt. [gemSpec_Perf]            tns:pd: Produkttyp-ID lt. [gemSpec_Perf]            tns:perftype: Performance-Kenngrößen-ID lt. [gemSpec_Perf]</p> <p>Dieses Element kann die folgenden Attribute enthalten.            tns:certtype: Zertifikats-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]</p> <p>Mit einer SOAP-Nachricht können mehrere Werte für gleiche Zeitintervalle übergeben werden.</p>
tns:value	Wert der Performance-Kenngröße
tns:alarm_list	<p>enthält die Alarmstatus-Informationen.</p> <p>Dieses Element muss die folgenden Attribute enthalten.            tns:interface: Schnittstellenoperationen-ID lt. [gemSpec_Perf]            tns:pd: Produkttyp-ID lt. [gemSpec_Perf]            tns:perftype: Performance-Kenngrößen-ID lt. [gemSpec_Perf]</p> <p>Dieses Element kann die folgenden Attribute enthalten.            tns:certtype: Zertifikats-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]</p>
tns:status	<p>enthält den Alarm-Status.</p> <p>open: Alarmstatus gesetzt            close: Alarmstatus gelöscht            warn: nicht benutzt            grace: nicht genutzt</p>
tns:systemtime	Alarmzeit des sendenden Systems zur Erkennung von Inkonsistenzen (z.B. Alarmer 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	<p>beinhaltet Abnahmebestätigung der Nachricht.</p> <p>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.</p>

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.

#### **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].

[<=]

#### **A\_15166 - Nutzer der Schnittstelle I\_Monitoring\_Update, Zertifikatsprüfung**

Der Nutzer der Schnittstelle `I_Monitoring_Update` SOLL die Vertrauenswürdigkeit der Verbindung durch die Auswertung des Serverzertifikats überprüfen. Die Prüfung SOLL gemäß `gemSpec_PKI# TUC_PKI_018` mit

- PolicyList: `oid_zd_tls_s` (gemäß `gemSpec_OID`)
- KeyUsage: `digitalSignature` (Prüfung auf Vorhandensein des Bits)
- ExtendedKeyUsages: `serverAuth` (1.3.6.1.5.5.7.3.1)
- OCSP-Graceperiod: 0
- Offlinemodus: nein
- `TOLERATE_OCSP_FAILURE`: false
- Prüfmodus: OCSP

erfolgen. Alternativ ist die Prüfung gemäß `GS-A_5541` zulässig. [≤]

## **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**

<b>Name</b>	<code>TUC_SM_001_DNS_Name_Resolution</code>
-------------	---

<b>Beschreibung</b>	Dieser TUC führt die Auflösung eines FQDN in eine IP-Adresse durch.	
<b>Vorbedingungen</b>	<ul style="list-style-type: none"> <li>Keine</li> </ul>	
<b>Eingangsdaten</b>	<ul style="list-style-type: none"> <li>IP-Adresse Namensdienst</li> <li>Aufzulösender FQDN</li> <li>Bisher ermittelte Service Monitoring Daten</li> <li>Ein Flag für die DNS-Record Validierung (DNSSEC). Ist es gesetzt wird die Validierung durchgeführt.</li> </ul>	
<b>Komponenten</b>	<ul style="list-style-type: none"> <li>Service Monitoring Probe, DNS-Nameserver</li> </ul>	
<b>Ausgangsdaten</b>	<ul style="list-style-type: none"> <li>Aufgelöste IP-Adresse</li> <li>Ermittelte Service Monitoring Daten für die DNS Namensauflösung</li> </ul>	
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	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 DNS-Anfrage keine Antwort (und kein DNS-Fehler) ermittelt werden konnte	<p>Prüfung der Erreichbarkeit des DNS-Nameserver über TUC_SM_002_Erreichbarkeitsprüfung.</p> <p>Der Service Monitoring Datensatz für die DNS-Namensauflösung wird in diesem Fall in TUC_SM_002_Erreichbarkeitsprüfung erstellt.</p>
	Falls bei der DNS-Anfrage eine Antwort oder ein DNS-Fehler ermittelt werden konnte	<p>Die Service Monitoring-Daten (aus den Eingangsdaten) werden entsprechend der durchgeführten Aktionen, Tab_Service_Monitoring_Probe_Daten und um die Performance-Kenngröße „Bearbeitungszeit“ ergänzt.</p> <p>Dabei wird das „Probe-Ergebnis“ dieses Datensatzes</p> <ul style="list-style-type: none"> <li>auf OK gesetzt, falls der FQDN in eine IP-Adresse aufgelöst wurde.</li> <li>auf 7102 gesetzt, falls der DNS-Server mit einem Fehler geantwortet hat.</li> <li>Auf 7108 gesetzt, falls die DNS-Record Validierung (DNSSEC) fehlgeschlagen ist.</li> </ul>
	Rückgabe der Daten	Rückgabe der Ausgangsdaten

[&lt;=]

**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**

<b>Name</b>	TUC_SM_002_Erreichbarkeitsprüfung	
<b>Beschreibung</b>	Dieser TUC prüft die Erreichbarkeit einer Schnittstelle/Dienstes.	
<b>Vorbedingungen</b>	<ul style="list-style-type: none"> <li>Keine</li> </ul>	
<b>Eingangsdaten</b>	<ul style="list-style-type: none"> <li>IP-Adresse</li> <li>Port(s)</li> <li>TCP/UDP (soll ein TCP oder UDP Scan durchgeführt werden)</li> <li>Bisher ermittelte Service Monitoring-Daten</li> </ul>	
<b>Komponenten</b>	Service Monitoring Probe, jeweiliger Dienst	
<b>Ausgangsdaten</b>	<ul style="list-style-type: none"> <li>Ermittelte Kenngröße „Verfügbarkeit“</li> </ul>	
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	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.
	Ergänzen der Service Monitoring-Daten	<p>Die Service Monitoring-Daten (aus den Eingangsdaten) werden entsprechend der durchgeführten Aktionen bzw. deren Ergebnis ergänzt.</p> <p>Falls</p> <ul style="list-style-type: none"> <li>alle Ports geöffnet sind (für alle Ports wurde ein Datenpaket mit SYN/ACK Flags empfangen), wird das „Probe-Ergebnis“ dieses Datensatzes auf OK gesetzt.</li> <li>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.</li> <li>beim Port-Scan keine Antwort empfangen wurde, wird das „Probe-Ergebnis“ dieses Datensatzes auf 7100 gesetzt.</li> </ul>
	Rückgabe der Daten	Rückgabe der Ausgangsdaten

[&lt;=]

## 5.4 Probes

Die Probes werden im Normalfall in allen Umgebungen (RU (Referenzumgebung), TU (Testumgebung) und PU (Produktivumgebung)) eingesetzt. Eine Ausnahme stellen Probes dar, welche sich mit SMC-B-Zertifikaten authentifizieren müssen. *Offener Punkt: Die Verfügbarkeit von SMC-B-Zertifikaten für die PU befindet sich noch in der Klärung. Deshalb werden diese Probes derzeit nur für die Testumgebungen RU und PU TU gefordert. Diese Probes werden im Titel des entsprechenden Unterkapitels mit "\*" gekennzeichnet.*

### 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 spezifikationskonforme 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.

[<=]

**A\_13496 - Service Monitoring, Auswertung der Antworten von Diensten**

Das Service Monitoring MUSS die Antworten von überwachten Diensten analysieren und daraus den Status von dem Dienst ableiten. Für diese Analyse MUSS mindestens die Prüfung auf das Vorhandensein bzw. Nichtvorhandensein von konfigurierbaren Textteilen in der Antwort möglich sein. Die Analyse MUSS für jede Probe/Fachdienst-Kombination individuell konfigurierbar sein.[<=]

**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\_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**

Das Service Monitoring MUSS in Probes die Konfiguration der Konfigurationsvariante erlauben. Die Konfigurationsvariante identifiziert den Satz von Konfigurationsdaten, welche für diese Probe-Ausführung genutzt werden. Die Konfigurationsvariante MUSS für jede Probe-Ausführung 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 in Sekunden
- Zu einem bestimmten Zeitpunkt
- Sofortige (manuelle) Ausführung

Jede Probe MUSS mehrfach mit unterschiedlichen Konfigurationsdatensätzen zum gleichen und zu verschiedenen Ausführungszeitpunkt(en) ausführbar sein.[<=]

#### **A\_13500 - Service Monitoring, Probes, Einsicht in Ausführungszeitpunkte**

Das Service Monitoring MUSS Nutzern entsprechend ihren Berechtigungen auf Dienstinstanzen für die vorhandenen Probes Einsicht in die konfigurierten Ausführungszeitpunkte gewährleisten.

[<=]

#### **A\_13497 - Service Monitoring, Probes, Ausführungszeitpunkt pro Dienst**

Das Service Monitoring MUSS berechtigten Nutzern die vorhandenen Probes anzeigen und für jede Probe in Kombination mit einem Konfigurationsdatensatz den/die Ausführungszeitpunkt(e) für jede Dienstinstanz individuell wählen lassen.[<=]

#### **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 Dienstanstalten) 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?)
- Die Instanz des Dienstes (Dienstinstanz), dessen Schnittstelle von der Probe überwacht wird.

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\_7093 - Service Monitoring, Probes, Kartenterminals**

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

[<=]

In vorliegender Spezifikation müssen für alle Probes, die mit SMC-B-Zertifikaten (OSIG und AUT) arbeiten, Kartenterminals nutzbar sein.

#### 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**

Element	Beschreibung
<b>Benennung der Probe</b>	DNS_Name_Resolution
<b>Dienst</b>	Namensdienst
<b>Schnittstelle</b>	I_DNS_Name_Resolution
<b>Operation</b>	get_IP_Address
<b>Netzwerk</b>	Internet zentrales Netz der TI
<b>Beschreibung</b>	<p>Diese Probe wird ausgeführt für</p> <ul style="list-style-type: none"> <li>• die autoritativen Nameserver des Namensdienstes</li> <li>• alle Bestandsnetze (implizit I_Secure_Access_Bestandsnetz)</li> </ul>
<b>Vorbedingung</b>	<p>Für die Probe müssen folgende Informationen konfigurierbar sein:</p> <ul style="list-style-type: none"> <li>• Die DNS-Nameserver, für die diese Probe ausgeführt wird.</li> <li>• Die aufzulösenden FQDN für jeden DNS-Nameserver.</li> <li>• Ein Flag für jeden DNS-Nameserver. Ist es gesetzt wird eine DNS-Record Validierung (DNSSEC) in der Probe durchgeführt.</li> </ul>
<b>Nachbedingung</b>	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jeden DNS-Nameserver verfügbar sein.
<b>Standardablauf</b>	1. Die Probe ruft für jeden DNS-Nameserver TUC_SM_001_DNS_Name_Resolution mit der FQDN, dem Flag für die DNS-Record Validierung 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
<b>Benennung der Probe</b>	Konnektorregistrierung
<b>Dienst</b>	Registrierungsserver
<b>Schnittstelle</b>	I_Registration_Service
<b>Operation</b>	registerKonnektor deregisterKonnektor
<b>Netzwerk</b>	Internet
<b>Beschreibung</b>	<p>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.</p>
<b>Vorbedingung</b>	<p>Der Betreiber des Registrierungsservers muss informiert sein, dass für eine festgelegte Contract-ID durch die Probes häufig eine Registrierung und Deregistrierung erfolgt.</p> <p>Der Konnektor (den die Probe simuliert) muss für alle VPN-Zugangsdienste registriert sein.</p> <p>In der Probe müssen für jeden VPN-Zugangsdienstanbieter folgende Daten konfigurierbar sein:</p> <ul style="list-style-type: none"> <li>- DNS_SERVERS_INT (DNS-Server im Internet)</li> <li>- DNS_DOMAIN_VPN_ZUGD_INT (alle DNS-Domainnamen für die Service Discovery der VPN-Konzentratoren)</li> <li>- ContractID</li> </ul> <p>Das Zertifikat ID.NK.VPN (SMC-K) muss vorliegen (für die Erstellung des registerKonnektor Requests nötig).</p> <p>Sie SMC-B muss für die Signatur des Registrierungsrequests freigeschaltet sein.</p>
<b>Nachbedingung</b>	<p>Im Service Monitoring müssen die definierten Daten für jeden VPN-Konzentrator des entsprechenden VPN-Zugangsdienstes verfügbar sein:</p> <ul style="list-style-type: none"> <li>• für die Teilschritte des Standardablaufs der Probe (wie im Standardablauf definiert)</li> <li>• für jede Probe-Ausführung für einen VPN-Konzentrator</li> </ul>
<b>Standardablauf</b>	<p>1. Ermittlung der URI aller Registrierungsservers für alle DNS-Domänen (siehe auch TIP1-A_4825 [gemSpec_Kon]).</p> <ul style="list-style-type: none"> <li>• 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“             <ul style="list-style-type: none"> <li>• 7100 Namensdienst nicht erreichbar oder</li> <li>• 7101 Ports vom Namensdienst geschlossen oder</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>beendet.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>
	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])
	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 die gesamte Probe 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.
<b>Ursachen-Analyse im Fehlerfall</b>	<p>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</p> <ul style="list-style-type: none"> <li>• 7100 Registrierungsserver nicht erreichbar oder</li> <li>• 7101 Ports vom Registrierungsserver geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>

[&lt;=]

### 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
<b>Benennung der Probe</b>	VPN Tunnel
<b>Dienst</b>	VPN-Zugangsdienst
<b>Schnittstelle</b>	I_Secure_Channel_Tunnel I_IP_Transport
<b>Operation</b>	I_Secure_Channel_Tunnel::connect I_Secure_Channel_Tunnel::send_secure_IP_Packet I_Secure_Channel_Tunnel::disconnect
<b>Netzwerk</b>	Internet
<b>Beschreibung</b>	<p>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).</p> <p>Die Probe wird für jeden VPN-Konzentrator ausgeführt.</p> <p>Es wird ein VPN-Tunnel auf- und – nach Senden von Datenpaketen – wieder abgebaut.</p> <p>Bei dem VPN-Tunnel-Aufbau wird die Gültigkeitsdauer der VPN-Konzentrator-Zertifikate ermittelt und in den Service-Monitoring-Daten gespeichert.</p>
<b>Vorbedingung</b>	<p>Der Konnektor (den die Probe simuliert) muss für alle VPN-Zugangsdienste registriert sein.</p> <p>Die Probe muss für jeden VPN-Zugangsdienstanbieter mit folgenden Daten konfigurierbar sein:</p> <ul style="list-style-type: none"> <li>• DNS_SERVERS_INT (DNS Server im Internet)</li> <li>• DNS_DOMAIN_VPN_ZUGD_INT (alle DNS-Domainnamen für die Service Discovery der VPN-Konzentratoren)</li> <li>• ContractID</li> <li>• VPN-Zertifikat des simulierten Konnektors (C.NK.VPN)</li> <li>• Dauer der IPSec-Verbindung</li> </ul>
<b>Nachbedingung</b>	<p>Im Service Monitoring müssen die definierten Daten den VPN-Konzentrator verfügbar sein:</p> <ul style="list-style-type: none"> <li>• für die Teilschritte des Standardablaufs der Probe (wie im Standardablauf definiert)</li> <li>• für jede Probe-Ausführung für einen VPN-Konzentrator</li> </ul> <p>In den Service-Monitoring-Daten werden die Gültigkeitsdauern der VPN-Konzentrator-Zertifikate aktualisiert. Für jeden geprüften VPN-</p>

	<p>Konzentrator müssen mindestens folgende Daten erfasst werden:</p> <ul style="list-style-type: none"> <li>• Name des VPN-Konzentrators</li> <li>• Adresse des Dienstes bzw. der Schnittstelle</li> <li>• Gültigkeitsende des Zertifikats</li> <li>• Subject, IssuerDN und SerialNumber des Zertifikats</li> </ul> <p>Diese Daten müssen im Service Monitoring GUI in Tabellenform – mindestens sortierbar nach Gültigkeitsende des Zertifikats und IssuerDN – darstellbar sein. Generierung einer Warnung oder eines Alarms falls ein Zertifikat in x Tagen (entsprechend Konfiguration) ausläuft.</p>
<b>Standardablauf</b>	<p>1. Liste der VPN-Konzentratoren über DNS-SRV ermitteln (siehe auch TIP1-A_4373 [gemSpec_VPN_ZugD]).</p> <ul style="list-style-type: none"> <li>• 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“             <ul style="list-style-type: none"> <li>• 7100 Namensdienst nicht erreichbar oder</li> <li>• 7101 Ports vom Namensdienst geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul>             beendet.           </li> <li>• 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.</li> </ul> <p>2. Für jeden ermittelten VPN-Konzentrator muss die Probe mit den folgenden Unterpunkten einen Tunnelaufbau-Test durchführen.</p> <p>2.1. Aufbau einer Verbindung zum VPN-Konzentrator (siehe auch TUC_VPN-ZD_0001 [gemSpec_VPN_ZugD] bzw. TIP1-A_4783 [gemSpec_Kon]).</p> <p>2.2. Ermittlung der Service Monitoring-Daten für den Verbindungsaufbau entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.</p> <p>Analyse Server-Zertifikat</p> <ul style="list-style-type: none"> <li>• Prüfung des Ablaufdatums des Server Zertifikats</li> <li>• Auslösen einer Warnung oder eines Alarms über die Service-Monitoring- Alarmierung, falls das Zertifikat in x Tagen (entsprechend Konfigurationsdaten) ausläuft.</li> </ul> <p>Ablage der ermittelten Daten (siehe Nachbedingungen).</p> <p>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.</p>

	2.4. Ermittlung der Service Monitoring-Daten für die Übertragung des Datenpakets entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	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 Durchlauf der Probe 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.
<b>Ursachen-Analyse im Fehlerfall</b>	<p>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</p> <ul style="list-style-type: none"> <li>• 7100 VPN-Konzentrator nicht erreichbar oder</li> <li>• 7101 Ports vom VPN-Konzentrator geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>

[&lt;=]

#### 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.

- Standardablauf Punkt 2.3: Folgende Prüfungen werden durchgeführt:
  - DNS-Abfrage zum SIS-zugehörigen DNS-Server.
  - ICMP Request auf drei Server und Auswertung der Response (Laufzeit und Erhalt werden erfasst)
  - HTTPS GET auf drei Server 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
<b>Benennung der Probe</b>	Zeitinformation TI
<b>Dienst</b>	Zeitdienst
<b>Schnittstelle</b>	I_NTP_Time_Information
<b>Operation</b>	sync_Time
<b>Netzwerk</b>	zentrales Netz der TI
<b>Beschreibung</b>	Diese Probe wird ausgeführt für alle Stratum-1-NTP-Server der TI.
<b>Vorbedingung</b>	Die NTP-Server der TI müssen für die Probe konfigurierbar sein.
<b>Nachbedingung</b>	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jeden NTP-Server verfügbar sein.
<b>Standardablauf</b>	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“
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.

<b>Ursachen-Analyse im Fehlerfall</b>	<p>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</p> <ul style="list-style-type: none"> <li>• 7100 NTP-Servers nicht erreichbar oder</li> <li>• 7101 Ports vom NTP-Servers geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>
---------------------------------------	--

[&lt;=]

#### 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 Zugangsdienst
- Vorbedingung:
  - Die Stratum-2-NTP-Server der TI MÜSSEN für die Probe konfigurierbar sein.
  - VPN-Tunnel zu allen VPN Zugangsdiensten sind aufgebaut.

[&lt;=]

#### 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
<b>Benennung der Probe</b>	CRL Download
<b>Dienst</b>	Trust Service Provider X.509 nonQES
<b>Schnittstelle</b>	I_CRL_Download
<b>Operation</b>	download_CRL
<b>Netzwerk</b>	Internet
<b>Beschreibung</b>	Diese Probe wird ausgeführt für alle CRL Distribution Points (CDP).

<b>Vorbedingung</b>	<p>Die CRL Distribution Points (CDP) müssen für die Probe konfigurierbar sein.</p> <p>Die minimale zeitliche Gültigkeit der CRL (KONF_ZG_CRL) muss konfigurierbar sein (in Minuten oder Sekunden).</p>
<b>Nachbedingung</b>	<p>Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jeden CRL Distribution Point (CDP) verfügbar sein.</p>
<b>Standardablauf</b>	<p>1. Die Probe führt für jeden CRL Distribution Point (CDP) die folgenden Schritte durch:</p>
	<p>1.1. Ermittlung der IP-Adresse des CRL Distribution Points durch TUC_SM_001_DNS_Name_ResolutionResolution ohne DNS-Record Validierung (DNSSEC).</p>
	<p>1.2. Die Probe lädt die CRL vom CRL Distribution Point (siehe auch TIP1-A_4248 [gemSpec_X.509_TSP]).</p> <p>Falls die CRL nicht auf dem CRL Distribution Point vorliegt wird der gelieferte Fehlercode in den Service Monitoring Daten erfasst.</p>
	<p>1.3 Prüfung der CRL-Signatur</p> <ul style="list-style-type: none"> <li>• Prüfung auf zeitliche Gültigkeit des CRL-Signer-Zertifikats mittels TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats" mit Referenzzeitpunkt = aktuelle Systemzeit.</li> <li>• Auswahl des öffentlichen Schlüssels des CRL-Signer-Zertifikats.</li> <li>• Die Signatur und der verwendete Algorithmus werden aus der CRL ausgelesen.</li> <li>• Verifikation der Signatur und Hashwert-Vergleich (Verfahren siehe [RFC5280]).</li> <li>• Prüfung ob die aktuelle Systemzeit + Konfigurationsparameter KONF_ZG_CRL den Wert NextUpdate aus der CRL erreicht oder überschritten hat.</li> </ul>
	<p>1.4. Ermittlung der Service Monitoring-Daten für den CRL Distribution Point entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.</p>
	<p>2. Rückgabe der ermittelten Daten an das Service Monitoring.</p> <p>Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.</p>
<b>Ursachen-Analyse im Fehlerfall</b>	<p>Falls im Standardablauf (Punkt 1.2) 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</p> <ul style="list-style-type: none"> <li>• 7100 CRL Distribution Point nicht erreichbar oder</li> <li>• 7101 Ports vom CRL Distribution Point geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p> <p>Falls im Standardablauf (Punkt 1.3) bei der CRL-Signaturprüfung</p>

	Fehler auftreten, muss das „Probe-Ergebnis“ für diesen CRL Distribution Point auf <ul style="list-style-type: none"> <li>• 7109 Minimale zeitliche Gültigkeit der CRL unterschritten oder</li> <li>• 7110 CRL Signaturprüfung fehlgeschlagen</li> </ul> gesetzt werden.
--	---

[&lt;=]

#### 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
<b>Benennung der Probe</b>	TSL Download
<b>Dienst</b>	TSL-Dienst
<b>Schnittstelle</b>	I_TSL_Download
<b>Operation</b>	download_TSL
<b>Netzwerk</b>	zentrales Netz der TI
<b>Beschreibung</b>	Diese Probe wird ausgeführt für den TSL Dienst.
<b>Vorbedingung</b>	Die URL(s) für den Download der TSL vom TSL-Dienst muss für die Probe konfigurierbar sein.
<b>Nachbedingung</b>	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für den TSL Dienst verfügbar sein.
<b>Standardablauf</b>	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.
<b>Ursachen-Analyse im Fehlerfall</b>	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

	<p>werden. Das „Probe-Ergebnis“ wird für diesen TSL Download-Punkt auf</p> <ul style="list-style-type: none"> <li>• 7100 TSL Download-Punkt nicht erreichbar oder</li> <li>• 7101 Ports vom TSL Download-Punkt geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>
--	--

[&lt;=]

#### 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:
  - 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

[&lt;=]

#### 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.

[&lt;=]

#### 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

[<=]

#### 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
<b>Benennung der Probe</b>	BNetzA Download
<b>Dienst</b>	TSL-Dienst
<b>Schnittstelle</b>	I_BNetzA_VL_Download
<b>Operation</b>	download_VL
<b>Netzwerk</b>	zentrales Netz der TI
<b>Beschreibung</b>	Diese Probe wird ausgeführt für alle ServiceSupplyPoints für die BNetzA-VL.
<b>Vorbedingung</b>	Die Download-Adressen der BNetzA-VL müssen konfigurierbar sein.
<b>Nachbedingung</b>	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
<b>Standardablauf</b>	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.
<b>Ursachen-Analyse im Fehlerfall</b>	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

	<ul style="list-style-type: none"> <li>• 7100 Download-Punkt der BNetzA-VL nicht erreichbar oder</li> <li>• 7101 Ports vom Download-Punkt der BNetzA-VL geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet gesetzt.</li> </ul>
--	--

[&lt;=]

#### 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 beachten:

- 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.

[&lt;=]

#### 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
<b>Benennung der Probe</b>	OCSP
<b>Dienst</b>	TSL-Dienst
<b>Schnittstelle</b>	I_OCSP_Status_Information
<b>Operation</b>	check_Revocation_Status
<b>Netzwerk</b>	zentrales Netz der TI
<b>Beschreibung</b>	Diese Probe wird ausgeführt für alle ServiceSupplyPoints in der TSL (inkl. alle ServiceSupplyPoints in der VL über den OCSP-Responder Proxy).
<b>Vorbedingung</b>	In der Probe müssen folgende Daten konfigurierbar sein: <ul style="list-style-type: none"> <li>• OCSP-Responder Adressen</li> <li>• Für jeden OCSP-Responder müssen Zertifikatsdaten für die OCSP-Abfrage konfigurierbar sein</li> </ul>



	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.
<b>Nachbedingung</b>	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
<b>Standardablauf</b>	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.
<b>Ursachen-Analyse im Fehlerfall</b>	<p>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</p> <ul style="list-style-type: none"> <li>• 7100 OCSP nicht erreichbar oder</li> <li>• 7101 Ports vom OCSP geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>

[&lt;=]

#### 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 beachten:

- 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:

- 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.

[&lt;=]

#### 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.

[&lt;=]

##### 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
<b>Benennung der Probe</b>	UFS
<b>Dienst</b>	Update Flag Service
<b>Schnittstelle</b>	I_UFS
<b>Operation</b>	GetUpdateFlags
<b>Netzwerk</b>	zentrales Netz der TI
<b>Beschreibung</b>	Diese Probe wird ausgeführt für alle UFS-Fachdienste.
<b>Vorbedingung</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• URL des Fachdienstes UFS</li> <li>• ServiceType (UFS)</li> <li>• ICCSN</li> <li>• Provider ID</li> <li>• Erwartete Fachdienstantwort/Fehlercode</li> </ul> <p>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.</p>
<b>Nachbedingung</b>	<p>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.</p>

<b>Standardablauf</b>	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.
<b>Ursachen-Analyse im Fehlerfall</b>	<p>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</p> <ul style="list-style-type: none"> <li>• 7100 Fachdienst nicht erreichbar oder</li> <li>• 7101 Ports vom Fachdienst geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>

[&lt;=]

#### 5.4.16.2 Fachdienst VSDD\_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
<b>Benennung der Probe</b>	VSDD_CMS
<b>Dienst</b>	VSDD- und CMS-Fachdienste
<b>Schnittstelle</b>	I_CCS

<b>Operation</b>	PerformUpdates
<b>Netzwerk</b>	zentrales Netz der TI
<b>Beschreibung</b>	Diese Probe wird ausgeführt für alle VSDD- und CMS-Fachdienste.
<b>Vorbedingung</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• URL des Fachdienstes</li> <li>• ICCSN</li> <li>• ServiceType (VSD   CMS)</li> <li>• Provider ID</li> <li>• UpdateID</li> </ul> <p>Die UpdateID muss konfigurierbar und aus der vorangehenden Operation GetUpdateFlags übernehmbar sein.</p> <ul style="list-style-type: none"> <li>• Der kartenindividuelle symmetrische Schlüssel für die ICCSN muss optionaler konfigurierbar sein.</li> <li>• Update Flag verbrauchen (ja/nein)</li> <li>• Erwartete Fachdienstantwort/Fehlercode</li> </ul> <p>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.</p>
<b>Nachbedingung</b>	Im Service Monitoring müssen für die gesamte Probe und für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
<b>Standardablauf</b>	<p>1. Für jeden Fachdienst:</p> <p>1.1. Ermittlung der IP-Adresse des Fachdienstes durch eine DNS-Anfrage (DNS-SRV-Fachdienst) mit TUC_SM_001_DNS_Name_Resolution.</p> <p>1.2. Verbindungsaufbau zum Fachdienst unter Nutzung des TLS-Client-Zertifikats.</p> <p>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 die Probe 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.</p>

	<p>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.</p> <p>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-Identifizier liegt kein Update vor) erwartet.</p>
	<p>1.5. Ermittlung der Service Monitoring-Daten für Operation PerformUpdates entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.</p>
	<p>2. Ermittlung der Service Monitoring-Daten für die gesamte Probe und Rückgabe aller Datensätze an das Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.</p>
<b>Ursachen-Analyse im Fehlerfall</b>	<p>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</p> <ul style="list-style-type: none"> <li>• 7100 Fachdienst nicht erreichbar oder</li> <li>• 7101 Ports vom Fachdienst geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>

[&lt;=]

#### 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
<b>Benennung der Probe</b>	Intermediär VSDM
<b>Dienst</b>	Intermediär VSDM
<b>Schnittstelle</b>	I_TLS Intermediär
<b>Operation</b>	GetUpdateFlags via Intermediär
<b>Netzwerk</b>	zentrales Netz der TI
<b>Beschreibung</b>	Diese Probe wird ausgeführt für jeden Intermediär.

<b>Vorbedingung</b>	<p>Für den Aufruf von Operation I_UFS::GetUpdateFlags via Intermediär müssen folgende Werte in der Probe für den jeden Intermediär individuell konfigurierbar sein.</p> <ul style="list-style-type: none"> <li>• URL des Intermediär</li> <li>• ServiceType (UFS)</li> <li>• Schnittstellen-Version UFS (2.0)</li> <li>• ICCSN</li> <li>• Provider ID</li> </ul> <p>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. Die SM-B muss freigeschaltet sein. Weiterhin muss für die Probe mit einem Fachdienstbetreiber die Verwendung von einem Fachdienst UFS abgesprochen sein.</p>
<b>Nachbedingung</b>	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
<b>Standardablauf</b>	<p>1. Für jeden Intermediär:</p> <p>1.1. Ermittlung der IP-Adresse des Intermediär VSDM durch eine DNS-Anfrage (DNS-SRV Intermediär) mit TUC_SM_001_DNS_Name_Resolution.</p> <p>1.2. Verbindungsaufbau zum Intermediär VSDM unter Nutzung des TLS-Client-Zertifikats (SM-B AUT Zertifikat).</p> <p>1.3. Senden des GetUpdateFlags Requests zum Intermediär VSDM unter Nutzung der Konfigurationsparameter [gemSpec_SST_FD_VSDM#3.1].</p> <p>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.</p> <p>1.5. Ermittlung der Service Monitoring-Daten für Operation GetUpdateFlags entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.</p> <p>2. Ermittlung der Service Monitoring-Daten für die gesamte Probe und Rückgabe aller Datensätze an das Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.</p>
<b>Ursachen-Analyse im Fehlerfall</b>	<p>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</p> <ul style="list-style-type: none"> <li>• 7100 Intermediär nicht erreichbar oder</li> <li>• 7101 Ports vom Intermediär geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>

[&lt;=]

#### 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:
  - 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.

[&lt;=]

#### 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.

[&lt;=]

#### 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
<b>Benennung der Probe</b>	KSRS Upload
<b>Dienst</b>	KSR



<b>Schnittstelle</b>	P_KSRS_Upload
<b>Operation</b>	Erreichbarkeit KSRS-Upload-Schnittstelle
<b>Netzwerk</b>	Internet
<b>Beschreibung</b>	Diese Probe wird ausgeführt für den KSR.
<b>Vorbedingung</b>	Für die Prüfung der Erreichbarkeit der KSRS-Upload-Schnittstelle müssen folgende Werte in der Probe konfigurierbar sein. <ul style="list-style-type: none"> <li>• URL der KSRS-Upload-Schnittstelle</li> </ul>
<b>Nachbedingung</b>	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
<b>Standardablauf</b>	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 <a href="#">[RFC 7231#4.3.2]</a> 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“.

[&lt;=]

#### 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
<b>Benennung der Probe</b>	KSRS Download
<b>Dienst</b>	KSR
<b>Schnittstelle</b>	I_KSRS_Download
<b>Operation</b>	I_KSRS_Download::list_Updates I_KSRS_Download::get_Updates
<b>Netzwerk</b>	zentrales Netz der TI
<b>Beschreibung</b>	Diese Probe wird ausgeführt für den KSR.
<b>Vorbedingung</b>	Für die Operationen von Schnittstelle I_KSRS_Download müssen folgende Werte in der Probe konfigurierbar sein. <ul style="list-style-type: none"> <li>• URL der KSRS-Download-Schnittstelle</li> <li>• ProductVendorID</li> </ul>

	<ul style="list-style-type: none"> <li>• ProductCode</li> <li>• Hardware Version (HWVersion)</li> <li>• Firmware Version (FMVersion)</li> </ul>
<b>Nachbedingung</b>	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
<b>Standardablauf</b>	<ol style="list-style-type: none"> <li>1. Ermittlung der IP-Adresse der KSRS-Download-Schnittstelle durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.</li> <li>2. TLS Verbindungsaufbau zum Konfigurationsdienst.</li> <li>3. Senden von Request I_KSRS_Download::listUpdates gemäß [gemSpec_KSR] an den Konfigurationsdienst</li> <li>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“.</li> <li>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.</li> <li>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“.</li> <li>7. Speicherung der ermittelten Daten für die KSRS-Download-Schnittstelle im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.</li> </ol>
<b>Ursachen-Analyse im Fehlerfall</b>	<p>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</p> <ul style="list-style-type: none"> <li>• 7100 KSR nicht erreichbar oder</li> <li>• 7101 Ports vom KSR geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>

[&lt;=]

#### 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.
- 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 die gesamte Probe 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
<b>Benennung der Probe</b>	KSRS Download Bestandsnetze
<b>Dienst</b>	KSR
<b>Schnittstelle</b>	I_KSRS_Net_Config
<b>Operation</b>	I_KSRS_Net_Config::get_Ext_Net_Config
<b>Netzwerk</b>	zentrales Netz der TI
<b>Beschreibung</b>	Diese Probe wird ausgeführt für den KSR.
<b>Vorbedingung</b>	Für die Operationen von Schnittstelle I_KSRS_Net_Config müssen folgende Werte in der Probe konfigurierbar sein: <ul style="list-style-type: none"> <li>• URL der KSRS-Download-Schnittstelle</li> </ul>
<b>Nachbedingung</b>	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
<b>Standardablauf</b>	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.
	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.
<b>Ursachen-Analyse im Fehlerfall</b>	<p>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</p> <ul style="list-style-type: none"> <li>• 7100 KSR nicht erreichbar oder</li> <li>• 7101 Ports vom KSR geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>

[&lt;=]

#### 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.

[&lt;=]

#### 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**

Element	Beschreibung
---------	--------------

<b>Benennung der Probe</b>	Verzeichnisdienst Query
<b>Dienst</b>	Verzeichnisdienst
<b>Schnittstelle</b>	I_Directory_Query
<b>Operation</b>	I_Directory_Query::search_Directory
<b>Netzwerk</b>	zentrales Netz der TI
<b>Beschreibung</b>	Diese Probe wird ausgeführt für den Verzeichnisdienst.
<b>Vorbedingung</b>	Für die Operation I_Directory_Query::search_Directory müssen folgende Werte in der Probe konfigurierbar sein: <ul style="list-style-type: none"> <li>Suchkriterien für die LDAP Verzeichnisdienstabfrage</li> </ul>
<b>Nachbedingung</b>	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
<b>Standardablauf</b>	<ol style="list-style-type: none"> <li>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.</li> <li>2. LDAPS-Verbindungsaufbau zum Verzeichnisdienst (analog zu A_5517 [gemSpec_Kon#4.1.12.4.1]).</li> <li>3. Abfrage des Verzeichnisdienstes mit den konfigurierten Eingangsdaten analog zu TIP1-A_5518 [gemSpec_Kon#4.1.12.4.2].</li> <li>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“.</li> <li>5. Die Probe beendet die Verbindung zum Verzeichnisdienst (analog zu A_5519 [gemSpec_Kon#4.1.12.4.3]).</li> <li>6. Speicherung der ermittelten Daten für die Verzeichnisdienst I_Directory_Query Schnittstelle im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.</li> </ol>
<b>Ursachen-Analyse im Fehlerfall</b>	<p>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</p> <ul style="list-style-type: none"> <li>7100 Verzeichnisdienst nicht erreichbar oder</li> <li>7101 Ports vom Verzeichnisdienst geschlossen oder</li> <li>7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>

[&lt;=]

#### 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
<b>Benennung der Probe</b>	Verzeichnisdienst Application Maintenance
<b>Dienst</b>	Verzeichnisdienst
<b>Schnittstelle</b>	I_Directory_Application_Maintenance
<b>Operation</b>	I_Directory_Application_Maintenance::add_Directory_FA-Attributes
<b>Netzwerk</b>	zentrales Netz der TI
<b>Beschreibung</b>	Diese Probe wird ausgeführt für den Verzeichnisdienst. Es wird die Webservice (SOAP) Ausprägung der Operationen genutzt.
<b>Vorbedingung</b>	<p>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.</p> <p>Für diese Probe müssen folgende Werte konfigurierbar sein:</p> <ul style="list-style-type: none"> <li>• Telematik-ID</li> <li>• fachdienstspezifische Attribute, welche mit dem SOAP-Request dem Verzeichniseintrag hinzugefügt (bzw. überschrieben) werden</li> </ul>

<b>Nachbedingung</b>	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
<b>Standardablauf</b>	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 I_Directory_Application_Maintenance im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
<b>Ursachen-Analyse im Fehlerfall</b>	<p>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</p> <ul style="list-style-type: none"> <li>• 7100 Verzeichnisdienst nicht erreichbar oder</li> <li>• 7101 Ports vom Verzeichnisdienst geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>

[&lt;=]

#### 5.4.28 Ablauf von Server-Zertifikaten (TI)

##### A\_15579 - Service Monitoring, Probe Ablauf von Server-Zertifikaten (TI)

Das Service Monitoring MUSS die Probe Ablauf von Server-Zertifikaten (TI) entsprechend Tab\_Service\_Monitoring\_Probes\_Ablauf\_von\_Server\_Zertifikaten bereitstellen.

**Tabelle 24: Tab\_Service\_Monitoring\_Probes\_Ablauf\_von\_Server\_Zertifikaten**

Element	Beschreibung
<b>Benennung der Probe</b>	Ablauf von Server-Zertifikaten



Dienst	Alle in der Probe konfigurierten Server
Schnittstelle	TLS
Operation	TLS-Verbindungsaufbau
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle in der Probe konfigurierten Server.
Vorbedingung	<p>Für diese Probe müssen folgende Werte konfigurierbar sein:</p> <ul style="list-style-type: none"> <li>• Ausführungszeitpunkt und Frequenz der Probe</li> <li>• Wieviel Tage vor Zertifikatsablauf soll eine Warnung versendet werden?</li> <li>• Wieviel Tage vor Zertifikatsablauf soll ein Alarm versendet werden?</li> <li>• Die zentralen Dienste, deren Server-Zertifikate überwacht werden. Für jeden Server müssen mindestens folgende Werte konfiguriert werden:               <ul style="list-style-type: none"> <li>• Name des Servers</li> <li>• Adresse des Servers bzw. der Schnittstelle</li> <li>• Port des Servers</li> <li>• Optional: Client Zertifikat</li> </ul> </li> </ul>
Nachbedingung	<p>In den Service-Monitoring-Daten werden die Gültigkeitsdauern der Server-Zertifikate aktualisiert. Für jeden geprüften Server müssen mindestens folgende Daten erfasst werden:</p> <ul style="list-style-type: none"> <li>• Name des Servers</li> <li>• Adresse des Dienstes bzw. der Schnittstelle</li> <li>• Gültigkeitsende des Zertifikats</li> <li>• Subject, IssuerDN und SerialNumber des Zertifikats</li> </ul> <p>Diese Daten müssen im Service-Monitoring-GUI in Tabellenform – mindestens sortierbar nach Gültigkeitsende des Zertifikats und IssuerDN – darstellbar sein.</p> <p>Generierung einer Warnung oder eines Alarms falls ein Zertifikat in x Tagen (entsprechend Konfiguration) ausläuft.</p> <p>Die ermittelten Daten entsprechend Tab_Service_Monitoring_Probe_Daten sind für die</p>

	Probe im Service Monitoring gespeichert.
<b>Standardablauf</b>	1. Ermittlung der IP-Adresse des Servers durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	2. Für jeden konfigurierten Server: <ul style="list-style-type: none"> <li>• TLS-Verbindungsaufbau zum Server und Übergabe des Server Zertifikats an den nächsten Schritt des Standardablaufs. <ul style="list-style-type: none"> <li>• Falls der Server ein Client-Zertifikat anfordert, wird das konfigurierte Zertifikat verwendet. Falls kein konfiguriertes Client-Zertifikat vorhanden ist, wird der Verbindungsaufbau abgebrochen.</li> </ul> </li> <li>• Beenden der TLS-Verbindung.</li> </ul>
	3. Analyse Server-Zertifikat <ul style="list-style-type: none"> <li>• Prüfung des Ablaufdatums des Server-Zertifikats</li> <li>• Auslösen einer Warnung oder eines Alarms über die Service-Monitoring-Alarmierung falls das Zertifikat in x Tagen (entsprechend Konfigurationsdaten) ausläuft.</li> <li>• Ablage der ermittelten Daten (siehe Nachbedingungen)</li> </ul>
	4. Speicherung der ermittelten Daten für die Probe im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.

Ursachen-Analyse im Fehlerfall	<p>Falls im Standardablauf bei den Aufrufen der Server Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Servers mit TUC_SM_002_Erreichbarkeitsprüfung geprüft werden. Das „Probe-Ergebnis“ wird für diesen TLS-Verbindungsaufbau auf</p> <ul style="list-style-type: none"> <li>• 7100 Dienst nicht erreichbar oder</li> <li>• 7101 Ports vom Dienst geschlossen oder</li> <li>• 7103 Aufruf mit Fehler beendet</li> </ul> <p>gesetzt.</p>
--------------------------------	---

[&lt;=]

#### 5.4.29 Ablauf von Server Zertifikaten (Internet)

##### A\_15580 - Service Monitoring, Probe Ablauf von Server Zertifikaten (Internet)

Das Service Monitoring MUSS die Probe Ablauf von Server-Zertifikaten (Internet) entsprechend Tab\_Service\_Monitoring\_Probes\_Ablauf\_von\_Server\_Zertifikaten bereitstellen.

Folgende Abweichungen von Tab\_Service\_Monitoring\_Probes\_TSL\_Download MÜSSEN beachtet werden:

- Benennung der Probe: Ablauf von Server-Zertifikaten (Internet)
- Netzwerk: Internet

[&lt;=]

#### 5.4.30 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

- die gesamte Probe ein Datensatz 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 -Ausführungszeitpunkten erfasst und für Aggregationsregeln auswertbar sein.

[&lt;=]

**Tabelle 25: 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.
<b>ProbeBeschreibung</b>			Beschreibung der Probe Wird bei Erstellung der Probe erstellt. Ist im GUI anzeigbar.
<b>Betriebsumgebung</b>	P & O		RU/TU/PU Die Umgebung muss nicht in jedem Datensatz enthalten sein. Die Datensätze müssen aber der Umgebung zuordenbar sein.
<b>TeilnehmerID</b>	O		ID des Teilnehmers wie in TI-ITSM für den diese Operation aufgerufen wurde
<b>Dienstinstanz</b>	O		Operation-Datensatz: Instanz des Dienstes für den die Operation ausgeführt wird.
<b>ProductType</b>	O		ID zu Eintrag aus Tab_gemSpec_Perf_Produkttypen
<b>Schnittstelle</b>	O		ID zu Eintrag aus Tab_gemSpec_Perf_Schnittstellenoperationen
<b>Zertifikatstyp</b>	O		ID zu Eintrag aus Tab_gemSpec_Perf_Zertifikatstypen
<b>AnfrageQuelle</b>	O		Angabe, ob die Schnittstelle, zu der reportet wird, in der TI oder im Internet bereitgestellt wird. Werte aus Tab_gemSpec_Perf_Aufrufquelle
<b>Zeitstempel</b>	P & O	ms	Probe-Datensatz: Zeitpunkt der Probe-Ausführung Operation-Datensatz: Zeigt zusammen mit der ProbelD durch welche Probe-Ausführung die Daten ermittelt wurden
<b>Bearbeitungszeit</b>	P & O	ms	Probe Datensatz: Ausführungsdauer der Probe Operation-Datensatz: Ausführungsdauer der Operation. Wird als Performance-Kenngröße erfasst.
<b>Ergebnis</b>	P & O		Probe-Datensatz: Ergebnis der Probe-Ausführung Operation Datensatz: Ergebnis der Operation Das Ergebnis kann auch „Erfolgreich“ sein, wenn das erwartete Ergebnis einer Einzeloperation ein Fehler war.
<b>Mitschnitt der Kommunikation</b>	P		Aufzeichnung der gesamten Kommunikation der Probe mit den Diensten für die Probe-Ausführung, im Fehlerfall auch für die Ursachen-Analyse. Die Operation-Datensätze enthalten keinen

		Mitschnitt der Kommunikation, verweisen aber auf die aufrufende ProbeAusführung (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.

## 6 Anhang A – Verzeichnisse

### 6.1 Abkürzungen

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

### 6.2 Glossar

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

### 6.3 Abbildungsverzeichnis

Abbildung 1: ABB_ServMon_301 Komponenten und Außensicht des Service Monitorings .....	7
Abbildung 2: ABB_ServMon_304 Übersicht Service Monitoring-Datenquellen.....	8
Abbildung 3: ABB_ServMon_303 Datenfluss Service Monitoring .....	9
Abbildung 4: ABB_ServMon_300 – Komponentendiagramm des Service Monitorings....	10

Abbildung 5: Abb_Service_Monitoring_SOAP-Request .....	26
--	----

## 6.4 Tabellenverzeichnis

Tabelle 1: Tab_Service_Monitoring_Akteure_und_Rollen.....	18
Tabelle 2: Tab_Service_Monitoring_I_Monitoring_Update .....	23
Tabelle 3: Tab_Service_Monitoring_Attribute .....	25
Tabelle 4: Tab_Service_Monitoring_SOAP-Request, Beschreibung der Elemente .....	26
Tabelle 5: Tab_Service_Monitoring_SOAP-Response, Beschreibung der Elemente .....	27
Tabelle 6: Tab_Service_Monitoring_TUC_SM_001_DNS_Name_Resolution .....	28
Tabelle 7: Tab_Service_Monitoring_TUC_SM_002_Erreichbarkeitsprüfung .....	30
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 .....	43
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_Probes_Ablauf_von_Server_Zertifikaten .....	60
Tabelle 25: Tab_Service_Monitoring_Probe_Daten .....	63
Tabelle 26 - Tab_Service_Monitoring_Fehlercodes .....	69



## 6.5 Referenzierte Dokumente

### 6.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemKPT_Betr]	gematik: Spezifisches Betriebskonzept
[gemSpec_Intermediär_VSDM]	gematik: Spezifikation Intermediär VSDM
[gemSpec_Kon]	gematik: Spezifikation Konnektor
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation – Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_KSR]	gematik: Spezifikation Konfigurationsdienst
[gemSpec_Net]	gematik: Übergreifenden Spezifikation Netzwerk
[gemSpec_OM]	gematik: Übergreifenden Spezifikation Operations und Maintenance
[gemSpec_Perf]	gematik: Performancespezifikation TI-Plattform
[gemSpec_PKI]	gematik: Spezifikation PKI

[gemSpec_SST_FD_VSDM]	gematik: Schnittstellenspezifikation Fachdienste (UFS/VSDD/CMS)
[gemSpec_St_Ampel]	gematik: Spezifikation Störungsampel
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst
[gemSpec_VPN_ZugD]	gematik: Spezifikation VPN-Zugangsdienst
[gemSpec_VZD]	gematik: Spezifikation Verzeichnisdienst
[gemSpec_X.509_TSP]	gematik: Spezifikation Trust Service Provider X.509

### 6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[DIN EN ISO 9241]	Ergonomie der Mensch-System-Interaktion - Teil 110: Grundsätze der Dialoggestaltung (ISO 9241-110:2006); Deutsche Fassung EN ISO 9241-110:2006 Ausgabe 2008-09
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner <a href="http://tools.ietf.org/html/rfc2119">http://tools.ietf.org/html/rfc2119</a>
[RFC7159]	The JavaScript Object Notation (JSON) Data Interchange Format
[RFC7231]	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content

## 6.6 Fehlercodes

**Tabelle 26 - 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
7108	Technical	Fatal	DNS-Record Validierung fehlgeschlagen (DNSSEC)
7109	Technical	Fatal	Minimale zeitliche Gültigkeit der CRL unterschritten
7110	Technical	Fatal	CRL Signaturprüfung fehlgeschlagen

## 6.7 Offene Punkte / Klärungsbedarf

Kap.	Offener Punkt	Zuständig
5.4	Die Verfügbarkeit von SMC-B-Karten bzw. -Zertifikaten für die PU befindet sich noch in der Klärung. Bis zur Klärung werden in der PU keine Probes genutzt welche SMC-B-Zertifikate benötigen.	gematik