gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
Service Monitoring

Version:	1.4.0
Revision:	167595
Stand:	02.10.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_ServiceMon

Dokumentinformationen

Änderungen zur Vorversion

Die Änderungen zur Vorversion sind gelb markiert.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	14.05.18		freigegeben	gematik
1.1.0	26.10.18		Einarbeitung P15.9	gematik
1.2.0	18.12.18		Ergänzung ePA-Inhalte	gematik
1.3.0	15.05.19		Einarbeitung P18.1	gematik
			Einarbeitung P20.1	gematik
1.4.0	02.10.19		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes 5
1.1 Zielsetzung 5
1.2 Zielgruppe 5
1.3 Geltungsbereich 5
1.4 Abgrenzungen 5
1.5 Methodik 6
2 Systemüberblick 7
3 Zerlegung des Produkttyps 10
4 Übergreifende Festlegungen 12
4.1 Implementierung des Service Monitorings 12
4.1.1 Verwendung von Standardprodukten 12
4.1.2 Administration und Konfiguration 12
4.1.3 Nutzeroberfläche 15
4.1.4 Dokumentation 16
4.2 Betrieb des Service Monitorings 16
4.2.1 Verfügbarkeits- und Durchsatzanforderungen 16
4.2.2 Speicherungsdauer der übermittelten Daten 17
4.3 Zugriffs- und Berechtigungskonzept 17
4.3.1 Zugriffskonzept 17
4.3.2 Berechtigungskonzept 17
5 Funktionsmerkmale 21
5.1 Schnittstelle I_View_Service_Monitoring 21
5.1.1 Darstellung der Monitoring-Daten 21
5.1.2 Schnittstelle View Service Monitoring API Web Service 22
5.1.3 Umsetzung 23
5.2 Schnittstelle I_Monitoring_Update 23
5.2.1 Schnittstellendefinition 23
5.2.2 Umsetzung 25
5.2.3 Nutzung 26
5.3 Technische Use Cases – TUCs 31
5.4 Probes 33
5.4.1 DNS Name Resolution 37
5.4.2 Konnektorregistrierung* 37
5.4.3 VPN_Tunnel* 40
5.4.4 VPN_Tunnel SIS* 42
5.4.5 Zeitinformation_TI 43

5.4.6 Zeitinformation_VPN_Zugangsdienst....44
5.4.7 CRL Download....44
5.4.8 TSL Download....46
5.4.9 TSL Download mit Prüfung....47
5.4.10 TSL Download IPsecTunnel TI*....47
5.4.11 TSL Download Internet....48
5.4.12 BNetzA_VL Download....48
5.4.13 BNetzA Download IPsecTunnel TI*....49
5.4.14 OCSP....50
5.4.15 OCSP IPsecTunnel TI*....51
5.4.16 Fachdienste VSDM....51
5.4.16.1 Fachdienst VSDM UFS....51
5.4.16.2 Fachdienst VSDM_VSDD_CMS....53
5.4.17 Intermediär VSDM*....55
5.4.18 VSDM- Intermediär VSDM IPsecTunnel TI*....56
5.4.19 VSDM-Intermediär VSDM Erreichbarkeit....57
5.4.20 KSRS Upload....57
5.4.21 KSRS Download....58
5.4.22 KSRS Download IPsecTunnel TI*....60
5.4.23 KSRS Download Bestandsnetze....60
5.4.24 KSRS Download Bestandsnetze IPsecTunnel TI*....61
5.4.25 Verzeichnisdienst Query....62
5.4.26 Verzeichnisdienst Query IPsecTunnel TI*....63
5.4.27 Verzeichnisdienst Application_Maintenance....63
5.4.28 Ablauf von Server-Zertifikaten (TI)....65
5.4.29 Ablauf von Server-Zertifikaten (Internet)....67
5.4.30 ePA - Authentisierung TI....67
5.4.31 ePA - Authentisierung Internet....69
5.4.32 ePA - Autorisierung....69
5.4.33 ePA - I_Authorization_Management::checkRecordExists....71
5.4.34 ePA - Dokumentenverwaltung....73
5.4.35 ePA – Verfügbarkeitsmonitoring....75
5.4.36 ePA -Schlüsselgenerierungsdienst....77
5.4.37 aAdG-NetG....79
5.4.38 Erfassung von Service Monitoring-Daten in Probes....81
5.5 Performance-Kenngrößen....82
6 Anhang A – Verzeichnisse....84
6.1 Abkürzungen....84
6.2 Glossar....84
6.3 Abbildungsverzeichnis....84
6.4 Tabellenverzeichnis....85
6.5 Referenzierte Dokumente....86
6.5.1 Dokumente der gematik....86
6.5.2 Weitere Dokumente....87
6.6 Fehlercodes....88
6.7 Offene Punkte / Klärungsbedarf....88

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 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 zwischen Afo-ID und Textmarke angeführten Inhalte.

2 Systemüberblick

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

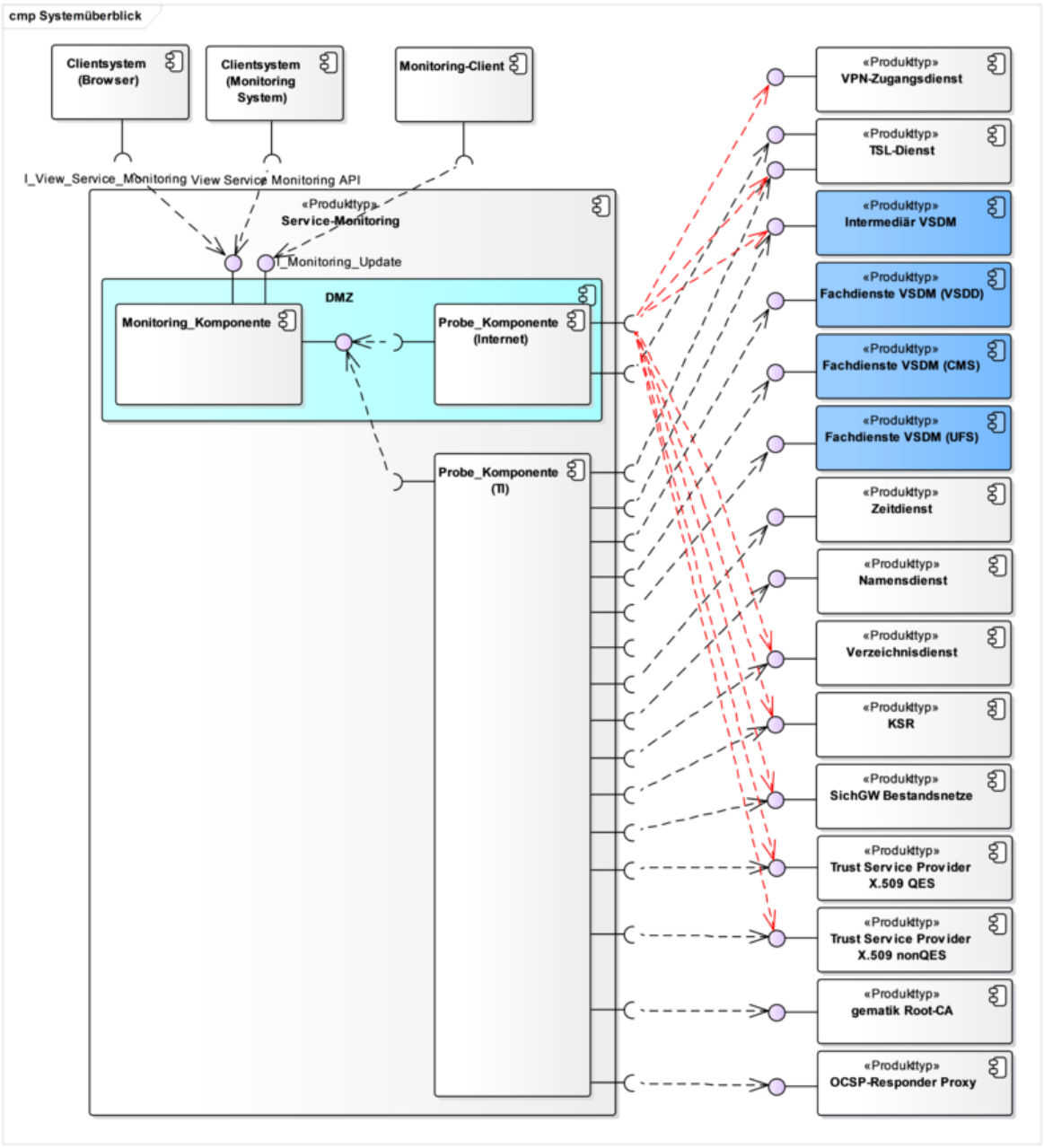


Abbildung 1: ABB_ServMon_301 Komponenten und Außensicht des Service Monitorings

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.

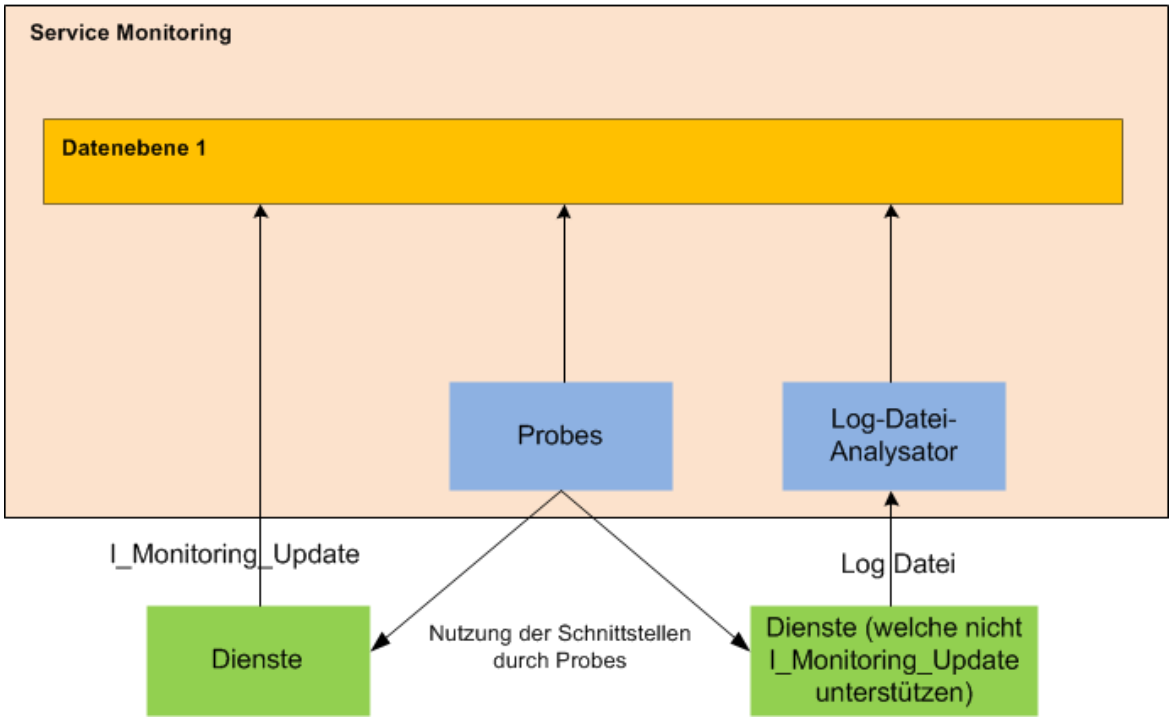


Abbildung 2: ABB_ServMon_304 Übersicht Service Monitoring-Datenquellen

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

- Probes ermitteln Kenngrößen und erzeugen Daten über die Probe-Ausführung (z.B. Zeitpunkt und Erfolg).
- Über I_Monitoring_Update werden Kenngrößen 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:

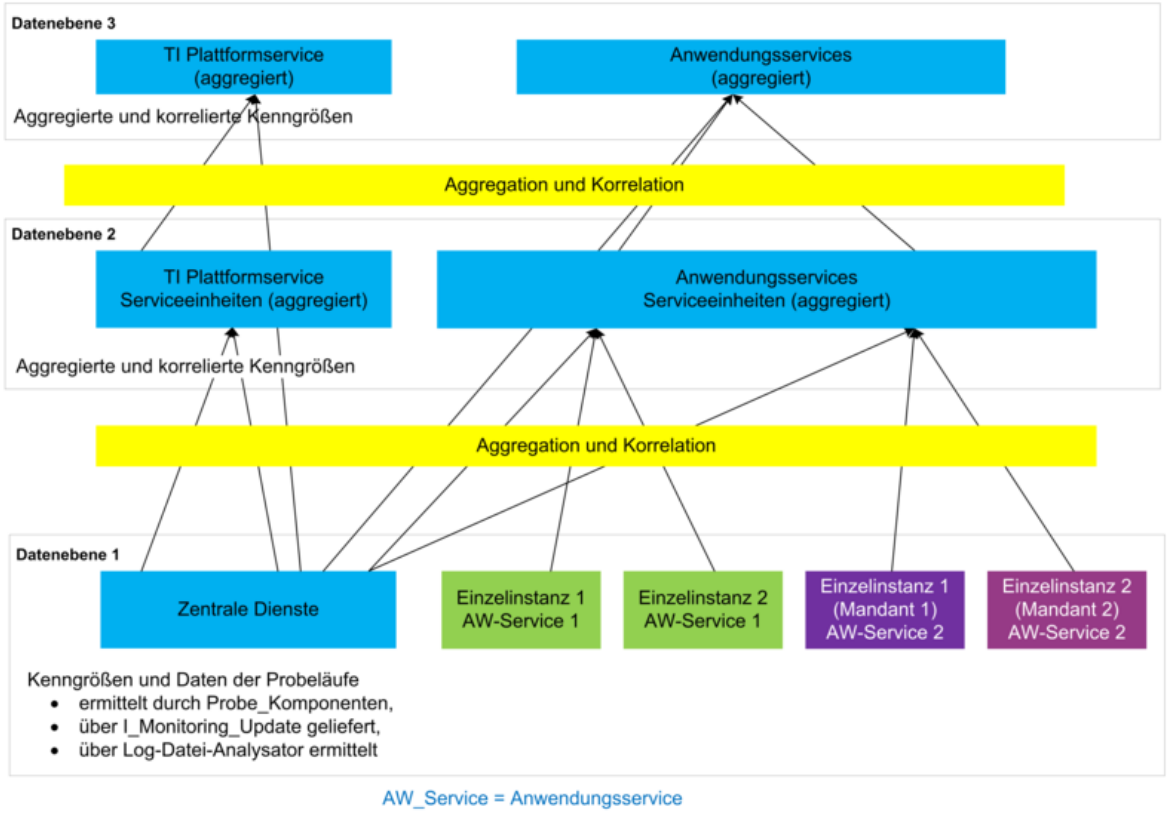


Abbildung 3: ABB_ServMon_303 Datenfluss Service Monitoring

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.

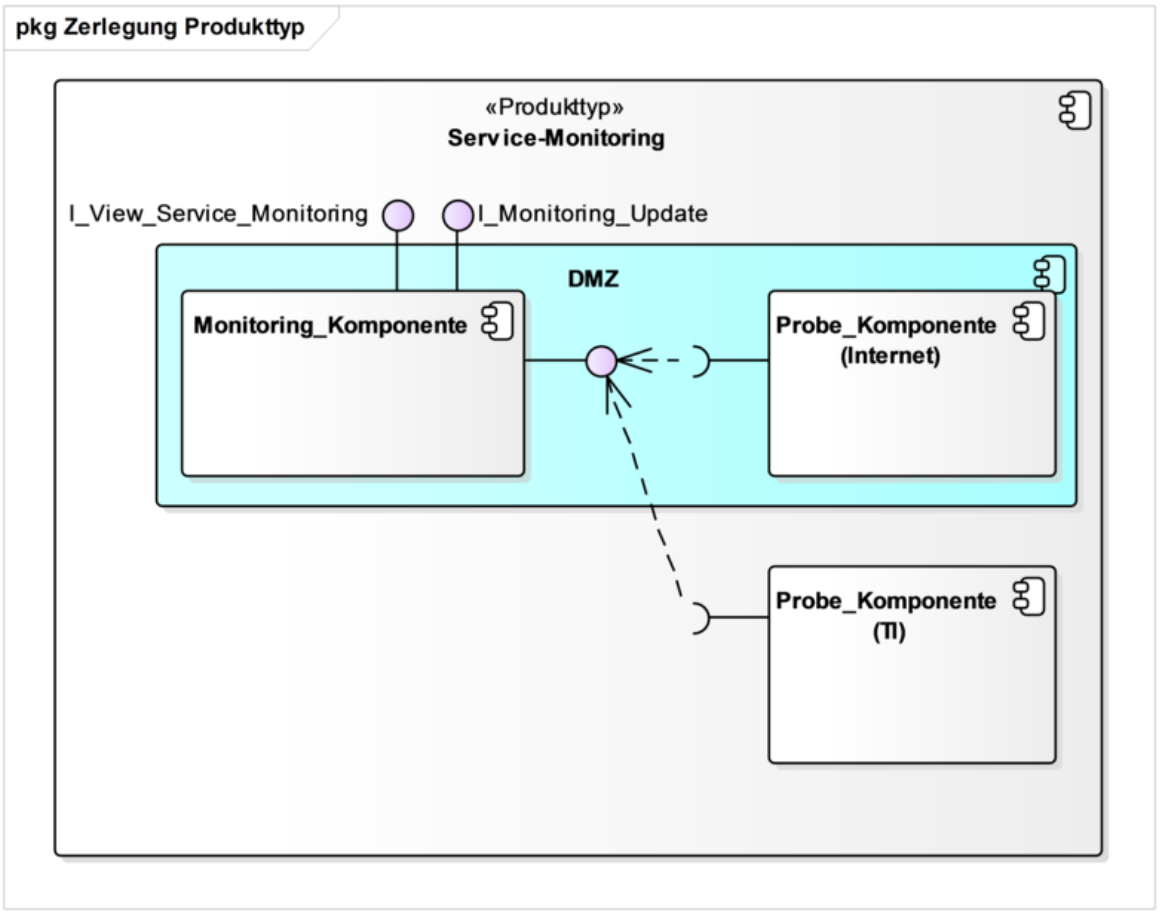


Abbildung 4: ABB_ServMon_300 – Komponentendiagramm des Service Monitorings

In Abbildung 4 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 dazugehörender 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-MonRead	Der Nutzer hat lesenden Zugriff (Sichtbar sind seine eigenen Daten sowie die – für seine Diensterbringung nötigen – TI-Plattformservices) auf Kenngrößen, Schwellwerte und Daten der Probe-Läufe.
I_View_Service_Monitoring (im Internet und in der TI erreichbar)	Registrierter Nutzer (ohne Zusatzberechtigungen Anwendungsservices)	SM-TI-User	Der Nutzer hat lesenden Zugriff (Sichtbar sind die Daten der TI-Plattformservices) auf Kenngrößen, Schwellwerte und Daten der Probe-Läufe.
	Registrierter Nutzer (mit Zusatzberechtigungen für einzelne Anwendungsservices)	SM-AS-User	Wie SM-TI-User Zusätzlich hat der Nutzer lesenden Zugriff auf die Daten (Kenngrößen, Schwellwerte und Daten der Probe-Läufe) der berechtigten Anwendungsservices. Diese Zugriff wird eingeschränkt auf die Daten von Dienstinstanzen des Anwendungsservices, welche dem Nutzer zugeordnet sind.
	Registrierter Nutzer (mit Administrationsberechtigungen)	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-Plattformservices zuordnen.

	Registrierter Nutzer (mit Nutzerverwaltungsberechtigungen)	SM-UserAdmin	Der Administrator kann
			• die Nutzer des Service Monitorings verwalten (anlegen, ändern, löschen, Anwendungsservices und Dienstinstanzen zuordnen),
			• dem Nutzer zusätzliche Berechtigungen zuweisen. Das beinhaltet mindestens:
			  • Übersicht über Alarmierungen anzeigen
			  • Wartungskalender ändern
			  • Probe Ausführung im GUI
			• Auditlogs einsehen.

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 anzeigt werden können.
[<=]

TIP1-A_7110 - Service Monitoring, Darstellung, Zeitachse mit verschiedenen Kenngrößen
Die Darstellung der Monitoring-Daten SOLL einen zeitlichen Bezug zwischen auswählbaren Kenngrößen darstellen können.
[<=]

5.1.2 Schnittstelle View Service Monitoring API Web Service

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

TIP1-A_7112 - Service Monitoring, View Service Monitoring API
Das Service Monitoring MUSS die Schnittstelle View Service Monitoring API unter einer URL im Internet und in der TI bereitstellen.
[<=]

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-Kenngroessen] festgelegt.

TIP1-A_7116 - Service Monitoring, Schnittstelle I_Monitoring_Update
Das Service MonitoringMUSS die Schnittstelle I_Monitoring_Update gemäß Tabelle Tab_Service_Monitoring_I_Monitoring_Update anbieten.

Tabelle 2: Tab_Service_Monitoring_I_Monitoring_Update

Name	I_Monitoring_Update	
Version	Webservice: v1.1	
Webservice Operationen	Name	Kurzbeschreibung
	update	Die Operation ermöglicht das Senden von Monitoringdaten an das Service Monitoring.
WSDL	I_Monitoring_Update10.wsdl Version: 1.1.0 TargetNamespace: http://ws.gematik.de/tel/stoerungsampel/wsdl/v1.1	
Schema	I_Monitoring_Update10.xsd Version: 1.1.0 TargetNamespace: http://ws.gematik.de/tel/stoerungsampel/v1.1 ProductInformation.xsd Version: 1.1.0 TargetNamespace: http://ws.gematik.de/tel/version/ProductInformation/v1.1 TelematikError.xsd Version: 2.0.0 TargetNamespace: http://ws.gematik.de/tel/error/v2.0	
Webservice Zugangspunkt	https://monitoring-update.stampel.telematik:8443/I_Monitoring_Update10	

[<=]

TIP1-A_7117 - Service Monitoring und Client, I_Monitoring_Update, WebService
Das Service Monitoringund 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 Nachrichtenübermittelung
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 Nachrichtenübermittelung keine Monitoringdaten über die Schnittstelle I_Monitoring_Update geliefert wurden – im GUI bzw. Dashboard hervorheben.
[<=]

TIP1-A_6744 - Service Monitoring, I_Monitoring_Update, Datenverarbeitung
Das Service Monitoring MUSS über die Schnittstelle I_Monitoring_Update gelieferte Daten in den Service Monitoring-Datenbestand als Kenngrößen entsprechend [gemSpec_Perf] übernehmen. Diese Kenngrößen MÜSSEN analog zu den durch Probes ermittelten Kenngrößen und den im Service Monitoring durch Aggregation/Korrelation ermittelten Kenngrößen

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

[<=]

5.2.2 Umsetzung

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

TIP1-A_7121 - Service Monitoring, I_Monitoring_Update, TLS-gesicherte Verbindung
Das Service Monitoring MUSS die Schnittstelle I_Monitoring_Update durch Verwendung von TLS mit serverseitiger Authentisierung sichern.
Das Service Monitoring MUSS sich mit der Identität ID.ZD.TLS-S und der enthaltenen

Admission-OID „oid_stamp“ gegenüber den nutzenden Systemen authentisieren.
[<=]

TIP1-A_7122 - Service Monitoring, Datenerhebung
Der Anbieter des Service Monitorings MUSS die Voraussetzungen dafür schaffen, dass die in der [gemSpec_Perf] unter GS-A_4147 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	Zertifkats-Typen-ID lt. [gemSpec_Perf]
querysource	Aufrufquellen-ID lt. [gemSpec_Perf]
connect	Eindeutige ID zur Identifikation bei Ende-zu-Ende-Messungen im Netzwerk-Bereich

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

Die folgende Abbildung zeigt die Datenstruktur des SOAP-Requests.

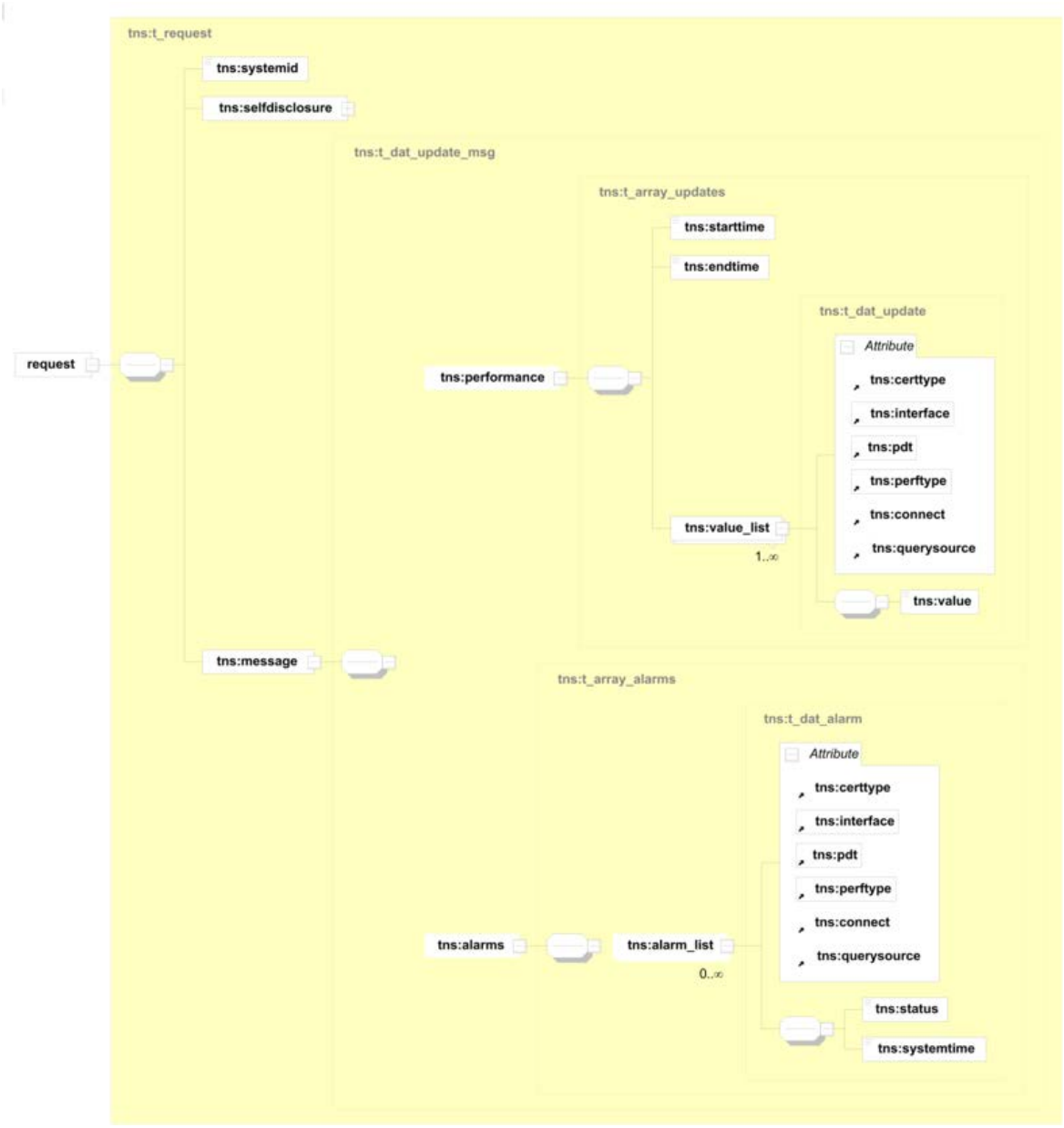


Abbildung 5: Abb_Service_Monitoring_SOAP-Request

Tabelle 4: Tab_Service_Monitoring_SOAP-Request, Beschreibung der Elemente

Element	Beschreibung
tns:request	definiert den SOAP-Request, der über die Operation update an das Service Monitoring gesendet wird.
tns:systemid	ermöglicht eine eindeutige Identifikation des sendenden Systems/Dienstes. Diese ID MUSS eindeutig sein und deren Vergabe erfolgt in Abstimmung zwischen dem Anbieter Service Monitoring und dem Dienstanbieter.

tns:selfdisclosure	enthält Informationen zur Selbstauskunft eines meldenden Systems, siehe [gemSpec_OM].
tns:message	beinhaltet die in [gemSpec_Perf] für den Dienst geforderten Verfügbarkeits-, Performance- und Auslastungsdaten.
tns:performance	beinhaltet die in [gemSpec_Perf] für den Dienst geforderten Performance- und Auslastungsdaten.
tns:alarms	beinhaltet die in [gemSpec_Perf] für den Dienst geforderten Verfügbarkeitsdaten.
tns:starttime, tns:endtime	definieren das zugrundeliegende Zeitintervall für Performance- und Auslastungswerte.
tns:value_list	enthält die Liste der Performance-Kenngrößen vom Typ t_dat_update. Dieses Element muss die folgenden Attribute enthalten. tns:interface: Schnittstellenoperationen-ID lt. [gemSpec_Perf] tns:pdt: Produkttyp-ID lt. [gemSpec_Perf] tns:perftype: Performance-Kenngrößen-ID lt. [gemSpec_Perf] Dieses Element kann die folgenden Attribute enthalten. tns:certtype: Zertifkats-Typen-ID lt. [gemSpec_Perf] tns:connect: Eindeutige ID zur Identifikation bei Ende-zu-Ende-Messungen im Netzwerk-Bereich tns:querysource: Aufrufquellen-ID lt. [gemSpec_Perf] Mit einer SOAP-Nachricht können mehrere Werte für gleiche Zeitintervalle übergeben werden.
tns:value	Wert der Performance-Kenngröße
tns:alarm_list	enthält die Alarmstatus-Informationen. Dieses Element muss die folgenden Attribute enthalten. tns:interface: Schnittstellenoperationen-ID lt. [gemSpec_Perf] tns:pdt: Produkttyp-ID lt. [gemSpec_Perf] tns:perftype: Performance-Kenngrößen-ID lt. [gemSpec_Perf] Dieses Element kann die folgenden Attribute enthalten. tns:certtype: Zertifkats-Typen-ID lt. [gemSpec_Perf] tns:connect: Eindeutige ID zur Identifikation bei Ende-zu-Ende-Messungen im Netzwerk-Bereich tns:querysource: Aufrufquellen-ID lt. [gemSpec_Perf]
tns:status	enthält den Alarm-Status. open: Alarmstatus gesetzt close: Alarmstatus gelöscht warn: nicht benutzt grace: nicht genutzt

tns:systemtime	Alarmzeit des sendenden Systems zur Erkennung von Inkonsistenzen (z.B. Alarme aus historischen Daten).

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

Tabelle 5: Tab_Service_Monitoring_SOAP-Response, Beschreibung der Elemente

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

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

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_5581 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_Resolutionbereitstellen. Dieser TUC MUSS in allen Probes zur DNS-Namensauflösung genutzt werden.

Tabelle 6: Tab_Service_Monitoring_TUC_SM_001_DNS_Name_Resolution

Name	TUC_SM_001_DNS_Name_Resolution	
Beschreibung	Dieser TUC führt die Auflösung eines FQDN in eine IP-Adresse durch.	
Vorbedingungen	• Keine	
Eingangsdaten	• IP-Adresse Namensdienst • Aufzulösender FQDN • Bisher ermittelte Service Monitoring Daten • Ein Flag für die DNS-Record Validierung (DNSSEC). Ist es gesetzt wird die Validierung durchgeführt.	
Komponenten	• Service Monitoring Probe, DNS-Nameserver	
Ausgangsdaten	• Aufgelöste IP-Adresse • Ermittelte Service Monitoring Daten für die DNS Namensauflösung	
Standardablauf	**Aktion**	**Beschreibung**
	IP-Adresse der Schnittstelle ermitteln	Durch eine DNS-Anfrage (I_DNS_Name_Resolution:: get_IP_Address.) wird der FQDN in eine IP-Adresse aufgelöst.
	Falls bei der DNS-Anfrage keine Antwort (und kein DNS-Fehler)	Prüfung der Erreichbarkeit des DNS-Nameserver über TUC_SM_002_Erreichbarkeitsprüfung. Der Service Monitoring Datensatz für die DNS-Namensauflösung wird in diesem Fall in

	ermittelt werden konnte	TUC_SM_002_Erreichbarkeitsprüfung erstellt.
	Falls bei der DNS-Anfrage eine Antwort oder ein DNS-Fehler ermittelt werden konnte	Die Service Monitoring-Daten (aus den Eingangsdaten) werden entsprechend der durchgeführten Aktionen, Tab_Service_Monitoring_Probe_Daten und um die Performance-Kenngröße „Bearbeitungszeit“ ergänzt. Dabei wird das „Probe-Ergebnis“ dieses Datensatzes • auf OK gesetzt, falls der FQDN in eine IP-Adresse aufgelöst wurde. • auf 7102 gesetzt, falls der DNS-Server mit einem Fehler geantwortet hat. • Auf 7108 gesetzt, falls die DNS-Record Validierung (DNSSEC) fehlgeschlagen ist.
	Rückgabe der Daten	Rückgabe der Ausgangsdaten

[<=]

TIP1-A_7148 - Service Monitoring, TUC_SM_002_Erreichbarkeitsprüfung
Das Service Monitoring MUSS TUC_SM_002_Erreichbarkeitsprüfung entsprechend Tab_Service_Monitoring_TUC_SM_002_Erreichbarkeitsprüfung bereitstellen. Dieser TUC MUSS in Probes genutzt werden wenn

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

Tabelle 7: Tab_Service_Monitoring_TUC_SM_002_Erreichbarkeitsprüfung

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

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

[<=]

5.4 Probes

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 Dienstinstanzen) ausführbar sein.**[<=]**

TIP1-A_7141 - Service Monitoring, Probes, Übersicht über active Probes
Das Service Monitoring MUSS berechtigten Nutzern eine Übersicht über die aktiven Probes mit ihren Ausführungszeitpunkten anzeigen können. Aktive Probes sind Probes mit Ausführungszeitpunkten in der Zukunft.
Das Service Monitoring MUSS den berechtigten Nutzern die Änderung und Stornierung der Ausführungszeitpunkte der Probes erlauben.**[<=]**

TIP1-A_7142 - Service Monitoring, Probes, Details zu den Probe-Messungen
Das Service Monitoring MUSS für alle Probe Ausführungen folgende Daten erfassen

- Die Ausführung der Probe inklusive der in der Probe Beschreibung definierten Daten.
- Den Mitschnitt der Kommunikation (gesendete und empfangene Daten) für eine konfigurierbare Anzahl der letzten Messungen.
- Das Ergebnis der Probe Messung (Entspricht das Ergebnis der Probe dem erwarteten Ergebnis?)
- 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
Benennung der Probe	DNS_Name_Resolution
Dienst	Namensdienst
Schnittstelle	I_DNS_Name_Resolution
Operation	get_IP_Address
Netzwerk	Internet zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für • die autoritativen Nameserver des Namensdienstes • alle Bestandsnetze (implizit I_Secure_Access_Bestandsnetz)
Vorbedingung	Für die Probe müssen folgende Informationen konfigurierbar sein: • Die DNS-Nameserver, für die diese Probe ausgeführt wird. • Die aufzulösenden FQDN für jeden DNS-Nameserver. • Ein Flag für jeden DNS-Nameserver. Ist es gesetzt wird eine DNS-Record Validierung (DNSSEC) in der Probe durchgeführt.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jeden DNS-Nameserver verfügbar sein.
Standardablauf	1. Die Probe ruft für jeden DNS-Nameserver TUC_SM_001_DNS_Name_Resolution mit der FQDN, 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
Benennung der Probe	Konnektorregistrierung
Dienst	Registrierungsserver
Schnittstelle	I_Registration_Service
Operation	registerKonnektor deregisterKonnektor
Netzwerk	Internet
Beschreibung	Diese Probe wird ausgeführt für alle Standorte des VPN-ZugD, inkl. der Schnittstelle I_DNS_Name_Resolution (implizit für Namensraum Internet). Es wird ein Konnektor registriert und gleich wieder deregistriert. Dieser Konnektor bzw. die ContractID wird nur für diese Probe genutzt. In anderen Probes benötigte VPN-Kanäle werden mit separaten Konnektorregistrierungen/ContractIDs realisiert.
Vorbedingung	Der Betreiber des Registrierungsservers muss informiert sein, dass für eine festgelegte Contract-ID durch die Probes häufig eine Registrierung und Deregistrierung erfolgt. Der Konnektor (den die Probe simuliert) muss für alle VPN-Zugangsdienste registriert sein. In der Probe müssen für jeden VPN-Zugangsdienstanbieter folgende Daten konfigurierbar sein: - DNS_SERVERS_INT (DNS-Server im Internet) - DNS_DOMAIN_VPN_ZUGD_INT (alle DNS-Domainnamen für die Service Discovery der VPN-Konzentratoren) - ContractID Das Zertifikat C.NK.VPN (SMC-K) muss vorliegen (für die Erstellung des registerKonnektor Requests nötig). Sie SMC-B muss für die Signatur des Registrierungsrequests freigeschaltet sein.
Nachbedingung	Im Service Monitoring müssen die definierten Daten für jeden VPN-Konzentrator des entsprechenden VPN-Zugangsdienstes verfügbar sein: • für die Teilschritte des Standardablaufs der Probe (wie im Standardablauf definiert) • für jede Probe-Ausführung für einen VPN-Konzentrator
Standardablauf	1. Ermittlung der URI aller Registrierungsservers für alle DNS-Domänen (siehe auch TIP1-A_4825 [gemSpec_Kon]). • Falls der DNS-Namensdienst keine erwartete Antwort und keine Fehlermeldung liefert, wird die Erreichbarkeit des DNS-Namensdienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit Punkt 3 und „Probe-Ergebnis“ • 7100 Namensdienst nicht erreichbar oder

	• 7101 Ports vom Namensdienst geschlossen oder • 7103 Aufruf mit Fehler beendet beendet. • Falls der DNS-Namensdienst eine valide Antwort ohne Informationen über die Registrierungsserver oder eine Fehlermeldung liefert wird die Probe mit Punkt 3 („Probe-Ergebnis“ = 7104) beendet.
	2. Für jeden ermittelten Registrierungsservers:
	2.1. Erstellung eines registerKonnektor-Requests inklusive Signatur durch SM-B / C.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 / C.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.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Registrierungsservers Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten Registrierungsserver fortgesetzt werden. Das „Probe-Ergebnis“ für den Aufruf dieses Registrierungsservers wird auf • 7100 Registrierungsserver nicht erreichbar oder • 7101 Ports vom Registrierungsserver geschlossen oder • 7103 Aufruf mit Fehler beendet

	gesetzt.

[<=]

5.4.3 VPN_Tunnel*

TIP1-A_7151 - Service Monitoring, Probe VPN Tunnel
Das Service Monitoring MUSS die Probe VPN-Tunnel entsprechend Tab_Service_Monitoring_Probes_VPN_Tunnel bereitstellen.

Tabelle 10: Tab_Service_Monitoring_Probes_VPN_Tunnel

Element	Beschreibung
Benennung der Probe	VPN Tunnel
Dienst	VPN-Zugangsdienst
Schnittstelle	I_Secure_Channel_Tunnel I_IP_Transport
Operation	I_Secure_Channel_Tunnel::connect I_Secure_Channel_Tunnel::send_secure_IP_Packet I_Secure_Channel_Tunnel::disconnect
Netzwerk	Internet
Beschreibung	Diese Probe wird ausgeführt für alle VPN-Konzentratoren aller Standorte des VPN-ZugD, inkl. der Schnittstelle I_DNS_Name_Resolution (implizit für Namensraum Internet und TI). Die Probe wird für jeden VPN-Konzentrator ausgeführt. Es wird ein VPN-Tunnel auf- und – nach Senden von Datenpaketen – wieder abgebaut. Bei dem VPN-Tunnel-Aufbau wird die Gültigkeitsdauer der VPN-Konzentrator- Zertifikate ermittelt und in den Service-Monitoring-Daten gespeichert.
Vorbedingung	Der Konnektor (den die Probe simuliert) muss für alle VPN-Zugangsdienste registriert sein. Die Probe muss für jeden VPN-Zugangsdienstanbieter mit folgenden Daten konfigurierbar sein: • DNS_SERVERS_INT (DNS Server im Internet) • DNS_DOMAIN_VPN_ZUGD_INT (alle DNS-Domainnamen für die Service Discovery der VPN-Konzentratoren) • ContractID • VPN-Zertifikat des simulierten Konnektors (C.NK.VPN) • Dauer der IPSec-Verbindung
Nachbedingung	Im Service Monitoring müssen die definierten Daten den VPN-Konzentrator verfügbar sein: • für die Teilschritte des Standardablaufs der Probe (wie im

	Standardablauf definiert) • für jede Probe-Ausführung für einen VPN-Konzentrator In den Service-Monitoring-Daten werden die Gültigkeitsdauern der VPN-Konzentrator-Zertifikate aktualisiert. Für jeden geprüften VPN-Konzentrator müssen mindestens folgende Daten erfasst werden: • Name des VPN-Konzentrators • Adresse des Dienstes bzw. der Schnittstelle • Gültigkeitsende des Zertifikats • Subject, IssuerDN und SerialNumber des Zertifikats 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.
Standardablauf	1. Liste der VPN-Konzentratoren über DNS-SRV ermitteln (siehe auch TIP1-A_4373 [gemSpec_VPN_ZugD]). • Falls der DNS-Namensdienst keine erwartete Antwort und keine Fehlermeldung liefert, wird die Erreichbarkeit des DNS-Namensdienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit Punkt 3 und „Probe-Ergebnis“ • 7100 Namensdienst nicht erreichbar oder • 7101 Ports vom Namensdienst geschlossen oder • 7103 Aufruf mit Fehler beendet beendet. • Falls der DNS-Namensdienst eine valide Antwort ohne Informationen über die Registrierungsserver oder eine Fehlermeldung liefert, wird die Probe mit Punkt 3 („Probe-Ergebnis“ = 7104) beendet.
	2. Für jeden ermittelten VPN-Konzentrator muss die Probe mit den folgenden Unterpunkten einen Tunnelaufbau-Test durchführen.
	2.1. Aufbau einer Verbindung zum VPN-Konzentrator (siehe auch TUC_VPN-ZD_0001 [gemSpec_VPN_ZugD] bzw. TIP1-A_4783 [gemSpec_Kon]).
	2.2. Ermittlung der Service Monitoring-Daten für den Verbindungsaufbau entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“. Analyse Server-Zertifikat • Prüfung des Ablaufdatums des Server-Zertifikats • Auslösen einer Warnung oder eines Alarms über die Service-Monitoring- Alarmierung, falls das Zertifikat in x Tagen (entsprechend Konfigurationsdaten) ausläuft. Ablage der ermittelten Daten (siehe Nachbedingungen).

	2.3. Senden eines Datenpakets über den VPN Tunnel und Empfang eines Antwortpakets (siehe auch [gemSpec_VPN_ZugD#5.1.3]). Das kann z.B. ein Ping (ICMP-„Echo-Request“) zu einem zentralen Dienst der TI sein. Das Senden des Datenpakets muss mit dem Betreiber des zentralen Dienstes abgestimmt sein.
	2.4. Ermittlung der Service Monitoring-Daten für die Übertragung des Datenpakets entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	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.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des VPN-Konzentrators Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung (TCP Ports 500 und 4500) geprüft und die Probe mit dem nächsten VPN-Konzentrator fortgesetzt werden. Das „Probe-Ergebnis“ für diesen VPN-Konzentrator wird auf • 7100 VPN-Konzentrator nicht erreichbar oder • 7101 Ports vom VPN-Konzentrator geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.4 VPN_Tunnel SIS*

TIP1-A_7152 - Service Monitoring, Probe VPN Tunnel SIS
Das Service Monitoring MUSS die Probe VPN Tunnel SIS entsprechend Tab_Service_Monitoring_Probes_VPN_Tunnel mit folgenden Änderungen für den VPN-Konzentrator SIS realisieren:

- Benennung der Probe: VPN Tunnel SIS
- Dienst: VPN-Zugangsdienst SIS

- Schnittstelle: I_Secure_Internet_Tunnel
- Operation:
  I_Secure_Internet_Tunnel::connect
  I_Secure_Internet_Tunnel::send_secure_IP_Packet
  I_Secure_Internet_Tunnel::disconnect
- Vorbedingung:Zusätzlich muss mit der genutzten ContractID ein VPN Tunnel aufgebaut sein.
- 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
Benennung der Probe	Zeitinformation TI
Dienst	Zeitdienst
Schnittstelle	I_NTP_Time_Information
Operation	sync_Time
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle Stratum-1-NTP-Server der TI.
Vorbedingung	Die NTP-Server der TI müssen für die Probe konfigurierbar sein.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jeden NTP-Server verfügbar sein.
Standardablauf	1. Die Probe führt für jeden NTP-Server die folgenden Schritte durch:
	1.1. Ermittlung der IP-Adresse des NTP-Servers durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.

	1.2. Die Probe ermittelt von dem NTP-Server die Zeit über das NTPv4 Protokoll (siehe auch GS-A_3934 [gemSpec_Net]).
	1.3. Ermittlung der Service Monitoring-Daten für den NTP-Server entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des NTP-Servers Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten NTP-Server fortgesetzt werden. Das „Probe-Ergebnis“ für diesen NTP-Server wird auf • 7100 NTP-Servers nicht erreichbar oder • 7101 Ports vom NTP-Servers geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.6 Zeitinformation_VPN_Zugangsdienst

TIP1-A_7154 - Service Monitoring, Probe Zeitinformation VPN Zugangsdienst
Das Service Monitoring MUSS die Probe Zeitinformation VPN-Zugangsdienst entsprechend Tab_Service_Monitoring_Probes_Zeitinformation_TI für die Stratum-2-NTP-Server mit folgenden Änderungen für die Zeitinformation VPN-Zugangsdienst realisieren:

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

[<=]

5.4.7 CRL Download

TIP1-A_7155 - Service Monitoring, Probe CRL Download
Das Service Monitoring MUSS die Probe CRL Download entsprechend Tab_Service_Monitoring_Probes_CRL_Download bereitstellen.

Tabelle 12: Tab_Service_Monitoring_Probes_CRL_Download

Element	Beschreibung
Benennung der Probe	CRL Download
Dienst	Trust Service Provider X.509 nonQES
Schnittstelle	I_CRL_Download
Operation	download_CRL
Netzwerk	Internet
Beschreibung	Diese Probe wird ausgeführt für alle CRL Distribution Points (CDP).
Vorbedingung	Die CRL Distribution Points (CDP) müssen für die Probe konfigurierbar sein. Die minimale zeitliche Gültigkeit der CRL (KONF_ZG_CRL) muss konfigurierbar sein (in Minuten oder Sekunden).
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jeden CRL Distribution Point (CDP) verfügbar sein.
Standardablauf	1. Die Probe führt für jeden CRL Distribution Point (CDP) die folgenden Schritte durch:
	1.1. Ermittlung der IP-Adresse des CRL Distribution Points durch TUC_SM_001_DNS_Name_ResolutionResolution ohne DNS-Record Validierung (DNSSEC).
	1.2. Die Probe lädt die CRL vom CRL Distribution Point (siehe auch TIP1-A_4248 [gemSpec_X.509_TSP]). Falls die CRL nicht auf dem CRL Distribution Point vorliegt wird der gelieferte Fehlercode in den Service Monitoring Daten erfasst.
	1.3 Prüfung der CRL-Signatur • Prüfung auf zeitliche Gültigkeit des CRL-Signer-Zertifikats mittels TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats" mit Referenzzeitpunkt = aktuelle Systemzeit. • Auswahl des öffentlichen Schlüssels des CRL-Signer-Zertifikats. • Die Signatur und der verwendete Algorithmus werden aus der CRL ausgelesen. • Verifikation der Signatur und Hashwert-Vergleich (Verfahren siehe [RFC5280]). • Prüfung ob die aktuelle Systemzeit + Konfigurationsparameter KONF_ZG_CRL den Wert NextUpdate aus der CRL erreicht oder überschritten hat.
	1.4. Ermittlung der Service Monitoring-Daten für den CRL Distribution Point entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.

Ursachen-Analyse im Fehlerfall	Falls im Standardablauf (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 • 7100 CRL Distribution Point nicht erreichbar oder • 7101 Ports vom CRL Distribution Point geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt. Falls im Standardablauf (Punkt 1.3) bei der CRL-Signaturprüfung Fehler auftreten, muss das „Probe-Ergebnis“ für diesen CRL Distribution Point auf • 7109 Minimale zeitliche Gültigkeit der CRL unterschritten oder • 7110 CRL Signaturprüfung fehlgeschlagen gesetzt werden.

[<=]

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
Benennung der Probe	TSL Download
Dienst	TSL-Dienst
Schnittstelle	I_TSL_Download
Operation	download_TSL
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für den TSL Dienst.
Vorbedingung	Die URL(s) für den Download der TSL vom TSL-Dienst muss für die Probe konfigurierbar sein.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für den TSL Dienst verfügbar sein.
Standardablauf	1. Die Probe führt für jede TSL-Download-Adresse die folgenden Schritte durch:
	1.1. Ermittlung der IP-Adresse des TSL-Dienstes durch

	TUC_SM_001_DNS_Name_Resolution.
	1.2. Die Probe lädt die TSL (siehe auch [gemSpec_TSL#6.3.1]).
	1.3. Ermittlung der Service Monitoring-Daten für den Download entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf beim Laden der TSL Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit der nächsten TSL-Download-Adresse fortgesetzt werden. Das „Probe-Ergebnis“ wird für diesen TSL Download-Punkt auf • 7100 TSL Download-Punkt nicht erreichbar oder • 7101 Ports vom TSL Download-Punkt geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.9 TSL Download mit Prüfung

TIP1-A_7157 - Service Monitoring, Probe TSL Download mit Prüfung
Das Service Monitoring MUSS die Probe TSL Download mit Prüfung entsprechend Tab_Service_Monitoring_Probes_TSL_Download bereitstellen.
Folgende Abweichungen von Tab_Service_Monitoring_Probes_TSL_Download MÜSSEN beachtet werden:

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

[<=]

5.4.10 TSL Download IPsecTunnel TI*

TIP1-A_7158 - Service Monitoring, Probe TSL Download IPsecTunnel TI
Das Service Monitoring MUSS die Probe TSL Download IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_TSL_Download bereitstellen. Die Probe TSL Download IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI einen IPsecTunnel nutzen.
Folgende Abweichungen von Tab_Service_Monitoring_Probes_TSL_Download MÜSSEN beachtet werden:

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

[<=]

5.4.11 TSL Download Internet

TIP1-A_7159 - Service Monitoring, Probe TSL Download Internet
Das Service Monitoring MUSS die Probe TSL Download Internet entsprechend Tab_Service_Monitoring_Probes_TSL_Download bereitstellen. Die Probe TSL Download Internet MUSS die TSL vom TSL-Dienst im Internet laden.
Folgende Abweichungen von Tab_Service_Monitoring_Probes_TSL_Download MÜSSEN beachtet werden:

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

[<=]

5.4.12 BNetzA_VL Download

TIP1-A_7160 - Service Monitoring, Probe BNetzA Download
Das Service Monitoring MUSS die Probe BNetzA Download entsprechend Tab_Service_Monitoring_Probes_BNetzA_Download bereitstellen.

Tabelle 14: Tab_Service_Monitoring_Probes_BNetzA_Download

Element	Beschreibung
Benennung der Probe	BNetzA Download
Dienst	TSL-Dienst
Schnittstelle	I_BNetzA_VL_Download
Operation	download_VL
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle ServiceSupplyPoints für die BNetzA-VL.
Vorbedingung	Die Download-Adressen der BNetzA-VL müssen konfigurierbar sein.

Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Die Probe führt für jede Download-Adresse der BNetzA-VL die folgenden Schritte durch:
	1.1. Ermittlung der IP-Adresse der BNetzA-VL Download-Adresse durch TUC_SM_001_DNS_Name_Resolution.
	1.2. Die Probe lädt die BNetzA-VL vom Download-Adresse (siehe auch GS-A_5484 [gemSpec_PKI]).
	1.3. Ermittlung der Service Monitoring-Daten für den BNetzA-VL Download entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf beim Laden der BNetzA-VL Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit der nächsten BNetzA-VL Adresse fortgesetzt werden. Das „Probe-Ergebnis“ wird für diese Download-Punkt der BNetzA-VL auf • 7100 Download-Punkt der BNetzA-VL nicht erreichbar oder • 7101 Ports vom Download-Punkt der BNetzA-VL geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.13 BNetzA Download IPsecTunnel TI*

TIP1-A_7310 - Service Monitoring, Probe BNetzA Download IPsecTunnel TI
Das Service Monitoring MUSS die Probe BNetzA Download IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_BNetzA_Download bereitstellen. Die Probe BNetzA Download IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI einen IPsec-Tunnel nutzen.
Folgende Abweichungen von Tab_Service_Monitoring_Probes_BNetzA_Download sind zu beachteten:

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

[<=]

5.4.14 OCSP

TIP1-A_7311 - Service Monitoring, Probe OCSP
Das Service Monitoring MUSS die Probe OCSP entsprechend Tab_Service_Monitoring_Probes_OCSP bereitstellen.

Tabelle 15: Tab_Service_Monitoring_Probes_OCSP

Element	Beschreibung
Benennung der Probe	OCSP
Dienst	TSL-Dienst
Schnittstelle	I_OCSP_Status_Information
Operation	check_Revocation_Status
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle ServiceSupplyPoints in der TSL (inkl. alle ServiceSupplyPoints in der VL über den OCSP-Responder Proxy).
Vorbedingung	In der Probe müssen folgende Daten konfigurierbar sein: • OCSP-Responder Adressen • Für jeden OCSP-Responder müssen Zertifikatsdaten für die OCSP-Abfrage konfigurierbar sein Die OCSP-Responder Adressen können optional auch aus der TSL ermittelt werden. Die manuelle Konfiguration der OCSP-Adressen muss auch in diesem Fall alternativ möglich sein.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Die Probe führt für jeden OCSP-Responder die folgenden Schritte durch:
	1.1. Ermittlung der IP-Adresse des OCSP-Responder ServiceSupplyPoints durch TUC_SM_001_DNS_Name_Resolution.
	1.2. Die Probe führt eine OCSP-Abfrage entsprechend GS-A_4657 TUC_PKI_006 [gemSpec_PKI] durch.
	1.3. Ermittlung der Service Monitoring-Daten für die OCSP-Abfrage entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den OCSP Abfragen Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten OCSP-Responder fortgesetzt

	werden. Das „Probe-Ergebnis“ wird für diesen OCSP auf • 7100 OCSP nicht erreichbar oder • 7101 Ports vom OCSP geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.15 OCSP IPsecTunnel TI*

TIP1-A_7312 - Service Monitoring, Probe OCSP IPsecTunnel TI
Das Service Monitoring MUSS die Probe OCSP IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_OCSP bereitstellen. Die Probe BNetzA Download IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI einen IPsecTunnel nutzen.
Folgende Abweichungen von Tab_Service_Monitoring_Probes_OCSP sind zu beachteten:

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

  Diese Probe wird ausgeführt für jeden VPN-Zugangsdienst und jeden Standort eines VPN-Zugangsdienstes (für alle ServiceSupplyPoints in der TSL über den http-Forwarder)
- Standardablauf: Die OCSP-Abfrage wird über den http-Forwarder ausgeführt
- Vorbedingung:
  - Zusätzlich wird für den Aufbau des IPsec Tunnels das SMC-K Zertifikat C.NK.VPN benötigt.
  - Der der IPsec Tunnel zur TI muss aufgebaut sein.

[<=]

5.4.16 Fachdienste VSDM

TIP1-A_7313 - Service Monitoring, Probe Fachdienste VSDM
Das Service Monitoring MUSS die Konfiguration der Fachdienste VSDM Probes mit jedem Fachdienstbetreiber abstimmen und individuell für jeden Fachdienst konfigurieren.
[<=]

5.4.16.1 Fachdienst VSDM UFS

TIP1-A_7314 - Service Monitoring, Probe UFS
Das Service Monitoring MUSS die Probe UFS entsprechend Tab_Service_Monitoring_Probes_UFS bereitstellen.

Tabelle 16: Tab_Service Monitoring_Probes_UFS

Element	Beschreibung
Benennung der Probe	UFS
Dienst	Update Flag Service
Schnittstelle	I_UFS
Operation	GetUpdateFlags
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle UFS-Fachdienste.
Vorbedingung	Die Daten für alle UFS-Fachdienste – welche durch die Probe aufgerufen werden – müssen konfigurierbar sein. Für den Aufruf von Operation I_UFS::GetUpdateFlags müssen folgende Werte in der Probe für den jeweiligen UFS konfigurierbar sein: • URL des Fachdienstes UFS • ServiceType (UFS) • ICCSN • Provider ID • Erwartete Fachdienstantwort/Fehlercode Die Probe muss sowohl eine korrekte Fachdienst-Antwort (mit UpdateID oder ServiceReceipt) wie auch einen SOAP-Fehler mit Fehlercode (z.B. 11101) als erwartete Antwort akzeptieren können. Die Probe muss über ein TLS-Client-Zertifikat (C.FD.TLS-C) für den Verbindungsaufbau zum UFS verfügen.
Nachbedingung	Im Service Monitoring müssen für die gesamte Probe und für die Teilschritte des Probe-Ablaufs die dort definierten Daten für den UFS verfügbar sein. Falls der Fachdienst UFS eine UpdateID liefert, muss sie in einem folgenden Aufruf des VSDD- oder CMS-Fachdienstes als Eingangsparameter nutzbar sein.
Standardablauf	1. Für jeden Fachdienst:
	1.1. Ermittlung der IP-Adresse des UFS durch eine DNS-Anfrage (DNS-SRV Fachdienst) mit TUC_SM_001_DNS_Name_Resolution.
	1.2. Verbindungsaufbau zum UFS unter Nutzung des TLS-Client-Zertifikats.
	1.3. Senden des GetUpdateFlags Requests zum UFS unter Nutzung der Konfigurationsparameter ICCSN und Provider ID [gemSpec_SST_FD_VSDM#3.1].
	1.4. Das vom Fachdienst gelieferte Ergebnis wird mit der erwarteten Fachdienstantwort/Fehlercode verglichen. Das Fachdienstergebnis ist von den Konfigurationsparametern ProviderId und ICCSN abhängig. Für eine nicht existierende ICCSN wird als Ergebnis ein Gematik SOAP Fault mit Fehlercode 11101 (für die eGK mit der angegebenen ICCSN ist der aufgerufene Dienst nicht zuständig) erwartet.

	Für eine existierende ICCSN wird eine korrekte Fachdienst Antwort (mit UpdateID oder ServiceReceipt) erwartet.
	1.5. Ermittlung der Service Monitoring-Daten für Operation GetUpdateFlags entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Ermittlung der Service Monitoring-Daten für die gesamte Probe und Rückgabe aller Datensätze an das Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Fachdienstes Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten Fachdienst fortgesetzt werden. Das „Probe-Ergebnis“ wird für diesen Fachdienst auf • 7100 Fachdienst nicht erreichbar oder • 7101 Ports vom Fachdienst geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.16.2 Fachdienst VSDM_VSDD_CMS

TIP1-A_7315 - Service Monitoring, Probe VSDD_CMS
Das Service Monitoring MUSS die Probe VSDD_CMS entsprechend Tab_Service_Monitoring_Probes_VSDD_CMS bereitstellen.

Tabelle 17: Tab_Service_Monitoring_Probes_VSDD_CMS

Element	Beschreibung
Benennung der Probe	VSDD_CMS
Dienst	VSDD- und CMS-Fachdienste
Schnittstelle	I_CCS
Operation	PerformUpdates
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle VSDD- und CMS-Fachdienste.
Vorbedingung	Die Daten für alle VSDD- und CMS-Fachdienste – welche durch die Probe aufgerufen werden – müssen konfigurierbar sein. Für den Aufruf der Operationen PerformUpdates müssen folgende Werte in der Probe individuell für den jeweiligen Fachdienst konfigurierbar sein: • URL des Fachdienstes • ICCSN • ServiceType (VSD | CMS)

	• Provider ID • UpdateID Die UpdateID muss konfigurierbar und aus der vorangehenden Operation GetUpdateFlags übernehmbar sein. • Der kartenindividuelle symmetrische Schlüssel für die ICCSN muss optionaler konfigurierbar sein. • Update Flag verbrauchen (ja/nein) • Erwartete Fachdienstantwort/Fehlercode Die Probe muss sowohl korrekte Fachdienst-Antworten wie auch einen SOAP-Fehler mit Fehlercode (z.B. 12101) oder den Abbruch der Kommunikation beim Aufbau des sicheren Kanals vom Fachdienst zur eGK als erwartete Antwort akzeptieren. Die Probe muss über ein TLS-Client-Zertifikat (C.FD.TLS-C) für den Verbindungsaufbau zum Fachdienst verfügen.
Nachbedingung	Im Service Monitoring müssen für die gesamte Probe und für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Für jeden Fachdienst:
	1.1. Ermittlung der IP-Adresse des Fachdienstes durch eine DNS-Anfrage (DNS-SRV-Fachdienst) mit TUC_SM_001_DNS_Name_Resolution.
	1.2. Verbindungsaufbau zum Fachdienst unter Nutzung des TLS-Client-Zertifikats.
	1.3 Durchführung einer komplette Aktualisierung der eGK mit den SOAP-Requests PerformUpdates und GetNextCommandPackage gemäß [gemSpec_SST_FD_VSDM#4] unter Nutzung der Konfigurationsparameter. Abhängig von den Konfigurationsparametern kann der Fachdienst mit einem SOAP-Fehler antworten wenn z.B. keine „echte“ ICCSN genutzt wird oder kein Update vorliegt. Falls der kartenindividuelle symmetrische Schlüssel für die ICCSN nicht vorliegt, wird nach Senden des PerformUpdates an den Fachdienst 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.
	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. Zum Beispiel wird für eine nicht existierende ICCSN und UpdateId als Ergebnis ein gematik-SOAP-Fault mit Fehlercode 12101 (Für die angegebene Kombination aus ICCSN und Update-Identifier liegt kein Update vor) erwartet.

	1.5. Ermittlung der Service Monitoring-Daten für Operation PerformUpdates entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Ermittlung der Service Monitoring-Daten für die gesamte Probe und Rückgabe aller Datensätze an das Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Fachdienstes Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten Fachdienst fortgesetzt werden. Das „Probe-Ergebnis“ wird für diesen Fachdienst auf • 7100 Fachdienst nicht erreichbar oder • 7101 Ports vom Fachdienst geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.17 Intermediär VSDM*

TIP1-A_7316 - Service Monitoring, Probe Intermediär VSDM
Das Service Monitoring MUSS die Probe Intermediär VSDM entsprechend Tab_Service Monitoring_Probes_Intermediär_VSDM bereitstellen.

Tabelle 18: Tab_Service_Monitoring_Probes_ Intermediär_VSDM

Element	Beschreibung
Benennung der Probe	Intermediär VSDM
Dienst	Intermediär VSDM
Schnittstelle	I_TLS Intermediär
Operation	GetUpdateFlags via Intermediär
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für jeden Intermediär.
Vorbedingung	Für den Aufruf von Operation I_UFS::GetUpdateFlags via Intermediär müssen folgende Werte in der Probe für den jeden Intermediär individuell konfigurierbar sein. • URL des Intermediär • ServiceType (UFS) • Schnittstellen-Version UFS (2.0) • ICCSN • Provider ID

	Die Probe muss über eine SM-B-Prüfkarte (bzw. das AUT-Zertifikat dieser Karte entsprechend [gemSpec_SST_VSDM#2.4.1]) für den Verbindungsaufbau zum Intermediär verfügen. Die SM-B muss freigeschaltet sein. Weiterhin muss für die Probe mit einem Fachdienstbetreiber die Verwendung von einem Fachdienst UFS abgesprochen sein.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Für jeden Intermediär:
	1.1. Ermittlung der IP-Adresse des Intermediär VSDM durch eine DNS-Anfrage (DNS-SRV Intermediär) mit TUC_SM_001_DNS_Name_Resolution.
	1.2. Verbindungsaufbau zum Intermediär VSDM unter Nutzung des TLS-Client-Zertifikats (SM-B AUT Zertifikat).
	1.3. Senden des GetUpdateFlags Requests zum Intermediär VSDM unter Nutzung der Konfigurationsparameter [gemSpec_SST_FD_VSDM#3.1].
	1.4. Als Ergebnis wird ein Gematik SOAP Fault mit Fehlercode 11101 (Für die eGK mit der angegebenen ICCSN ist der aufgerufene Dienst nicht zuständig) erwartet.
	1.5. Ermittlung der Service Monitoring-Daten für Operation GetUpdateFlags entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Ermittlung der Service Monitoring-Daten für die gesamte Probe und Rückgabe aller Datensätze an das Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Intermediärs Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten Intermediär fortgesetzt werden. Das „Probe-Ergebnis“ wird für diesen Intermediär auf • 7100 Intermediär nicht erreichbar oder • 7101 Ports vom Intermediär geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.18 VSDM- Intermediär VSDM IPsecTunnel TI*

TIP1-A_7317 - Service Monitoring, Probe Intermediär VSDM IPsecTunnel TI
Das Service Monitoring MUSS die Probe Intermediär VSDM IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_Intermediär_VSDM bereitstellen. Die Probe Intermediär VSDM IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI/Intermediär VSDM einen IPsecTunnel zum VPN-ZugD nutzen. Folgende Abweichungen von Tab_Service_Monitoring_Probes_Intermediär_VSDM müssen beachtet werden:

- Benennung der Probe: Intermediär VSDM IPsecTunnel TI
- Netzwerk: IPsec Tunnel TI
- Vorbedingung:
  - Zusätzlich wird für den Aufbau des IPsec Tunnels das SMC-K Zertifikat C.NK.VPN benötigt.
  - Der der IPsec-Tunnel zur TI muss aufgebaut sein.

[<=]

5.4.19 VSDM-Intermediär VSDM Erreichbarkeit

TIP1-A_7318 - Service Monitoring, Probe Intermediär VSDM Erreichbarkeit
Das Service Monitoring MUSS die Probe Intermediär Erreichbarkeit entsprechend Tab_Service_Monitoring_Probes_Intermediär_VSDM bereitstellen. Mit dieser Probe wird die Erreichbarkeit des Intermediär VSDM geprüft. Mit einer fehlerhaften „Provider ID“ wird die Weiterleitung der UFS Anfrage an den Fachdienst verhindert.
Folgende Abweichungen von Tab_Service_Monitoring_Probes_Intermediär_VSDM MÜSSEN beachtet werden:

- Benennung der Probe: Intermediär VSDM Erreichbarkeit
- Vorbedingung:
  Es wird für „Provider ID“ eine nicht vorhandene Provider ID genutzt. Damit schlägt die Lokalisierung des Fachdienstes im Intermediär fehl. Der Intermediär liefert einen Fehlercode 502 [gemSpec_Intermediär_VSDM#3.5] an den Client.
  Ein Fachdienst UFS wird für diese Probe nicht benötigt.
- Standardablauf:
  Als Ergebnis wird vom Intermediär VSDM ein HTTP-Fehlercode 502 (Adresse des Fachdienstes nicht ermittelbar) erwartet.

[<=]

5.4.20 KSRS Upload

TIP1-A_7319 - Service Monitoring, Probe KSRS Upload
Das Service Monitoring MUSS die Probe KSRS Upload entsprechend Tab_Service_Monitoring_Probes_KSRS_Upload bereitstellen.

Tabelle 19: Tab_Service Monitoring_Probes_KSRS_Upload

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

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

[<=]

5.4.21 KSRS Download

TIP1-A_7320 - Service Monitoring, Probe KSRS Download
Das Service Monitoring MUSS die Probe KSRS Download entsprechend Tab_Service_Monitoring_Probes_KSRS_Download bereitstellen.

Tabelle 20: Tab_Service_Monitoring_Probes_KSRS_Download

Element	Beschreibung
Benennung der Probe	KSRS Download
Dienst	KSR
Schnittstelle	I_KSRS_Download
Operation	I_KSRS_Download::list_Updates I_KSRS_Download::get_Updates
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für den KSR.
Vorbedingung	Für die Operationen von Schnittstelle I_KSRS_Download müssen folgende Werte in der Probe konfigurierbar sein. • URL der KSRS-Download-Schnittstelle • ProductVendorID

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

[<=]

5.4.22 KSRS Download IPsecTunnel TI*

TIP1-A_7321 - Service Monitoring, Probe KSRS Download IPsecTunnel TI
Das Service Monitoring MUSS die Probe KSRS Download IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_KSRS_Download bereitstellen. Die Probe KSRS Download IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI/Intermediär einen IPsecTunnel nutzen.
Folgende Abweichungen von Tab_Service_Monitoring_Probes_KSRS_Download sind zu beachten:

- Benennung der Probe: KSRS Download IPsecTunnel TI
- Beschreibung:
  Diese Probe wird ausgeführt für jeden VPN-Zugangsdienst Standort.
- Vorbedingung:
  - Zusätzlich wird für den Aufbau des IPsec-Tunnels das SMC-K-Zertifikat C.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
Benennung der Probe	KSRS Download Bestandsnetze
Dienst	KSR
Schnittstelle	I_KSRS_Net_Config
Operation	I_KSRS_Net_Config::get_Ext_Net_Config
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für den KSR.

Vorbedingung	Für die Operationen von Schnittstelle I_KSRS_Net_Config müssen folgende Werte in der Probe konfigurierbar sein: • URL der KSRS-Download-Schnittstelle
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Ermittlung der IP-Adresse der KSRS-Download-Schnittstelle durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	2. TLS Verbindungsaufbau zum Konfigurationsdienst.
	3. Download des Files „Bestandsnetze.xml“ mit I_KSRS_Net_Config::get_Ext_Net_Config Updates gemäß [gemSpec_KSR] vom Konfigurationsdienst.
	4. Auswerten des Downloads gemäß I_KSRS_Net_Config::get_Ext_Net_Config und Ermittlung der Service Monitoring-Daten für diese Operation entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	5. Speicherung der ermittelten Daten für die KSRS-Download-Schnittstelle im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des KSR Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft werden. Das „Probe-Ergebnis“ wird auf • 7100 KSR nicht erreichbar oder • 7101 Ports vom KSR geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.24 KSRS Download Bestandsnetze IPsecTunnel TI*

TIP1-A_7323 - Service Monitoring, Probe KSRS Download Bestandsnetze IPsecTunnel TI
Das Service Monitoring MUSS die Probe KSRS Download Bestandsnetze IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_KSRS_Download_Bestandsnetze bereitstellen. Die Probe KSRS Download IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI/Intermediär einen IPsecTunnel nutzen. Folgende Abweichungen von Tab_Service_Monitoring_Probes_KSRS_Download_Bestandsnetze MÜSSEN beachtet werden:

- Benennung der Probe: KSRS Download Bestandsnetze IPsecTunnel TI
- Vorbedingung:
  - Zusätzlich wird für den Aufbau des IPsec-Tunnels das SMC-K-Zertifikat C.NK.VPN benötigt.

- Der der IPsec-Tunnel zur TI ist aufgebaut.

[<=]

5.4.25 Verzeichnisdienst Query

TIP1-A_7324 - Service Monitoring, Probe Verzeichnisdienst Query
Das Service Monitoring MUSS die Probe Verzeichnisdienst Query entsprechend Tab_Service_Monitoring_Probes_Verzeichnisdienst_Query bereitstellen.

Tabelle 22: Tab_Service_Monitoring_Probes_Verzeichnisdienst_Query

Element	Beschreibung
Benennung der Probe	Verzeichnisdienst Query
Dienst	Verzeichnisdienst
Schnittstelle	I_Directory_Query
Operation	I_Directory_Query::search_Directory
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für den Verzeichnisdienst.
Vorbedingung	Für die Operation I_Directory_Query::search_Directory müssen folgende Werte in der Probe konfigurierbar sein: • Suchkriterien für die LDAP Verzeichnisdienstabfrage
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Ermittlung FQDN und Port des Verzeichnisdienstes analog zu TIP1-A_5517 [gemSpec_Kon#4.1.12.4.1] entsprechend Tab_Service_Monitoring_Probes_DNS_Name_Resolution.
	2. LDAPS-Verbindungsaufbau zum Verzeichnisdienst (analog zu A_5517 [gemSpec_Kon#4.1.12.4.1]).
	3. Abfrage des Verzeichnisdienstes mit den konfigurierten Eingangsdaten analog zu TIP1-A_5518 [gemSpec_Kon#4.1.12.4.2].
	4. Auswerten der Verzeichnisdienst-Antwort und Ermittlung der Service Monitoring-Daten für diese Operation entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	5. Die Probe beendet die Verbindung zum Verzeichnisdienst (analog zu A_5519 [gemSpec_Kon#4.1.12.4.3]).
	6. Speicherung der ermittelten Daten für die Verzeichnisdienst I_Directory_Query Schnittstelle im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.

Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Verzeichnisdienstes Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft werden. Das „Probe-Ergebnis“ wird für diese Verzeichnisdienst Operation auf • 7100 Verzeichnisdienst nicht erreichbar oder • 7101 Ports vom Verzeichnisdienst geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.26 Verzeichnisdienst Query IPsecTunnel TI*

TIP1-A_7325 - Service Monitoring, Probe Verzeichnisdienst Query IPsecTunnel TI
Das Service Monitoring MUSS die Probe Verzeichnisdienst Query IPsecTunnel TI entsprechend Tab_Service_Monitoring_Probes_Verzeichnisdienst_Query bereitstellen. Die Probe Verzeichnisdienst Query IPsecTunnel TI MUSS sich wie ein Konnektor verhalten und für die Verbindung zur TI/-Verzeichnisdienst einen IPsecTunnel nutzen. Folgende Abweichungen von Tab_Service_Monitoring_Probes_Verzeichnisdienst_Query MÜSSEN beachtet werden:

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

[<=]

5.4.27 Verzeichnisdienst Application_Maintenance

TIP1-A_7326 - Service Monitoring, Probe Verzeichnisdienst Application Maintenance
Das Service Monitoring MUSS die Probe Verzeichnisdienst Application Maintenance entsprechend Tab_Service_Monitoring_Probes_Verzeichnisdienst_Application_Maintenance bereitstellen.

Tabelle 23: Tab_Service_Monitoring_Probes_Verzeichnisdienst_Application_Maintenance

Element	Beschreibung
Benennung der Probe	Verzeichnisdienst Application Maintenance
Dienst	Verzeichnisdienst

Schnittstelle	I_Directory_Application_Maintenance
Operation	I_Directory_Application_Maintenance::add_Directory_FA-Attributes
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für den Verzeichnisdienst. Es wird die Webservice (SOAP) Ausprägung der Operationen genutzt.
Vorbedingung	Die Probe muss beim Verzeichnisdienst für die Nutzung der Schnittstelle registriert sein (TIP1-A_5604 [gemSpec_VZD]). Für den Aufbau einer TLS Verbindung muss die Probe über ein C.FD.TLS-C Zertifikat verfügen (TIP1-A_5585 [gemSpec_VZD]). Für diese Probe muss im Verzeichnisdienst ein Basisdatensatz verfügbar sein, dem ein Fachdatensatz hinzugefügt (bzw. ein existierender Fachdatensatz überschrieben) wird. Der Basisdatensatz muss mit dem Verzeichnisdienst-Betreiber abgestimmt sein. Für diese Probe müssen folgende Werte konfigurierbar sein: • Telematik-ID • fachdienstspezifische Attribute, welche mit dem SOAP-Request dem Verzeichniseintrag hinzugefügt (bzw. überschrieben) werden
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Ermittlung FQDN und Port der Schnittstelle I_Directory_Application_Maintenance vom Verzeichnisdienst entsprechend Tab_Service_Monitoring_Probes_DNS_Name_Resolution.
	2. Ermittlung der IP-Adresse des Verzeichnisdienstes durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	3. TLS-Verbindungsaufbau zum Verzeichnisdienst. Die Probe muss sich mit dem Client Zertifikat C.FD.TLS-C authentisieren (TIP1-A_5585 [gemSpec_VZD]).
	4. Senden des add_Directory_FA-Attributes Requests an den Verzeichnisdienst mit den konfigurierten Eingangsdaten.
	5. Auswerten der Verzeichnisdienst Antwort und Ermittlung der Service Monitoring-Daten für diese Operation entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	6. Die Probe beendet die TLS-Verbindung zum Verzeichnisdienst.
	7. Speicherung der ermittelten Daten für die Verzeichnisdienst Schnittstelle _Directory_Application_Maintenance im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Verzeichnisdienstes Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft werden. Das „Probe-Ergebnis“ wird für diese Verzeichnisdienst Operation auf

	• 7100 Verzeichnisdienst nicht erreichbar oder • 7101 Ports vom Verzeichnisdienst geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.28 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
Benennung der Probe	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	Für diese Probe müssen folgende Werte konfigurierbar sein:
	• Ausführungszeitpunkt und Frequenz der Probe
	• Wieviel Tage vor Zertifikatsablauf soll eine Warnung versendet werden?
	• Wieviel Tage vor Zertifikatsablauf soll ein Alarm versendet werden?
	• Die zentralen Dienste, deren Server-Zertifikate überwacht werden. Für jeden Server müssen mindestens folgende Werte konfiguriert werden:
	  • Name des Servers
	  • Adresse des Servers bzw. der Schnittstelle
	  • Port des Servers
	  • Optional: Client Zertifikat

Nachbedingung	In den Service-Monitoring-Daten werden die Gültigkeitsdauern der Server-Zertifikate aktualisiert. Für jeden geprüften Server müssen mindestens folgende Daten erfasst werden: • Name des Servers • Adresse des Dienstes bzw. der Schnittstelle • Gültigkeitsende des Zertifikats • Subject, IssuerDN und SerialNumber des Zertifikats 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. Die ermittelten Daten entsprechend Tab_Service_Monitoring_Probe_Daten sind für die Probe im Service Monitoring gespeichert.
Standardablauf	1. Ermittlung der IP-Adresse des Servers durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	2. Für jeden konfigurierten Server: • TLS-Verbindungsaufbau zum Server und Übergabe des Server Zertifikats an den nächsten Schritt des Standardablaufs. • Falls der Server ein Client-Zertifikat anfordert, wird das konfigurierte Zertifikat verwendet. Falls kein konfiguriertes Client-Zertifikat vorhanden ist, wird der Verbindungsaufbau abgebrochen. • Beenden der TLS-Verbindung.
	3. Analyse Server-Zertifikat • Prüfung des Ablaufdatums des Server-Zertifikats • Auslösen einer Warnung oder eines Alarms über die Service-Monitoring-Alarmierung falls das Zertifikat in x Tagen (entsprechend Konfigurationsdaten) ausläuft. • Ablage der ermittelten Daten (siehe Nachbedingungen)
	4. Speicherung der ermittelten Daten für die Probe im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.

Ursachen-Analyse im Fehlerfall	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 • 7100 Dienst nicht erreichbar oder • 7101 Ports vom Dienst geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

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

[<=]

5.4.30 ePA - Authentisierung TI

A_15662 - Service Monitoring, Probe ePA-Authentisierung TI
Das Service Monitoring MUSS die Probe ePA-Authentisierung TI entsprechend Tab_Service_Monitoring_Probes_ePA- Authentisierung_TI bereitstellen.

Tabelle 25: Tab_Service_Monitoring_Probes_ePA- Authentisierung_TI

Element	Beschreibung
Benennung der Probe	ePA-Authentisierung TI
Dienst	ePA
Schnittstelle	I_Authentication_Insurant
Operation	I_Authentication_Insurant::LoginCreateChallenge
Netzwerk	zentrales Netz der TI

Beschreibung	Diese Probe wird ausgeführt für jede ePA-Instanz.
Vorbedingung	ePA DNS Service Records sind konfiguriert.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Ermittlung I_Authentication_Insurant FQDN aller ePA-Aktensysteme Das Probe muss die zur Kommunikation mit der Komponente Zugangsgateway für Versicherte aller ePA-Aktensysteme notwendigen Lokalisierungsinformationen per DNS-Abfrage nach den in [gemSpec_Aktensystem#Tab_ePA_Service Discovery] und [gemSpec_Aktensystem#Tab_ePA_FQDN] dargestellten Parametern ermitteln.
	2. Ermittlung der IP-Adresse aller Zugangsgateways durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	3. TLS-Verbindungsaufbau mit Serverauthentisierung zu jedem Zugangsgateway.
	4. Senden des RequestSecurityToken an jeden Zugangsgateway.
	5. Auswerten der RequestSecurityTokenResponse 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 Zugangsgateway.
	7. Speicherung der ermittelten Daten für die Schnittstelle I_Authentication_Insurant im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Zugangsgateways 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 ePA-Aktensystem-Operation auf • 7100 Dienst ist nicht erreichbar oder • 7101 Ein oder mehrere Port(s) vom Dienst sind geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt werden.

[<=]

5.4.31 ePA - Authentisierung Internet

A_15694 - Service Monitoring, Probe ePA-Authentisierung Internet
Das Service Monitoring MUSS die Probe ePA-Authentisierung Internet entsprechend Tab_Service_Monitoring_Probes_ePA- Authentisierung bereitstellen. Die Probe ePA-Authentisierung Internet MUSS sich wie ein ePA-Frontend des Versicherten verhalten. Folgende Abweichungen von Tab_Service_Monitoring_Probes_Verzeichnisdienst_Query MÜSSEN beachtet werden:

- Benennung der Probe: ePA-Authentisierung Internet
- Netzwerk: Internet

[<=]

5.4.32 ePA - Autorisierung

A_15669 - Service Monitoring, Probe ePA-Autorisierung
Das Service Monitoring MUSS die Probe ePA-Autorisierung entsprechend Tab_Service_Monitoring_Probes_ePA-Autorisierung bereitstellen.

Tabelle 26: Tab_Service_Monitoring_Probes_ePA-Autorisierung

Element	Beschreibung
Benennung der Probe	ePA-Autorisierung
Dienst	ePA
Schnittstelle	I_Authorization
Operation	I_Authorization::getAuthorizationKey
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für jede ePA-Instanz.

Vorbedingung	ePA DNS Service Records sind konfiguriert.
	
	Für diese Probe müssen folgende Werte für Operation getAuthorizationKey pro ePA-Anbieter (identifiziert durch homeCommunityID) konfigurierbar sein:
	• Parameter für den Request
	  • RecordIdentifier
	  • AuthenticationAssertion
	  • ActorID
	  • DeviceID

	• erwartete Antwort/Fehlermeldung (GetAuthorizationKeyResponse)
	  • positive Antwort mit AuthorizationAssertion und AuthorizationKey
	  • Fehlercode ASSERTION_INVALID
	  • Fehlercode KEY_ERROR
	  • Fehlercode SYNTAX_ERROR
	  • Fehlercode INTERNAL_ERROR

Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jede ePA-Instanz verfügbar sein.
Standardablauf	1. Ermittlung aller ePA-Autorisierungs-Dienste Das Probe muss die zur Kommunikation mit der Komponente Autorisierungs-Dienste aller ePA-Aktensysteme notwendigen Lokalisierungsinformationen per DNS-Abfrage nach den in [gemSpec_Aktensystem#Tab_ePA_Service Discovery] und [gemSpec_Aktensystem#Tab_ePA_FQDN] dargestellten Parametern ermitteln.
	2. Ermittlung der IP-Adresse aller Autorisierungs-Dienste durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	3. TLS-Verbindungsaufbau mit Serverauthentisierung zu jedem Autorisierungs-Dienst.
	4. Senden des getAuthorizationKey (mit den Konfigurationsparametern für diese homeCommunityID) an jeden Autorisierungs-Dienst. Falls für einen ePA-Anbieter keine Konfigurationsdaten vorhanden sind, wird das „Probe-Ergebnis“ für diesen ePA-Anbieter auf • 7111 Keine Konfigurationsparameter für diesen Dienst hinterlegt gesetzt.
	5. Auswerten der GetAuthorizationKeyResponse 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 Autorisierungs-Dienst.
	7. Speicherung der ermittelten Daten für die Schnittstelle I_Authorization im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.

Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des-ePA Autorisierungs-Dienstes 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 ePA-Aktensystem-Operation auf • 7100 Dienst ist nicht erreichbar oder • 7101 Ein oder mehrere Port(s) vom Dienst sind geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt werden.

[<=]

5.4.33 ePA - I_Authorization_Management::checkRecordExists

A_16186 - Service Monitoring, Probe ePA - I_Authorization_Management::checkRecordExists
Das Service Monitoring MUSS die Probe ePA - I_Authorization_Management::checkRecordExists entsprechend Tab_Service_Monitoring_Probes_ePA-I_Authorization_Management::checkRecordExists bereitstellen.

Tabelle 27: Tab_Service_Monitoring_Probes_ePA-I_Authorization_Management::checkRecordExists

Element	Beschreibung
Benennung der Probe	ePA - I_Authorization_Management::checkRecordExists
Dienst	ePA
Schnittstelle	I_Authorization_Management
Operation	I_Authorization_Management::checkRecordExists
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für jede ePA-Instanz.
Vorbedingung	ePA DNS Service Records sind konfiguriert. Für diese Probe müssen folgende Werte für Operation checkRecordExists pro ePA-Anbieter (identifiziert durch homeCommunityID) konfigurierbar sein: • Parameter für den Request

	• KVNR
	  • Defaultwert "Z999999999" (ungültige KVNR)
	  • Die KVNR kann optional nach Abstimmung mit dem Betreiber der ePA-Instanz auf einen anderen ungültigen KVNR-Wert gesetzt werden.
	• erwartete Antwort/Fehlermeldung (Parameter "RecordState")
	  • Jede einzelne positive Antwort entsprechend Schema von Operation checkRecordExistsResponse (UNKNOWN, REGISTERED, ...)
	  • Fehlercode SYNTAX_ERROR
	  • Fehlercode INTERNAL_ERROR

Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jede ePA-Instanz verfügbar sein.
Standardablauf	1. Ermittlung aller ePA-Autorisierungs-Dienste Das Probe muss die zur Kommunikation mit der Komponente Autorisierungs-Dienste aller ePA-Aktensysteme notwendigen Lokalisierungsinformationen per DNS-Abfrage nach den in [gemSpec_Aktensystem#Tab_ePA_Service Discovery] und [gemSpec_Aktensystem#Tab_ePA_FQDN] dargestellten Parametern ermitteln.
	2. Ermittlung der IP-Adresse aller Autorisierungs-Dienste durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	3. TLS-Verbindungsaufbau mit Serverauthentisierung zu jedem Autorisierungs-Dienst.
	4. Senden des checkRecordExists (mit den Konfigurationsparametern für diese homeCommunityID) an jeden Autorisierungs-Dienst. Falls für einen ePA-Anbieter keine Konfigurationsdaten vorhanden sind, wird das „Probe-Ergebnis“ für diesen ePA-Anbieter auf • 7111 Keine Konfigurationsparameter für diesen Dienst hinterlegt gesetzt.
	5. Auswerten der checkRecordExistsResponse 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 Autorisierungs-Dienst.
	7. Speicherung der ermittelten Daten für die Schnittstelle I_Authorization im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.

Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des ePA-Autorisierungs-Dienstes 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 ePA-Aktensystem-Operation auf • 7100 Dienst ist nicht erreichbar oder • 7101 Ein oder mehrere Port(s) vom Dienst sind geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt werden.

[<=]

5.4.34 ePA - Dokumentenverwaltung

A_15672 - Service Monitoring, Probe ePA-Dokumentenverwaltung
Das Service Monitoring MUSS die Probe ePA-Dokumentenverwaltung ePA-Autorisierung entsprechend Tab_Service_Monitoring_Probes_ePA-Dokumentenverwaltung Autorisierung bereitstellen.

Tabelle 28: Tab_Service_Monitoring_Probes_ePA_Dokumentenverwaltung

Element	Beschreibung
Benennung der Probe	ePA-Dokumentenverwaltung
Dienst	ePA
Schnittstelle	I_Account_Management
Operation	I_Account_Management - Aufbau eines sicheren Kanals auf Anwendungsebene
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für jede ePA-Instanz.
Vorbedingung	ePA DNS Service Records sind konfiguriert. Für diese Probe müssen folgende Werte für den Aufbau eines sicheren Kanals auf Anwendungsebene pro ePA-Anbieter (identifiziert durch homeCommunityID) konfigurierbar sein: • Parameter für den Request • AuthorizationAssertion

	• erwartete Antwort/Fehlermeldung
	  • HTTP-Fehler 403 bei ungültiger Authorization Assertion
	  • positive Antwort

Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Ermittlung aller ePA-Dokumentenverwaltungs-Dienste Das Probe muss die zur Kommunikation mit der Komponente Dokumentenverwaltung-Dienste aller ePA-Aktensysteme notwendigen Lokalisierungsinformationen per DNS-Abfrage nach den in [gemSpec_Aktensystem#Tab_ePA_Service Discovery] und [gemSpec_Aktensystem#Tab_ePA_FQDN] dargestellten Parametern ermitteln.
	2. Ermittlung der IP-Adresse aller Dokumentenverwaltungs-Dienste durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	3. TLS-Verbindungsaufbau mit Serverauthentisierung zu jedem Dokumentenverwaltungs-Dienst.
	4. Aufbau eines sicheren Kanals auf Anwendungsebene (mit den Konfigurationsparametern für diese homeCommunityID) zu jedem Dokumentenverwaltungs-Dienst analog zu Anforderungen A_15199 und A_15200. Falls für einen ePA-Anbieter keine Konfigurationsdaten vorhanden sind, wird das „Probe-Ergebnis“ für diesen ePA-Anbieter auf • 7111 Keine Konfigurationsparameter für diesen Dienst hinterlegt gesetzt.
	5. Auswerten der Antwort auf den Verbindungsaufbau und Ermittlung der Service-Monitoring-Daten für diese Operation entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“. Falls der sichere Kanal erfolgreich aufgebaut wurde, wird er wieder abgebaut.
	6. Die Probe beendet die TLS-Verbindung zum ePA-Dokumentenverwaltungs-Dienst.
	7. Speicherung der ermittelten Daten für die Schnittstelle I_Account_Management im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.

Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des ePA-Dokumentenverwaltungs-Dienstes 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 ePA-Aktensystem-Operation auf • 7100 Dienst ist nicht erreichbar oder • 7101 Ein oder mehrere Port(s) vom Dienst sind geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.35 ePA – Verfügbarkeitsmonitoring

A_18381 - Service Monitoring, Probe ePA-Verfügbarkeitsmonitoring
Das Service Monitoring MUSS die Probe ePA-Verfügbarkeitsmonitoring entsprechend Tab_Service_Monitoring_Probes_ePA-Verfügbarkeitsmonitoring bereitstellen.

Tabelle 29: Tab_Service_Monitoring_Probes_ePA-Verfügbarkeitsmonitoring

Element	Beschreibung
Benennung der Probe	ePA-Verfügbarkeitsmonitoring
Dienst	ePA
Netzwerk	Internet
Beschreibung	Diese Probe wird ausgeführt für jede ePA-Instanz.
Vorbedingung	Kartenterminal mit eGK-Prüfkarten. eGK MRPIN.home muss nötigen Sicherheitszustand haben. ePA DNS Service Records sind konfiguriert. Für jedes ePA-Aktensystem ist ein RecordIdentifier konfiguriert. In jedem ePA-Aktensystem ist ein abrufbares Dokument eingestellt.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Ermittlung I_Authentication_Insurant FQDN aller ePA-Aktensysteme Das Probe muss die zur Kommunikation mit der Komponente Zugangsgateway für Versicherte aller ePA-Aktensysteme notwendigen Lokalisierungsinformationen per DNS-Abfrage nach den in [gemSpec_Aktensystem#Tab_ePA_Service Discovery] und [gemSpec_Aktensystem#Tab_ePA_FQDN] dargestellten Parametern ermitteln.

	2. Das Login erfolgt entsprechend Anwendungsfall "UC 1.1 - Login durch einen Versicherten" aus [gemSysL_ePA]. Aktivitäten im Ablauf 1. Session-Daten für RecordIdentifier prüfen (falls bereits eine gültige Session besteht, dann werden die weiteren Login-Aktivitäten übersprungen) 2. Authentisieren mittels eGK-Prüfkarte 3. Authentisieren des Nutzers 4. Autorisieren des Nutzers 5. Status des Aktenkontos prüfen 6. Aktenkontext öffnen Die Authentisierung erfolgt mittels Prüfkarte im Kartenterminal. Falls die MRPIN.home nicht den nötigen Sicherheitszustand hat, wird die Probe mit Fehler 7111 beendet. Wenn nach der Aktivität "Autorisieren des Nutzers" ein Autorisierungstoken mit RecordState = REGISTERED oder REGISTERED_FOR_MIGRATION vorliegt, dann wird die Probe mit Fehler 7107 abgebrochen und der Anwendungsfall "Logout Aktensession" gestartet.
	3. Das Suchen des konfigurierten Dokuments aus dem Aktenkonto erfolgt entsprechend Anwendungsfall "UC 4.10 - Dokumente durch einen Versicherten anzeigen" aus [gemSysL_ePA]. 4. Das Herunterladen des konfigurierten Dokuments aus dem Aktenkonto erfolgt entsprechend Anwendungsfall "UC 4.10 - Dokumente durch einen Versicherten anzeigen" aus [gemSysL_ePA].
	5. Das Logout aus der Aktensession erfolgt entsprechend Anwendungsfall "UC 1.3 - Logout durch einen Nutzer" aus [gemSysL_ePA]. Aktivitäten im Ablauf 1. Aktenkontext schließen 2. Authentisierungstoken abmelden 3. Session-Daten löschen
	6. Auswerten der RequestSecurityTokenResponse und Ermittlung der Service-Monitoring-Daten für diese Operation entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	7. Speicherung der ermittelten Daten für jede ePA-Instanz und Schnittstelle im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.

Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des Zugangsgateways 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“ muss für diese ePA-Aktensystem-Operation auf • 7100 Dienst ist nicht erreichbar oder • 7101 Ein oder mehrere Port(s) vom Dienst sind geschlossen oder • 7103 Aufruf mit Fehler beendet • 7107 In der Probe ist ein Fehler aufgetreten • 7111 eGK MRPIN.home hat nicht den nötigen Sicherheitszustand gesetzt werden.

[<=]

5.4.36 ePA -Schlüsselgenerierungsdienst

A_17849 - Service Monitoring, Probe ePA-Schlüsselgenerierungsdienst
Das Service Monitoring MUSS die Probe ePA-Schlüsselgenerierungsdienst entsprechend Tab_Service_Monitoring_Probes_ePA-Schlüsselgenerierungsdienst bereitstellen.

Tabelle 30: Tab_Service_Monitoring_Probes_ePA_Schlüsselgenerierungsdienst

Element	Beschreibung
Benennung der Probe	ePA-Schlüsselgenerierungsdienst
Dienst	ePA-Schlüsselgenerierungsdienst
Schnittstelle	I_GetPublicKey I_KeyDerivation I_GetEventLog
Operation	GetPublicKey - Lesen des öffentlichen ECDH-Schlüssels KeyDerivation - Schlüsselableitung GetEventLog - Auslesen des Ereignisprotokolls des Versicherten
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für jede Instanz des ePA-Schlüsselgenerierungsdienstes.
Vorbedingung	ePA DNS Service Records sind konfiguriert. Für diese Probe müssen folgende Werte für den Aufbau eines sicheren Kanals auf Anwendungsebene pro ePA-Schlüsselgenerierungsdienst konfigurierbar sein:

	• Request-Body für den POST-Request { "Command" : "GetPublicKey", "Certificate" : "", "OCSPResponse" : "" } oder { "Command" : "KeyDerivation", "PublicKeyECDH" : "", "Signature" : "", "Certificate" : "", "OCSPResponse" : "", "Message" : "" } oder { "Command" : "GetEventLog", "PublicKeyECDH" : "", "Signature" : "", "Certificate" : "", "OCSPResponse" : "", "Message" : "" } • erwartete Antwort/Fehlermeldungen { "Status" : "certificate not valid" } oder { "Status" : "request not valid" }
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten verfügbar sein.
Standardablauf	1. Ermittlung aller ePA-Schlüsselgenerierungsdienste Die Probe muss alle die zur Kommunikation mit der Komponente Schlüsselgenerierungsdienst notwendigen Lokalisierungsinformationen per DNS-Abfrage nach den in [gemSpec_Aktensystem#Tab_ePA_Service Discovery] und [gemSpec_Aktensystem#Tab_ePA_FQDN] dargestellten Parametern ermitteln.
	2. Ermittlung der IP-Adresse allerSchlüsselgenerierungsdienste durch eine DNS-Anfrage mit TUC_SM_001_DNS_Name_Resolution.
	3. TLS-Verbindungsaufbau mit Serverauthentisierung zu jedem Schlüsselgenerierungsdienst.
	4. Senden des GetPublicKey Es wird ein HTTP POST mit dem konfigurierten Body für Operation GetPublicKey gesendet.

	5. Auswerten der Antwort auf den Request 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 ePA Schlüsselgenerierungsdienst.
	7. Speicherung der ermittelten Daten für die Schnittstelle I_GetPublicKey im Service Monitoring entsprechend Tab_Service_Monitoring_Probe_Daten.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf bei den Aufrufen des ePA - Schlüsselgenerierungsdienst 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 ePA Schlüsselgenerierungsdienst Operation auf • 7100 Dienst ist nicht erreichbar oder • 7101 Ein oder mehrere Port(s) vom Dienst sind geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.37 aAdG-NetG

~~Die Verbindungen in aAdG-NetG Netze müssen durch regelmäßige Abfragen eines Nameservers im jeweiligen aAdG-NetG Netz geprüft werden.~~

Die TI agiert für die aAdG-NetG-Kommunikation als Transportnetz. Die Überwachung dieser Transportnetz-Funktionalität ist Aufgabe der Probe "aAdG-NetG Erreichbarkeit".

Für diese Prüfung wird die Probe ~~DNS_Name_Resolution (TIP1-A_7149)~~ "aAdG-NetG Erreichbarkeit" für das aAdG-NetG-Netz konfiguriert und periodisch ausgeführt. Für jedes aAdG-NetG-Netz wird ein – vom jeweiligen Netzanbieter genannter – Endpunkt (IP-Adresse oder URL) in der Probe konfiguriert.

Zudem soll bei der Etablierung neuer Kommunikationsziele im aAdG-NetG-Netz die Verbindung im Rahmen der Einrichtung überprüft werden können.

A_18400 - Service Monitoring, Probe aAdG-NetG Erreichbarkeit
Das Service Monitoring MUSS die Probe aAdG-NetG Erreichbarkeit entsprechend Tab_Service_Monitoring_Probes_aAdG-NetG_Erreichbarkeit bereitstellen.

Tabelle 31: Tab_Service_Monitoring_Probes_aAdG-NetG_Erreichbarkeit

Element	Beschreibung
Benennung der Probe	aAdG-NetG Erreichbarkeit
Dienst	aAdG-NetG
Schnittstelle	I_IP_Transport
Operation	ICMP Request HTTPS GET
Netzwerk	zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für alle aAdG-NetG-Netze.
Vorbedingung	IP-Adressen bzw. URLs aus dem aAdG-NetG müssen für die Probe konfiguriert sein.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jedes aAdG-NetG verfügbar sein.
Standardablauf	1. Die Probe führt für jedes konfigurierte aAdG-NetG die folgenden Schritte durch:
	1.1. Für alle konfigurierten URLs: • TUC_SM_001_DNS_Name_ResolutionResolution ohne DNS-Record Validierung (DNSSEC) für die URL. • Aufruf der URL und Auswertung der Response (Laufzeit und Erhalt werden erfasst)
	1.2 Für alle konfigurierten IP-Adressen: ICMP Request auf die IP-Adresse und Auswertung der Response (Laufzeit und Erhalt werden erfasst)
	1.3. Ermittlung der Service-Monitoring-Daten für alle konfigurierten IP-Adressen und URLs entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.

Ursachen-Analyse im Fehlerfall	Falls im Standardablauf (Punkt 1 inklusive Unterpunkte) 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 konfigurierten IP-Adresse oder URL fortgesetzt werden. Das „Probe-Ergebnis“ wird auf • 7100 Dienst ist nicht erreichbar oder • 7102 Zu einem DNS-Namen konnte keine IP-Adresse gefunden werden oder • 7103 Aufruf mit Fehler beendet gesetzt.

[<=]

5.4.38 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.
[<=]

Tabelle 32: Tab_Service_Monitoring_Probe_Daten

Monitoring Daten	Datensatz	Einheit	Erläuterung
ProbeID	P & O		Identifikation der Probe Wird bei Erstellung der Probe vergeben und muss eindeutig sein. Probe-Datensatz: Dient der Identifikation der Probe Operation-Datensatz: Zeigt, durch welche Probe die Daten ermittelt wurden. Falls nicht vorhanden, wurden die Daten nicht durch eine Probe ermittelt.
ProbeBeschreibung			Beschreibung der Probe Wird bei Erstellung der Probe erstellt. Ist im GUI anzeigbar.
Betriebsumgebung	P & O		RU/TU/PU Die Umgebung muss nicht in jedem Datensatz enthalten sein. Die Datensätze müssen aber der

			Umgebung zuordenbar sein.
TeilnehmerID	O		ID des Teilnehmers wie in TI-ITSM für den diese Operation aufgerufen wurde
Dienstinstanz	O		Operation-Datensatz: Instanz des Dienstes für den die Operation ausgeführt wird.
ProductType	O		ID zu Eintrag aus Tab_gemSpec_Perf_Produkttypen
Schnittstelle	O		ID zu Eintrag aus Tab_gemSpec_Perf_Schnittstellenoperationen
Zertifikatstyp	O		ID zu Eintrag aus Tab_gemSpec_Perf_Zertifikatstypen
AnfrageQuelle	O		Angabe, ob die Schnittstelle, zu der reportet wird, in der TI oder im Internet bereitgestellt wird. Werte aus Tab_gemSpec_Perf_Aufrufquelle
Zeitstempel	P & O	ms	Probe-Datensatz: Zeitpunkt der Probe-Ausführung Operation-Datensatz: Zeigt zusammen mit der ProbeID durch welche Probe-Ausführung die Daten ermittelt wurden
Bearbeitungszeit	P & O	ms	Probe Datensatz: Ausführungsdauer der Probe Operation-Datensatz: Ausführungsdauer der Operation. Wird als Performance-Kenngröße erfasst.
Ergebnis	P & O		Probe-Datensatz: Ergebnis der Probe-Ausführung Operation Datensatz: Ergebnis der Operation Das Ergebnis kann auch „Erfolgreich“ sein, wenn das erwartete Ergebnis einer Einzeloperation ein Fehler war.
Mitschnitt der Kommunikation	P		Aufzeichnung der gesamten Kommunikation der Probe mit den Diensten für 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 28

6.4 Tabellenverzeichnis

Tabelle 1: Tab_Service_Monitoring_Akteure_und_Rollen 18
Tabelle 2: Tab_Service_Monitoring_I_Monitoring_Update 24
Tabelle 3: Tab_Service_Monitoring_Attribute 27
Tabelle 4: Tab_Service_Monitoring_SOAP-Request, Beschreibung der Elemente 28
Tabelle 5: Tab_Service_Monitoring_SOAP-Response, Beschreibung der Elemente 30
Tabelle 6: Tab_Service_Monitoring_TUC_SM_001_DNS_Name_Resolution 31
Tabelle 7: Tab_Service_Monitoring_TUC_SM_002_Erreichbarkeitsprüfung 32
Tabelle 8: Tab_Service_Monitoring_Probes_DNS_Name_Resolution 37
Tabelle 9: Tab_Service_Monitoring_Probes_Konnektorregistrierung 38
Tabelle 10: Tab_Service_Monitoring_Probes_VPN_Tunnel 40
Tabelle 11: Tab_Service_Monitoring_Probes_Zeitinformation_TI 43
Tabelle 12: Tab_Service_Monitoring_Probes_CRL_Download 45
Tabelle 13: Tab_Service_Monitoring_Probes_TSL_Download 46
Tabelle 14: Tab_Service_Monitoring_Probes_BNetzA_Download 48
Tabelle 15: Tab_Service_Monitoring_Probes_OCSP 50
Tabelle 16: Tab_Service Monitoring_Probes_UFS 52
Tabelle 17: Tab_Service_Monitoring_Probes_VSDD_CMS 53
Tabelle 18: Tab_Service_Monitoring_Probes_ Intermediär_VSDM 55
Tabelle 19: Tab_Service Monitoring_Probes_KSRS_Upload 57
Tabelle 20: Tab_Service_Monitoring_Probes_KSRS_Download 58
Tabelle 21: Tab_Service_Monitoring_Probes_KSRS_Download_Bestandsnetze 60
Tabelle 22: Tab_Service_Monitoring_Probes_Verzeichnisdienst_Query 62
Tabelle 23: Tab_Service_Monitoring_Probes_Verzeichnisdienst_Application_Maintenance 63
Tabelle 24: Tab_Service_Monitoring_Probes_Ablauf_von_Server_Zertifikaten 65
Tabelle 25: Tab_Service_Monitoring_Probes_ePA- Authentisierung_TI 67
Tabelle 26: Tab_Service_Monitoring_Probes_ePA-Autorisierung 69

Tabelle 27: Tab_Service_Monitoring_Probes_ePA-I_Authorization_Management::checkRecordExists 71
Tabelle 28: Tab_Service_Monitoring_Probes_ePA_Dokumentenverwaltung 73
Tabelle 29: Tab_Service_Monitoring_Probes_ePA-Verfügbarkeitsmonitoring 75
Tabelle 30: Tab_Service_Monitoring_Probes_ePA_Schlüsselgenerierungsdienst 77
Tabelle 31: Tab_Service_Monitoring_Probes_aAdG-NetG_Erreichbarkeit 80
Tabelle 32: Tab_Service_Monitoring_Probe_Daten 81
Tabelle 33: Tab_Service_Monitoring_Fehlercodes 88

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 jeweils gültige Versionsnummern sind in der aktuellen, 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 http://tools.ietf.org/html/rfc2119
[RFC7159]	The JavaScript Object Notation (JSON) Data Interchange Format
[RFC7231]	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content

6.6 Fehlercodes

Tabelle 33: 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
7111	Technical	Fatal	eGK MRPIN.home hat nicht den nötigen Sicherheitszustand

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