
C_12805_Anlage

Inhaltsverzeichnis

1	Änderungsbeschreibung.....	2
2	Bereinigung in gemSpec_Net.....	3
2.1	Änderung in Kapitel 2.5.4 Priorisierung des markierten Datenverkehrs....	3
2.2	Änderung in Kapitel 2.6.2 Anforderungen an Sicherheitskomponenten....	3
2.3	Änderung in Kapitel 2.6.5 Erlaubter Verkehr.....	3
2.4	Änderung in Kapitel 3.2 Übergreifende Festlegungen.....	3
2.5	Änderung in Kapitel 5.7 Anforderungen an den Produkttyp Namensdienst	4
2.6	Änderung in Kapitel 6.3 Anforderungen an den Produkttyp Zeitdienst.....	5
2.7	Änderung in Kapitel 8.5.1 Dokumente der gematik.....	6
3	Bereinigung in gemSpec_VPN_ZugD.....	7
3.1	Änderungen in Kapitel 5 Funktionsmerkmale.....	7
4	Bereinigung in gemSpec_KSR.....	9
4.1	Änderung in Kapitel 4.4. Schnittstellen.....	9
4.2	Änderung in Kapitel 5.6.1 TLS Transport Layer Security (TLS).....	9
4.3	Änderungen in Kapitel 6.1.1.5 KSR Download Cache.....	10
4.4	Änderung in Kapitel 6.2 organisatorische Schnittstellen.....	10
4.5	Änderungen in Kapitel 7.5.1 Dokumente der gematik.....	10

1 Änderungsbeschreibung

Mit diesem Änderungseintrag wird die Entfernung der Störungsampel in den folgenden Spezifikationen :

- gemSpec_KSR
- gemSpec_NET
- gemSpec_VPN_ZugD

vorgenommen. Bei Bedarf werden auch normativen Festlegungen auf den Dienst Betriebsdatenerfassung umgeschrieben. Zudem werden die Referenz auf das Dokument gemKPT-Arch-TIP entfernt, da dieses Dokument seit Jahren nicht mehr gepflegt wird.

2 Bereinigung in gemSpec_Net

2.1 Änderung in Kapitel 2.5.4 Priorisierung des markierten Datenverkehrs

In der Tabelle Tab_QoS_Mapping_Dienstklasse_Anwendung wird die folgende Zeile wie folgt geändert:

Anwendung/Dienstc	Dienstklasse TI
Störungssammel (SNMP; SOAP) Dienst Betriebsdatenerfassung	Interactive ZD

2.2 Änderung in Kapitel 2.6.2 Anforderungen an Sicherheitskomponenten

Der informative Text wird wie folgt angepasst:

Implementieren Produkttypen Übergänge zu Fremdnetzen mit niedrigerem oder unbekanntem Sicherheitsniveau ~~(z.B. bei den Produkttypen OCSP-Responder-Proxy und Störungssammel)~~, insbesondere zum Internet, müssen besondere Vorkehrungen getroffen werden, die sich an die Anforderungen des BSI für Netzübergänge anlehnen.

2.3 Änderung in Kapitel 2.6.5 Erlaubter Verkehr

Die Anforderung GS-A_4069 wird durch die nachfolgende Festlegung ersetzt.

GS-A_4069-01 -Erlaubter Verkehr Produkttypen

Die Produkttypen Konnektor, Zugangsdienst, Sicherheitsgateway Bestandsnetze MÜSSEN bei Einsatz von Sicherheitsgatewaysden ~~Verkehr mit Sicherheitsgateways auf den Verkehr einschränken, der in der Kommunikationsmatrix in der Architektur der TI-Plattform [gemKPT_Arch_TIP#Kommunikationsmatrix] aufgeführt ist. Datenverkehr auf die in der Kommunikationsmatrix aufgeführten Kommunikationsbeziehungen beschränken.~~

[<=,Konnektor Highspeed, Konnektor PTV5, Konnektor PTV5Plus, Konnektor PTV6, SG_BestNetze, Zugangsdienst,funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA]

2.4 Änderung in Kapitel 3.2 Übergreifende Festlegungen

Die Anforderung GS-A_4970 wird durch die nachfolgende Festlegung ersetzt.

GS-A_4790-01 -Zentrales Netz, nur erlaubte Kommunikation

Das Zentrale Netz MUSS sicherstellen, dass im Zentralen Netz der TI und zwischen den angeschlossenen Produkttypen ausschließlich erlaubte IP-Kommunikation in Richtung Produkttypen und fachanwendungsspezifischer Dienste gesendet wird.

Die erlaubte Kommunikation umfasst:

- Verkehr wie spezifiziert durch die Kommunikationsmatrix in der Architektur der TI-Plattform [gemKPT_Arch_TIP#Kommunikationsmatrix]
- Datenverkehr wie in der Kommunikationsmatrix festgelegt
- DNS-Anfragen an den Produkttyp Namensdienst und an Nameserver-Implementierungen in der TI, die die Zone des Produkttyps Störungsampel verwalten
- NTP-Anfragen an den Produkttyp Zeitdienst
- Übertragung von Monitoringdaten Betriebsdaten an die Störungsampel den Dienst Betriebsdatenerfassung
- Verkehr Datenverkehr zur Steuerung des Netzwerks

[<=, Zentrales-Netz, funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA]

2.5 Änderung in Kapitel 5.7 Anforderungen an den Produkttyp Namensdienst

Die Anforderung GS-A_4812 wird durch die nachfolgende Festlegung ersetzt.

GS-A_4812-01 -Produkttyp Namensdienst, Festlegung der Schnittstellen

Der Produkttyp Namensdienst MUSS die Schnittstellen gemäß Tabelle Tab_PT_Namensdienst_Schnittstellen implementieren („bereitgestellte“ Schnittstellen) und nutzen („benötigte“ Schnittstellen).

Tabelle 1: Tab_PT_Namensdienst_Schnittstellen

Schnittstelle	bereitgestellt / benötigt	obligatorisch / optional	Bemerkung
I_DNS_Name_Resolution	bereitgestellt	obligatorisch	Definition in Abschnitt 4.6
I_DNS_Service_Localization	bereitgestellt	obligatorisch	Definition in Abschnitt 4.6
P_DNS_Name_Entry_Announcement	bereitgestellt	obligatorisch	Definition in Abschnitt 4.7.1
P_DNS_Service_Entry_Announcement	bereitgestellt	obligatorisch	Definition in Abschnitt 4.7.1
P_DNS_Zone_Delegation	bereitgestellt	obligatorisch	Definition in Abschnitt 4.7.3
P_DNSSEC_Key_Distribution	bereitgestellt	obligatorisch	Definition in Abschnitt 4.7.2
I_NTP_Time_Information	benötigt	obligatorisch	Definition in Abschnitt 5.1
I_IP_Transport	benötigt	obligatorisch	Definition in Abschnitt 3.3.2.1
I_Monitoring_Update	benötigt	obligatorisch	Definition durch den Anbieter der Störungsampel

I_Monitoring_Read	benötigt	obligatorisch	Definition durch den Anbieter der Störungsampel
-------------------	----------	---------------	---

[<=, Namensdienst, funkt. Eignung: Herstellererklärung]

Die Anforderung GS-A_4813 wird durch die nachfolgende Festlegung ersetzt.

GS-A_4813-01 -Produkttyp Namensdienst, nur erlaubte Kommunikation

Der Produkttyp Namensdienst MUSS sicherstellen, dass vom Namensdienst aus, über das Zentrale Netz der TI, nur erlaubte IP-Kommunikation in Richtung Produkttypen der TI-Plattform und fachanwendungsspezifischer Dienste gesendet wird.

Zur erlaubten Kommunikation des Namensdienstes zählen:

- DNS-Nachrichten an Fachanwendungsspezifische Dienste und an Zentrale Dienste der TI-Plattform
- NTP-Nachrichten an den Produkttyp Zeitdienst
- Übertragung von Monitoringdaten Betriebsdaten an die Störungsampel den Dienst Betriebsdatenerfassung

[<=, Namensdienst, funkt. Eignung: Test Produkt/FA]

2.6 Änderung in Kapitel 6.3 Anforderungen an den Produkttyp Zeitdienst

Die Anforderung GS-A_4822 wird durch die nachfolgende Festlegung ersetzt.

GS-A_4822-01 -Produkttyp Zeitdienst, Festlegung der Schnittstellen

Der Produkttyp Zeitdienst MUSS die Schnittstellen gemäß Tabelle Tab_PT_Zeitdienst_Schnittstellen implementieren („bereitgestellte“ Schnittstellen) und nutzen („benötigte“ Schnittstellen).

Tabelle 2: Tab_PT_Zeitdienst_Schnittstellen

Schnittstelle	bereitgestellt / benötigt	obligatorisch / optional	Bemerkung
I_NTP_Time_Information	bereitgestellt	obligatorisch	Definition in Abschnitt 5.1
DCF77	benötigt	obligatorisch	Zeitzeichensender DCF77 der PTB
I_IP_Transport	benötigt	obligatorisch	Definition in Kapitel 3 Zentrales Netz der TI
I_DNS_Name_Resolution	benötigt	obligatorisch	Definition in Kapitel 4 Namensdienst
I_Monitoring_Update	benötigt	obligatorisch	Definition durch den Anbieter der Störungsampel
I_Monitoring_Read	benötigt	obligatorisch	Definition durch den Anbieter der Störungsampel
P_DNS_Name_Entry_Announcement	benötigt	obligatorisch	Definition in Kapitel 4

			Namensdienst
Schnittstelle zur GLONASS Zeitquelle	benötigt	optional	NTP Server mit GLONASS Zeitquelle.
Schnittstelle zur GPS Zeitquelle	benötigt	optional	NTP Server mit GPS Zeitquelle.
NTP Schnittstelle zu ptbtime1.ptb.de, ptbtime2.ptb.de, ptbtime3.ptb.de	benötigt	optional	NTP Zeitserver der Physikalisch Technischen Bundesanstalt ptbtime1.ptb.de, ptbtime2.ptb.de und ptbtime3.ptb.de.

Die Client-Funktionalität von mindestens einer der drei optionalen Schnittstellen muss implementiert werden.

[<=,Zeitdienst,funkt. Eignung: Herstellererklärung]

Die Anforderung GS-A_4825 wird durch die nachfolgende Festlegung ersetzt.

GS-A_4825-01 -Produkttyp Zeitdienst, nur erlaubte Kommunikation

Der Produkttyp Zeitdienst MUSS sicherstellen, dass vom Zeitdienst aus, über das Zentrale Netz der TI, ausschließlich erlaubte IP-Kommunikation in Richtung Produkttypen der TI-Plattform und fachanwendungsspezifischer Dienste gesendet wird.

Zur erlaubten Kommunikation des Zeitdienstes zählen:

- NTP-Nachrichten an Fachanwendungsspezifische Dienste und an Zentrale Dienste der TI-Plattform gemäß [RFC5905]
- DNS-Anfragen an den Produkttyp Namensdienst ~~und an Nameserver-Implementierungen in der TI, die die Zone des Produkttyps Störungsampel verwalten.~~
- Übertragung von ~~Monitoringdaten Betriebsdaten~~ an die ~~Störungsampel den Dienst Betriebsdatenerfassung~~

[<=,Zeitdienst,funkt. Eignung: Test Produkt/FA]

2.7 Änderung in Kapitel 8.5.1 Dokumente der gematik

In der Tabelle werden die folgenden Zeilen gelöscht.

[Quelle]	Herausgeber: Titel
[gemSpec_St_Ampel]	gematik: Spezifikation Störungsampel
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform

3 Bereinigung in gemSpec_VPN_ZugD

3.1 Änderungen in Kapitel 5 Funktionsmerkmale

Die Anforderung TIP1-A_4369 wird durch die nachfolgende Festlegung ersetzt.

TIP1-A_4369-01 -VPN-Zugangsdienst, Festlegung der Schnittstellen

Der Produkttyp VPN-Zugangsdienst MUSS die Schnittstellen gemäß Tabelle Tab_PT_VPN-Zugangsdienst_Schnittstellen implementieren („bereitgestellte“ Schnittstellen) und nutzen („benötigte“ Schnittstellen).

Tabelle 3: Tab_PT_VPN-Zugangsdienst_Schnittstellen

Schnittstelle	bereitgestellt / benötigt	obligatorisch/ optional	Bemerkung
I_Secure_Channel_Tunnel	bereitgestellt	obligatorisch	
I_Secure_Internet_Tunnel	bereitgestellt	obligatorisch	
I_DNS_Name_Resolution (Namensraum TI)	bereitgestellt	obligatorisch	
I_DNS_Name_Resolution (Namensraum Internet)	bereitgestellt	obligatorisch	zur Auflösung von FQDN der VPN- Konzentrato ren und des Download- Punktes der CRL
I_DNS_Name_Resolution (Namensraum Internet)	bereitgestellt	obligatorisch	zur Auflösung von FQDN von Diensten im Internet (über den SIS)
I_NTP_Time_Information	bereitgestellt	obligatorisch	
I_Registration_Service	bereitgestellt	obligatorisch	
P_DNSSEC_Key_Distributio n	bereitgestellt	obligatorisch	
I_NTP_Time_Information	benötigt	obligatorisch	Definition in [gemSpec_Net]
I_IP_Transport	benötigt	obligatorisch	Definition in [gemSpec_Net]

I_Monitoring_Update	benötigt	obligatorisch	Definition durch den Anbieter der Störungssampe ↓
I_Monitoring_Read	benötigt	obligatorisch	Definition durch den Anbieter der Störungssampe ↓
I_OCSP_Status_Information	benötigt	obligatorisch	Definition in [gemSpec_PKI]

【<=,Zugangsdienst,funkt. Eignung: Herstellererklärung】

4 Bereinigung in gemSpec_KSR

4.1 Änderung in Kapitel 4.4. Schnittstellen

Der nachfolgende informative Text und die Tabelle wird gelöscht.

Die Tabelle Tab_KSR_002 zeigt die Abbildung der – in vorliegender Spezifikation definierten – Spezifikationsschnittstellen des Konfigurationsdienstes auf die konzeptionellen Schnittstellen aus [gemKPT_Arch_TIP].

Tabelle 1: Tab_KSR_002 Schnittstellenabbildung Konfigurationsdienst

Spezifikationsschnittstelle [gemSpec_KSR]	Konzeptionelle Schnittstelle [gemKPT_Arch_TIP]
I_KSRS_Download	I_KSRS_Download I_KSRS_Net_Config
P_KSRS_Upload	P_KSRS_Maintenance
P_KSRS_Operations	P_KSRS_Maintenance

4.2 Änderung in Kapitel 5.6.1 TLS Transport Layer Security (TLS)

Der nachfolgende informative Text wird angepasst.

Wie in [gemKPT_Arch_TIP] dargestellt, wird die Verbindung zwischen Konnektor und Konfigurationsdienst durch TLS abgesichert, um dem Schutzbedarf der übertragenen Informationen (Operationen listUpdates und getUpdates) zu entsprechen.

Die Verbindung zwischen Konnektor und Konfigurationsdienst wird durch TLS abgesichert, um dem Schutzbedarf der übertragenen Informationen (Operationen listUpdates und getUpdates) zu entsprechen.

Die Anforderung TIP1-A_3324 wird durch die nachfolgende Festlegung ersetzt.

TIP1-A_3324-01 -Konfigurationsdienst TLS-Zertifikatserstellung

Der Anbieter des Konfigurationsdienstes MUSS beim zuständigen PKI-Registrierungsdienst über die Schnittstelle I_Cert_Provisioning [gemKPT_Arch_TIP] das X.509-Komponentenzertifikat mit der TLS-Server-Identität ID.ZD.TLS_S zur TLS Serverauthentisierung beantragen.

[<=,Konfigdienst,funkt. Eignung: Herstellererklärung]

4.3 Änderungen in Kapitel 6.1.1.5 KSR Download Cache

Die Anforderung TIP1-A_6125 wird durch die nachfolgende Festlegung ersetzt.

TIP1-A_6125-01 -KSR - Monitoringdaten an die BDE

Der Konfigurationsdienst MUSS für alle seine Komponenten inklusive der KSR Download Cache Server Monitoringdaten Betriebsdaten an die Störungsampel den Dienst Betriebsdatenerfassung (BDE) senden[gemSpec_St_Ampel] (Schnittstelle [Monitoring_Update]).[<=,Konfigdienst,funkt. Eignung: Test Produkt/FA]

4.4 Änderung in Kapitel 6.2 organisatorische Schnittstellen

Der nachfolgende informative Text wird gelöscht.

~~Das vorliegende Kapitel spezifiziert die organisatorischen Interfaces P_KSRS Upload und P_KSRS Operations auf Basis der konzeptionellen Schnittstelle P_KSRS Maintenance (siehe [gemKPT_Arch_TIP#TIP1-A_2394]). Dieses Interface kann vom Anbieter des Konfigurationsdienstes durch technische Schnittstellen und/oder organisatorische Prozesse umgesetzt werden.~~

4.5 Änderungen in Kapitel 7.5.1 Dokumente der gematik

In der Tabelle wird die folgende Zeile gelöscht.

[Quelle]	Herausgeber: Titel
[gemSpec_St_Ampel]	gematik: Spezifikation Störungsampel