
C_12311_Anlage

Integrationsanforderungen für den ZETA Guard in Bezug zu den TI2.0 Diensten

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Ergänzungen von Anforderungen für den Betrieb.....	3
2.1 Änderung in Kapitel 5.8 Betrieb der gemSpec_ZETA.....	3
2.1.1 Anforderungen an Hersteller einer ZETA Komponente.....	3
2.1.2 Anforderungen an Hersteller eines TI2.0 Dienstes.....	3
2.1.3 Anforderungen an Anbieter eines TI2.0 Dienstes.....	3
3 Ergänzungen von Anforderungen für den Test.....	5
3.1 Änderung in gemKPT_Test.....	5

1 Änderungsbeschreibung

Vorabinformation zum Änderungseintrag:
Folgende Änderungen sind Bestandteil des Änderungseintrages:

- **C_12311 ZETA Integrationsanforderungen**

Die Nummerierung der Kapitel entspricht nicht der Nummerierung aus den referenzierenden Dokumenten, da diese durch die Formatierung automatisch erzeugt wird. Dies wird bei der Einarbeitung der Änderungen entsprechend beachtet.

Erläuterung:
hier nur normativ notwendige Texte
in Begleitdokument der dynamische Teil
beide zusammen beschreiben den aktuellen Stand des Prozesses

Hinweise zur Lesart:
<<Text, der zur Erklärung der Änderung dient - wird nicht mit eingearbeitet/übernommen.>>

Text, der neu ist.

Text, der entfernt wird.

~~**Text, der entfernt wird.**~~

2 Ergänzungen von Anforderungen für den Betrieb

2.1 Änderung in Kapitel 5.8 Betrieb der gemSpec_ZETA

In dem Kapitel 5.8 müssen die Anforderungen an Anbieter eines TI2.0 Dienstes, Hersteller eines TI2.0 Dienstes und Hersteller des ZETA Guards sowie das ZETA Clients beschrieben werden und zur besseren Lesbarkeit werden neue Unterkapitel geschaffen. Um die Integration vollumfänglich zu gewährleisten, muss jeder Beteiligte die dazugehörigen Anforderungen erfüllen.

2.1.1 Anforderungen an Hersteller einer ZETA Komponente

A_27851 -ZETA Guard - Rückwärtskompatibilität

Der Hersteller des ZETA Guard MUSS sicher stellen, dass bei Änderungen an den öffentlichen Schnittstellen keine Breaking-Changes eingeführt werden, bei gleichzeitiger Wahrung der Rückwärtskompatibilität für alle aktiv unterstützten Releases.
[<=,ZT_Cluster,funkt. Eignung: Herstellererklärung]

2.1.2 Anforderungen an Hersteller eines TI2.0 Dienstes

A_27818 -Unterstützung der Wartbarkeit des ZETA Guard-Dienstes

Der Hersteller eines Dienstes der TI2.0 MUSS regelmäßige Updates seines Produktes einplanen, damit die Aktualisierung der ZETA Guard gewährleistet ist. Ein Regelupdate erfolgt maximal einmal pro Quartal. Diese Anforderung gilt über den gesamten Lebenszyklus des Produktes hinweg.[<=,Herst_TI-D_ZT,funkt. Eignung: Herstellererklärung]

2.1.3 Anforderungen an Anbieter eines TI2.0 Dienstes

A_27792 -ZETA Guard - Verbot der Nutzung bestimmter ZETA Guard Versionen

Der Anbieter eines Dienstes der TI2.0 DARF eine zurückgezogene oder ungültige ZETA Guard Version NICHT produktiv einsetzen.[<=,Anb_TI-D_ZT,organ./betriebl. Eignung: Anbietererklärung]

A_27793 -ZETA Guard - Reguläre Aktualisierung von ZETA Guard

Der Anbieter eines Dienstes der TI2.0 MUSS in der Lage sein, regelmäßig Patchupdates der integrierten ZETA Guard Version, die keine Auswirkung auf das Zusammenspiel mit dem Ressource Server haben, durchzuführen. Ein Regelupdate erfolgt maximal einmal pro Quartal.[<=,Anb_TI-D_ZT,organ./betriebl. Eignung: Anbietererklärung]

A_27794 -ZETA Guard - Prüfung auf neue ZETA Guard Versionen

Der Anbieter eines Dienstes der TI2.0 MUSS regelmäßig auf neue freigegebene ZETA Guard Versionen prüfen und - wenn vorhanden - Aktualisierungen im Rahmen des

Gültigkeitszeitraums einplanen. Ein Regelupdate erfolgt maximal einmal pro Quartal.
[<=,Anb_TI-D_ZT,organ./betriebl. Eignung: Anbietererklärung]

A_27795 -ZETA Guard - Gewährleistung der Verbindung zu PIP/PAP

Der Anbieter eines Dienstes der TI2.0 MUSS gewährleisten, dass der eingesetzte ZETA Guard jederzeit auf Aktualisierungen am PIP/PAP-Service abrufen kann.[<=,Anb_TI-D_ZT,organ./betriebl. Eignung: Anbietererklärung]

Hinweis: Notwendige Freischaltungen sind vom Anbieter zu beauftragen und deren Funktionsfähigkeit sicherzustellen.

A_27796 -ZETA Guard - Gewährleistung der Verbindung zur Telemetriedatenlieferung der gematik

Der Anbieter eines Dienstes der TI2.0 MUSS gewährleisten, dass der eingesetzte ZETA Guard jederzeit Datenlieferungen an die gematik übermitteln kann.[<=,Anb_TI-D_ZT,organ./betriebl. Eignung: Anbietererklärung]

Hinweis: Notwendige Freischaltungen sind vom Anbieter zu beauftragen und deren Funktionsfähigkeit sicherzustellen.

3 Ergänzungen von Anforderungen für den Test

3.1 Änderung in gemKPT_Test

Diese Anforderungen sollen in Kapitel 3.2.2.2 von gemKPT_Test hinzugefügt werden

A_27850 -Generalprobe - Wartung ZETA Guard

Der Zulassungsnehmer MUSS sein Produkt in Integration mit ZETA-Guard im Rahmen der Generalprobe verifizieren, jedes Mal, wenn eine Versionsänderung von ZETA Guard erfolgt. Diese Anforderung gilt für den gesamten Lebenszyklus des Produkts.

[<=,Anb_PoPP_Service, Anb_VSDM_2_FD,organ./betriebl. Eignung: Test]

Hinweis: Hinweis: Die genaue Testausführung in der Generalprobe ist im Testkonzept der jeweiligen Zielanwendung definiert.

Diese Anforderungen sollen in Kapitel 6.6 von gemKPT_Test hinzugefügt werden

A_27790 -Schnittstelle zur ZETA Guard - Funktionale Einigung

Der Zulassungsnehmer MUSS die Integration mit ZETA Guard vollständig mit allen Schnittstellenregeln gemäß [gemSpec_ZETA] ausführen. Bestandteil der Integration-Nachweis MUSS mindestens die folgende Funktionalitäten abdecken:

- A_25669 - PEP HTTP Proxy - Zusätzliche HTTP-Header
- A_26974 - PEP HTTP Proxy - Fehler vom Resource Server
- A_27494 - Telemetrie-Daten Service, Custom Collector für Selbstauskunft

[<=,VSDM_2_FD, PoPP_Service,funkt. Eignung: Test Produkt/FA]

A_27815 -Schnittstelle zur ZETA Guard - Funktionale Eignung - Shared Signals

Der Zulassungsnehmer MUSS die Integration mit ZETA Guard vollständig mit allen Schnittstellenregeln gemäß [gemSpec_ZETA] ausführen. Bestandteil der Integration-Nachweis MUSS mindestens die folgende Funktionalitäten abdecken:

- A_25419 - Security Monitoring - Erkennungsfähigkeit
- A_25420 - Security Monitoring - Kommunikationsmerkmale signalisieren
- A_25484 - Security Monitoring - Security KPIs
- A_25485 - Security Monitoring - Sicherheitsmeldung bei Aktualisierung von PIP Daten oder PDP-Policies
- A_25606 - Security Monitoring - Fehlermeldung bei Aktualisierung von PIP Daten oder PDP-Policies

[<=,Anb_PoPP_Service, Anb_VSDM_2_FD,organ./betriebl. Eignung: Test]

A_27816 -Schnittstelle zur ZETA Guard - Funktionale Eignung - Push Notification

Der Zulassungsnehmer MUSS die Integration mit ZETA Guard vollständig mit allen Schnittstellenregeln gemäß [gemSpec_ZETA] und [gemF_PushNotification] ausführen. Bestandteil der Integration-Nachweis MUSS mindestens die folgende Funktionalitäten abdecken:

- A_25652 - ZETA Guard - Push Gateway

- A_25737 - ZETA Guard - Push Notification
- A_27104 - Fachdienst - Push Notifications - OpenApi_Notification_Fachdienst
- A_27610 - Fachdienst - Push Notification senden - Größe des Nachrichteninhalts verschleiern

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

Hinweis: A_27816 gilt ausschließlich für TI-Dienste, die Push-Benachrichtigungen verwenden.

A_27791 -Schnittstelle zur ZETA Guard - Konfigurierbarkeit

Der Zulassungsnehmer MUSS die Integration mit ZETA Guard vollständig mit den Zielkonfigurationen gemäß [gemSpec_ZETA] ausführen. Bestandteil der Integration-Nachweis MUSS mindestens die folgende Funktionalitäten abdecken:

- A_26561 - PEP HTTP Proxy - Caching

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

A_27829 -Schnittstelle zur ZETA Guard - Konfigurierbarkeit - Umgebung

Der Zulassungsnehmer MUSS die Integration mit ZETA Guard vollständig mit den Zielkonfigurationen gemäß [gemSpec_ZETA] ausführen. Bestandteil der Integration-Nachweis MUSS mindestens die folgende Funktionalitäten abdecken:

- A_26480 - PEP HTTP Proxy - Umsetzen eines ZETA/ASL-Kanals
- A_26560 - PEP HTTP Proxy - Weiterleitungskonfiguration

[<=,Anb_PoPP_Service, Anb_VSDM_2_FD,organ./betriebl. Eignung: Test]

Hinweis: Wenn eine Funktionalität nicht Teil der Zweckbestimmung eines Produkts ist, kann sie ausgelassen werden.