
**C_12389_Anlage - Rückbau splitdns -
Implementierungsleitfäden synchronisieren**

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemILF_PS.....	3
2.1.1 Parallelbetrieb-Szenario mit Internetzugriff über IAG als Default-Gateway des Clientsystems.....	3
3 Änderung in gemILF_PS_eRp.....	4
3.1 Namensauflösung.....	4
4 Änderungen in Steckbriefen.....	6

1 Änderungsbeschreibung

Angleichung der DNS Namensauflösung in den verschiedenen Implementierungsleidfäden an den Stand aus
https://github.com/gematik/api-erp/blob/master/docs/*ti_configuration.adoc*:

2 Änderung in gemILF_PS

Änderungen in Kapitel 3.2.3

2.1.1 Parallelbetrieb-Szenario mit Internetzugriff über IAG als Default-Gateway des Clientsystems

Im Falle einer bereits vorhandenen Infrastruktur im dezentralen Bereich können die Produkte der TI, insbesondere der Konnektor, so in die Infrastruktur integriert werden, dass Bestandsanwendungen bereits erprobte Kommunikationswege weiter nutzen können.

Für die Clientsysteme muss in diesem Szenario je nach individuellem Anforderungsprofil entschieden werden, ob das jeweilige Clientsystem über die Telematikinfrastruktur kommunizieren können soll und den gesicherten Internetzugang (SIS) nutzen soll oder nicht.

Soll ein Clientsystem nicht über die Telematikinfrastruktur kommunizieren (Parallelbetrieb), bleibt der IAG als Default-Gateway dieses Clientsystems konfiguriert. In diesem Fall routet der IAG die eingehenden IP-Pakete mit öffentlichen Zieladressen weiter in das Internet.

Im Parallelbetrieb **oder bei Nutzung des TI-Gateways** soll das Primärsystem einen DNS-Resolver integrieren, der Anfragen zu den Domänen ***.splitdns.ti-dienste.de und *.telematik** an den Konnektor sendet. **Die Domänen *.splitdns.ti-dienste.de wird über den Namensdienst im Internet aufgelöst.** ~~Im Parallelbetrieb soll das Primärsystem für~~ Für offene Fachdienste (ePA, eRezept, KIM, ...) und WANDA Smart **muss** eine Weiterleitung für Zieladressen aus dem Adressbereich 100.102.0.0/15 durch Konfigurieren einer Route **einrichten eingerichtet werden**. Für die Referenzumgebung RU ist der Adressbereich mit 10.30.0.0/15 zu konfigurieren.

Im Parallelbetrieb **oder bei Nutzung des TI-Gateways** soll das Primärsystem eine Liste von Telematikservern (z.B. Bestandsnetze, KIM-Fachdienste oder E-Rezept-Dienste) abrufen und für die dort enthaltenen Dienste Routen zum **(virtuellen)** Konnektor auf dem Primärsystemrechner hinterlegen.

Der Downloadpunkt im Internet für die Datei Bestandsnetze.xml lautet

<http://download.crl.ti-dienste.de/bestandsnetze>

Neben der Datei Bestandsnetze.xml befindet sich unter dem Downloadpunkt auch die Signaturdatei Bestandsnetze.sig.

Bevor das Clientsystem die Datei Bestandsnetze.xml verarbeitet, muss ihre Gültigkeit geprüft werden. Diese Prüfung muss aus zwei Schritten bestehen:

- Das Clientsystem prüft die Signatur der Datei Bestandsnetze.xml (die Datei Bestandsnetze.sig) auf Gültigkeit über die Außenoperation VerifyDocument des Konnektors.
- Das Clientsystem prüft das dazugehörige Signaturzertifikat über die Außenoperation VerifyCertificate des Konnektors.
 - Das Clientsystem untersucht dabei das Ergebnis von VerifyCertificate, ob die zurückgegebene technische Rolle "oid_bestandsnetze" ist.

3 Änderung in gemILF_PS_eRp

Änderung in Kapitel 4.2

3.1 Namensauflösung

Der E-Rezept-Fachdienst ist für Primärsysteme gemäß den Festlegungen in [gemSpec_FD_eRp] über die Adresse `erp.zentral.erp.splitdns.ti-dienste.de` lokalisierbar. Das Redundanzkonzept sieht mehrere Instanzen vor, die über verschiedene IP-Adressen angesprochen werden. Folglich liefert die DNS-Namensauflösung verschiedene IP-Adressen zum FQDN zurück. Diese Adressen werden vom DNS-Server in zufälliger Reihenfolge geschickt, sodass es legitim ist, immer den ersten Eintrag für den folgenden Operationsaufruf zu verwenden. Üblicherweise wird die DNS-Auflösung vom Betriebssystem gekapselt, eine Lastverteilung am E-Rezept-Fachdienst ergibt sich aus der zufälligen Reihenfolge der IP-Adressen der DNS-Abfrage. Unspezifiziert ist das Verhalten, wenn die erste Zieladresse nicht erreichbar ist. Empfehlenswert ist die Nutzung der anderen/weiteren IP-Adressen der DNS-Abfrage. Es muss aber angenommen werden, dass bestimmte Betriebssysteme bzw. Laufzeitumgebungen des Primärsystems diese mit der Nutzung der ersten Adresse bereits verworfen haben. Bei Nicht-Erreichbarkeit des Zielhosts der ersten IP-Adresse wird daher empfohlen, weitere Verbindungsversuche auf Basis einer neuen DNS-Abfrage zu tätigen, mit dem Ziel, eine andere IP-Adresse an erster Stelle der DNS-Antwort zu erhalten, als die des nicht erreichbaren Zielhosts.

Das Primärsystem erreicht den E-Rezept-Fachdienst und IDP-Dienst über den Konnektor geroutet. Je nach Installationsumgebung des Primärsystems ist der Konnektor evtl. nicht das Default-Gateway. Um diese offenen Fachdienste zu erreichen, müssen ggfs. feste Routen und eine DNS-Konfiguration für das [Split-DNS] pro Arbeitsplatz-Computer im Rahmen der Installation festgelegt werden.

A_21468 -PS: Handbuch-Hinweis Konnektor Default-Gateway für offene Fachdienste

Der Hersteller des Primärsystems MUSS in seinem Handbuch auf die verschiedenen Installationsszenarien und Konfigurationen des Konnektors in [gemSpec_KON#Anhang K] hinweisen, damit der Konnektor im Rahmen der Installation und Konfiguration des PS für das E-Rezept als Default-Gateway bzw. notwendige Routinginformationen und DNS-Konfigurationen im Gerät festgelegt werden können. [≤,PS_E-Rezept_abgebend, PS_E-Rezept_verordnend,funkt. Eignung: Herstellererklärung]

Der Hersteller des Primärsystems kann die Konfiguration zum Installationszeitpunkt unterstützen, indem er bspw. eine Batch-Datei zum Hinterlegen der Netzwerkeinstellungen für die verschiedenen FQDN für E-Rezept-Fachdienst und IDP-Dienst über den Konnektor als Gateway bereitstellt.

Auch wenn der Domainname anderes suggeriert, werden für `*.splitdns.ti-dienste.de` in der TI und im Internet gleiche DNS Informationen verauskunftet, die Notwendigkeit für spezielle DNS-Konfiguration entfällt für diese Domain.

Mit dem E-Rezept wird ein Split-DNS eingeführt, um die Domainadresse `"ti-dienste.de"` auch im zentralen Netz für Fachdienste nutzen zu können. Für diesen Zweck wird `"splitdns.ti-dienste.de"` in die Bestandsnetzkonfiguration des Konnektors ergänzt. Der Konnektor übernimmt dann für die Domain `splitdns.ti-dienste.de` die Namensauflösung. Für lokale Netzwerkinstallation, die den Konnektor nicht als Nameserver und Gateway

in ihrem Netzwerk nutzen, müssen entsprechende Netzwerkkonfigurationen manuell vorgenommen werden.

Die gematik plant, ergänzende Ergänzende Informationen zu Netzwerkkonfigurationen zu veröffentlichen, bspw. wurden auf der github-Seite <https://github.com/gematik> https://github.com/gematik/api-erp/blob/master/docs/ti_configuration.adoc veröffentlicht.

4 Änderungen in Steckbriefen

keine