Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Änderungen in gemSpec_Net

4.6 Schnittstellen I_DNS_Name_Resolution und I_DNS_Service_Localization

⌦ **GS-A_5582 Namensdienst, Caching Nameserver TI**

Der Produkttyp Namensdienst MUSS mindestens zwei Caching Nameserver TI (full service resolver) bereitstellen, die rekursive DNS-Anfragen zur Auflösung von Namen im Namensraum TI beantworten, und Antworten entsprechend der TTL zwischenspeichern (Caching). Sie MÜSSEN sich netzwerktechnisch im Netzbereich „zentrale Dienste“ befinden und an das zentrale Netz der TI angeschlossen sein.⌫

Der Caching Nameserver TI erlaubt rekursive Anfragen. Er leitet die Anfragen an die autoritativen Nameserver der TI weiter.

4.6.1 Umsetzung

⌦ **GS-A_3931 DNSSEC-Protokoll, Nameserver-Implementierungen**

Produkttypen die autoritative Nameserver implementieren, MÜSSEN [RFC4033], [RFC4034] und [RFC4035] für DNSSEC unterstützen.

Zusätzlich müssen diese Nameserver-Implementierungen Aktualisierungen und Ergänzungen zu den oben genannten RFCs unterstützen. Dies sind Abschnitt 6.1 in [RFC1123], [RFC1982], [RFC1995], [RFC1996], [RFC2181], [RFC2308], [RFC6891], [RFC2782], [RFC2930], [RFC2931], [RFC3225], [RFC5155].⌫

4.6.2 Nutzung

~~**GS-A_3833 DNSSEC-Protokoll, Resolver-Implementierungen**~~

~~Produkttypen von Fachanwendungsspezifischen Diensten und Zentraler Dienste der TI-Plattform sowie der Konnektor MÜSSEN DNS-Resolver implementieren die [RFC4033], [RFC4034] und [RFC4035] für DNSSEC unterstützen.~~

~~**GS-A_3840 DNS-Resolver, Nutzung von DNSSEC**~~

~~Produkttypen von Fachanwendungsspezifischen Diensten und Zentraler Dienste der TI-Plattform sowie der Produkttyp Konnektor MÜSSEN DNS-Resolver implementieren die „security-aware“ gemäß [RFC4035] sind. Dies beinhaltet insbesondere die Validierung der DNS-Response.~~

© gematik – öffentlich_Entwurf

Änderungen in gemSpec_Kon

4.2.6.1 Funktionsmerkmalsweite Aspekte

TIP1-A_4796 Grundlagen des Namensdienstes

Der Konnektor MUSS einen Recursive Caching Nameserver zur Auflösung von DNS-Anfragen sowie einen autoritativen Nameserver zur Verwaltung der Zone „konlan." bereitstellen.

Der Caching-Nameserver des Konnektors MUSS für Clientsysteme aus dem lokalen Netzwerk (ANLW_LAN_NETWORK_SEGMENT oder ANLW_LEKTR_INTRANET_ROUTES) erreichbar sein.

Der Caching-Nameserver des Konnektors MUSS einen Timeout von max. ANLW_SERVICE_TIMEOUT Sekunden beachten. Konnte in dieser Zeit eine DNS-Abfrage nicht durchgeführt werden, MUSS die Bearbeitung abgebrochen werden.

~~Der Caching-Nameserver des Konnektors MUSS DNS-Abfragen immer mit gesetztem CD-Bit senden.~~

~~Der Caching-Nameserver des Konnektors MUSS als Validating Resolver konfiguriert sein und DNS-Anfragen wenn möglich (RRSIG Resource Record und ZSK sind für angefragte Daten verfügbar) gemäß DNSSEC Protokoll validieren.~~

~~**TIP1-A_4799 Aktualität der DNS-Vertrauensanker sicherstellen**~~

~~Der Hersteller des Konnektors MUSS gewährleisten, dass mit jedem Firmware-Update auch die jeweils aktuellen Vertrauensanker mitgeliefert werden.~~

~~Der Konnektor SOLL den DNSSEC-Vertrauensanker gemäß den DNSSEC-Standards bei der Namensermittlung aktualisieren.~~

~~Der Konnektor MUSS den DNSSEC-Vertrauensanker der TI aus dem Zertifikatspeicher in den Caching-Nameserver übernehmen, wenn ein Fehler bei der Validierung der Namensauflösung der TI aufgetreten ist.~~

~~Für DNSSEC muss der Konnektor die Vorgaben aus [gemSpec_Krypt#3.3.3] befolgen.~~

Änderungen in gemProdT_NamD

Tabelle 1: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5582	Namensdienst, Caching Nameserver TI	gemSpec_Net
~~GS-A_3833~~	~~DNSSEC-Protokoll, Resolver-Implementierungen~~	~~gemSpec_Net~~
~~GS-A_3840~~	~~DNS-Resolver, Nutzung von DNSSEC~~	~~gemSpec_Net~~

© gematik – öffentlich_Entwurf

Änderungen in gemProdT_Kon_PTV3

Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_4796	Grundlagen des Namensdienstes	gemSpec_Kon
~~TIP1-A_4799~~	~~Aktualität der DNS-Vertrauensanker sicherstellen~~	~~gemSpec_Kon~~
~~GS-A_3833~~	~~DNSSEC-Protokoll, Resolver-Implementierungen~~	~~gemSpec_Net~~
~~GS-A_3840~~	~~DNS-Resolver, Nutzung von DNSSEC~~	~~gemSpec_Net~~

Änderungen in anderen Produkttypsteckbriefenen

Betroffen sind folgende Produkttypsteckbriefe:

- gemProdT_FD_KOMLE
- gemProdT_FD_VSDM
- gemProdT_Intermediaer_VSDM
- gemProdT_KSR
- gemProdT_OCSP_Proxy
- gemProdT_SG_BestNetze
- gemProdT_St_Ampel
- gemProdT_TSL
- gemProdT_VPN_ZugD
- gemProdT_VZD.doc
- gemProdT_X.509_TSP_nonQES_eGK
- gemProdT_X.509_TSP_nonQES_HBA
- gemProdT_X.509_TSP_nonQES_Komp
- gemProdT_X.509_TSP_nonQES_SMC-B
- gemProdT_X.509_TSP_QES
- gemProdT_ZeitD
- gemProdT_ZentrNetz

Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~GS-A_3833~~	~~DNSSEC-Protokoll, Resolver-Implementierungen~~	~~gemSpec_Net~~
~~GS-A_3840~~	~~DNS-Resolver, Nutzung von DNSSEC~~	~~gemSpec_Net~~

© gematik – öffentlich_Entwurf