

## Änderung in gemSpec\_Perf

Es wird Kapitel 3.2.1 wie folgt angepasst:

### A\_19733-04 - Performance - Rohdaten-Performance-Berichte - Format der Einträge des Performance-Berichts E-Rezept-Fachdienst

Der Produkttyp E-Rezept-Fachdienst MUSS beim Übermitteln der Performance-Messwerte in einem Rohdaten-Performance-Bericht sämtliche Zeilen (Einträge) der Berichte in der folgenden Weise formatieren:

```
INFO: start[$timestamp] time[$duration_in_ms] tag[$operation] size[$size_in_kb] message[{"UA":
"$useragent ", " Status ": $status, "clientid": "$clientid", "LEIPS": "$leipseudonym"}],
```

mit

- \$timestamp ein Unixzeit-Zeitstempel in Millisekunden,
- \$duration\_in\_ms die gemessene Bearbeitungszeit einer Operation in Millisekunden,
- \$operation ist die ausgeführte Operation \$FD-Operation des Produkttyps gemäß Tabelle Tab\_gemSpec\_Perf\_Berichtsformat\_E-Rezept-Fachdienst
- \$size\_in\_kb ist die gemessene, übertragene Datenmenge einer Operation in Kilobyte
- \$useragent (gemäß [gemSpec\_FD\_eRp#A\_20013-01])
- \$status ist der HTTP-Statuscode der inneren bzw. äußeren http-Operation:  
Typ Status: number (int)
- \$clientid ist der Wert client\_id aus dem für die Operation verwendeten Access Token
- \$leipseudonym ist der pseudonymisierte Wert der Telematik-ID der Leistungserbringerinstitution gemäß A\_22698

<=

Prüfverfahren: funkt. Eignung: Test/Produkt FA ; organ./betriebl. Eignung:  
Anbietererklärung

[<=]

## Änderung in gemSpec\_Krypt

Am Ende von Abschnitt "3.16 E-Rezept-spezifische Vorgaben" wird hinzugefügt:

### A\_22698 - E-Rezept, Erzeugung des Nutzerpseudonyms LEI

Der Fachdienst E-Rezept MUSS folgende Punkte sicherstellen.

1. Die VAU MUSS einen mindestens 120-Bit-Entropie-haltigen Pseudonymisierungsschlüssel (PS) erzeugen und zur Verwendung durch die VAU vorhalten.
2. Dieser PS MUSS ausschließlich durch die VAU verwendbar sein (Backups durch den Betreiber, welche durch ein Mehr-Augen-Prinzip geschützt werden, sind zulässig).
3. Dieser PS MUSS halbjährlich automatisch durch die VAU neu erzeugt (gewechselt) werden.
4. Die VAU MUSS im Falle, dass der Nutzer eine LEI ist, die Telematik-ID des Nutzers ermitteln und dann mittels der HKDF nach [RFC-5869] auf Basis von SHA-256, dem geheimen Schlüssel PS und der Telematik-ID ein 256 Bit langes LEI-Pseudonym erzeugen (d. h., Ausgabelänge der HKDF ist also 256 Bit (32 Byte),

IKM (vgl. [RFC-5869] = PS, info (vgl. [RFC-5869]) = Telematik-ID, salt (vgl. [RFC-5869] = „" (leere Zeichenkette)).

5. Die VAU MUSS das in (4) erzeugte LEI-Pseudonym zusammen mit den weiteren, für die Rohdatenlieferung definierten, Informationen an den äußeren E-Rezept-FD (!= VAU) weiter geben.

<=

Prüfverfahren: funkt. Eignung: Herstellererklärung, Sich.techn. Eignung:  
Produktgutachten[<=]

Erläuterung zu A\_22698-\*:

Der Pseudonymisierungsschlüssel kann auch nur in Software vorliegen – muss also nicht zwangsweise in einem HSM vorliegen.

Für die Unterstützung von betrieblichen Prozessen soll dem E-Rezept-Projekt ein Überblick über die Anzahl der aktuell im Feld befindlichen Primärsystem-Versionen zur Verfügung gestellt werden. Der E-Rezept-FD übermittelt die Pseudonyme als Teil der Rohdatenlieferung an die gematik.