

---

## C\_12143\_Anlage

---

# Inhaltsverzeichnis

<b>1 Änderungsbeschreibung.....</b>	<b>2</b>
<b>2 Änderung in gemSpec_Krypt.....</b>	<b>3</b>
<b>3 Änderung in gemSpec_Aktensystem_ePAfueralle.....</b>	<b>13</b>
<b>3.1 Änderungen in Abschnitt 3.3.....</b>	<b>13</b>
<b>3.2 Änderungen in Abschnitt 3.4.....</b>	<b>18</b>
3.2.1 Änderungen in Abschnitt 3.4.1.....	18
3.2.2 Änderungen in Abschnitt 3.4.2.....	20
3.2.3 Änderungen in Abschnitt 3.9.2.2.....	23
<b>4 Änderung in gemILF_PS_ePA.....</b>	<b>26</b>
<b>5 Änderung in gemSpec_FD_eRp.....</b>	<b>27</b>
<b>5.1 Änderung in "6.1.1 HTTP-Operation GET".....</b>	<b>27</b>
<b>5.2 Neues Kapitel "HTTP-Operation GET - Prüfung VSDM Prüfungsnachweis (Version 2)".....</b>	<b>28</b>
<b>6 Änderung in gemILF_PS_eRP.....</b>	<b>29</b>
<b>6.1 Änderung in 5.3.1 E-Rezepte von einem Versicherten abrufen.....</b>	<b>29</b>
<b>7 Änderungen an I_Entitlement_Management.yaml.....</b>	<b>32</b>

---

## 1 Änderungsbeschreibung

---

Es erfolgt eine Anpassung an der VSDM-plus-Prüfziffer, als Teil eines VSDM-Prüfnachweises. Der innere Aufbau der Prüfziffer wird verändert. Deshalb gibt es Anpassungen beim Erzeuger (VSDM-FD) der Prüfziffer und den auswertenden Fachdiensten (E-Rezept-Fachdienst und ePA-Aktensystemen). Eine neue VSDM-plus-Prüfziffer Version 2 hat die gleiche Länge und "äußere Form" wie eine bislang verwendete VSDM-plus-Prüfziffer. Deshalb ergibt sich keine Änderung an anderen Systemen wie dem Konnektor oder am Intermediär. Weitere Änderung: Primärsysteme müssen ein Hashwert aus Teilen einer ReadVSD()-Antwort berechnen und bei der Befugnisvergabe ePA3 dem ePA-Aktensystem übergeben.

---

## 2 Änderung in gemSpec\_Krypt

---

### A\_27274 - VSDM-Betreiber: jährliche Erzeugung des gemeinsamen Geheimnisses

Ein Betreiber eines VSDM-Dienstes MUSS (min.) jährlich ein Geheimnis für die kryptographische Sicherung der VSDM-Prüfziffern zufällig mit einer Länge von 256 Bit (= 32 Byte) und einer Mindestentropie von 120 Bit erzeugen. [**<=**]

[<=, Anb\_FD\_VSDM, Sich.techn. Eignung: Herstellererklärung (Betrieb)]

In gemSpec\_Krypt wird der Abschnitt "3.17 HMAC-Sicherung der Prüfziffer VSDM" nach "3.17 kryptographisch gesicherte VSDM-Prüfziffer Version 1" umbenannt und ein neuer Abschnitt "3.18 VSDM-Prüfziffer Version 2" wie folgt eingefügt (auf die Gelbfärbung des ganzen Abschnitts wird verzichtet, weil in Gänze neuer Text).

### 3.18 Kryptographisch gesicherte VSDM-Prüfziffer Version 2

Bei der kryptographischen Sicherung der VSDM-Prüfziffer Version 1 wird im VSDM-FD im Jahresrhythmus ein Geheimnis erzeugt, das als Grundlage für die kryptographische Sicherung der Integrität einer VSDM-Prüfziffer über einen HMAC dient. Für Version 2 der kryptographischen Sicherung der VSDM-Prüfziffer werden die wesentlichen Teile der Prüfziffer vertraulichkeitsgeschützt (verschlüsselt) und authentizitäts-/integritätsgeschützt. Dabei wird wie in der TI üblich AES/GCM als "Authenticated Encryption with Associated Data (AEAD)"-Verfahren verwendet. Damit werden die Klartext-Daten bei der AES/GCM-Verschlüsselung ebenfalls authentizitäts- und integritätsgeschützt (GMAC-Wert/Authentication-Tag). Deshalb kommt bei der Version 2 kein HMAC mehr bei der eigentlichen Sicherung der Prüfziffern Version 2 zur Anwendung sondern AES/GCM (inkl. GMAC).

Hinweis: es gelten die Anforderungen aus Abschnitt "2.2 Zufallszahlengeneratoren" (Güte der Zufallsquellen) auch für die VSDM-Betreiber (Anbietersteckbrief).

Die erzeugten Geheimnisse müssen für die prüfenden System E-Rezept-VAU und ePA-Aktensystem-VAU (Plural) verschlüsselt (A\_27275-\*) überführt werden. Dafür gibt es im Kontext Prüfziffer Version 1 einen etablierten Prozess, bei dem die Authentizität und Integrität der verschlüsselten Geheimnisse sichergestellt wird. Dieser Prozess wird unverändert weitergeführt auch für den sicheren Transport der gemeinsamen Geheimnisse im Kontext Prüfziffer 2.

Hinweis: Die gematik stellt Beispiel-Code bereit.

Beispiel für ein Export-Paket

```
{
  "betreiberkennung": "X",
  "version": "2",
  "exp": "2025-07-31",
  "encrypted_key":
    "019cd8fd69893e0cca78284b73281cb5e6978f9ec69f8475e30da8709d582d1241188e5f11
    ae14b68defcb28f55b279a61e2b0a03314a9d105c67089602c0904f76f0f90b93547f02078f
    2c6c3d0469b6e43fe2e5a512c3594537184b15c9aaf4b77b7da792e2e1eaae92d812ddf7633
    c8b6e9bfe3fa7ff67daedb1185",
  "hmac_empty_string":
```

```
"b9cda130455534eca5c767d8e1a6e62ff896c2e4a3a02fd7515466f4de2eb0e6"
```

Hinweis: Auch bei dem Export-Paket für Version 2 wird als Integritätssicherung des Exports ein HMAC -- wie bei Version 1 -- verwendet. Für die Sicherung der Prüfziffern selbst im Betrieb wird dann AES/GCM verwendet.

Die Betreiberkennungen werden durch die gematik zugewiesen, es handelt sich um Großbuchstaben A bis Z.

Die gematik stellt Beispiel-Code für die Erzeugung eines Export-Pakets gemäß A\_27276-\* bereit.

Erläuterung zu A 27356-\*:

Als Beispiel ein VSDM-FD verwendet die Schlüsselversion 3, keine anderen Schlüsselversionen liegen im VSDM-FD vor. Dann kommt es zur (im Regelfall jährlichen) Erneuerung. Dabei muss ein Betreiber angeben können das neu erzeugte Schlüsselmaterial soll die Version "1" haben. Dafür wird ein Export-Paket erzeugt und die Geheimnisse wurde in die ePA-Aktensysteme und den E-Rezept-FD erfolgreich importiert. Dann muss der Betreiber des VSDM-FD konfigurieren können: ab jetzt soll Version "1" aktiv sein (Version "3" ist dann inaktiv). Der Betreiber wird im Normalfall dann Version "3" löschen.

Hinweis: Die gematik stellt Beispiel-Code zur Verfügung.

Beispiel:

Sei das gemeinsame 256-Bit lange Geheimnis (hexdump):

[illegible]

dann ist der nach A 27286-\* abgeleitete 128-Bit lange AES/GCM-Schlüssel (hexdump):

b453cd39ea09dbc3a4ff47ebc8bbbfb2

Erläuterung zu A 27323-\*

Für die Kodierung von Daten in der Prüfziffer Version 2 stehen nur 18 Byte zur Verfügung deshalb wird die iat-Zeiten nicht wie bei der Unix-Zeit üblich von 1.1.1970 00:00:00 (UTC) startend kodiert, sondern vor der Kodierung in der Prüfziffer die für die Kodierung notwendige Bitlänge durch Subtraktion eines entsprechenden Offsets reduziert.

Die Kodierungslänge von iat wird wie in A\_27278-\* definiert sogar nochmal um 3 Bit reduziert (r iat 8).

Erläuterungen zu A 27352-\*:

Die Versicherten-Daten müssen nach Spezifikation VSDM [gemSpec\_eGK\_Fach\_VSDM], in ISO-8859-15 (Latin-9) vom eGK-Personalisierer und vom VSDM-FD kodiert eingebracht werden ("Die persönlichen Versichertendaten PD [...]. Der zu verwendende Zeichensatz für die fachlichen Inhalte ist ISO8859-15."). Der Konnektor (genauer das VSDM-Fachmodul im Konnektor) verändert diese Kodierung nicht. D. h. die Versicherten-Daten, die ein Primärsystem über ReadVSD erhält, sind schon in der (im Sinne von A\_27352-\*) "korrekten" Zeichenkodierung und müssen ohne Umkodierung für die Hashwert-Erzeugung verwendet werden.

Das VB-Datum ist nach

[https://github.com/gematik/api-telematik/blob/OPB5/fa/vsds/Schema\\_VSD.xsd](https://github.com/gematik/api-telematik/blob/OPB5/fa/vsds/Schema_VSD.xsd) in einer dort definierten Datentyps "VSD:ISO8601Date". Auszug aus der Definition

```
<xs:pattern value="\d{4}(0[0-9]|1[012])(0[0-9]|1[12][0-9]|3[01])"/>
```

Beispiele:

VB	SAS	Data-to-be-hashed (hexdump)	H_40_0-Wert (hexdump)
20190212	(leere Zeichenkette)	3230313930323132	4885ee8394
19981123	Berliner Straße	31393938313132334265726c696e65722053747261df65	6545491d14
19841003	Angermünder Straße	3139383431303033416e6765726dfc6e6465722053747261df65	7cc49e7af4
20010119	Björnsonstraße	3230303130313139426af6726e736f6e73747261df65	186269e4f7
20040718	Schönhauser Allee	3230303430373138536368f66e68617573657220416c6c6565	353646b5c8

Hinweise zu A\_27278-\*:

Am ersten Byte (Feld\_1) kann man eine Prüfziffer Version 1 (beginnt immer mit Zeichen aus dem Intervall [0x4a, 0x5a]) und eine Prüfziffer Version 2 eindeutig unterscheiden. Wenn das erste Byte von Feld\_1 kleiner als 128 ist, so muss es eine Prüfziffer der Version 1 sein, anderenfalls ist es eine Prüfziffer der Version 2.

Aktuell (Januar 2024) besitzen alle gemeinsamen Geheimnisse in den VSDM-Fachdiensten die Versionsnummer 2. Mit der nächsten regulären Erneuerung (Q2/Q3 2025, A\_27274-\*) wird die Versionsnummer 3 verwendet, usw..

Mit der Erzeugungsvorschrift und Kodierung von r\_iat\_8 kommt es mit dem 03.04.2029 um 10:42:07 (UTC) zum Zählerüberlauf bei r\_iat\_8. Dies ist also eine obere Schranke für die Verwendbarkeit der Prüfziffer Version 2.

Die gematik stellt Beispiel-Code für die Erstellung und Prüfung einer Prüfziffer bereit.

Erläuterung:

Bei ePA erfolgt die Administration (also auch die konfigurative Änderungen) der VAU-HSM im technisch durchgesetzten 4-Augen-Prinzip mit ePA-Aktensystem-Betreiber und gematik zusammen.

Hinweis zu A\_27279-\*:

Je nach Anwendung und Implementierung (ePA oder E-Rezept) werden Teile der Anforderung im VAU-HSM und in der VAU erbracht.

Nur als Verständnishinweis: bei Prüfschritt 8 (hcv-Wertprüfung) ist die Prüfreihefolge motiviert durch Abhängigkeiten im Umsetzungsplan. Erst wenn `enforce_hcv_check` auf `True` gesetzt wird, ist die Prüfung aus Sicherheitssicht effektiv.

Die gematik stellt Beispiel-Code für die Erstellung und Prüfung einer Prüfziffer bereit.

**A\_27275 - VSDM-Betreiber: verschlüsselter Export des gemeinsamen Geheimnisses für Prüzfiffer prüfende Fachdienste-VAUs**

Ein Betreiber eines VSDM-Dienstes MUSS das gemeinsame Geheimnis (vgl. A\_27274-\*) mittels des ECIES-Verfahrens [SEC1-2009] für den Export an die VAUs der prüfenden Fachdienste (E-Rezept-FD, ePA-Aktensysteme) verschlüsseln und dabei folgende Vorgaben umsetzen

1. Er MUSS ein ephemeres ECDH-Schlüsselpaar erzeugen, auf der Kurve des EE-Schlüssels aus dem Verschlüsselungszertifikat des Empfängers (VAUENC) -- also P-256 oder brainpoolP256r1, und mit diesem und dem VAU-Schlüssel aus A\_20160-\* ein ECDH gemäß [NIST-800-56-A] durchführen. Das somit erzeugte gemeinsame Geheimnis ist Grundlage für die folgende Schlüsselableitung.
2. Als Schlüsselableitungsfunktion MUSS er die HKDF nach [RFC-5869] auf Basis von SHA-256 verwenden.
3. Dabei MUSS er den Ableitungsvektor "ecies-vau-transport" verwenden, d. h. in der Formulierung von [RFC-5869] info="ecies-vau-transport" .
4. Er MUSS mit dieser Schlüsselableitung einen AES-128-Bit Content-Encryption-Key für die Verwendung von AES/GCM ableiten.
5. Er MUSS für Verschlüsselung mittels AES/GCM einen 96 Bit langen IV zufällig erzeugen.
6. Er MUSS mit dem CEK und dem IV mittels AES/GCM den Klartext verschlüsseln, wobei dabei ein 128 Bit langer Authentication-Tag zu verwenden ist.
7. Er MUSS das Ergebnis wie folgt kodieren: chr(0x01) || <32 Byte X-Koordinate vom öffentlichen Schlüssel aus "1." > || <32 Byte Y-Koordinate> || <12 Byte IV> || <AES-GCM-Chiffre> || <16 Byte AuthenticationTag> (vgl. auch Tab\_KRYPT\_ERP und folgende die Beispielschlüsselung).  
Die Koordinaten sind (wie üblich) vorne mit chr(0) zu paden solange bis sie eine Kodierungslänge von 32 Byte erreichen.

[<=, Anb\_FD\_VSDM, Sich.techn. Eignung: Herstellererklärung (Betrieb)]

**A\_27276 - VSDM: Export-Paket**

Ein VSDM-FD MUSS bei der Erstellung der Export-Pakete für den Export der gemeinsamen Geheimnisse (vgl. A\_27274-\*) an die prüfenden Systeme (E-Rezept-VAU, ePA-Aktensystem-VAU-HSM etc.) die gleiche Export-Paket-Struktur verwenden wie im Kontext Prüzfiffer Version 1.[<=, Anb\_FD\_VSDM, Sich.techn. Eignung: Anbietererklärung]

**A\_27356 - VSDM: explizite Angabe der Geheimnis-Version bei Erzeugung**

Ein VSDM-FD MUSS es einem VSDM-FD-Betreiber ermöglichen:

1. bei der (im Regelfall jährlichen) Erzeugung des Geheimnisses die Schlüsselversion, die bei der Erzeugung zu verwenden ist, explizit und beliebig (außer die aktuell aktive Schlüsselversion) anzugeben,  
(Es ist also keine strenge Monotonie bei der Folge der Schlüsselversionen durchzusetzen.)
2. explizit und beliebig auszuwählen welche Schlüsselversion aktiv (zur Erzeugung von Prüzfiffern) verwendet werden soll, und
3. explizit auszuwählen welche Schlüsselversion zu löschen ist.

[<=, FM\_VSDM, funkt. Eignung: Herstellererklärung]

**A\_27277 - VSDM-Betreiber: Schlüsselwechsel**

Ein Betreiber eines VSDM-Dienstes MUSS folgendes sicherstellen.

1. Nach der jährlicher Erneuerung des gemeinsamen Geheimnisses (vgl. A\_27274-\*) MUSS dieses mittels A\_27275-\* und A\_27276-\* und des schon für die Prüzfiffer Version

- 1 etablierten Prozess jeweils für die prüfenden Systeme (E-Rezept-VAU und ePA-Aktensystem-VAUs) verschlüsselt und an diese übermittelt werden.
2. Das gemeinsame Geheimnis MUSS zunächst "inaktiv" sein.
3. Erst nach erfolgreichen Import durch alle prüfenden Systeme MUSS das gemeinsame Geheimnis aktiviert werden und mittels A\_27286-\* der entsprechende AES/GCM-Schlüssel abgeleitet werden. Dieser ist dann aktiv und der jüngste AES/GCM-Schlüssel und MUSS nach A\_27278-\* für die Erzeugung der Prüzziffern Version 2 verwendet werden.

[<=, Anb\_FD\_VSDM, Sich.techn. Eignung: Anbietererklärung, funkt. Eignung: Anbietererklärung]

#### **A\_27286 - VSDM-FD: Ableitung des AES/GCM-Schlüssel für die Sicherung der Prüzziffern Version 2 aus dem gemeinsamen Geheimnis**

Ein VSDM-FD MUSS nach der Erzeugung eines gemeinsamen Geheimnisses (vgl. A\_27274-\*), mit dem Geheimnis eine Schlüsselableitung durchführen. Mittels der HKDF nach [RFC-5869] auf Basis von SHA-256 und dem Ableitungsvektor "VSDM+ Version 2 AES/GCM" ein 128 Bit (=16 Byte) Wert (Bitfolge) abgeleitet werden. Diese 128 Bit Bitfolge MUSS als AES/GCM-Schlüssel für die Erzeugung der Prüzziffern Version 2 gemäß A\_27278-\* verwendet werden.

D. h. Es wird nach A\_27274-\* ein neuer Schlüssel mindestens jährlich erzeugt, der dann die Versionsnummer x habe. Anschließend erfolgt einmalig eine Schlüsselableitung wie in A\_27286-\* definiert. Damit wird der AES/GCM-Schlüssel-Version x erzeugt. Nach "Aktivierung" (vgl. A\_27277-\*) wird dieser gemäß A\_27278-\* verwendet um Prüzziffern zu erzeugen. [<=, Anb\_FD\_VSDM, Sich.techn. Eignung: Anbietererklärung]

#### **A\_27323 - VSDM-FD: relative Zeit (Zeit-offset) Prüzziffer Version 2**

Ein VSDM-FD MUSS als Offset für die Zeitkodierung (iat) bei der Erstellung der Prüzziffer Version 2 (A\_27278-\*) folgende Vorgabe verwenden:

offset-Name	Wert	Erläuterung
iat_offset	173568960 0	offset für die Erzeugungszeit (iat) der Prüzziffer Version 2  Hinweis: Die Zeit "2025-01-01T00:00:00+00:00" (ISO-Format 8601) nach Unix-Zeit (UTC) konvertiert ist 1735689600.

[<=, Anb\_FD\_VSDM, Sich.techn. Eignung: Anbietererklärung]

#### **A\_27352 - VSDM-Prüzziffer Version 2: Erzeugung von hcv**

Ein den hcv-Wert (Hash Check Value) erzeugendes System (VSDM-FD oder Primärsystem) MUSS bei der Erzeugung des hcv-Wertes, wie folgt vorgehen:

1. Es sei VB gleich der Versicherungsbeginn (UC\_AllgemeineVersicherungsdatenXML.Versicherter.Versicherungsschutz.Beginn, [https://github.com/gematik/api-telematik/blob/OPB5/fa/vsds/Schema\\_VSD.xsd](https://github.com/gematik/api-telematik/blob/OPB5/fa/vsds/Schema_VSD.xsd) ). VB MUSS keine Leerzeichen enthalten. (siehe Erläuterungen nach A\_27352-\*)
2. Falls der Versicherte eine "StrassenAdresse" (vgl. XML-Schema) und darin ein nichtleeres Element "Strasse" besitzt, dann sei SAS gleich der Wert in diesem Element. Andernfalls sei SAS="" (leere Zeichenfolge). Ggf. Führende oder endende Leerzeichen MÜSSEN entfernt werden. Die Kodierung der Inhalte von "Strasse" MUSS ISO-8859-15 (Latin-9) sein. (siehe Erläuterungen nach A\_27352-\*)
3. Sei SHA-256 wie in [FIPS-180-4] definiert.



4. Sei  $H = \text{SHA-256}(\text{VB} \parallel \text{SAS})$ .
  5. Sei  $H_{40}$  die ersten 5 Bytes (40 Bit) von  $H$ .
  6. Von  $H_{40}$  setzt man das MSBit im ersten Byte auf 0, das Ergebnis sei  $H_{40\_0}$ .
- Der hcv-Wert ist gleich  $H_{40\_0}$ .

[<=, PS\_E-Rezept\_abgebend, PS\_ePA, Anb\_FD\_VSDM, Sich.techn. Eignung:  
Anbietererklärung, funkt. Eignung: Konformitätsbestätigung]

### A\_27278 - VSDM-FD: Struktur einer Prüfziffer der Version 2

Ein VSDM-FD MUSS zunächst folgende innere Datenstruktur (Klartext) erstellen:

Name	Länge	Festlegungen und Erläuterung
I_Feld_1	5	<p>In diesem Feld sind Sperrinformationen und ein gekürzter Hashwert kodiert.</p> <p><u>Sperrinformation:</u> Falls die eGK ungültig/gesperrt ist, sei <math>S=128</math>, anderenfalls sei <math>S=0</math>.</p> <p><u>Hashwert:</u> Der hcv-Wert MUSS wie in A_27352-* definiert berechnet werden. Und wird im Folgenden als <math>H_{40\_0}</math> bezeichnet. Sei <math>H_{40\_0}[0]</math> das erste Byte von <math>H_{40\_0}</math> und <math>H_{40\_0}[1:]</math> alle restlichen Bytes von <math>H_{40\_0}</math>.</p> <p>Dann ist <math>I\_Feld\_1 = (H_{40\_0}[0] \mid S) \parallel H_{40\_0}[1:]</math>.</p> <p>(Erläuterung zum besseren Verständnis: das MSBit im ersten Byte von <math>H_{40}</math> wird auf 0 gesetzt (A_27352-*, Schritt 6) und man erhält <math>H_{40\_0}</math>. Anschließend wird die Sperrinformation auf das erste Byte aufaddiert. D. h. wenn von <math>I\_Feld\_1</math> das MSBit des ersten Bytes 1 ist, dann ist die eGK ungültig/gesperrt.)</p>
r_iat_8	3	<p>Sei <math>iat</math> die aktuelle Unix-Zeit (UTC) in Sekunden (also keine Nachkommastellen) im VSDM-FD zum Erzeugungszeitpunkt der Prüfziffer. Dann MUSS <math>r\_iat\_8 = (iat - iat\_offset) \gg 3</math></p> <p>Alle Zahlenwerte MÜSSEN in Network-Byte-Order (= Byte-Order Big) kodiert werden. Alle Zeiten sind wie bei der Unix-Zeit üblich UTC.</p> <p>Hinweis: für <math>iat\_offset</math> vgl. A_27323-.*.</p> <p>Beispiel: Wird die Prüfziffer um "2025-01-02T00:00:00+00:00" = 1735776000 erzeugt, dann ist  <math>r\_iat = (1735776000 - 1735689600) \gg 3 = 10800</math></p>
KVNR	10	10 Stellige KVNR, ASCII-kodiert (Beispiel: A123456789)

Der Klartext hat damit eine Länge von 18 Byte.

Name	Länge	
Feld_1	1	<p>In diesem Feld sind drei Informationen kodiert:</p> <p>(1) Kennzeichnung für Version 2 der Prüfziffer Sei <math>V = 128</math>.</p> <p>(2) Betreiberkennung Die Betreiberkennung (wie bspw. im Export-Paket (A_27276-*) übertragen) ist zunächst ein Buchstabe von 'A' bis 'Z'. Sei BK diese Betreiberkennung als ASCII-Zeichen. Sei <math>BK\_D = BK - 65</math> und sei <math>BK\_D\_4 = BK\_D \ll 2</math>.</p> <p>(3) Geheimnis/Schlüssel-Version Sei SV gleich die Geheimnis/Schlüssel-Version, die für die Verschlüsselung des Klartextes (siehe Tabelle oben) verwendet wird. SV wird binär kodiert, bspw. wenn <math>SV = 2</math> ist, so ist SV kodiert <math>\backslash x02</math>. SV MUSS kleiner 4 sein (vgl. auch A_27356-*).</p> <p>Sei <math>Feld\_1 = V + BK\_D\_4 + SV</math></p> <p>Beispiel: Sei die Betreiberkennung gleich 'B' und die Schlüssel-Version gleich 2, dann ist <math>BK\_D\_4</math> gleich 4. Und damit <math>Feld\_1 = 128 + 4 + 2 = 134</math>.</p>
Initialisierungsvektor für AES/GCM	12	wie bei AES/GCM üblich MUSS der 96 Bit lange IV (= 12 Bytes) pro Verschlüsselung zufällig über eine kryptographisch hochwertige Zufallsquelle erzeugt werden
eigentliches Chiffre	18	mittels AES/GCM verschlüsselter Klartext (innere Datenstruktur, s. o.) mit dem jüngsten aktivierten AES/GCM-Schlüssel (vgl. A_27286-*)
AES/GCM Authentication-Tag (GMAC)	16	128-Bit Authentication-Tag, der bei der AES/GCM entsteht (berechnet wird)

Die oben aufgeführte Datenstruktur hat die Gesamtgröße von 47 Byte. Diese Datenstruktur MUSS base64-kodiert werden. Das Ergebnis der Kodierung ist "die Prüfziffer Version 2". Deren Länge ist 64 Byte (Hinweis: gleiche Länge wie eine Prüfziffer Version 1).

【<=, Anb\_FD\_VSDM, Sich.techn. Eignung: Anbietererklärung】

#### **A\_27299 - VSDM-Prüfziffer Version 2: prüfenden Systeme, Import der gemeinsamen Geheimnisse und AES/GCM-Schlüsselableitung**

Ein die Prüfziffer Version 2 prüfendes System (E-Rezept-FD-VAU, ePA-Aktensystem-VAU/VAU-HSM etc.) MUSS Export-Pakete gemäß A\_27276-\* importieren. Es werden dabei gemeinsame Geheimnisse gemäß A\_27274-\* importiert. Diese MUSS die im Export-Paket aufgeführte Betreiberkennung und Version zugeordnet werden. Mit dem gemeinsamen Geheimnis MUSS das prüfende System eine Schlüsselableitung gemäß

A\_27286-\* durchführend und dem erhaltenen AES/GCM-Schlüssel die Betreiberkennung und Version des gemeinsamen Geheimnisses (also aus dem entsprechenden Import) zuordnen.

Anschließend MÜSSEN die AES/GCM über Betreiberkennung und Version (vgl. Kodierung der beiden Werte in einer Prüfziffer Version 2 in A\_27278-\*) im prüfenden System verfügbar/adressierbar sein.

Ein prüfendes System MUSS die Möglichkeit besitzen alte gemeinsame Geheimnisse und abgeleitete AES/GCM-Schlüssel (Kontext Prüfung Prüfziffer Version 2) im System per Administration zu löschen.

[<=, Aktensystem\_ePA, eRp\_FD, funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Produktgutachten]

### **A\_27342 - Konfigurationsvariable enforce\_hcv\_check**

Ein die Prüfziffer Version 2 prüfendes System (E-Rezept-VAU, ePA-Aktensystem-VAU-HSM etc.) MUSS eine Konfigurationsvariable `enforce_hcv_check` besitzen, die standardmäßig auf `false` gesetzt ist. [<=, Aktensystem\_ePA, eRp\_FD, funkt. Eignung: Herstellererklärung]

### **A\_27279 - VSDM-Prüfziffer Version 2: Prüfung und Entschlüsselung**

Ein die Prüfziffer Version 2 prüfendes System (E-Rezept-VAU, ePA-Aktensystem-VAU-HSM etc.) MUSS folgende Prüfungen der Prüfziffer Version 2 vornehmen. Ergibt eine der Prüfungen ein nicht-positives Prüfergebnis, so MUSS die Prüfziffer als ungültig abgelehnt werden.

1. Prüfung: besitzt die Prüfziffer eine Länge von 64 Bytes.
2. Prüfung: kann die Prüfziffer erfolgreich base64-dekodiert werden.  
Die nun erhaltene erfolgreich base64-dekodierte 47 Byte lange Bytefolge wird als `dtbc` (data to be checked) im Folgenden bezeichnet.
3. Prüfung: ist das erste Byte von `dtbc` größer als 128 (das MSBit ist also auf 1 gesetzt).  
Hinweis: ansonsten handelt es sich um eine Prüfziffer Version 1 (für die Prüfung in A\_27279-\* also nicht geeignet).
4. Prüfung: gibt es im prüfenden System einen AES/GCM-Schlüssel mit der im ersten Byte von `dtbc` aufgeführter Betreiberkennung und aufgeführter Version (vgl. A\_27299-\* und A\_27278-\*).
5. Die folgenden 12 Byte in `dtbc` werden als IV bezeichnet. Die darauf folgenden 18 Bytes werden als ciphertext bezeichnet. Die darauf folgenden 16 Bytes werden als Authentication-Tag bezeichnet.  
Prüfung: ist die AES/GCM-Entschlüsselung erfolgreich mittels des in Schritt 4 identifizierten AES/GCM-Schlüssels und mit IV, ciphertext, Authentication-Tag  
D. h. gibt es gerade kein Symbol FAIL als Ergebnis der AES/GCM-Entschlüsselung -- die Authentizität und Integrität des Chiphertexts/Klartexts ist damit festgestellt.  
Im folgenden wird der erfolgreich entschlüsselte Klartext betrachtet.
6. Prüfung: ist das MSBit im ersten Byte des Klartextes gleich 0 (ansonsten ist die eGK gesperrt).
7. Prüfung zeitliche Gültigkeit der Prüfziffer:  
Sei, wie in A\_27278-\*, definiert `r_iat_8` die Bytefolge von Byte-Offset 5 bis inkl. Byte-Offset 7 (also 3 Byte groß) aus dem Klartext. `r_iat_8` MUSS im Network-Byte-Order (= Byte-Order Big) kodierte unsigned Zahl interpretiert werden.  
Zunächst MUSS der Wert `iat` mit  $iat = (r\_iat \ll 3) + iat\_offset$  (vgl. A\_27323-\*) berechnet werden.  
Anschließend MUSS anwendungsspezifisch `iat` mit der aktuellen Zeit überprüft werden:

ePA: A\_24573-\* (20 Minuten Fenster)

E-Rezept: A\_23451-\* (30 Minuten Fenster)

8. Prüfung hcv:

Im folgenden werden die ersten 5 Byte des Klartextes als H\_40\_0 bezeichnet.

Wenn vom Primärsystem ein hcv-Wert übergeben wurde, prüfe ob H\_40\_0 gleich dem vom Primärsystem übergebenen hcv-Wert ist (vgl. A\_24590-\*).

Wenn vom Primärsystem kein hcv-Wert übergeben wurde: Wenn enforce\_hcv\_check (vgl. A\_27342-\*) auf true gesetzt ist, dann FAIL, anderen falls OK.

(Der hcv-Wert aus A\_24590-\* MUSS vor dem Vergleich base64-dekodiert werden.)

9. Die letzten 10 Byte des Klartextes werden als KVNR bezeichnet.

Prüfung: ist die KVNR aus dem Klartext gleich der KVNR, die im Anwendungskontext erwartet wird.

**[<=, Aktensystem\_ePA, eRp\_FD, Sich.techn. Eignung: Produktgutachten]**

---

## 3 Änderung in gemSpec\_Aktensystem\_ePAfueralle

---

### 3.1 Änderungen in Abschnitt 3.3

#### **ALT:**

#### **A\_24611-02 - ePA-Aktensystem - Im VAU-HSM gespeicherte Schlüssel und Informationen für VAU-Betrieb**

Das ePA-Aktensystem MUSS sicherstellen, dass folgende, für den Betrieb der VAU notwendigen Schlüssel und Informationen in einem HSM (als VAU-HSM bezeichnet) gespeichert werden:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU (u.a. genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und Überschlüsselung")
- symmetrische Schlüssel für die HMAC-Prüfung der VSDM-Prüfziffern (jeweils einen pro VSD-Dienst-Betreiber)
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=, Aktensystem\_ePA, Sich.techn. Eignung: Produktgutachten]

#### **NEU:**

#### **A\_24611-03 - ePA-Aktensystem - Im VAU-HSM gespeicherte Schlüssel und Informationen für VAU-Betrieb**

Das ePA-Aktensystem MUSS sicherstellen, dass folgende, für den Betrieb der VAU notwendigen Schlüssel und Informationen in einem HSM (als VAU-HSM bezeichnet) gespeichert werden:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU (u.a. genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und Überschlüsselung")
- symmetrische Schlüssel für die HMAC-Prüfung der VSDM-Prüfziffern (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

Hinweis: Es gelten die Anforderungen aus [gemSpec\_Krypt#3.18 VSDM-Prüfziffer Version 2] für ein ePA-Aktensystem in der Rolle "Prüfziffer Version 2 prüfendes System". Aus den ins HSM importierten gemeinsamen Geheimnissen erfolgt im HSM eine Schlüsselableitung (A\_27299-\*) der für die Entschlüsselung der Prüfziffer Version 2 benötigten AES/GCM-Schlüssel.

#### **ALT:**

#### **A\_24612-03 - ePA-Aktensystem - Erzwingen von 4-Augen-Prinzip für Einbringen und Verwalten von Informationen ins VAU-HSM**

Das ePA-Aktensystem MUSS technisch erzwingen, dass die folgenden, für den Betrieb der VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip in das VAU-HSM eingebracht und verwaltet werden können:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- ggf. privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber)

- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=, Aktensystem\_ePA, Sich.techn. Eignung: Produktgutachten]

#### **NEU:**

#### **A\_24612-04 - ePA-Aktensystem - Erzwingen von 4-Augen-Prinzip für Einbringen und Verwalten von Informationen ins VAU-HSM**

[https://gemspec.gematik.de/docs/gemSpec/gemSpec\\_Aktensystem\\_ePAfueralle/latest/#A\\_24612-03](https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest/#A_24612-03)

Das ePA-Aktensystem MUSS technisch erzwingen, dass die folgenden, für den Betrieb der VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip in das VAU-HSM eingebracht und verwaltet werden können:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- ggf. privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

#### **ALT:**

#### **A\_24614-02 - ePA-Aktensystem - Einbringung von Informationen ins VAU-HSM im 4-Augen-Prinzip mit der gematik**

Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass die folgenden, für den Betrieb der VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip ins VAU-HSM eingebracht und im VAU-HSM verwaltet werden, bei dem eine von der gematik benannte Person beteiligt ist:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU



- Zertifikat C.FD.ENC mit policyIdentifier oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber)
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=, Anb\_Aktensystem\_ePA, Sich.techn. Eignung: Gutachten (Anbieter)]

#### **NEU:**

#### **A\_24614-03 - ePA-Aktensystem - Einbringung von Informationen ins VAU-HSM im 4-Augen-Prinzip mit der gematik**

[https://gemspec.gematik.de/docs/gemSpec/gemSpec\\_Aktensystem\\_ePAfueralle/latest/#A\\_24614-02](https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest/#A_24614-02)

Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass die folgenden, für den Betrieb der VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip ins VAU-HSM eingebracht und im VAU-HSM verwaltet werden, bei dem eine von der gematik benannte Person beteiligt ist:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

#### **ALT:**

#### **A\_24618-02 - ePA-Aktensystem - Zugriff auf Schlüssel und Informationen im VAU-HSM**

Das ePA-Aktensystem MUSS sicherstellen, dass auf die folgenden, für den Betrieb der VAU notwendigen und im VAU-HSM gespeicherten Schlüssel und Informationen ausschließlich über attestierte VAU-Instanzen zugegriffen werden kann:

- privater Schlüssel der Authentisierungsidentität der VAU ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz



- privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU ausschließlich durch eine Befugnisverifikations-VAU-Instanz
- privater Schlüssel der Authentisierungsidentität eines Service-VAU-Typs ausschließlich durch eine Service-VAU-Instanz dieses Service-VAU-Typs
- privater Schlüssel der Verschlüsselungsidentität der VAU ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- privater Schlüssel der Signaturidentität der VAU ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Zertifikat C.FD.ENC mit policyIdentifier oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Masterkeys für die Ableitung der versichertenindividuellen Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und Überschlüsselung") ausschließlich durch die Aktenkontoverwaltungs-VAU-Instanz oder durch eine dedizierte Überschlüsselungs-VAU
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber) ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse) ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz.

[<=, Aktensystem\_ePA, Sich.techn. Eignung: Produktgutachten]

#### **NEU:**

#### **A\_24618-03 - ePA-Aktensystem - Zugriff auf Schlüssel und Informationen im VAU-HSM**

Das ePA-Aktensystem MUSS sicherstellen, dass auf die folgenden, für den Betrieb der VAU notwendigen und im VAU-HSM gespeicherten Schlüssel und Informationen ausschließlich über attestierte VAU-Instanzen zugegriffen werden kann:

- privater Schlüssel der Authentisierungsidentität der VAU ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU ausschließlich durch eine Befugnisverifikations-VAU-Instanz
- privater Schlüssel der Authentisierungsidentität eines Service-VAU-Typs ausschließlich durch eine Service-VAU-Instanz dieses Service-VAU-Typs
- privater Schlüssel der Verschlüsselungsidentität der VAU ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- privater Schlüssel der Signaturidentität der VAU ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Zertifikat C.FD.ENC mit policyIdentifier oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz

- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Masterkeys für die Ableitung der versichertenindividuellen Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und Überschlüsselung") ausschließlich durch die Aktenkontoverwaltungs-VAU-Instanz oder durch eine dedizierte Überschlüsselungs-VAU
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden, ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse) ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz.

[&lt;=]

## 3.2 Änderungen in Abschnitt 3.4

### 3.2.1 Änderungen in Abschnitt 3.4.1

#### ALT:

#### **A\_25282-01 - ePA-Aktensystem - Regeln des VAU-Token-Moduls**

Das VAU-Token-Modul MUSS die in Tabelle *Tab\_AS\_VAU-Token\_Modul\_Rules* definierten Regeln umsetzen. [<=]

**Tabelle 1: Tab\_AS\_VAU-Token\_Modul\_Rules -Prüfregeln VAU Token**

hsm-r3	<p><i>Diese Regel dient zur Nutzung des HMAC bzgl. VSDM-Prüfziffern</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Daten</li> <li>• Bezeichner des HMAC-Schlüssels</li> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.)</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• HMAC der Daten mit dem symmetrischen Schlüssel, der zum übergebenen Bezeichner des HMAC-Schlüssels gehört</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> <li>3. (opt.) prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> </ol>
--------	---

Falls die Prüfungen 1) - 3) erfolgreich waren, wird der HMAC mit dem gewünschten HMAC-Schlüssel über die Daten gebildet.

**NEU:****A\_25282-02 - ePA-Aktensystem - Regeln des VAU-Token-Moduls**

Das VAU-Token-Modul MUSS die in Tabelle *Tab\_AS\_VAU-Token\_Modul\_Rules* definierten Regeln umsetzen. [**<=**]

**Tabelle 2: Tab\_AS\_VAU-Token\_Modul\_Rules -Prüfregeln VAU Token**

hsm-r3	<p><i>Diese Regel dient zur Nutzung des HMAC bzgl. VSDM-Prüfziffern der Version 1 oder der Entschlüsselung der VSDM-Prüfziffern der Version 2</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.)</li> <li>Szenario VSDM-Prüfziffer Version 1 <ul style="list-style-type: none"> <li>Daten</li> <li>Bezeichner des HMAC-Schlüssels</li> </ul> </li> <li>Szenario VSDM-Prüfziffer Version 2 <ul style="list-style-type: none"> <li>VSDM-Prüfziffer in Version 2</li> </ul> </li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>Szenario VSDM-Prüfziffer Version 1: HMAC der Daten mit dem symmetrischen Schlüssel, der zum übergebenen Bezeichner des HMAC-Schlüssels gehört</li> <li>Szenario VSDM-Prüfziffer Version 2: innere Struktur der VSDM-Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVN) bei erfolgreicher Entschlüsselung</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch)</li> <li>prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> <li>(opt.) prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> </ol> <p><b>Szenario VSDM-Prüfziffer Version 1:</b> Falls die Prüfungen 1) - 3) erfolgreich waren, wird der HMAC mit dem gewünschten HMAC-Schlüssel über die Daten gebildet.</p> <p><b>Szenario VSDM-Prüfziffer Version 2:</b> Falls die Prüfungen 1) - 3) erfolgreich waren, wird die VSDM-Prüfziffer gemäß den Prüfschritten 4. und 5. aus A_27279-* geprüft und entschlüsselt. Bei erfolgreicher Entschlüsselung der VSDM-Prüfziffer wird die innere Struktur der VSDM-Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVN) zurückgeliefert, ansonsten ein Fehler.</p>
--------	---

### 3.2.2 Änderungen in Abschnitt 3.4.2

#### ALT:

#### A\_24573-03 - ePA-Aktensystem - Regeln des Befugnisverifikations-Moduls

[https://gemspec.gematik.de/docs/gemSpec/gemSpec\\_Aktensystem\\_ePAfueralle/latest/#A\\_24573-02](https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest/#A_24573-02)

Das Befugnisverifikations-Modul MUSS die in den Tabellen *Tab\_AS\_Entitlement\_Registration\_Rules* und *Tab\_AS\_SDS-Key\_Rules* definierten Regeln umsetzen. [**<=**]

Tabelle 3: *Tab\_AS\_Entitlement\_Registration\_Rules* - Regeln zur Registrierung von Befugnissen

rr3	<p><i>Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das <b>Stecken der eGK in einer Leistungserbringerumgebung</b> ergeben.</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• Prüfziffer des VSDM-Prüfungsnachweises signiert mit AUT-Identität der SMC-B</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Befugnis = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. prüfen der SMC-B-Signatur der signierten VSDM-Prüfziffer gemäß A_25042-* (C.HCI.AUT)</li> <li>2. prüfen, dass das JWT gemäß A_24590-* zeitlich gültig ist ( <math>iat - 15s \leq \text{aktuelle Zeit} &lt; exp + 15s</math> )</li> <li>3. prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer nicht länger als 20 Minuten zurückliegt</li> <li>4. prüfen des HMAC der VSDM-Prüfziffer mittels VAU-HSM Regel hsm-r3             <ol style="list-style-type: none"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>5. Falls die Prüfungen in 1) bis 4) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt:             <ul style="list-style-type: none"> <li>• Aktenkonto: die KVNR aus dem VSDM-Prüfziffer</li> <li>• Telematik-ID: die Telematik-ID aus der SMC-B-Signatur</li> <li>• Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur.</li> </ul> </li> <li>6. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis             <ol style="list-style-type: none"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>7. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis</li> </ol>
-----	--

	als Ergebnis des Regelaufrufs zurück.
--	---------------------------------------

**NEU:****A\_24573-04 - ePA-Aktensystem - Regeln des Befugnisverifikations-Moduls**

[https://gemspec.gematik.de/docs/gemSpec/gemSpec\\_Aktensystem\\_ePAfueralle/latest/#A\\_24573-02](https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest/#A_24573-02)

Das Befugnisverifikations-Modul MUSS die in den Tabellen *Tab\_AS\_Entitlement\_Registration\_Rules* und *Tab\_AS\_SDS-Key\_Rules* definierten Regeln umsetzen. [**<=**]

Tabelle 4: *Tab\_AS\_Entitlement\_Registration\_Rules* - Regeln zur Registrierung von Befugnissen

rr3	<p>Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das <b>Stecken der eGK in einer Leistungserbringumgebung</b> ergeben.</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>VSDM-Prüfziffer in Version 1 oder 2 des VSDM-Prüfungsnachweises signiert mit AUT-Identität der SMC-B</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>Befugnis = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC</li> <li>falls VSDM-Prüfziffer in Version 2, zusätzlich die innere Struktur der Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR)</li> </ul> <p><b>Prüfschritte:</b></p> <p>Prüfen, ob die übergebene VSDM-Prüfziffer eine Version 1 oder Version 2 ist: Führe für die VSDM-Prüfziffer die Prüfschritte 1. und 2. gemäß A_27279-* durch. Es ergibt sich die dekodierte VSD-Prüfziffer, an der man am Most-significant-Bit erkennt, ob es sich um Version 1 oder Version 2 der Prüfziffer handelt.</p> <p><u>Szenario VSDM-Prüfziffer in Version 1:</u></p> <ol style="list-style-type: none"> <li>prüfen der SMC-B-Signatur der signierten VSDM-Prüfziffer gemäß A_25042-* (C.HCI.AUT)</li> <li>prüfen, dass das JWT gemäß A_24590-* zeitlich gültig ist (<math>iat - 15s \leq \text{aktuelle Zeit} \leq exp + 15s</math>) Hinweis: ein im JWT evtl. vorhandener iat-Wert bzw. exp-Wert wird ignoriert.</li> <li>prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer nicht länger als 20 Minuten zurückliegt mit <math>pruefziffer.timestamp - 30s \leq \text{aktuelle Zeit} &lt; pruefziffer.timestamp + 20 \text{ Minuten} + 15s</math>)</li> <li>prüfen des HMAC der VSDM-Prüfziffer mittels VAU-HSM Regel hsm-r3             <ol style="list-style-type: none"> <li>Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>Falls die Prüfungen in 1) bis 4) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt:</li> </ol>
-----	--

- Aktenkonto: die KVNR aus dem VSDM-Prüfziffer
  - Telematik-ID: die Telematik-ID aus der SMC-B-Signatur
  - Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur.
6. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis
    - a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
  7. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis als Ergebnis des Regelaufrufs zurück.

#### Szenario VSDM-Prüfziffer in Version 2:

1. prüfen der SMC-B-Signatur der signierten VSDM-Prüfziffer gemäß A\_25042-\* (C.HCI.AUT)
2. Hinweis: ein im JWT evtl. vorhandener iat-Wert bzw. exp-Wert wird ignoriert.
3. Aufruf von VAU-HSM Regel hsm-r3 mit der dekodierten VSDM-Prüfziffer
  - a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
4. prüfen der inneren Struktur nach Prüfschritt 6 gemäß A\_27279-\* (d.h. eGK ist nicht gesperrt)
5. prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer (prüfziffer.iat) nicht länger als 20 Minuten zurückliegt ( $\text{prüfziffer.iat} - 30s \leq \text{aktuelle Zeit} < \text{prüfziffer.iat} + 20 \text{ Minuten} + 15s$ , Hinweis in der Prüfziffer gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben)
6. prüfen des prüfziffer.hcv nach Prüfschritt 8 gemäß A\_27279-\* bzgl. des hcv im JWT
7. Falls die Prüfungen in 1) bis 6) erfolgreich waren, und die VAU-HSM Regel hsm-r3 den Klartext der inneren Struktur der Prüfziffer zurückgeliefert hat, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt:
  - Aktenkonto: KVNR, die als Ergebnis der VAU-HSM Regel hsm-r3 zurückgeliefert wird
  - Telematik-ID: die Telematik-ID aus der SMC-B-Signatur
  - Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur.
8. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis
  - a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
9. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis sowie die entschlüsselte innere Struktur der Prüfziffer im Klartext gemäß A\_27278-\* als Ergebnis des Regelaufrufs zurück.

### 3.2.3 Änderungen in Abschnitt 3.9.2.2

#### **A\_27288 - Entitlement Management - Abgleich der KVNR bei Erstellen einer Befugnis über VSDM-Prüfziffer**

Das Entitlement Management MUSS sicherstellen, dass für die in setEntitlementPs vom Primärsystem in x-insurantid übergebene KVNR und die übergebene Befugnis (signiertes JWT) folgendes gilt: die KVNR in x-insurantid stimmt mit der KVNR überein, die in der CMAC-gesicherten Befugnis enthalten ist, die als Ergebnis des Aufrufs der Regel rr3 mit der vom Primärsystem erhaltenen Befugnis (signiertes JWT) vom HSM zurückgegeben wird.

[<=, Aktensystem\_ePA, Sich.techn. Eignung: Produktgutachten]

*Neue Anforderungen in Kapitel 3.9.2.2 „Befugnisvergabe durch ein Primärsystem“:*

#### **A\_27321 - Entitlement Management - Abgleich hcv bei Erstellen einer Befugnis über VSDM-Prüfziffer in Version 2**

Falls vom Primärsystem in setEntitlementPs eine Befugnis (signiertes JWT) mit einer Prüfziffer in Version 2 übergeben wird und das Ergebnis des Aufrufs der Regel rr3 eine interne Datenstruktur der VSDM-Prüfziffer zurückliefert, MUSS das Entitlement Management sicherstellen, dass

- bei einem JWT mit Attribut "hcv" der Wert von "hcv" mit dem Wert von hcv aus der VSDM-Prüfziffer übereinstimmt und ansonsten die Operation setEntitlementPs abbricht,
- bei einem JWT ohne Attribut "hcv" die Operation setEntitlementPs abbricht, falls der Konfigurationsparameter enforce\_hcv\_check (vgl. A\_27342-\*) auf true gesetzt ist.

[<=, Aktensystem\_ePA, Sich.techn. Eignung: Produktgutachten]

#### **A\_27289 - Entitlement Management - Maximale Anzahl fehlerhafter Abgleiche der KVNR bei Erstellen einer Befugnis über VSDM-Prüfziffer**

Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer Stunde maximal fünfmal eine Befugnis (signiertes JWT) über setEntitlementPs übermitteln kann, bei der die mitgelieferte KVNR in x-insurantId von der KVNR abweicht, die in der Prüfziffer der übermittelten Befugnis (signiertes JWT) enthalten ist, andernfalls für den Nutzer für diesen Zeitraum die Operation setEntitlementPs abbrechen. [<=, Aktensystem\_ePA, Sich.techn. Eignung: Produktgutachten]

#### **A\_27322 - Entitlement Management - Maximale Anzahl fehlerhafter Abgleiche der VSD-Update-Zeit bei Erstellen einer Befugnis über VSDM-Prüfziffer in Version 2**

Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer Stunde maximal fünfmal eine Befugnis (signiertes JWT) mit einer Prüfziffer in Version 2 über setEntitlementPs übermitteln kann, bei der die Operation setEntitlementPs gemäß A\_27321-\* abbricht. [<=, Aktensystem\_ePA, Sich.techn. Eignung: Produktgutachten]

#### **A\_24590-02 - Entitlement Management - Befugnis durch ein Primärsystem**

Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ein Primärsystem über die Schnittstelle I\_Entitlement\_Management durch Verwendung eines gültig signierten JWT mit den dargestellten Mindest-Inhalten erfolgt:



Befugnis	Claim Name	Claim
Protected Header		
	"typ"	"JWT"
	"alg"	"ES256" oder "PS256"
	"x5c"	Signaturzertifikat C.HCI.AUT
Payload		
	"iat"	Zeitstempel Ausgabezeitpunkt
	"exp"	Verfalldatum, = "iat" + 20 min
	"auditEvidence"	VSDM-Prüfziffer aus dem VSDM-Prüfungsnachweis, base64-kodiert.
	"hcv"	optional solange enforce_hcv_check = FALSE; Hash check value der als Ergebnis der Operation ReadVSD gemäß A_27352-* berechnet wird. Der berechnete hcv-Wert MUSS base64 kodiert werden.

【<=, Aktensystem\_ePA, PS\_ePA\_Apotheke, PS\_ePA, funkt. Eignung:  
Konformitätsbestätigung, funkt. Eignung: Test Produkt/FA】



---

## 4 Änderung in gemILF\_PS\_ePA

---

### A\_27402 - Kodierung der Daten zur Berechnung von hcv

Das PS MUSS bei der Erstellung einer Befugnis den hcv gemäß A\_27352 ermitteln und dabei sicherstellen, dass VB und SAS aus ReadVSDResponse ohne Änderung und Umkodierung für die Erzeugung des hcv verwendet werden. [≤, PS\_ePA, funkt. Eignung: Konformitätsbestätigung]

#### Änderung in Kapitel 3.9.1 Umsetzung:

Die Aktivitäten des Anwendungsfalles *Erstellen einer Befugnis* sind:

#### Vorbedingung:

- Ermittelter Service-Endpunkt zum Aktenkonto
- erfolgreiches ReadVSD mit Online-Prüfung

#### Auslöser:

- Erhalt einer Prüfziffer durch Lesen der eGK mit erfolgreicher Online-Prüfung (Prüfnachweis 1 oder 2)
- manuelle Auslösung
- Nachfrage bei uploadpflichtigen PVS-Aktionen und fehlender Befugnis

#### Aktivitäten:

- Auswahl KVNR
- Auswahl des Service-Endpunkts zum Aktenkonto
- Auswahl der Prüfziffer des Versicherten
- Bildung des Hash Check Value (hcv) gemäß A\_27352: Die Werte für die Berechnung des hcv-Wertes werden aus UC\_AllgemeineVersicherungsdatenXML.Versicherter.Versicherungsschutz.Beginn (VB) und UC\_PersoentlicheVersichertendatenXML.Versicherter.Person.StrassenAdresse.Strasse (SAS) der ReadVSDResponse entnommen. Die Daten sind dort in der Zeichenkodierung ISO-8859-15 (Latin 9) kodiert. Diese Kodierung ist auch bei der Berechnung des hcv-Wertes zu verwenden.
- Bildung eines JWS mit Prüfziffer und Zertifikat
- JWS signieren mit SMC-B
- JWS als Entitlement einstellen
- Auswertung des Ergebnisses

#### Resultat:

...

#### neue Anforderung in Kapitel 3.9.2 Nutzung:

Hinweis:

Die Versicherten-Daten werden nach Spezifikation VSDM [gemSpec\_eGK\_Fach\_VSDM], in ISO-8859-15 (Latin-9) vom eGK-Personalisierer und vom VSDM-FD kodiert eingebracht. Der verwendete Zeichensatz für die fachlichen Inhalte ist ISO8859-15.

---

## 5 Änderung in gemSpec\_FD\_eRp

---

### 5.1 Änderung in "6.1.1 HTTP-Operation GET"

alt:

#### **A\_25208 - E-Rezept-Fachdienst - Rezepte lesen - Apotheke - VSDM - PN3 - URL kvnr**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task mit den URL-Parameter pnw="..." durch eine abgebende LEI, falls das Ergebnis im VSDM Prüfungsnachweis gleich 3 ist, prüfen, ob ein URL-Parameter kvnr="..." übermittelt wurde und bei fehlerhafter Prüfung mit dem Fehler 455 abbrechen. [≤, eRp\_FD, funkt. Eignung: Test Produkt/FA]

neu:

#### **A\_25208-01 - E-Rezept-Fachdienst - Rezepte lesen - Apotheke - VSDM - URL kvnr**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task mit den URL-Parameter pnw="..." durch eine abgebende LEI prüfen, ob ein URL-Parameter kvnr="..." übermittelt wurde und bei fehlerhafter Prüfung mit dem Fehler 455 abbrechen. [≤, eRp\_FD, funkt. Eignung: Test Produkt/FA]

neu:

#### **A\_27346 - E-Rezept-Fachdienst - Rezepte lesen - Apotheke - VSDM - URL hcv**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task mit den URL-Parameter pnw="..." durch eine abgebende LEI prüfen, falls `force_hcv_check = TRUE`, ob ein URL-Parameter hcv="..." übermittelt wurde und bei fehlerhafter Prüfung mit dem Fehler 457 abbrechen. [≤, eRp\_FD, funkt. Eignung: Test Produkt/FA]

alt:

#### **A\_23450 - E-Rezept-Fachdienst - Rezepte lesen - Apotheke - VSDM - Prüfung Prüfungsnachweis**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task mit den URL-Parametern pnw="..." durch eine abgebende LEI, den im Parameter pnw übermittelten Prüfungsnachweis extrahieren, prüfen und bei Fehlen oder fehlerhafter Prüfung mit dem Fehler 403 abbrechen, damit nur Clients die Operation aufrufen können, welche einen Anwesenheitsnachweis erfolgreich durchgeführt haben. [≤, eRp\_FD, funkt. Eignung: Test Produkt/FA]

neu:

#### **A\_23450-01 - E-Rezept-Fachdienst - Rezepte lesen - Apotheke - VSDM - Prüfung Prüfungsnachweis**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task mit den URL-Parametern pnw="..." durch eine abgebende LEI, den im Parameter pnw übermittelten Prüfungsnachweis extrahieren, die Version der Prüfziffer bestimmen, den Prüfungsnachweis prüfen und bei Fehlen oder fehlerhafter Prüfung mit dem Fehler 403 abbrechen, damit nur Clients die Operation aufrufen können, welche einen

Anwesenheitsnachweis erfolgreich durchgeführt haben. [≤, eRp\_FD, funkt. Eignung: Test Produkt/FA]

Die Version der Prüfziffer wird aus der Struktur der Prüfziffer abgeleitet.

In der Version 1 beginnt die Prüfziffer mit einem Großbuchstaben. Die Prüfung des Prüfungsnachweises für Prüfziffer Version 1 ist in Kapitel "HTTP-Operation GET - Prüfung VSDM Prüfungsnachweis (Version 1)" beschrieben.

In der Version 2 ist das erste Byte der Prüfziffer > 128. Die Prüfung des Prüfungsnachweises für Prüfziffer Version 2 ist in Kapitel "HTTP-Operation GET - Prüfung VSDM Prüfungsnachweis (Version 2)" beschrieben.

neu:

#### **A\_27287 - E-Rezept-Fachdienst - Rezepte lesen - Apotheke - VSDM - Vergleich KVNR**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task mit den URL-Parameter pnw="..." durch eine abgebende LEI prüfen, ob die in der Prüfziffer übermittelte KVNR identisch ist mit dem Wert im URL-Parameter kvnr="..." und bei Ungleichheit mit dem Fehler 456 abbrechen. [≤, eRp\_FD, funkt. Eignung: Test Produkt/FA]

#### **A\_27347 - E-Rezept-Fachdienst - Rezepte lesen - Apotheke - VSDM - Vergleich hcv**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task mit den URL-Parameter pnw="..." durch eine abgebende LEI prüfen, falls im Operationsaufruf der URL-Parameter hcv übermittelt wurde, den im URL-Parameter übermittelten Wert transformieren, miteinander vergleichen und bei Ungleichheit mit dem Fehler 458 abbrechen. [≤, eRp\_FD, funkt. Eignung: Test Produkt/FA]

Die Kodierung und das Format den in der Prüfziffer übermittelten Wert für hcv ist in A\_27278-\* beschrieben. Das Primärsystem übermittelt hcv Base64URLSafe-kodiert.

## **5.2 Neues Kapitel "HTTP-Operation GET - Prüfung VSDM Prüfungsnachweis (Version 2)"**

Der VSDM Prüfungsnachweis wird URL-codiert übertragen.

Das Informationsmodell des VSDM Prüfungsnachweises ist in [gemSysL\_VSDM] beschrieben.

Die Struktur der VSDM Prüfziffer Version 2 ist in [gemSpec\_Krypt#A\_27278-\* VSDM-FD: Struktur einer Prüfziffer der Version 2] beschrieben.

#### **A\_27301 - E-Rezept-Fachdienst - Prüfung und Entschlüsselung Prüfziffer Version 2**

Der E-Rezept-Fachdienst MUSS eine Prüfziffer Version 2 gemäß [gemSpec\_Krypt#A\_27279-\*] entschlüsseln und prüfen. [≤, eRp\_FD, Sich.techn. Eignung: Produktgutachten]

Hinweis: Der Abgleich der erfolgreich entschlüsselten KVNR mit der vom Client gesendeten KVNR erfolgt in A\_27287-\*. Der Abgleich des erfolgreich entschlüsselten Hashwert hcv mit der vom Client übermittelten hcv erfolgt in A\_27347-\*.

## 6 Änderung in gemILF\_PS\_eRP

### 6.1 Änderung in 5.3.1 E-Rezepte von einem Versicherten abrufen

alt:

#### **A\_23448 - PS abgebende LEI: E-Rezepte von Versicherten abrufen (VSDM)**

Das PS der abgebenden LEI MUSS den Anwendungsfall "E-Rezepte eines Versicherten durch Abgebenden abrufen" gemäß TAB\_ILFERP\_020 umsetzen.

**Tabelle 5 : TAB\_ILFERP\_020 - E-Rezepte von Versicherten abrufen (VSDM)**

Name	E-Rezepte von Versicherten abrufen (VSDM)
Auslöser	<ul style="list-style-type: none"> <li>Aufruf des Anwendungsfalls in der GUI</li> </ul>
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none"> <li>Der eGK des Versicherten ist im eHealth-Kartenterminal gesteckt.</li> <li>Die LEI hat sich gegenüber der TI authentisiert.</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>Es steht eine Liste von Informationen mit Task-ID und zugehörigen AccessCode zu einlösbaren E-Rezepten des Versicherten für die Weiterverarbeitung zu Verfügung.</li> </ul>
Standardablauf	<ol style="list-style-type: none"> <li>VSD der eGK lesen</li> <li>VSDM Prüfungsnachweis ermitteln</li> <li>E-Rezepte abrufen</li> </ol>

【<=, PS\_E-Rezept\_abgebend, funkt. Eignung: Konformitätsbestätigung】

neu:

#### **A\_23448-01 - PS abgebende LEI: E-Rezepte von Versicherten abrufen (VSDM)**

Das PS der abgebenden LEI MUSS den Anwendungsfall "E-Rezepte eines Versicherten durch Abgebenden abrufen" gemäß TAB\_ILFERP\_020 umsetzen.

**Tabelle 6 : TAB\_ILFERP\_020 - E-Rezepte von Versicherten abrufen (VSDM)**

Name	E-Rezepte von Versicherten abrufen (VSDM)
Auslöser	<ul style="list-style-type: none"> <li>Aufruf des Anwendungsfalls in der GUI</li> </ul>
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none"> <li>Der eGK des Versicherten ist im eHealth-Kartenterminal gesteckt.</li> </ul>

	<ul style="list-style-type: none"> <li>Die LEI hat sich gegenüber der TI authentisiert.</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>Es steht eine Liste von Informationen mit Task-ID und zugehörigen AccessCode zu einlösbaren E-Rezepten des Versicherten für die Weiterverarbeitung zu Verfügung.</li> </ul>
Standardablauf	<ol style="list-style-type: none"> <li>VSD der eGK lesen</li> <li>VSDM Prüfungsnachweis ermitteln</li> <li>Hashwert hcv ermitteln</li> <li>E-Rezepte abrufen</li> </ol>

【<=, PS\_E-Rezept\_abgebend, funkt. Eignung: Konformitätsbestätigung】

Der Prüfungsnachweis wird aus dem ReadVSD Response entnommen, URL-kodiert und in den Aufruf des E-Rezept-Fachdienstes übernommen.

Die Werte für den Hashwert hcv werden aus  
 UC\_PersoeneleVersichertendatenXML.Versicherter.Person.StrassenAdresse.Strasse  
 und UC\_AllgemeineVersicherungsdatenXML.Versicherter.Versicherungsschutz.Beginn entnommen. Der Hashwert hcv wird Base64URLSafe-kodiert und in den Aufruf des E-Rezept-Fachdienstes übernommen.

Die Versicherten-ID kann aus  
 UC\_PersoeneleVersichertendatenXML.Versicherter.Versicherten\_ID ermittelt werden.

neu:

#### **A\_27354 - PS abgebende LEI: E-Rezepte von Versicherten abrufen - Hashwert hcv erzeugen**

Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezepte von Versicherten abrufen" den Hashwert hcv erzeugen.【<=, PS\_E-Rezept\_abgebend, funkt. Eignung: Konformitätsbestätigung】

Die Bildungsvorschrift für den Hashwert hcv ist in [gemSpec\_Krypt#A\_27352-\*] beschrieben.

#### **A\_27355 - PS abgebende LEI: E-Rezepte von Versicherten abrufen - Hashwert hcv Base64URLSafe kodieren**

Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezepte von Versicherten abrufen" den Hashwert hcv Base64URLSafe kodieren.【<=, PS\_E-Rezept\_abgebend, funkt. Eignung: Konformitätsbestätigung】

Die Vorschrift zum Kodieren ist in <https://www.educative.io/answers/what-is-base64urlsafeb64encodes-in-python> beschrieben.

alt:

#### **A\_23449-01 - PS abgebende LEI: E-Rezepte von Versicherten abrufen - E-Rezepte abrufen**

Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezepte von Versicherten abrufen" die HTTP-OperationGET /Task mit

- ACCESS\_TOKEN im Authorization-Header
- base64- und URL-codierter Prüfungsnachweis in URL-Parameter pnw

- Versicherten-ID in URL-Parameter kvnr

ausführen.【<=, PS\_E-Rezept\_abgebend, funkt. Eignung: Konformitätsbestätigung】  
neu:

**A\_23449-02 - PS abgebende LEI: E-Rezepte von Versicherten abrufen - E-Rezepte abrufen**

Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezepte von Versicherten abrufen" die HTTP-OperationGET /Task mit

- ACCESS\_TOKEN im Authorization-Header
- base64- und URL-codierter Prüfungsnachweis in URL-Parameter pnw
- Versicherten-ID in URL-Parameter kvnr
- Base64URLSafe-kodierter Hashwert hcv in URL-Parameter hcv

ausführen.【<=, PS\_E-Rezept\_abgebend, funkt. Eignung: Konformitätsbestätigung】

## 7 Änderungen an I\_Entitlement\_Management.yaml

*Wenn enforce\_hcv\_check == true und hcv im JWT ist nicht enthalten, dann wird die Operation mit Fehler 409 hcvMissing abgebrochen.*

*Wenn hcv aus JWT nicht identisch ist zu hcv aus HSM rule rr3, dann wird die Operation mit Fehler 403 invalidToken abgebrochen.*

*Wenn die Anzahl fehlerhafter hcv Prüfungen und KVNR-Prüfungen die Zahl 5 übersteigt, dann wird die Operation mit Fehler 423 locked abgebrochen.*

1. description in EntitlementRequestType für neues JWT wird angepasst

2. Beispiel in EntitlementRequestType für neues JWT wird angepasst

3. Weitere Anpassungen:

**\*\*Provider\*\*:**</br>

This operation does not require an existing entitlement for the requesting user. Instead, an entitlement for this user shall be the result of this operation.

The lack of an existing entitlement for this operation is substituted by verifiable evidence (JWT) associated to the health record owner acting as health record owner's explicit permission for the requesting user to establish a new entitlement.

The operation shall count the number of failed comparison check of `_hcv_` values and also `_kvnr_` for each user (telematik-id). In case of more than 5 failed comparison checks (5 checks for each counter) within 1 hour the operation shall be aborted.

...

The completed entitlement shall NOT be stored and cause operation abortion in cases:

- `_oid_` is not in the list of allowed usergroups (role)
- `_actorId_` is referenced by a Blocked User Policy assignment
- if `enforce_hcv_check == true` or `_hcv_` value of JWT and `_hcv_` from hsm rule `_rr3_` are both available:
  - `_hcv_` value of JWT does not match `_hcv_` from hsm rule `_rr3_`
  - `_x-insurantid_` does not match `_kvnr_` from hsm rule `_rr3_`

Conditions	Status code	Error code	Remarks
...			

...

HSM Token verification failed	403	invalidToken	
-------------------------------	-----	--------------	--

...

hcv value of jwt does not exist	409	hcvMissing	
---------------------------------	-----	------------	--

to many failed attempts	423	locked	_hcv_ check limit
to many failed attempts	423	locked	_kvn_ check limit