

---

## C\_12235\_Anlage

---

# Inhaltsverzeichnis

<b>1 Änderungsbeschreibung.....</b>	<b>2</b>
<b>2 Änderung in gemSpec_Aktensystem_ePAfueralle.....</b>	<b>3</b>
<b>2.1 Änderung in Abschnitt 3.3. "Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM".....</b>	<b>3</b>
<b>2.2 Änderung in Abschnitt 3.4.2 Regeln des Befugnisverifikations-Moduls.....</b>	<b>6</b>
<b>2.3 Änderung in Abschnitt 3.9 Entitlement Management.....</b>	<b>9</b>
2.3.1 Änderung in Abschnitt 3.9.2.2 Befugnisvergabe durch ein Primärsystem.....	9

---

## 1 Änderungsbeschreibung

---

Das ePA-Aktensystem wird befähigt, PoPP-Token bei der Registrierung von Befugnissen über das PS zu akzeptieren und zu verarbeiten.

---

## 2 Änderung in gemSpec\_Aktensystem\_ePAfueralle

---

### 2.1 Änderung in Abschnitt 3.3. "Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM"

#### **A\_24611-06 - 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 professionOID oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- Zertifikat C.ZD.SIG mit professionOID oid\_popp-token für die Token-Signatur-Identität des PoPP-Services
- 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).

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

#### **A\_24612-05 - 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 professionOID oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- Zertifikat C.ZD.SIG mit professionOID oid\_popp-token für die Token-Signatur-Identität des PoPP-Services
- 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).

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

#### **A\_24614-05 - 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 professionOID oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- Zertifikat C.ZD.SIG mit professionOID oid\_popp-token für die Token-Signatur-Identität des PoPP-Services
- 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).

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

Beim Einbringen der Hashwertrepräsentation der erlaubten VAU-Software ins VAU-HSM prüft die von der gematik benannte Person, dass die Hashwertrepräsentation des VAU-Images zuvor vom Hersteller des ePA-Aktensystems an die gematik übermittelt wurde und zulässig für den Produktivbetrieb ist.

Die von der gematik benannte Person prüft, dass das Zertifikat für die Token-Signatur-Identität des PoPP-Services gültig ist und die geforderten Inhalte enthält (Zertifikatsprofil oid\_zd\_sig (OID 1.2.276.0.76.4.287, "C.ZD.SIG"), technische Rolle oid\_popp-token (OID 1.2.276.0.76.4.320)).

#### **A\_24618-05 - 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 professionOID oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Zertifikat C.ZD.SIG mit professionOID oid\_popp-token für die Token-Signatur-Identität des PoPP-Services
- 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.

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

## 2.2 Änderung in Abschnitt 3.4.2 Regeln des Befugnisverifikations-Moduls

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

Das Befugnisverifikations-Modul MUSS die in den Tabellen *Tab\_AS\_Entitlement\_Registration\_Rules* und *Tab\_AS\_SDS-Key\_Rules* definierten Regeln umsetzen. [≤, Aktensystem\_ePA, Sich.techn. Eignung: Produktgutachten]

**Tabelle 1: Tab\_AS\_Entitlement\_Registration\_Rules - Regeln zur Registrierung von Befugnissen**

rr3	<p>Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das Stecken der eGK in einer Leistungserbringenumgebung 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 signiert mit AUT-Identität der SMC-B oder signiertes PoPP-Token</li> <li>falls PoPP-Token übergeben wird: ID-Token oder HSM-ID-Token gesichert mit CMAC</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>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>\text{prüfziffer.timestamp} - 30s \leq \text{aktuelle Zeit} &lt; \text{prüfziffer.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</li> </ol>

Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt:

- 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:

Falls `enforce_popp_only = true`, dann FAIL, ansonsten führe die folgenden Prüfschritte durch:

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

#### Szenario PoPP-Token:

1. prüfen des ID-Tokens gemäß A\_24690-\* (Zertifikatsprofil C.FD.SIG)
  - a. prüfen, ob die professionOID im Signaturzertifikat oid\_idpd ist  
oder prüfen des HSM-ID-Tokens
  - b. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und HSM-ID-Token und Vergleich des Rückgabewerts mit dem CMAC des übergebenen HSM-ID-Tokens
    - i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
  - c. prüfen, ob die professionOID im HSM-ID-Token oid\_idpd ist
2. prüfen des PoPP-Tokens via TI-PKI gemäß Abschnitt "PoPP-Token Prüfung" in [gemSpec\_PoPP\_Service], wobei im HSM bis auf den OCSP-Sperrstatus keine Prüfung des Signaturzertifikats des PoPP-Tokens erfolgt, da das Signaturzertifikat kontrolliert im 4-Augenprinzip in das HSM eingebracht wird. Da das in das HSM eingebrachte TI-PKI-Signaturzertifikat genutzt wird, ist auch kein Bezug und keine Verarbeitung von Entity Statements im HSM erforderlich. Der Claim iss im PoPP-Token muss nicht geprüft werden.
3. prüfen, dass der Ausstellungszeitpunkt des PoPP-Tokens (PoPP-Token.iat) nicht länger als 20 Minuten zurückliegt ( $\text{PoPP-Token.iat} - 30s \leq \text{aktuelle Zeit} < \text{PoPP-Token.iat} + 20 \text{ Minuten} + 15s$ , Hinweis: im der PoPP-Token gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben)
4. prüfen, dass die Telematik-ID aus PoPP-Token.actorID gleich der Telematik-ID im ID-Token bzw. HSM-ID-Token ist
5. Falls die Prüfungen in 1) bis 4) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt:
  - Aktenkonto: KVN-R aus PoPP-Token.patientId
  - Telematik-ID: Telematik-ID aus PoPP-Token.actorID
  - Gültigkeitszeitraum: ergibt sich aus PoPP-Token.actorProfessionOid.
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 zurück.

## 2.3 Änderung in Abschnitt 3.9 Entitlement Management

*Es wird folgende Anforderung ergänzt:*



**A\_27671 - Entitlement Management - PoPP-Token kann höchstens einmal genutzt werden**

Das Entitlement Management MUSS sicherstellen, dass ein PoPP-Token höchstens einmal zur Registrierung einer Befugnis genutzt werden kann.

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

**A\_27681 - Entitlement Management - Konfigurationsvariable enforce\_popp\_only**

Das Entitlement Management MUSS eine Konfigurationsvariable `enforce_popp_only` besitzen, die standardmäßig auf `false` gesetzt ist. [<=, Aktensystem\_ePA, Sich.techn. Eignung: Produktgutachten]

**2.3.1 Änderung in Abschnitt 3.9.2.2 Befugnisvergabe durch ein Primärsystem****A\_27679 - Entitlement Management - Telematik-ID im PoPP-Token ist gleich der Telematik-ID des angemeldeten Nutzers**

Das Entitlement Management MUSS bei der Befugnisvergabe durch ein Primärsystem unter Verwendung eines PoPP-Tokens sicherstellen, dass die Telematik-ID in PoPP-Token.actorID gleich der Telematik-ID des Nutzers der User Session ist.

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