Änderung in gemSpec_Aktensystem_ePA4fueralle

Es werden die Abschnitte 3.3 und 3.4 geändert.

3.2 Health Relocation Service

A_24787-01 - Health Record Relocation Service - Verschlüsselung des Exportpaktes

Der Health Record Relocation Service MUSS sicherstellen, dass Exportpakete ausschließlich verschlüsselt für den Download zu einem anderen Betreiber zur Verfügung stehen. Für die Verschlüsselung MUSS das kryptographische Material des ENC-Zertifikats ~~aus der Anfrage zur Erstellung eines Exportpakets~~ verwendet werden, welches mittels der Regel hsm-r7 vom VAU-HSM abgerufen wurde.

3.2.1.2 Abfrage existierendes Aktenkonto und Anfrage zum Transfer

Das Aktensystem (neu) fragt im Rahmen der Initialisierung des neuen Aktenkontos alle Aktensysteme der weiteren Betreiber an, ob bei diesen ein Aktenkonto für den Versicherten (KVNR) existiert. ~~Schon bei dieser Anfrage an Aktensystem (alt) wird ein ENC-Zertifikat für die Verschlüsselung eines Exportpakets übermittelt.~~ Das Aktensystem (alt), bei welchem das Aktenkonto existiert, bestätigt diese Anfrage zum Transfer mit einer Vorgangs-ID.

Starten des Transfers	
I_Information_Service_Accounts (bisheriges Aktensystem)	
`startRelocation`	~~Übergabe des ENC-Zertifikats,~~ initiieren der Exportpaketerstellung

Existiert bei keinem Anbieter (alt) ein Aktenkonto des Versicherten, ist eine Datenübernahme nicht erforderlich und das Aktenkonto (neu) kann in den Status ACTIVATED überführt und der Transferprozess abgeschlossen werden.

3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen Anbieter

Das Aktensystem (alt) informiert den Anbieter (alt) über die Anfrage zum Transfer ~~und übergibt das ENC-Zertifikat~~ und die Vorgangsnummer. Der Anbieter (alt) öffnet das existierende Aktenkonto des Versicherten und stößt in der VAU die Erzeugung des Exportpakets an. Der Health Record Relocation Service beantwortet diese Anfrage durch Rückgabe einer Url für den späteren Download des Exportpakets durch den neuen Anbieter und startet die Erzeugung des Exportpakets. Das Aktenkonto wird vor der Paketerstellung auf den Status SUSPENDED gesetzt, um weitere Aktivitäten seitens der Nutzer zu verhindern.

Erzeugen des Exportpakets	
I_Health_Record_Relocation_Service_ (bisheriger Anbieter)	
`startPackageCreation`	Starten der Erzeugung des Exportpakets in der VAU

In dieses Exportpaket werden alle Daten des Aktenkontos gemäß A_25005*übernommen. Das fertige Exportpaket wird mittels ENC-Zertifikat, welches im VAU-HSM eingebracht und gespeichert wurde, verschlüsselt und am vorbereiteten Downloadpunkt bereitgestellt.

3.3 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM

A_24611-01 - 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 VAU (genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- Privater Schlüssel der Verschlüsselungsidentität der VAU
- Privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier `oid_epa_vau` für die Verschlüsselungsidentiät des anderen ePA-Aktensystembetreibers
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel
- Symmetrische Schlüssel für HMAC der VSDM-Prüfungsnachweise (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 und ggf. für die Befugnisverifikations-VAU)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

A_24612-02 - 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 VAU
- Privater Schlüssel der Verschlüsselungsidentität der VAU
- Privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier `oid_epa_vau` für die Verschlüsselungsidentiät des anderen ePA-Aktensystembetreibers
- Symmetrische Schlüssel für HMAC der VSDM-Prüfungsnachweise (jeweils einen pro VSD-Dienst-Betreiber)
- Symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)

© gematik – öffentlich_Entwurf

- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU und ggf. für die Befugnisverifikations-VAU)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

A_24614-01 - 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 VAU
- Privater Schlüssel der Verschlüsselungsidentität der VAU
- Privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier `oid_epa_vau` für die Verschlüsselungsidentiät des anderen ePA-Aktensystembetreibers
- Symmetrische Schlüssel für HMAC der VSDM-Prüfungsnachweise (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 und ggf. für die Befugnisverifikations-VAU)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

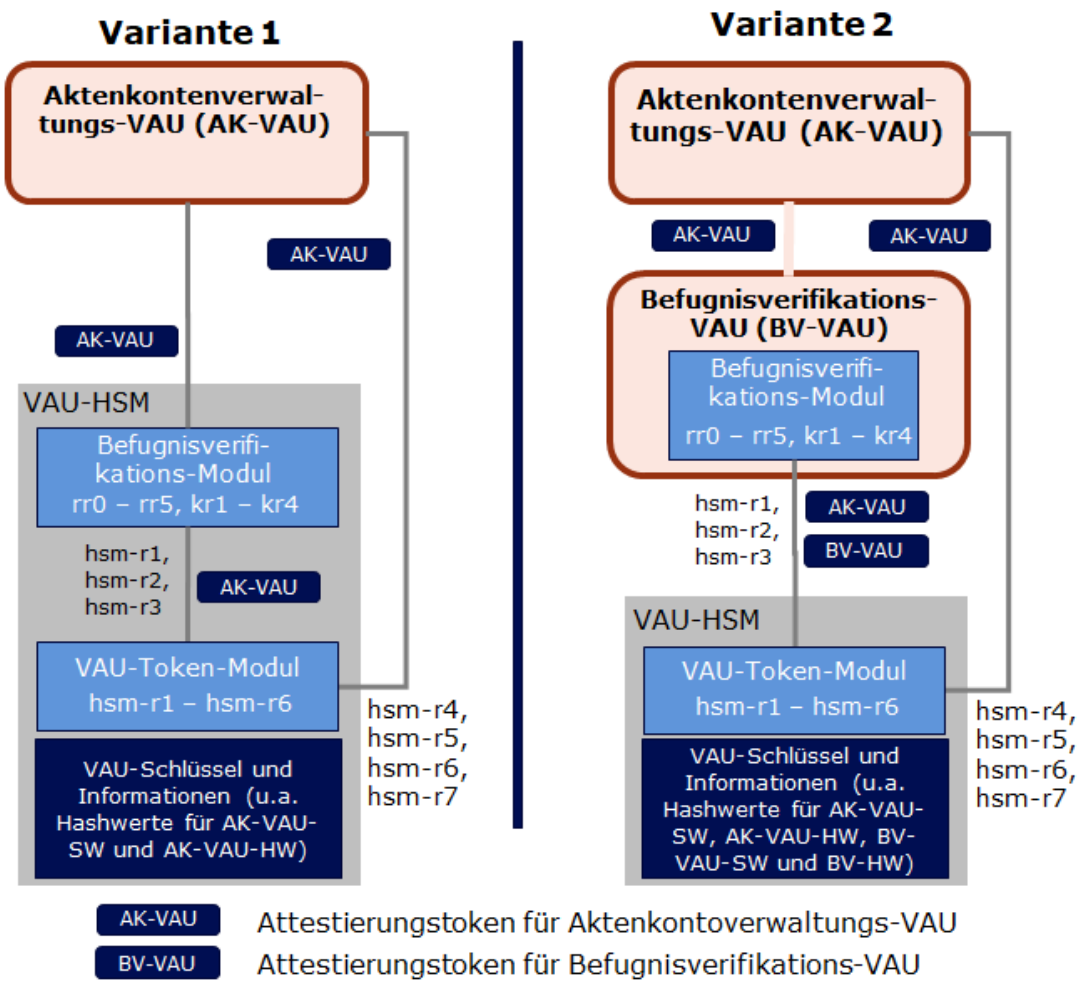
A_24618-01 - ePA-Aktensystem - Zugriff auf Schlüssel und Informationen im VAU-HSM ~~nur über Befugnisverifikations-Modul~~

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 ein Befugnisverifikations-Modul oder eine Aktenkontoverwaltungs-VAU zugegriffen werden kann:

- Privater Schlüssel der Authentisierungsidentität der VAU (genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- Privater Schlüssel der Verschlüsselungsidentität der VAU
- Privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier `oid_epa_vau` für die Verschlüsselungsidentiät des anderen ePA-Aktensystembetreibers
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel
- Symmetrische Schlüssel für HMAC der VSDM-Prüfungsnachweise (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 und ggf. für die Befugnisverifikations-VAU)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

3.4 Befugnisverifikations-Modul

Abbildung 1 wird durch folgende Abbildung ersetzt:



Es wird folgende Anforderung vor A_24574 ergänzt.

A_25281 - ePA-Aktensystem - VAU-Token-Modul ausschließlich im HSM

Das ePA-Aktensystem MUSS sicherstellen, dass ein VAU-Token-Modul ausschließlich in einem VAU-HSM ausgeführt wird. <=

3.4.1 VAU-Token-Modul

A_24712-01 - VAU-Token-Modul nur durch Befugnisverifikations-Modul oder Aktenkontoverwaltungs-VAU aufrufbar

Das ePA-Aktensystem MUSS sicherstellen, dass die Regeln hsm-r1 bis hsm-r3 des VAU-Token-Moduls ausschließlich von einem Befugnisverifikations-Modul und die Regeln hsm-r4 bis hsm-r7 ausschließlich von einer Aktenkontoverwaltungs-VAU aufgerufen werden.

A_25282 - 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 7: Tab_AS_VAU_Token_Modul_Rules - Prüfregeln VAU Token-Modul

Regel	Beschreibung
hsm-r1	*Diese Regel dient zur Sicherung von Befugnissen und HSM-ID-Token mittelsCMAC.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (optional) • Daten ~~Befugnis = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum (opt.))~~ **Ausgangsdaten**: • ~~Befugnis = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum (opt.))~~ Daten gesichert mittels CMAC **Prüfschritte**: 1. prüfen der Signatur(en)des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind Falls die Prüfungen 1) - 3) erfolgreich waren, ~~wird die übergebene Befugnis~~ werden die übergebenen Daten vom VAU-HSM mittels CMAC gesichert.
hsm-r3	*Diese Regel dient zur Nutzung des HMAC bzgl. VSDM-Prüfungsnachweisen* **Eingangsdaten**: • Daten • Bezeichner des HMAC-Schlüssels • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.) **Ausgangsdaten**: • HMAC der Daten mit dem symmetrischen Schlüssel, der zum übergebenen Bezeichner des HMAC-Schlüssels gehört **Prüfschritte**: 1. ~~(opt.)~~ prüfen der ~~Signaturdes VAU-Attestierungstokens für die Befugnisverifikations-VAU~~ Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind

	3. (opt.) prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind Falls die Prüfungen 1) - ~~2~~3) erfolgreich waren, wird der HMAC mit dem gewünschten HMAC-Schlüssel über die Daten gebildet.
hsm-r4	*Diese Regel dient zur Nutzung des privaten Schlüssels der AUT-Identität der VAU* **Eingangsdaten**: • Challenge • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ~~VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.)~~ **Ausgangsdaten**: • Challenge signiert mit privatem Schlüssel der AUT-Identität der VAU **Prüfschritte** 1. prüfen der Signatur~~(en)~~ des ~~(r)~~ VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. ~~ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind~~ Falls die Prüfungen in 1) bis ~~3~~2) erfolgreich waren, wird die übergebene Challenge mit dem privatem Schlüssel der AUT-Identität der VAU signiert.
hsm-r5	*Diese Regel dient zur Nutzung des privaten Schlüssels der ENC-Identität der VAU* **Eingangsdaten**: • verschlüsselte Daten • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ~~VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.)~~ **Ausgangsdaten**: • entschlüsselte Daten **Prüfschritte** 1. prüfen der Signatur~~(en)~~ des ~~(r)~~ VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind

© gematik – öffentlich_Entwurf

	3. ~~ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind~~ Falls die Prüfungen in 1) bis ~~3~~2) erfolgreich waren, werden die übergebenen verschlüsselten Daten mit dem privatem Schlüssel der ENC-Identität der VAU entschlüsselt.
~~hsm-r6~~	~~*Diese Regel dient zur Nutzung des CMAC-Schlüssels*~~ ~~**Eingangsdaten**:~~ • ~~Daten~~ • ~~VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.)~~ ~~**Ausgangsdaten**:~~ • ~~CMAC der Daten mit dem symmetrischen CMAC-Schlüssel~~ ~~**Prüfschritte**:~~ 1. ~~(opt.) prüfen der Signaturdes VAU-Attestierungstokens für die Befugnisverifikations-VAU (herstellerspezifisch)~~ 2. ~~(opt.) prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind~~ ~~Falls die Prüfungen 1) – 2) erfolgreich waren, wird der CMAC über die Daten gebildet.~~
hsm-r6	*Diese Regel dient zur Nutzung des privaten Schlüssels der Signaturidentität der VAU* **Eingangsdaten**: • zu signierende Daten • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU **Ausgangsdaten**: • signierte Daten **Prüfschritte** 1. prüfen der Signaturdes VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen Daten mit dem privatem Schlüssel der Signaturidentität der VAU signiert.
hsm-r7	*Diese Regel dient zum Auslesen des ENC-Zertifikats des anderen Aktensystembetreibers.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU

	Ausgangsdaten: • Verschlüsselungszertifikat C.FD.ENC des anderen Aktensystembetreibers **Prüfschritte**: 1. prüfen der Signaturdes VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind Falls die Prüfungen 1) - 2) erfolgreich waren, wird das ENC-Zertifikat des anderen Aktensystembetreibers zurückgeliefert.

3.4.2 Regeln des Befugnisverifikations-Moduls

Tabelle 8: Überblick über die Regeln des Befugnisverifikations-Moduls

Regel	Kurzbeschreibung	Vollständige Regelspezifikation in
rr0	Mit dieser Regel werden **ID-Token** im Aktensystem regstriert und zu einem HSM-ID-Token konvertiert.	*Tab_AS_Entitlement_Registration_Rules*
rr1	Mit dieser Regel werden vom **Aktenkontoinhaber** am ePA-FdV erstellte **Befugnisse** im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Versicherten mittels Signaturdienst signiert.	*Tab_AS_Entitlement_Registration_Rules*
rr2	Mit dieser Regel werden vom **Vertreter** am ePA-FdV erstellte **Befugnisse** für das Aktenkonto des Versicherten im Aktensystem registriert. Die im ePA-FdV erstellen Befugnisse sind vom Vertreter mittels Signaturdienst signiert.	*Tab_AS_Entitlement_Registration_Rules*
rr3	Mit dieser Regel werden **Befugnisse** im Aktensystem registriert, die sich durch das**Stecken der eGK in einer Leistungserbringerumgebung** ergeben.	*Tab_AS_Entitlement_Registration_Rules*
rr4	Mit dieser Regel werden die **Befugnisse** für den Kostenträger und die zuständige Ombudsstelle bei der **Anlage eines Aktenkontos** im Aktensystem registriert.	*Tab_AS_Entitlement_Registration_Rules*

rr5	Mit dieser Regel werden die **Befugnisse** bei einem **betreiberübergreifenden Anbieterwechsel** im Aktensystem registriert.	*Tab_AS_Entitlement_Registration_Rules*
kr1	Diese Regel wird für die **Anmeldung** des **Aktenkontoinhabers** genutzt.	*Tab_AS_SDS-Key_Rules*
kr2	Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssels genutzt. Sie wird für die **Anmeldung** von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.	*Tab_AS_SDS-Key_Rules*
kr3	Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels genutzt. Sie wird für die **Anmeldung** von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.	*Tab_AS_SDS-Key_Rules*
kr4	Diese Regel wird für die **Anmeldung** des **E-Rezept-Fachdienstes** verwendet.	*Tab_AS_SDS-Key_Rules*
~~autr~~	~~Diese Regel dient zum Nutzen des privaten Schlüssels der AUT-Identität der VAU.~~	~~*Tab_AS_AUT_ENC_Rules*~~
~~encr~~	~~Diese Regel dient zum Nutzen des privaten Schlüssels der ENC-Identität der VAU.~~	~~Tab_AS_AUT_ENC_Rules~~

A_24573-01 - 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* ~~und *Tab_AS_AUT_ENC_Rules*~~ definierten Regeln umsetzen.<=

Tabelle 9: Tab_AS_Entitlement_Registration_Rules - Regeln zur Registrierung von Befugnissen

Regel	Beschreibung
rr0	Mit dieser Regel werden **ID-Token** im Aktensystem regstriert und zu einem HSM-ID-Token konvertiert.

	Eingangsdaten: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token mit NutzerID=x signiert durch einen sektoralen Identity Provider, den IDP-Dienst oder den E-Rezept-Fachdienst **Ausgangsdaten**: • HSM-ID-Token mit NutzerID=x gesichert mittels CMAC **Prüfschritte**: 1. prüfen des ID-Tokens gemäß A_24690-* (C.FD.SIG) bei Token eines IDPs bzw. gemäß A_24658-* bei Token des E-Rezept-Fachdiensts (C.FD.AUT) 2. Falls die Prüfung in 1) erfolgreich war, a. erstellt das Befugnisverifikations-Modul ein HSM-ID-Token mit der NutzerID=x, einer Gültigkeitsdauer von 24 Stunden und der professionOID aus dem Signaturzertifikat (`oid_idpd_sek`, `oid_idpd` oder `oid_erp-vau`). b. ruft das Befugnisverifikations-Modul die VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und dem HSM-ID-Token auf. i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert das mittels CMAC gesicherte HSM-ID-Token als Ergebnis des Regelaufrufs zurück.
rr1	*Mit dieser Regel werden vom **Aktenkontoinhaber** am ePA-FdV erstellte Befugnisse im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Versicherten mittels Signaturdienst signiert.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • Befugnis1 = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum) signiert vom Versicherten **Ausgangsdaten**: • Befugnis2 = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum) gesichert mittels CMAC **Prüfschritte**: 1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) a. ~~prüfen der Signaturgemäß A_25042-* (Zertifikatsprofil C.FD.SIG)~~ b. prüfen, ob die professionOID im Signaturzertifikat `oid_idpd_sek` ist

	c. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt oder prüfen des HSM-ID-Tokens d. 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. e. prüfen, ob die professionOID im HSM-ID-Token `oid_idpd_sek` ist f. prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt. 2. prüfen der Befugnis1 a. prüfen der Signatur gemäß A_25042-* (Zertifikatsprofil C.CH.SIG) b. prüfen, ob die professionOID im Signaturzertifikat `oid_versicherter` ist c. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der "KVNR Aktenkonto" in der Befugnis1 übereinstimmt. d. prüfen, dass das JWT gemäß A_24587-* nicht abgelaufen ist (Feld: `exp`) 3. Falls die Prüfungen in 1) bis 2) erfolgreich waren, erstellt das Befugnisverifikations-Modul die Befugnis2. Die Inhalte werden aus Befugnis1 übernommen. 4. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis2 a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 5. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.
rr2	*Mit dieser Regel werden vom **Vertreter** am ePA-FdV erstellte Befugnisse für das Aktenkonto des Versicherten im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Vertreter mittels Signaturdienst signiert.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • Befugnis1 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) signiert vom Vertreter

- Befugnis2 = (KVNR Aktenkonto, KVNR Vertreter) gesichert mittels CMAC

Ausgangsdaten:

- Befugnis3 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC

Prüfschritte:

1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG)
   a. prüfen, ob die professionOID im Signaturzertifikat `oid_idpd_sek` ist
   b. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt

   oder prüfen des HSM-ID-Tokens

   c. 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.
   d. prüfen, ob die professionOID im HSM-ID-Token `oid_idpd_sek` ist
   e. prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt.
2. Prüfen der Befugnis1 und Befugnis2
   a. prüfen der Signatur von Befugnis1 gemäß A_25042-* (Zertifikatsprofil C.CH.SIG)
   b. prüfen, ob die professionOID im Signaturzertifikat `oid_idpd_sek` ist
   c. prüfen des CMAC von Befugnis2
   d. prüfen, dass die Telematik-ID in Befugnis 1 keine KVNR ist (Vertreter dürfen keine weiteren Vertreter befugen)
   e. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der „KVNR Vertreter" in der Befugnis2 übereinstimmt
   f. prüfen, ob die „KVNR Aktenkonto" in Befugnis 1 mit der „KVNR Aktenkonto" in Befugnis2 übereinstimmt
   g. prüfen, dass das JWT gemäß A_24587-* nicht abgelaufen ist (Feld: `exp`)
3. Falls die Prüfungen in 1) erfolgreich waren, wird die Befungnis3 vom Befugnisverifikations-Modul erstellt. Die Inhalte werden aus Befugnis1 übernommen.
4. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis3

© gematik – öffentlich_Entwurf

	a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 5. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis3 als Ergebnis des Regelaufrufs zurück.
rr3	*Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das**Stecken der eGK in einer Leistungserbringerumgebung** ergeben.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VSDM-Prüfungsnachweis signiert mit AUT-Identität der SMC-B **Ausgangsdaten**: • Befugnis = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC **Prüfschritte**: 1. prüfen der SMC-B-Signatur des signierten VSDM-Prüfungsnachweises gemäß A_25042-* (C.HCI.OSIG) 2. prüfen, dass das JWT gemäß A_24590-* nicht abgelaufen ist (Feld: `exp`) 3. prüfen, dass der Austellungszeitpunkt des VSDM-Prüfungsnachweises nicht länger als 20 Minuten zurückliegt 4. prüfen des HMAC des VSDM-Prüfungsnachweises mittels VAU-HSM Regel hsm-r3 a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 5. Falls die Prüfungen in 1) bis 4) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt: • Aktenkonto: die KVNR aus dem VSDM-Prüfungsnachweis • 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.
rr4	*Mit dieser Regel werden die Befugnisse für den Kostenträger und die zuständige Ombudsstelle bei der **Anlage eines Aktenkontos** im Aktensystem registriert.*

© gematik – öffentlich_Entwurf

	Eingangsdaten: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • Befugnis1 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) signiert mit SMC-B des Kostenträgers bzw. der Ombudsstelle **Ausgangsdaten**: • Befugnis2 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) gesichert mittels CMAC **Prüfschritte**: 1. Prüfen der Befugnis1 a. prüfen der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle gemäß A_25042-* (C.HCI.OSIG) b. prüfen, ob die professionOID im Signaturzertifikat `oid_kostentraeger` bzw. `oid_ombudsstelle` ist c. prüfen, ob die Telematik-ID im Signaturzertifikat C.HCI.OSIG der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle mit der Telematik-ID in der Befugnis1 übereinstimmt 2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 erstellt. Die Inhalte der Befugnis2 sind: • Aktenkonto: die KVNR des Aktenkontos aus Befugnis1 • Telematik-ID: die Telematik-ID aus Befugnis1 3. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 4. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.
rr5	*Mit dieser Regel werden die **Befugnisse** bei einem **betreiberübergreifenden Anbieterwechsel** im Aktensystem registriert.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • Befugnis1 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) signiert vom alten Aktensystembetreiber **Ausgangsdaten**: • Befugnis2 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) gesichert mittels CMAC

	Prüfschritte: 1. Prüfen der Befugnis1 a. prüfen der Signatur gemäß A_25042-* (C.FD.SIG) b. prüfen, ob im Signaturzertifikat C.FD.SIG der policyIdentifier `oid_epa_vau` ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 mit den Inhalten aus Befugnis1 erstellt. 3. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 4. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.

A_24690-01 - ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen des ID-Tokens

Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung eines ID-Tokens durchführen:

- das ID-Token muss gemäß A_25042-* valide signiert sein durch einen sektoralen Identity Provider oder den IDP-Dienst (professionOID ist `oid_idpd_sek` oder `oid_idpd`),
- das ID-Token muss zeitlich gültig sein (Felder: `iat`, `exp`),
- das ID-Token muss im Feld `aud` das ePA-Aktensystem eingetragen haben,
- ~~das Feld `nonce` muss mit der ausgelösten Authentisierungsanfrage übereinstimmen~~.

Tabelle 10: Tab_AS_SDS-Key_Rules Key Rules - Regeln zur Ableitung der versichertenindividuellen Persistierungsschlüssel

Regel	Beschreibung
kr1	*Diese Regel wird für die Anmeldung des **Aktenkontoinhabers** genutzt.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC **Ausgangsdaten**: • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) • versichertenindividueller Befugnispersistierungsschlüssel (Secure Entitlement Storage Key)

	Regelverhalten: 1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) a. ~~prüfen der Signaturgemäß A_25042-* (C.FD.SIG)~~ b. prüfen, ob die professionOID im Signaturzertifikat `oid_idpd_sek` ist oder prüfen des HSM-ID-Tokens c. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. d. prüfen, ob die professionOID im HSM-ID-Token `oid_idpd_sek` ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der KVNR aus dem ID-Token zur Ableitung von Befugnis- und Datenpersistierungsschlüssel aufgerufen. a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert die abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.
kr2	*Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssel genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • KVNR (Aktenkonten-ID) **Ausgangsdaten**: • versichertenindividueller Befugnispersistierungsschlüssel (Secure Entitlement Storage Key) **Prüfschritte**: 1. Aufruf der VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der KVNR aus dem ID-Token zur Ableitung des Befugnispersistierungsschlüssels a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 2. Das Befugnisverifikations-Modul liefert den abgeleiteten Befugnispersistierungschlüssel als Ergebnis des Regelaufrufs zurück.
kr3	*Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels genutzt. Sie wird für die Anmeldung von Nutzern*

verwendet, für die eine Befugnis im Aktensystem registriert wurde.

Eingangsdaten:

- VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU
- ID-Token oder HSM-ID-Token gesichert mit CMAC
- Befugnis = (KVNR Aktenkonto, BefugtenID (TID|KVNR), Gültigkeitszeitraum (opt.)) mit CMAC gesichert

Ausgangsdaten:

- versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key)

Prüfschritte:

1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG)
   a. ~~prüfen der Signaturgemäß A_25042-* (C.FD.SIG)~~

   oder prüfen des HSM-ID-Tokens

   b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung
      i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
2. Prüfen der Befugnis
   a. prüfen des CMAC der Befugnis mittels VAU-HSM Regel hsm-r~~6~~1
      i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
   b. prüfen, ob dieNutzer-ID im ID-Token bzw. im HSM-ID-Token (KVNR oder Telematik-ID) mit der Befugten-ID in der Befugnis übereinstimmt.
   c. prüfen, ob die Befugnis noch gültig ist, falls die Befugnis zeitlich begrenzt ist (d. h. ein Gültigkeitszeitraum in der Befugnis enthalten ist).
3. Falls alle Prüfungen in 1) bis 2) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der KVNR aus dem ID-Token bzw. im HSM-ID-Token zur Ableitung des Datenpersistierungsschlüssels aufgerufen.
   a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
4. Das Befugnisverifikations-Modul liefert den abgeleiteten Datenpersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.

kr4	*Diese Regel wird für die Anmeldung des **E-Rezept-Fachdienstes** verwendet.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • KVNR (Aktenkonten-ID) **Ausgangsdaten**: • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) • ~~versichertenindividueller Befugnispersistierungsschlüssel (Secure Entitlement Storage Key)~~ **Prüfschritte**: 1. Prüfen des ID-Tokens a. prüfen der Signaturgemäß A_25042-* (C.FD.~~SIG~~AUT) b. prüfen, ob die professionOID im ~~Signaturz~~Zertifikat C.FD.AUT gleich `oid_erp-vau` ist c. prüfen des ID-Tokens gemäß A_24658-* oder prüfen des HSM-ID-Tokens d. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. e. prüfen, ob die professionOID im HSM-ID-Token `oid_erp-vau` ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der KVNR aus dem ID-Token bzw. dem HSM-ID-Token zur Ableitung ~~von~~ des ~~Befugnis- und~~ Datenpersistierungsschlüssels aufgerufen. a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert ~~die~~ den abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.

"Tabelle 11: Tab_AS_AUT_ENC_Rules Regeln für den Zugriff auf die privaten AUT- und ENC-Schlüssel der VAU" wird gestrichen.

~~**Tabelle 11: Tab_AS_AUT_ENC_Rules Regeln für den Zugriff auf die privaten AUT- und ENC-Schlüssel der VAU**~~

~~**Regel**~~	~~**Beschreibung**~~

~~autr~~	~~**Eingangsdaten**:~~ • ~~VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU~~ • ~~Challenge~~ ~~**Ausgangsdaten**:~~ • ~~Challenge signiert mit privatem Schlüssel der AUT-Identität der VAU~~ ~~**Prüfschritte**:~~ 1. ~~Aufruf der VAU-HSM-Regel hsm-r4 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der Challenge~~ a. ~~Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.~~ 2. ~~Das Befugnisverifikations-Modul liefert die mit der AUT-Identität signierte Challenge als Ergebnis des Regelaufrufs zurück.~~
~~encr~~	~~**Eingangsdaten**:~~ • ~~VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU~~ • ~~verschlüsselte Daten~~ ~~**Ausgangsdaten**:~~ • ~~entschlüsselte Daten~~ ~~**Prüfschritte**:~~ 1. ~~Aufruf der VAU-HSM-Regel hsm-r5 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und den verschlüsselten Daten~~ a. ~~Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.~~ 2. ~~Das Befugnisverifikations-Modul liefert die mit der ENC-Identität entschlüsselten Daten als Ergebnis des Regelaufrufs zurück.~~

3.15 Zusätzliche Anforderungen an den Authorization Service

Es wird folgende Anforderung ergänzt:

A_25283 - Authorization Service - Konvertieren von ID-Token

Der Authorization Service MUSS sicherstellen, dass für ein nach erfolgreicher Authentifizierung des Nutzers vorliegendes ID-Token mittels Regel rr0 gemäß Tab_AS_Entitlement_Registration_Rules ein HSM-ID-Token erstellt wird, bevor das ID-Token zeitlich ungültig ist. <=