
C_12717_Anlage - ePA für alle: Wechsel des PoPP-Token-Signaturzertifikats im VAU-HSM und PoPP-Token Akzeptanzzeitraum

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_Aktensystem.....	3
2.1 Änderungen in Abschnitt "3.3. Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM".....	3
2.2 Änderungen in Abschnitt "3.4 Befugnisverifikations-Modul".....	7
2.2.1 Änderungen in Abschnitt "3.4.1 VAU-Token-Modul".....	8
2.2.2 Änderungen in Abschnitt "3.4.2 Regeln des Befugnisverifikations-Moduls".....	9

1 Änderungsbeschreibung

Im VAU-HSM ist das Zertifikat für die Token-Signatur-Identität des PoPP-Services hinterlegt. Bei einem Wechsel dieses Zertifikats sollen auch noch zeitlich gültige PoPP-Token vom Aktensystem akzeptiert werden, die auf dem Vorgängerzertifikat basieren. Daher muss im VAU-HSM nicht nur das aktuelle Zertifikat für die Token-Signatur-Identität des PoPP-Services hinterlegt werden, sondern auch das Vorgängerzertifikat. Um das gewünschte Signaturzertifikat des PoPP-Service aus dem HSM auszulesen, wird eine (optionale) HSM Regel hsm-r9 ergänzt.

Das VAU-HSM des ePA-Aktensystems akzeptiert PoPP-Token zur Registrierung von Befugnissen derzeit nur, wenn die Ausstellung des PoPP-Tokens nicht länger als 20 min zurückliegt. Diese Einschränkung ist aus Sicherheitssicht beim PoPP-Token (anders als beim VSDM++-Prüfungsnachweis) nicht notwendig und eine längere Nutzung des PoPP-Tokens kann akzeptiert werden. Dies ermöglicht dann eine Verbesserung der Workflows in der Leistungserbingerumgebung.

2 Änderung in gemSpec_Aktensystem

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

**A_24611-09 - ePA-Aktensystem - Im VAU-HSM gespeicherte Schlüssel und
Informationen für VAU-
Betrieb**[https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/
latest/#A_24611-06](https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest/#A_24611-06)

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
- **Paare (kid, C.ZD.SIG) für die Zertifikate C.ZD.SIG mit professionOID oid_popp-token für die aktuelle Token-Signatur-Identität des PoPP-Services und ggf. die vorherige Token-Signatur-Identität des PoPP-Services. Der Wert kid für ein Zertifikat C.ZD.SIG ergibt sich aus dem JWK-Set, welches der PoPP-Service veröffentlicht.**
- 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).

[<=]

**C_12717_Anlage - ePA für alle: Wechsel des
PoPP-Token-Signaturzertifikats im VAU-HSM
und PoPP-Token Akzeptanzzeitraum**



67

68

69

A_24612-07 - 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_24612-05

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
- **Paare (kid, C.ZD.SIG) für die Zertifikate C.ZD.SIG mit professionOID oid_popp-token für die aktuelle Token-Signatur-Identität des PoPP-Services und ggf. die vorherige Token-Signatur-Identität des PoPP-Services. Der Wert kid für ein Zertifikat C.ZD.SIG ergibt sich aus dem JWK-Set, welches der PoPP-Service veröffentlicht.**
- 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).

[<=]

A_24614-08 - 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_24614-05

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
- **Paare (kid, C.ZD.SIG) für die Zertifikate C.ZD.SIG mit professionOID oid_popp-token für die aktuelle Token-Signatur-Identität des PoPP-Services und ggf. die vorherige Token-Signatur-Identität des PoPP-Services. Der Wert kid für ein Zertifikat C.ZD.SIG ergibt sich aus dem JWK-Set, welches der PoPP-Service veröffentlicht.**
- 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).

[<=]

Um einen unterbrechungsfreien Betrieb des ePA-Aktensystems bei Wechsel des Zertifikats der Token-Signatur-Identität des PoPP-Services zu gewährleisten, sind im VAU-HSM im Normalfall zwei Zertifikate für die Token-Signatur-Identität des PoPP-Services hinterlegt, nämlich das aktuelle und das Vorgängerzertifikat. Wechselt der PoPP-Service das Zertifikat aufgrund einer Kompromittierung, muss das kompromittierte Zertifikat aus dem VAU-HSM gelöscht werden. In diesem Fall ist dann nur ein Zertifikat für den PoPP-Service im VAU-HSM gespeichert.

A_29007 -ePA-Aktensystem - Unverzügliches Löschen eines kompromittierten PoPP-Service-Zertifikats aus dem VAU-HSM

Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass ein kompromittiertes Zertifikat C.ZD.SIG mit professionOID oid_popp-token für die Token-Signatur-Identität des PoPP-Services unverzüglich aus dem VAU-HSM entfernt wird.

[<=,Anb_Aktensystem_ePA,Sich.techn. Eignung: Gutachten (Anbieter)]

A_24618-08 - 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 VAUausschließlich 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 VAUausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- privater Schlüssel der Signaturidentität der VAUausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz

- Zertifikat C.FD.ENC mit professionOID oid_epa_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibersausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- **Paare (kid, C.ZD.SIG) für die Zertifikate C.ZD.SIG mit professionOID oid_popp-token für die aktuelle Token-Signatur-Identität des PoPP-Services und ggf. die vorherige Token-Signatur-Identität des PoPP-Services. Der Wert kid für ein Zertifikat C.ZD.SIG ergibt sich aus dem JWK-Set, welches der PoPP-Service veröffentlicht.**
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüsselausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüsselausschließlich 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.

[<=]

2.2 Änderungen in Abschnitt "3.4 Befugnisverifikations-Modul"

In "Abbildung 1:Alternativen zur Ausführung des Befugnisverifikations-Moduls" wird die neue Regel hsm-r9 mit aufgenommen.

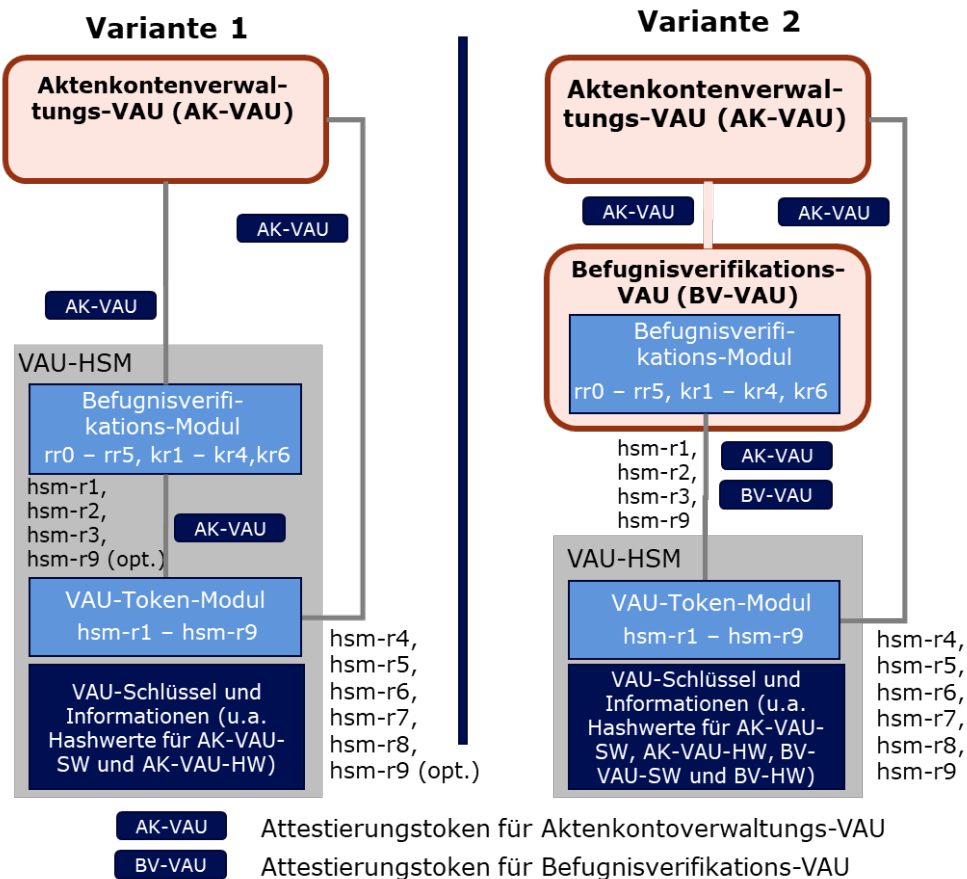


Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls

2.2.1 Änderungen in Abschnitt "3.4.1 VAU-Token-Modul"

In den Regeln für das VAU-Token Modul wird eine neue Regel hsm-r9 zum Auslesen des Signaturzertifikats des PoPP-Services ergänzt.

A_25282-05 - ePA-Aktensystem - Regeln des VAU-Token-Moduls
https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest/#A_25282-04

Das VAU-Token-Modul MUSS die in TabelleTab_AS_VAU-Token-Modul-Rules-05 definierten Regeln umsetzen. [≤]

Tabelle 4: Tab_AS_VAU-Token-Modul-Rules-05 -Prüfregeln VAU Token

Rege l	Beschreibung
hsm- r1	<unverändert>
...	<unverändert>

hsm-r8	<unverändert>
hsm-r9 (opt.)	Diese Regel dient zum Auslesen eines Signatur-Zertifikats des PoPP-Services. Falls Hersteller das Befugnisverifikations-Modul im VAU-HSM umsetzen, kann auf die Regel hsm-r9 verzichtet werden. Eingangsdaten: - VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU - VAU-Attestierungstoken einer Befugnisverifikations-VAU (falls der Regelaufwurf aus einer Befugnisverifikations-VAU heraus erfolgt) - kid Ausgangsdaten: (kid, C.ZD.SIG) mit Signaturzertifikat C.ZD.SIG des PoPP-Services Prüfschritte: - prüfen der Signatur(en)des(r) VAU-Attestierungstoken (herstellerspezifisch) - prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind - ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind - prüfen, ob im VAU-HSM ein Paar (kid, C.ZD.SIG) für den in den Eingangsdaten übergebenen Wertkid gespeichert ist Falls die Prüfungen 1) - 4) erfolgreich waren, wird (kid, C.ZD.SIG) zurückgeliefert.

2.2.2 Änderungen in Abschnitt "3.4.2 Regeln des Befugnisverifikations-Moduls"

A_24573-05 - ePA-Aktensystem - Regeln des Befugnisverifikations-Moduls https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest/#A_24573-04

Das Befugnisverifikations-Modul MUSS die in den Tabellen Tab_AS_Entitlement_Registration_Rules-05 und Tab_AS_SDS-Key_Rules-05 definierten Regeln umsetzen. [$\leq$]

Tabelle 6: Tab_AS_Entitlement_Registration_Rules-05 - Regeln zur Registrierung von Befugnissen

Regel	Beschreibung
rr0	<unverändert>
rr1	<unverändert>
rr2	<unverändert>

rr3	Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das Stecken der eGK in einer Leistungserbringerumgebung oder aufgrund eines PoPP-Tokens ergeben. Eingangsdaten: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VSDM-Prüfziffer in Version 2 signiert mit AUT-Identität der SMC-B oder signiertes PoPP-Token Ausgangsdaten: • Befugnis = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC • falls VSDM-Prüfziffer in Version 2, zusätzlich die innere Struktur der Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) Prüfschritte: <u>Szenario VSDM-Prüfziffer in Version 2:</u> <unverändert> <u>Szenario PoPP-Token:</u> 1. prüfen des PoPP-Tokens via TI-PKI gemäß Abschnitt "PoPP-Token Prüfung" in [gemSpec_PoPP_Service], wobei im HSMbis auf den OCSP-Sperrstatus keine Prüfung des Signaturzertifikats des PoPP-Tokens erfolgt, da das Signaturzertifikat kontrolliert im 4-Augenprinzip in das HSM eingebracht wird. Für die PoPP-Token Prüfung muss ein in das HSM eingebrachtes TI-PKI-Signaturzertifikat genutzt werden. 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.Das benötigte Signaturzertifikat des PoPP-Service kann bei Bedarf mittels Regel hsm-r9 und dem kid-Wert aus dem PoPP-Token-header vom VAU-HSM abgerufen werden. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird der Regel hsm-r9 zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU übergeben. 2. prüfen, dass der Ausstellungszeitpunkt des PoPP-Tokens (PoPP-Token.iat) nicht länger als 20 Minuten 2 Tage zurückliegt (PoPP-Token.iat - 30s <= aktuelle Zeit < PoPP-Token.iat + 20 Minuten 2 Tage + 15s , Hinweis: im PoPP-Token gibt es kein exp, deshalb wird im Vergleich explizit 20-Minuten2 Tage + 15 Sekunden angegeben). 3. prüfen, dass PoPP-Token.proofMethod keine Prüfmethode -* ist. 4. Falls die Prüfungen in 1) bis 3) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt: • Aktenkonto: KVNR aus PoPP-Token.patientId • Telematik-ID: Telematik-ID aus PoPP-Token.actorID • Gültigkeitszeitraum: das Ende der Gültigkeit (validTo) ergibt sich aus PoPP-Token.iat + maxEntitlementValidity, wobei maxEntitlementValidity die in A_23941-* festgelegte Standard-Befugnisdauer für die Rolle in PoPP-Token.actorProfessionOid in
-----	---

	Sekunden ist.ergibt sich aus PoPP-Token.actorProfessionOid ergibt sich aus PoPP-Token.actorProfessionOid 5. 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. 6. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis zurück.
rr4	<unverändert>
rr5	<unverändert>

Der Titel von Tabelle 7 wird geändert. Die Inhalte der Tabelle bleiben unverändert.

Tabelle 7: Tab_AS_SDS-Key_Rules Key Rules-05 - Regeln zur Ableitung der versichertenindividuellen Persistierungsschlüssel