
C_12440_Anlage - E-Rezept-Fachdienst: Entfernen des VAUCertificateOCSPResponse Endpunktes

Inhaltsverzeichnis

1 Änderungsbedarf.....	2
2 Änderungen in gemSpec_Krypt.....	3
3 Änderungen in gemILF_PS_eRp.....	6
4 Änderungen in gemSpec_FD_eRp.....	7
5 Änderungen in gemSpec_Perf.....	10

1 Änderungsbedarf

Primärsysteme sollen im Rahmen des Verbindungsaufbaus zum E-Rezept-Fachdienst die Zertifikatsprüfung des VAU-Zertifikats mittels der Konnektor-Operation VerifyCertificate durchführen (siehe https://gemspec.gematik.de/docs/gemILF/gemILF_PS_eRp/gemILF_PS_eRp_V1.11.0/#5.1.2).

Der E-Rezept-Fachdienst stellt aktuell den Endpunkt GET /VAUCertificateOCSPResponse bereit, der ursprünglich zur Unterstützung der Primärsysteme bei der Validierung des VAU-Zertifikats bei Nutzung eines Konnektors PTV3 gedacht war. (Der Konnektor PTV3 unterstützte noch keine ECC Zertifikate)

Dieser Endpunkt wird nicht mehr benötigt und mit diesem Änderungseintrag aus der Spezifikation entfernt.

Endpunkte für die E-Rezept-FdV Clients zum Beziehen von Zertifikaten für die PKI-Infrastruktur bleiben weiterhin bestehen und sind von dieser Änderung unberührt.

2 Änderungen in gemSpec_Krypt

alt:

A_20160-01 -E-Rezept-VAU, Schlüsselpaar und Zertifikat

Der Fachdienst E-Rezept MUSS folgende Punkte sicherstellen.

1. Die VAU MUSS ein EE-X.509-Zertifikat aus der Komponenten-PKI der TI besitzen (mit Rollenkennung-OID "oid_erp-vau"), das einen ECC-EE-Schlüssel der VAU bestätigt.
2. Die VAU MUSS die Vertraulichkeit des privaten Schlüssels für diese Zertifikat sicherstellen.
3. Die notwendige Sicherung (Backup) und Verteilung dieses privaten Schlüssels MUSS ausschließlich im Mehr-Augen-Prinzip und mit geeigneten Maßnahmen zur Wahrung der Vertraulichkeit des Schlüssels geschehen.
4. Der Fachdienst E-Rezept MUSS das VAU-Zertifikat in seinen Webschnittstellen unter dem Pfad /VAUCertificate (einer URL) durch Clients abrufbar machen. Dieses Zertifikat MUSS DER-kodiert sein.
5. Der Fachdienst E-Rezept MUSS eine maximal 12 Stunden alte OCSP-Response für das VAU-Zertifikat in seinen Webschnittstellen unter dem Pfad /VAUCertificateOCSPResponse für Clients abrufbar machen.

[<=,eRp_FD,Sich.techn. Eignung: Produktgutachten]

neu:

A_20160-03 -E-Rezept-VAU, Schlüsselpaar und Zertifikat

Der Fachdienst E-Rezept MUSS folgende Punkte sicherstellen.

1. Die VAU MUSS ein EE-X.509-Zertifikat aus der Komponenten-PKI der TI besitzen (mit Rollenkennung-OID "oid_erp-vau"), das einen ECC-EE-Schlüssel der VAU bestätigt.
2. Die VAU MUSS die Vertraulichkeit des privaten Schlüssels für diese Zertifikat sicherstellen.
3. Die notwendige Sicherung (Backup) und Verteilung dieses privaten Schlüssels MUSS ausschließlich im Mehr-Augen-Prinzip und mit geeigneten Maßnahmen zur Wahrung der Vertraulichkeit des Schlüssels geschehen.
4. Der Fachdienst E-Rezept MUSS das VAU-Zertifikat in seinen Webschnittstellen unter dem Pfad /VAUCertificate (einer URL) durch Clients abrufbar machen. Dieses Zertifikat MUSS DER-kodiert sein

[<=,eRp_FD,Sich.techn. Eignung: Produktgutachten]

*Anpassung des Hinweistextes unter A_20160-**

alt:

Hinweis: Unter "/VAUCertificateOCSPResponse" erhält ein Client (einfacher GET-Request) eine korrekte OCSP-Response für das VAU-Zertifikat (A_20160-*, Punkt 1). Dies ist analog wie OCSP-Stapling bei TLS zu sehen, nur auf einer höheren OSI-Schicht. Der FD stellt korrekte OCSP-Responses zur Verfügung damit nicht jeder Client selbst den OCSP-

Responder fragen muss. Diese Funktionalität hat nichts mit der OCSP-Proxy-Funktionalität zu tun wie sie bspw. beim Zugangsgateway des Versicherten bei ePA angeboten wird. Der FD fragt bspw. stündlich selbst den OCSP-Status für sein VAU-Zertifikat ab, prüft die Antwort und stellt sie unter "/VAUCertificateOCSPResponse" Clients zur Verfügung.

neu:

Hinweis: Die Validierung und Verifizierung des VAUCertificate für Primärsysteme erfolgt mittels Konnektoroperation `VerifyCertificate`. Das E-Rezept-FdV validiert das Zertifikat mit den vom E-Rezept-Fachdienst bereitgestellten Endpunkten `GET /PKICertificate` und `GET /OCSPResponse` (siehe 6.2.2 Client-seitige Prüfung der E-Rezept-VAU-Identität).

alt:

A_21216 -E-Rezept-Client, Zertifikatsprüfung auf TLS-Basis

Ein E-Rezept-Client, der nicht das E-Rezept-FdV ist, MUSS das VAU-Zertifikat vom E-Rezept-FD beziehen (vgl. A_20160-*, URL `/VAUCertificate`) und ebenfalls für dieses Zertifikat die OCSP-Response für dieses Zertifikat beziehen (vgl. A_20160-*, URL `/VAUCertificateOCSPResponse`). Er MUSS das Zertifikat mittels `TUC_PKI_018` (OCSP-Graceperiod=12h, PolicyList={oid_erp-vau}) prüfen und dabei die vom FD bezogene OCSP-Response verwenden. [`<=,PS_E-Rezept_abgebend, CS_E-Rezept_KTR, NCPeH_ePeDA, PS_E-Rezept_verordnend,funkt.` Eignung: Herstellererklärung, Sich.techn. Eignung: Produktgutachten]

neu:

A_21216-02 -E-Rezept-Client, Prüfung VAU-Zertifikat auf TLS-Basis

Ein E-Rezept-Client, der nicht das E-Rezept-FdV ist, MUSS das VAU-Zertifikat vom E-Rezept-FD beziehen und mittels `TUC_PKI_018` (OCSP-Graceperiod=12h, PolicyList={oid_erp-vau}) prüfen. [`<=,PS_E-Rezept_abgebend, CS_E-Rezept_KTR, NCPeH_ePeDA, PS_E-Rezept_verordnend,funkt.` Eignung: Herstellererklärung, Sich.techn. Eignung: Produktgutachten]

Hinweis: E-Rezept-Clients, die Konnektoren nutzen, verwenden zur Prüfung des VAU-Zertifikats die Operation `VerifyCertificate`. Die in der Response enthaltene Rolle muss der `oid1.2.276.0.76.4.258` (`oid_erp-vau`) entsprechen. Damit wird die Anforderung A_21216-* erfüllt.

Folgendes kann umgesetzt werden:

- (1) Beziehen des VAU-Zertifikat von `/VAUCertificate`
- (2) Lokales Speichern der aktuellen Zeit mit dem VAU-Zertifikat als Tupel
- (3) Prüfen des VAU-Zertifikates mittels der Konnektor-Operation `VerifyCertificate`
- (4) Abbrechen falls `INVALID`
- (5) if (`get_current_time()` < gespeicherte Zeit + 12h) { VAU-Zertifikat wird als gültig angesehen, Nutzen des VAU-Zertifikat }
if (`get_current_time()` >= gespeicherte Zeit + 12h) { VAU-Zertifikat neu beziehen, siehe (1) }
- (6) if (`VerificationStatus.RoleList.Role == 1.2.276.0.76.4.258`) {VAU-Zertifikat entspricht der Identität `oid_erp-vau`}

C_12440_Anlage - E-Rezept-Fachdienst: Entfernen des VAUCertificateOCSPResponse Endpunktes



Hinweis zum Fehlerhandling: Nur wenn der äußere Response der E-Rezept-Fachdienstes den Response-Code 200 liefert, enthält der payload eine mittels VAU-Protokoll verschlüsselte Response. Liefert der äußere Response eine Code ≥ 400 , ist im VAU-Protokoll ein Fehler aufgetreten. Das PS muss nicht versuchen, den payload zu entschlüsseln.

3 Änderungen in gemILF_PS_eRp

In "5.1.2 Verschlüsselte Kommunikation zur VAU des E-Rezept-Fachdienstes" unter A_19741-01 ist folgender Hinweis aufgeführt:

Für Informationen zum Kommunikationsprotokoll zwischen E-Rezept-FdV und der VAU des E-Rezept-Fachdienstes siehe [\[gemSpec_Krypt#E-Rezept-spezifische Vorgaben\]](#) und [\[gemSpec_Krypt#VAU-Protokoll für E-Rezept\]](#) .

Alle weiteren Hinweise in diesem Kapitel werden gelöscht und in gemSpec_Krypt verschoben.

4 Änderungen in gemSpec_FD_eRp

Entfernen der Bereitstellung von Endpunkten des E-Rezept-Fachdienst.

alt

A_19412-05 -Anbieter E-Rezept-Fachdienst - Schnittstellenadressierung Primärsysteme

Der Anbieter des E-Rezept-Fachdienstes MUSS die den Primärsystemen angebotenen Schnittstellen des E-Rezept-Fachdienstes unter den folgenden URLs zur Verfügung stellen:

- <https://erp.zentral.erp.splitdns.ti-dienste.de/VAU> - Schnittstelle E-Rezept
- <https://erp.zentral.erp.splitdns.ti-dienste.de/VAUCertificate> - Schnittstelle VAU-Verschlüsselungsidentität
- <https://erp.zentral.erp.splitdns.ti-dienste.de/VAUCertificateOCSPResponse> - Schnittstelle VAU-Verschlüsselungsidentität
- <https://erp.zentral.erp.splitdns.ti-dienste.de/ocspf> - Schnittstelle OCSP-Forwarder
- <https://erp.zentral.erp.splitdns.ti-dienste.de/TSL.xml> - Schnittstelle Download TSL-Datei
- <https://erp.zentral.erp.splitdns.ti-dienste.de/TSL.sha2> - Schnittstelle Download Hashwert TSL-Datei
- <https://erp.zentral.erp.splitdns.ti-dienste.de/.well-known> - Schnittstelle well-known locations
- <https://erp.zentral.erp.splitdns.ti-dienste.de/random> - Schnittstelle für Zufallsdaten
- <https://subscription.zentral.erp.splitdns.ti-dienste.de> - Schnittstelle Subscription Service

[<=,Anb_eRp_FD,Sich.techn. Eignung: Anbietererklärung]

neu:

A_19412-06 -Anbieter E-Rezept-Fachdienst - Schnittstellenadressierung Primärsysteme

Der Anbieter des E-Rezept-Fachdienstes MUSS die den Primärsystemen angebotenen Schnittstellen des E-Rezept-Fachdienstes unter den folgenden URLs zur Verfügung stellen:

- <https://erp.zentral.erp.splitdns.ti-dienste.de/VAU> - Schnittstelle E-Rezept
- <https://erp.zentral.erp.splitdns.ti-dienste.de/VAUCertificate> - Schnittstelle VAU-Verschlüsselungsidentität
- <https://erp.zentral.erp.splitdns.ti-dienste.de/ocspf> - Schnittstelle OCSP-Forwarder
- <https://erp.zentral.erp.splitdns.ti-dienste.de/TSL.xml> - Schnittstelle Download TSL-Datei
- <https://erp.zentral.erp.splitdns.ti-dienste.de/TSL.sha2> - Schnittstelle Download Hashwert TSL-Datei

- <https://erp.zentral.erp.splitdns.ti-dienste.de/.well-known> - Schnittstelle well-known locations
- <https://erp.zentral.erp.splitdns.ti-dienste.de/random> - Schnittstelle für Zufallsdaten
- <https://subscription.zentral.erp.splitdns.ti-dienste.de> - Schnittstelle Subscription Service

[<=,Anb_eRp_FD,Sich.techn. Eignung: Anbietererklärung]

alt:

A_21782-02 -Anbieter E-Rezept-Fachdienst - Schnittstellenadressierung Internet

Der Anbieter des E-Rezept-Fachdienstes MUSS die im Internet angebotenen Schnittstellen des E-Rezept-Fachdienstes unter den folgenden URLs zur Verfügung stellen:

- <https://erp.app.ti-dienste.de/VAU> - Schnittstelle E-Rezept
- <https://erp.app.ti-dienste.de/VAUCertificate> - Schnittstelle VAU-Verschlüsselungsidentität
- <https://erp.app.ti-dienste.de/VAUCertificateOCSPResponse> - Schnittstelle VAU-Verschlüsselungsidentität
- <https://erp.app.ti-dienste.de/ocspf> - Schnittstelle OCSP-Forwarder
- <https://erp.app.ti-dienste.de/TSL.xml> - Schnittstelle Download TSL-Datei
- <https://erp.app.ti-dienste.de/TSL.sha2> - Schnittstelle Download Hashwert TSL-Datei
- <https://erp.app.ti-dienste.de/.well-known> - Schnittstelle well-known locations
- <https://erp.app.ti-dienste.de/PKICertificates>
- <https://erp.app.ti-dienste.de/OCSPResponse>
- <https://erp.app.ti-dienste.de/random> - Schnittstelle für Zufallsdaten

[<=,Anb_eRp_FD,Sich.techn. Eignung: Anbietererklärung]

neu

A_21782-03 -Anbieter E-Rezept-Fachdienst - Schnittstellenadressierung Internet

Der Anbieter des E-Rezept-Fachdienstes MUSS die im Internet angebotenen Schnittstellen des E-Rezept-Fachdienstes unter den folgenden URLs zur Verfügung stellen:

- <https://erp.app.ti-dienste.de/VAU> - Schnittstelle E-Rezept
- <https://erp.app.ti-dienste.de/VAUCertificate> - Schnittstelle VAU-Verschlüsselungsidentität
- <https://erp.app.ti-dienste.de/ocspf> - Schnittstelle OCSP-Forwarder
- <https://erp.app.ti-dienste.de/TSL.xml> - Schnittstelle Download TSL-Datei
- <https://erp.app.ti-dienste.de/TSL.sha2> - Schnittstelle Download Hashwert TSL-Datei
- <https://erp.app.ti-dienste.de/.well-known> - Schnittstelle well-known locations
- <https://erp.app.ti-dienste.de/PKICertificates>
- <https://erp.app.ti-dienste.de/OCSPResponse>

C_12440_Anlage - E-Rezept-Fachdienst: Entfernen des VAUCertificateOCSPResponse Endpunktes



- <https://erp.app.ti-dienste.de/random> - Schnittstelle für Zufallsdaten
[<=,Anb_eRp_FD,Sich.techn. Eignung: Anbietererklärung]

5 Änderungen in gemSpec_Perf

Anpassung der Tabelle 20: Tab_gemSpec_Perf_Berichtsformat_E-Rezept-Fachdienst

\$FD-operation	Operation	Schnittstelle zu
ERP.UC_1_1	GET /Device	alle
ERP.UC_1_2	GET /metadata	alle
ERP.UC_2_1	POST /Task/\$create	verordnende LEI
ERP.UC_2_3	POST /Task/<id>/\$activate mit Flowtype 160	verordnende LEI
ERP.UC_2_3_162	POST /Task/<id>/\$activate mit Flowtype 162	verordnende LEI
ERP.UC_2_3_169	POST /Task/<id>/\$activate mit Flowtype 169	verordnende LEI
ERP.UC_2_3_200	POST /Task/<id>/\$activate mit Flowtype 200	verordnende LEI
ERP.UC_2_3_209	POST /Task/<id>/\$activate mit Flowtype 209	verordnende LEI
ERP.UC_2_5	POST /Task/<id>/\$abort	verordnende LEI
ERP.UC_3_1	GET /Task	Versicherte
ERP.UC_3_2	POST /Task/<id>/\$abort	Versicherte
ERP.UC_3_3	POST /Communication	Versicherte
ERP.UC_3_5	GET /AuditEvent	Versicherte
ERP.UC_3_6	GET /Task/<id>	Versicherte
ERP.UC_3_7	GET /ChargelItem/<id>	Versicherte
ERP.UC_3_8	DELETE /Communication/<id>	Versicherte
ERP.UC_3_9	GET /MedicationDispense?<parameter>=	Versicherte
ERP.UC_3_10	GET /ChargelItem	Versicherte
ERP.UC_3_11	DELETE /ChargelItem/<id>	Versicherte
ERP.UC_3_12	PATCH /ChargelItem/<id>	Versicherte

**C_12440_Anlage - E-Rezept-Fachdienst:
Entfernen des VAUCertificateOCSPResponse
Endpunktes**

ERP.UC_3_13	GET /Consent	Versicherte
ERP.UC_3_14	POST /Consent	Versicherte
ERP.UC_3_15	DELETE /Consent	Versicherte
ERP.UC_3_16	POST /\$grant-eu-access-permission	Versicherte
ERP.UC_3_17	DELETE /\$revoke-eu-access-permission	Versicherte
ERP.UC_3_18	GET /\$read-eu-access-permission	Versicherte
ERP.UC_4_1	POST /Task/<id>/\$accept	abgebende LEI
ERP.UC_4_2	POST /Task/<id>/\$reject	abgebende LEI
ERP.UC_4_3	POST /Task/<id>/\$abort	abgebende LEI
ERP.UC_4_4	POST /Task/<id>/\$close	abgebende LEI
ERP.UC_4_6	GET /Communication	abgebende LEI
ERP.UC_4_7	POST /Communication	abgebende LEI
ERP.UC_4_8	GET /Task/<id>?secret	abgebende LEI
ERP.UC_4_9	DELETE /Communication/<id>	abgebende LEI
ERP.UC_4_10	GET /Chargeltem/<id>	abgebende LEI
ERP.UC_4_11	POST /Chargeltem	abgebende LEI
ERP.UC_4_12	GET /Task(PNW)	abgebende LEI
ERP.UC_4_13	PUT /Chargeltem/<id>	abgebende LEI
ERP.UC_4_14	POST /Subscription	abgebende LEI
ERP.UC_4_16	POST /Task/<id>/\$dispense	abgebende LEI
ERP.UC_4_17	GET /Task/<id>?accesscode	abgebende LEI
ERP.UC_4_19	POST /\$get-eu-prescriptions mit Requesttype demographics	NCPeH-FD
ERP.UC_4_20	POST /\$get-eu-prescriptions mit Requesttype e-prescriptions-list	NCPeH-FD

**C_12440_Anlage - E-Rezept-Fachdienst:
Entfernen des VAUCertificateOCSPResponse
Endpunktes**

ERP.UC_4_21	POST /\$get-eu-prescriptions mit Requesttype e-prescriptions-retrieval	NCPeH-FD
ERP.UC_4_22	POST /Task/<id>/\$eu-close	NCPeH-FD
ERP.UC_5_1	Verordnungsdaten in Aktenkonto einstellen	ePA-Aktensystem
ERP.UC_5_2	Löschinformation Verordnungsdaten an Aktenkonto übermitteln	ePA-Aktensystem
ERP.UC_5_3	Dispensierinformationen in Aktenkonto einstellen	ePA-Aktensystem
ERP.UC_5_4	Löschinformation Dispensierinformationen an Aktenkonto übermitteln	ePA-Aktensystem
ERP.UC_5_5	ePA-Aktensystem ermitteln und Widerspruch prüfen	ePA-Aktensystem
ERP.UC_5_6	Login ePA-Aktensystem	ePA-Aktensystem
ERP.nonVAU_1	GET /VAUCertificate	alle
ERP.nonVAU_2	GET /VAUCertificateOCSPResponse	alle
ERP.nonVAU_5	POST /ocspf	alle
ERP.nonVAU_6	GET /PKICertificates	alle
ERP.nonVAU_7	GET /OCSPResponse	alle
ERP.nonVAU_8	GET /Random	alle