

Anlage zum Änderungseintrag C_10980 E-Rezept-Fachdienst: Nutzung C.FD.OSIG anstatt C.FD.SIG

Änderungsbedarf:

Das initial durch den E-Rezept-Fachdienst genutzte Signatursignifikat C.FD.SIG für die Signatur der Quittung und des Verordnungsdatensatzes für die App beinhaltet die keyUsage digitalSignature. Fachlich korrekt ist die Verwendung eines Signaturzertifikates mit der keyUsage nonRepudiation (Nichtabstreitbarkeit).

Zu diesem Zweck wird durch die Komponenten-PKI der TI das Zertifikatprofil C.FD.OSIG bereitgestellt. Dieses ist durch den E-Rezept-Fachdienst zu nutzen.

Änderungen in gemSpec_FD_eRp:

Alt:

A_20765 - E-Rezept-Fachdienst - Prüfung Signaturzertifikat E-Rezept-Fachdienst

Der E-Rezept-Fachdienst MUSS sein Signatur-Zertifikat für die Signatur der E-Rezept-Quittung gemäß [gemSpec_PKI#TUC_PKI_018] mit folgenden Parametern auf Gültigkeit prüfen:

Tabelle 1: TAB_eRPF010 Parameter Prüfung Signaturzertifikat

Parameter	
Zertifikat	Signaturzertifikat des E-Rezept-Fachdienstes C.FD.SIG
PolicyList	oid_fd_sig
intendedKeyUsage	nonRepudiation
intendedExtendedKeyUsage	(leer)
OCSP-Graceperiod	60 Minuten
Offline-Modus	nein
Prüfmodus	OCSP

Das Signaturzertifikat muss anhand der Zertifikatsprüfung für [mathematisch gültig UND zeitlich gültig UND online gültig] befunden werden und eingehende HTTP-Request zur Erstellung einer Quittung andernfalls mit dem HTTP-Status-Code 500 abgelehnt werden, damit sichergestellt wird, dass ausschließlich Quittungen mit einem gültigen Signaturzertifikat erstellt werden. [<=]

Neu:

A_20765-01 - E-Rezept-Fachdienst - Prüfung Signaturzertifikat E-Rezept-Fachdienst

Der E-Rezept-Fachdienst MUSS sein Signatur-Zertifikat für die Signatur der E-Rezept-Quittung gemäß [gemSpec_PKI#TUC_PKI_018] mit folgenden Parametern auf Gültigkeit prüfen:

Tabelle 2: TAB_eRPFD_010 Parameter Prüfung Signaturzertifikat

Parameter	
Zertifikat	Signaturzertifikat des E-Rezept-Fachdienstes C.FD.OSIG
PolicyList	oid_fd_osig
intendedKeyUsage	nonRepudiation
intendedExtendedKeyUsage	(leer)
OCSP-Graceperiod	60 Minuten
Offline-Modus	nein
Prüfmodus	OCSP

Das Signaturzertifikat muss anhand der Zertifikatsprüfung für [mathematisch gültig UND zeitlich gültig UND online gültig] befunden werden und eingehende HTTP-Request zur Erstellung einer Quittung andernfalls mit dem HTTP-Status-Code 500 abgelehnt werden, damit sichergestellt wird, dass ausschließlich Quittungen mit einem gültigen Signaturzertifikat erstellt werden. [**<=**]

Alt:

A_19029-03 - E-Rezept-Fachdienst - Serversignatur Rezept aktivieren

Der E-Rezept-Fachdienst MUSS das bei der Operation /Task/<id>/\$activate im QES-Datensatz enthaltene FHIR-E-Rezept-Bundle vom Profil https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Bundle in ein Bundle gleichen Typs in JSON-Repräsentation beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task/<id> zurückliefern.

Der E-Rezept-Fachdienst MUSS für diesen

- einen neuen, eindeutigen Identifier für die [Bundle.id](#) als UUID generieren,
- das Bundle entsprechend der Kanonisierungsregeln <http://hl7.org/fhir/canonicalization/json#static> normalisieren (Bundle.text und Bundle.meta im "root-Element" entfernen) und
- mit der Signaturidentität des Fachdienstes ID.FD.SIG gemäß [FHIR-Sig] signieren und
- das signierte Bundle mit Referenz in Task.input mit Codingsystem <https://gematik.de/fhir/CodeSystem/Documenttype> = 2 zurück liefern,

damit der Versicherte einen Nachweis über die Integrität der gespeicherten Daten einsehen kann.[**<=**]

Neu:

A_19029-04 - E-Rezept-Fachdienst - Serversignatur Rezept aktivieren

Der E-Rezept-Fachdienst MUSS das bei der Operation `/Task/<id>/$activate` im QES-Datensatz enthaltene FHIR-E-Rezept-Bundle vom Profil https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Bundle in ein Bundle gleichen Typs in JSON-Repräsentation beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Task/<id>` zurückliefern.

Der E-Rezept-Fachdienst MUSS für diesen

- einen neuen, eindeutigen Identifier für die [Bundle.id](#) als UUID generieren,
- das Bundle entsprechend der Kanonisierungsregeln <http://hl7.org/fhir/canonicalization/json#static> normalisieren (Bundle.text und Bundle.meta im "root-Element" entfernen) und
- mit der Signaturidentität des Fachdienstes ID.FD.OSIG gemäß [FHIR-Sig] signieren und
- das signierte Bundle mit Referenz in Task.input mit Codingsystem <https://gematik.de/fhir/CodeSystem/Documenttype> = 2 zurückliefern,

damit der Versicherte einen Nachweis über die Integrität der gespeicherten Daten einsehen kann. [≤]

Alt:

A_19233-03 - E-Rezept-Fachdienst - Serversignatur Rezept beenden (Quittung erstellen)

Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks mittels `/Task/<id>/$close` ein Quittungsbundle gemäß des FHIR-

Profils <https://gematik.de/fhir/StructureDefinition/erxReceipt> mit folgenden Informationen erstellen:

- Telematik-ID der aufrufenden Apotheke als `Beneficiary` in die `erxComposition`
- Zeitstempel des Statuswechsel des Tasks "in-progress" in `event.period.start`
- aktueller Zeitstempel in `event.period.end`
- Identifier `PrescriptionID` des Task als Identifier des Quittungs-Bundle
- Device-Ressource mit Fachdienstinformationen als Autor der Signatur
- Base64Binary-Ressource mit `Binary.data` = <base64-codierter Hashwert aus der QES-Signatur des dem Task zugrunde liegenden Verordnungsdatensatzes> und `contentType` = "application/octet-stream"

und dieses Quittungs-Bundle mit der Signaturidentität des Fachdienstes ID.FD.SIG gemäß [RFC5652] mit Profil CADES-BES ([CADES]) im Enveloping signieren.

In die Signatur wird die letzte OCSP-Antwort der regelmäßigen Statusprüfung des Signaturzertifikats C.FD.SIG eingebettet.

Das Signatur-Ergebnis wird als `dss:Base64Signature`-Objekt in `Bundle.signature` eingebettet und dieses Quittungs-Bundle mit Referenz in `Task.output` mit Codingsystem <https://gematik.de/fhir/CodeSystem/Documenttype> = 3 gespeichert sowie als Response des http-Requests an den Aufrufer zurückgeben, damit der Apotheker einen Nachweis über den ordnungsgemäßen Abschluss des E-Rezept-Workflows als Quittung erhält. [≤]

Neu:

A_19233-04 - E-Rezept-Fachdienst - Serversignatur Rezept beenden (Quittung erstellen)

Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks mittels `/Task/<id>/$close` ein Quittungsbundle gemäß des FHIR-Profiles <https://gematik.de/fhir/StructureDefinition/erxReceipt> mit folgenden Informationen erstellen:

- Telematik-ID der aufrufenden Apotheke als `Beneficiary` in die `erxComposition`
- Zeitstempel des Statuswechsel des Tasks "in-progress" in `event.period.start`
- aktueller Zeitstempel in `event.period.end`
- Identifier `PrescriptionID` des Task als identifier des Quittungs-Bundle
- Device-Ressource mit Fachdienstinformationen als Autor der Signatur
- `Base64Binary`-Ressource mit `Binary.data` = <base64-codierter Hashwert aus der QES-Signatur des dem Task zugrunde liegenden Verordnungsdatensatzes> und `contentType` = "application/octet-stream"

und dieses Quittungs-Bundle mit der Signaturidentität des Fachdienstes `ID.FD.OSIG` gemäß [RFC5652] mit Profil `CAAdES-BES` ([`CAAdES`]) im `Envelope` signieren.

In die Signatur wird die letzte OCSP-Antwort der regelmäßigen Statusprüfung des Signaturzertifikats `C.FD.OSIG` eingebettet.

Das Signatur-Ergebnis wird als `dss:Base64Signature`-Objekt in `Bundle.signature` eingebettet und dieses Quittungs-Bundle mit Referenz in `Task.output` mit Codingsystem <https://gematik.de/fhir/CodeSystem/Documenttype> = 3 gespeichert sowie als Response des `http-Requests` an den Aufrufer zurückgeben, damit der Apotheker einen Nachweis über den ordnungsgemäßen Abschluss des E-Rezept-Workflows als Quittung erhält. [`<=`]