
C_12269_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_FD_eRp.....	3

1 Änderungsbeschreibung

In der Produktionsumgebung wurde festgestellt, dass Signaturprüfungen unter bestimmten Umständen fehlschlagen. Dies tritt insbesondere dann auf, wenn eine OCSP-Response in der Signatur enthalten ist und diese zu einem Zeitpunkt ausserhalb der erlaubten Zeittoleranz zum Signaturzeitraum erstellt wurde ist.

In solchen Fällen führt die negative Prüfung der eingebetteten OCSP-Response dazu, dass die gesamte Signaturprüfung als ungültig bewertet wird, was wiederum den weiteren Verarbeitungsprozess blockiert. Dies kann dazu führen, dass E-Rezepte abgelehnt werden und der Arbeitsablauf bei Leistungserbringern beeinträchtigt wird.

Der vorgeschlagene Änderungseintrag zielt darauf ab, diesen Prozess zu optimieren, indem der E-Rezept-Fachdienst bei negativer Prüfung der eingebetteten OCSP-Response eigenständig eine OCSP-Response für das Signaturzertifikat abrufen und diese zur Validierung verwendet. Der E-Rezept-Fachdienst wird dabei auf einen vertrauenswürdigen OCSP-Responder zugreifen, um die Gültigkeit des Signaturzertifikats sicherzustellen.

Durch diese Änderung wird die Robustheit und Zuverlässigkeit des Systems in der Produktionsumgebung erheblich gesteigert. Dies trägt dazu bei, Fehler im Verarbeitungsprozess zu vermeiden und die Nutzererfahrung für alle Beteiligten zu verbessern.

2 Änderung in gemSpec_FD_eRp

Alt:

A_20159-03 -E-Rezept-Fachdienst - Task aktivieren - QES Prüfung Signaturzertifikat des HBA

Der E-Rezept-Fachdienst MUSS das QES-Signaturzertifikat C.HP.QES in der Signatur des übergebenen QES-Datensatzes gemäß [gemSpec_PKI#TUC_PKI_030] mit folgenden Parametern auf Gültigkeit prüfen:

Tabelle 1 : TAB_eRPFD_006 Parameter Prüfung Signaturzertifikat QES des HBA

Parameter	
Zertifikat	Signaturzertifikat des HBA (eingebettet in Signatur-Objekt des QES-Datensatzes): <ul style="list-style-type: none"> • C.HP.QES (oid_hba_qes = 1.2.276.0.76.4.72 gemäß gemSpec_OID) • bzw. für HBA-Vorläuferkarten C.HP.ENC (oid_vk_eaa_enc = 1.3.6.1.4.1.24796.1.10 gemäß gemSpec_OID) Hinweis: die OID dieses Profil wird für Ärzte- und Zahnärzteschaft gleichermaßen genutzt
Referenzzeitpunkt	<Zeitpunkt der QES.Erstellung gemäß signingTime im QES-Datensatz>
Offline-Modus	nein
OCSP-Response	eingebettet in QES-Datensatz

und darf die OCSP-Response für die Abfrage des Zertifikatsstatus für 12 Stunden zwischenspeichern.

Ist keine OCSP-Response eingebettet, MUSS der E-Rezept-Fachdienst die gecachte OCSP-Response verwenden oder eine OCSP-Response beim benannten TSP anfragen und die genutzte OCSP-Response nachträglich in den QES-Datensatz einbetten.

Das Signaturzertifikat muss anhand der Zertifikatsprüfung für [mathematisch gültig UND zeitlich gültig UND online gültig] befunden werden und der HTTP-Request andernfalls mit dem HTTP-Status-Code 400 abgelehnt werden, damit sichergestellt wird, dass ausschließlich E-Rezepte verwaltet werden, die von einer gültigen, nicht gesperrten Heilberufsidentität eines HBA signiert wurden.

Wenn die Abfrage des OCSP-Response für das Signaturzertifikat fehlschlägt, muss der HTTP-Request mit dem HTTP-Status-Code 512 abgelehnt werden. [<=, eRp_FD, Sich.techn. Eignung: Produktgutachten]

Neu:

A_20159-04 -E-Rezept-Fachdienst - Task aktivieren - QES Prüfung Signaturzertifikat des HBA

Der E-Rezept-Fachdienst MUSS das QES-Signaturzertifikat C.HP.QES in der Signatur des übergebenen QES-Datensatzes gemäß [gemSpec_PKI#TUC_PKI_030] mit folgenden Parametern auf Gültigkeit prüfen:

Tabelle 2 : TAB_eRPFD_006 Parameter Prüfung Signaturzertifikat QES des HBA

Parameter	
Zertifikat	Signaturzertifikat des HBA (eingebettet in Signatur-Objekt des QES-Datensatzes): <ul style="list-style-type: none"> • C.HP.QES (oid_hba_qes = 1.2.276.0.76.4.72 gemäß gemSpec_OID) • bzw. für HBA-Vorläuferkarten C.HP.ENC (oid_vk_eaa_enc = 1.3.6.1.4.1.24796.1.10 gemäß gemSpec_OID) Hinweis: die OID dieses Profil wird für Ärzte- und Zahnärzteschaft gleichermaßen genutzt
Referenzzeitpunkt	<Zeitpunkt der QES.Erstellung gemäß signingTime im QES-Datensatz>
Offline-Modus	nein
OCSP-Response	eingebettet in QES-Datensatz

und darf die OCSP-Response für die Abfrage des Zertifikatsstatus für 12 Stunden zwischenspeichern.

Ist keine OCSP-Response eingebettet oder die eingebettete OCSP Response nicht gültig, MUSS der E-Rezept-Fachdienst die gecachte OCSP-Response verwenden oder eine OCSP-Response beim benannten TSP anfragen und die genutzte OCSP-Response nachträglich in den QES-Datensatz einbetten.

Das Signaturzertifikat muss anhand der Zertifikatsprüfung für [mathematisch gültig UND zeitlich gültig UND online gültig] befunden werden und der HTTP-Request andernfalls mit dem HTTP-Status-Code 400 abgelehnt werden, damit sichergestellt wird, dass ausschließlich E-Rezepte verwaltet werden, die von einer gültigen, nicht gesperrten Heilberufsidentität eines HBA signiert wurden.

Wenn die Abfrage des OCSP-Response für das Signaturzertifikat fehlschlägt, muss der HTTP-Request mit dem HTTP-Status-Code 512 abgelehnt werden. [<=,eRp_FD,Sich.techn. Eignung: Produktgutachten]