
C_12768_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemF_PushNotification.....	3
2.1 Kapitel 5.5 Sicherheit.....	3
2.1.1 textuelle Anpassungen.....	3
2.1.2 abgelöste Anforderungen.....	3
2.1.2.1 alt.....	3
2.1.2.2 neu.....	3
2.1.3 neue Anforderungen.....	4

1 Änderungsbeschreibung

Da die vorgesehen Form des mTLS Verbindungsaufbaus in Zukunft von allen Zertifikatsausgabestellen eingestellt wird, (siehe z.B. <https://www.sectigo.com/blog/tls-client-authentication-public-ca-end-2026>) stellen wir auf die Verwendung von Client Zertifikaten der Komponenten-PKI.

2 Änderung in gemF_PushNotification

2.1 Kapitel 5.5 Sicherheit

2.1.1 textuelle Anpassungen

Da für das Übertragen der Push Notifications die Dienste der Anbieter von mobilen Plattformen (z.B. Google, Apple) genutzt werden, ist insbesondere das Thema der Datenverarbeitung in Drittstaaten zu beachten und die sich daraus ergebenden datenschutzrechtlichen Herausforderungen mit technischen Maßnahmen abzumildern.

Diese Maßnahmen sind:

- Es kann eine Verschlüsselung des Benachrichtigungsinhalts zwischen Fachdienst und FdV, die sowohl die Vertraulichkeit als auch die Authentizität/Integrität des Benachrichtigungsinhalts schützt, eingesetzt werden. Die Notwendigkeit dafür wird in der Spezifikation des jeweiligen Fachdienstes festgestellt.
- Vom Nutzer wird eine informierte Einwilligung eingeholt.

Die Einwilligung für den Empfang von Push Notifications und den Widerruf der Einwilligung kann der Versicherte im FdV vornehmen.

Die Kommunikation zwischen dem Fachdienst und dem Push Gateway erfolgt mittels TLS und beidseitiger Authentifizierung (mTLS). ~~Für diese Authentifizierung müssen Extended Validation TLS-Zertifikate eines Herausgebers gemäß [CAB Forum] verwendet werden.~~ Aus Sicht der jeweiligen Komponente ist es wichtig mit dem richtigen Partner zu kommunizieren. Der Fachdienst soll sicher sein, die Notifications an das richtigen Push Gateway zu senden und der Push Gateway soll sicher sein, die Notifications ~~vom richtigen Fachdienst~~ von einem legitimierten Fachdienst zu erhalten.

Die Verbindung vom Push Gateway zum Push Provider erfolgt ebenfalls über eine mittels des TLS-Protokolls geschützten Datenverbindung.

2.1.2 abgelöste Anforderungen

2.1.2.1 alt

A_28268 -Push Notifications - mTLS Authentifizierungszertifikat

Die Komponenten Push Gateway und Fachdienst MÜSSEN sich beim TLS-Verbindungsaufbau gegenüber dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] authentisieren. [≤, „]

2.1.2.2 neu

A_28268-02 -Push Notifications - mTLS TLS-Server-Authentifizierungszertifikat

Die Komponente Push Gateway MUSS sich TLS-Server-seitig mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] gegenüber einem TLS-Client authentisieren. [≤, Gesundheits-App_Option_PushNotification, FdV_Option_PushNotification, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Herstellererklärung]

2.1.3 neue Anforderungen

A_28981 -Push Notifications - mTLS Authentifizierungszertifikat TLS-Client

Ein Client der Komponente Push Gateway MUSS sich mit einem TLS-Client-Zertifikat aus der Komponenten-PKI beim TLS-Verbindungsaufbau authentisieren.

Das TLS-Client-Zertifikat MUSS das Profil C.FD.TLS-C besitzen und die technische Rolle des Clients enthalten (ePA-Aktensystem: oid_epa_mgmt/1.2.276.0.76.4.207, E-Rezept-FD: oid_erezept/1.2.276.0.76.4.259). [$\leq$, Aktensystem_ePA, TI-M_FD_ePA, TI-Flow_FD, eRp_FD, Sich.techn. Eignung: Produktgutachten]

A_28982 -Push Notifications - mTLS, Prüfung des TLS-Client-Zertifikats im TLS-Server

Die Komponente Push Gateway MUSS das TLS-Client-Zertifikat beim TLS-Verbindungsaufbau prüfen.

Dafür MUSS es eine der beiden Prüfmethoden umsetzen:

1. Prüfmethode 1: Das TLS-Client-Zertifikat wird über einen technisch/organisatorischen Prozess zwischen Push Gateway und Client authentitätsgeschützt sicher ausgetauscht und im Truststore des Push-Gateways hinterlegt. Bei der Prüfung wird auf Enthalten sein des TLS-Client-Zertifikats im Truststore geprüft.
2. Prüfmethode 2: Das TLS-Client-Zertifikat wird geprüft, ob es Teil der TI-PKI ist, zeitlich gültig und die korrekte technische Rolle des Clients enthält (ePA-Aktensystem: oid_epa_mgmt/1.2.276.0.76.4.207, E-Rezept-FD: oid_erezept/1.2.276.0.76.4.259). Falls alle Prüfungen ein positives Prüfergebnis besitzen, wird das TLS-Client-Zertifikat akzeptiert.

[$\leq$, Gesundheits-App_Option_PushNotification, FdV_Option_PushNotification, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Herstellererklärung]