

Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature: Anwendungsübergreifende Push Notification

Version:	1.0.0 CC
Revision:	1181178
Stand:	31.03.2025
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemF_PushNotification

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Versio n	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0 CC	31.03.202 5		zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	6
1.1 Zielsetzung.....	6
1.2 Zielgruppe.....	6
1.3 Geltungsbereich.....	6
1.4 Abgrenzungen.....	6
1.5 Methodik.....	7
2 Epic und User Story.....	8
2.1 Epic Push Notifications für Gesundheitsanwendungen.....	8
2.1.1 User Stories.....	8
3 Einordnung in die Telematikinfrastuktur.....	10
4 Technisches Konzept.....	11
5 Spezifikation.....	12
5.1 Anforderungen an den Fachdienst.....	12
5.1.1 Pusher registrieren.....	12
5.1.2 Operation Notify.....	13
5.2 Anforderungen an das Push Gateway.....	15
5.3 Anforderung an die FdV-Instanz.....	16
5.3.1 Schlüsselableitung für Push Notifications.....	16
5.3.2 FdV-Instanz Registrieren.....	17
5.3.2.1 Push Notifications empfangen.....	19
5.3.2.2 Notifications aktivieren und deaktivieren.....	20
5.4 Optionale Anforderungen.....	21
5.4.1 Channel/Trigger Konfiguration.....	21
5.4.1.1 Fachdienst.....	21
5.4.1.2 FdV.....	22
5.4.2 Push Notification Historie.....	22
5.4.2.1 Fachdienst.....	22
5.5 Sicherheit.....	23
5.6 Betrieb.....	27
5.6.1 Betriebliche Steuerung des Push-Gateways.....	27
6 Dokumentenhaushalt.....	28
7 Beispiele und Referenzimplementierungen.....	29
8 Anhang A - Verzeichnisse.....	30
8.1 Abkürzungen.....	30

8.2 Abbildungsverzeichnis.....	30
8.3 Tabellenverzeichnis.....	31
8.4 Referenzierte Dokumente.....	31
8.4.1 Dokumente der gematik.....	31
8.4.2 Weitere Dokumente.....	32
9 Anhang C - Offene Punkte, Fragen.....	33
9.1 Betriebliche Steuerung des Push-Gateways.....	33

1 Einordnung des Dokuments

Dieses Dokument beschreibt das Feature der Notifications eines Teilnehmers des Gesundheitswesens unabhängig von der konkreten Anwendung.

1.1 Zielsetzung

Die Beschreibung des Funktionsumfangs als Feature erleichtert das Verständnis und die Nachvollziehbarkeit der Lösung. Mit den hier aufgestellten Anforderungen sollen Hersteller in der Lage sein, den zusätzlichen Funktionsumfang ihrer verantworteten Komponente bzw. ihres Produkttyps bewerten und umsetzen zu können.

1.2 Zielgruppe

Das Dokument richtet sich zwecks der Realisierung an die Hersteller der mobilen FdVs (Frontend des Versicherten) und Fachdienste sowie an die Anbieter, welche diese Produkte betreiben.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Produkttypsteckbrief, Anbietertypsteckbrief u. a.) oder Webplattformen (z. B. gitHub u. a.) festgelegt und bekanntgegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Spezifiziert werden in diesem Dokument nur die notwendigen oder optionalen Komponenten und Schnittstellen für Push Notifications für mobile FdVs durch Fachdienste der TI.

Benutzte Schnittstellen werden in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt.

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief der Produkttypen verzeichnet.

1.5 Methodik

User Story

Eine User Story ist eine in Alltagssprache formulierte Software-Anforderung. Sie ist bewusst kurz gehalten und umfasst in der Regel nicht mehr als zwei Sätze. User Stories werden im Rahmen der agilen Softwareentwicklung zusammen mit Akzeptanztests zur Spezifikation von Anforderungen eingesetzt. [Wikipedia: User Story]

Aus diesem Grund kann in den User Stories eine abweichende Terminologie genutzt werden, welche für den Leser nachvollziehbar (bspw. Patient = Versicherter) ist.

Anforderungen

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Anforderungen werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke [<=] angeführten Inhalte.

Hinweise auf offene Punkte

Themen, die noch intern geklärt werden müssen oder eine Entscheidung seitens der Gesellschafter erfordern, sind wie folgt im Dokument gekennzeichnet:

Beispiel für einen offenen Punkt.

2 Epic und User Story

2.1 Epic Push Notifications für Gesundheitsanwendungen

Für die Praxistauglichkeit und die Akzeptanz einer mobilen Anwendung im Gesundheitswesen ist es von enormer Bedeutung, dass Nutzer eines FdV Push Notifications erhalten können. Push Notifications sollen dann erscheinen, wenn im Kontext des Versorgungsprozesses eine Aktivität des Nutzers erforderlich wird, oder um den Nutzer zum aktuellen Status zu informieren (z. B. wenn ein neues Dokument in die ePA (elektronische Patientenakte) eingestellt wurde, wenn ein neues E-Rezept ausgestellt wurde oder die Apotheke zu einem Bestellvorgang einen Abholzeitpunkt gemeldet hat).

Grundsätzlich muss ein Versicherter im entsprechenden Fachdienst angemeldet sein (bspw. mit eGK und PIN oder mit Gesundheits-ID), um Informationen vom Fachdienst abzurufen. Da diese Anmeldung zeitlich begrenzt ist, wird der Nutzer automatisch nach einem anwendungsabhängigen Zeitraum wieder abgemeldet. Damit der Nutzer auch über Änderungen im Fachdienst benachrichtigt wird, wenn die Anmeldung automatisch abgelaufen ist, soll die Benachrichtigungsfunktion nicht daran gebunden sein, ob ein Nutzer das FdV geöffnet hat oder aktuell an der TI angemeldet ist.

Um die Benachrichtigungsfunktion zu aktivieren, muss sich der Nutzer im Fachdienst anmelden. Der Nutzer muss im Smartphone einwilligen, dass das FdV Push Notifications anzeigen darf. Ohne diese Einwilligung durch den Nutzer sind Push Notifications nicht erlaubt. Die Einwilligung kann jederzeit durch den Nutzer widerrufen werden, wenn der Nutzer keine Push Notifications mehr erhalten möchte.

Fachdienste, die Push Notifications senden, welche Rückschlüsse auf den Gesundheitszustand des Nutzers zulassen, müssen die Push Notifications verschlüsseln. Fachdienste dürfen unverschlüsselte Push Notifications nur dann senden, wenn weder Gesundheitsdaten noch personenbeziehbare Daten in den Push Notifications enthalten sind. Beispiele hierfür sind: Eine verschlüsselte Benachrichtigung könnte Informationen über ein vom Arzt angelegtes Dokument in der ePA enthalten, während eine unverschlüsselte Benachrichtigung lediglich eine EventID für eine neue Nachricht im Messenger übermitteln kann. Das FdV könnte die eigentlichen Informationen dann als Folge der Push Notification mit Hilfe der EventID nachladen.

Es ist vorgesehen, dass Push Notifications auch dann für FdVs zur Verfügung stehen können, wenn Dienste außerhalb der TI verwendet werden. Zu diesem Zweck wird von jedem FdV-Hersteller neben der Push Implementierung im FdV auch gleichzeitig ein Push Gateway gefordert, der die nötige plattformspezifische Abstraktion realisiert, um auch mobile Geräte zentral erreichen zu können.

2.1.1 User Stories

Als Patient möchte ich von verschiedenen Fachdiensten benachrichtigt werden können, so dass ich über aktuelle Veränderungen informiert bin und, falls notwendig, selbst aktiv werden kann.

Als Patient möchte ich sicher sein, dass Push Notifications mich jederzeit erreichen können, so dass ich nicht regelmäßig nach neuen Informationen im FdV schauen muss, was ich vergessen könnte.

Als Patient möchte ich nicht jeden Tag meine Authentisierung gegenüber Fachdiensten erneuern müssen (bspw. durch eGK und PIN), um Push Notifications erhalten zu können, so dass ich sicher sein kann, dass mich Push Notifications erreichen und nicht von einem manuellen und repetitiven Schritt abhängig sind.

Als Patient möchte ich, dass eine Push Notification keine sensiblen Informationen enthält, so dass ich nicht in Situationen komme, bei denen Dritte solche Informationen auf dem Bildschirm meines Geräts lesen können.

Als Patient möchte ich leicht von einer Push Notification zu dem Bereich des FdV navigieren können, in dem ich mit der neuen Information etwas tun kann, so dass ich nicht manuell das FdV öffnen und über komplizierte Wege dorthin navigieren muss.

Als Patient möchte ich im FdV einstellen können, ob sie mir (z.B. via Fachdienst) Push Notifications schicken darf.

Als Patient möchte ich konfigurieren können, für welchen Situationen ich benachrichtigt werden möchte, sodass ich für mich unwichtige Push Notifications nicht angezeigt bekomme.

3 Einordnung in die Telematikinfrastruktur

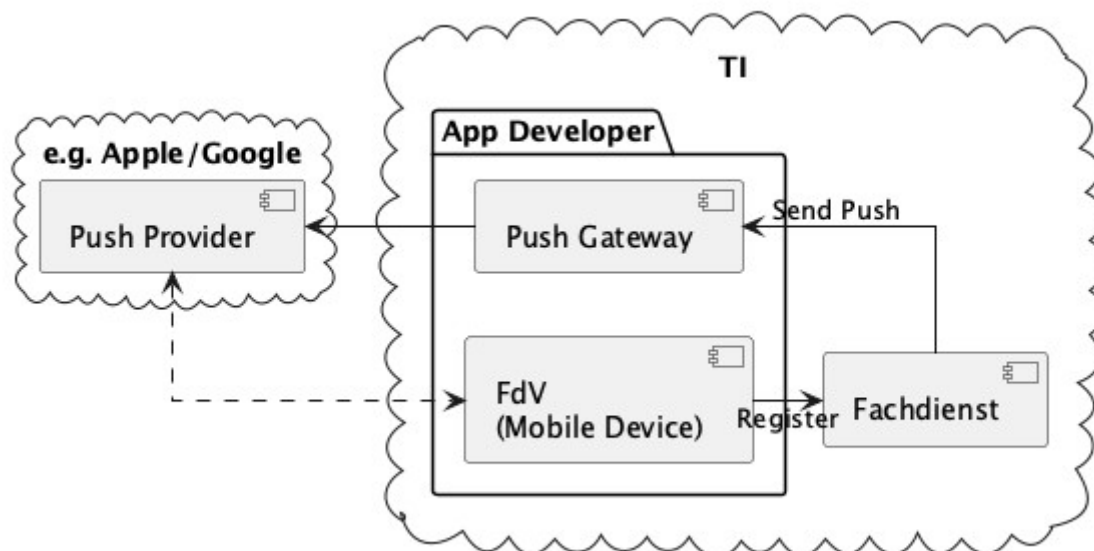


Abbildung 1: Systemüberblick

Komponenten

1. Fachdienst: Neben seinen normalen Aufgaben bietet der Fachdienst in diesem Konzept weitere Interface für FdVs an. Diese umfassen unter anderem die Registrierung für Push Notifications sowie die Verwaltung dieser Registrierungen. Er ist ebenso dafür verantwortlich Trigger zu implementieren, die dann (unter Berücksichtigung einer eventuellen Channel-Konfiguration) als Push Notifications via Push Gateway zum FdV gesendet werden.
2. FdV: Das FdV ist die (mobile) Anwendung (App), die von einem Versicherten genutzt wird, um Anwendungsfälle durchzuführen.
3. Push Gateway: Das Push Gateway ist eine Art Proxy das die Kommunikation zum FdV für Notifications mittels Push Provider implementiert. Jedes Push Gateway kann eine oder mehrere FdVs bedienen. Zum Beispiel könnten das iOS FdV und das Android FdV gebündelt in einem Push Gateway angebunden oder je ein Push Gateway pro Plattform existieren. Ebenso ist eine Mandantenfähigkeit des Push Gateways denkbar.
4. Push Provider: Push Provider sind die Dienste der mobilen Betriebssystemplattformbetreiber (z.B. iOS, Android), welche die Push Notifications an das FdV auf dem Gerät des Versicherten senden. Diese Dienste sind nicht Teil der Telematikinfrastruktur.

4 Technisches Konzept

Der Zweck dieses Konzepts besteht darin, eine flexible und sichere Push Infrastruktur bereitzustellen, die es ermöglicht, dass verschiedene Fachdienste Push Notifications an eine mobile Anwendung senden können. Durch die Implementierung eines zentralen Push Gateways pro FdV wird eine einheitliche Schnittstelle geschaffen, die als Fassade für die plattformspezifischen APIs von Anbietern wie Google und Apple fungiert. Dies erlaubt es mehreren Fachdiensten, gleichzeitig Push Notifications für vorher unbekannte FdVs bereitzustellen, ohne dass jeder Fachdienst individuell mit den plattformspezifischen APIs interagieren muss. Eine Anpassung der Fachdienste für zukünftige neue Push Provider ist ebenso nicht notwendig, da dafür ein neues oder angepasstes Push Gateway ausreicht.

Ein weiterer Vorteil dieses Ansatzes ist, dass die Credentials, die das Push Gateway gegenüber dem Push Provider autorisieren eine Push Nachricht an ein FdV zu senden, beim Push Gateway bleiben und nicht an alle Fachdienste weitergegeben werden müssen. Dadurch wird das Risiko eines unbefugten Zugriffs auf diese Geheimnisse minimiert und die Integrität der Kommunikation gewährleistet. Als Vorbild dient die Push Implementierung wie sie im Matrix Protokoll beschrieben ist.

Weitere Details und Beispiele sind auf Github ([Push_Notification_Generic_Concept]) zu finden. Neben einer detaillierten Beschreibung finden sich dort auch OpenAPI Dokumente für die konkreten Schnittstellen.

5 Spezifikation

Dieses Kapitel beschreibt die technischen Anforderungen und Spezifikationen für die Implementierung des Push Notification-Systems, das in den Fachdiensten und FdVs integriert wird. Ziel ist es, eine sichere und effiziente Kommunikation zwischen den Systemkomponenten zu gewährleisten, die den Nutzern zeitnahe Push Notifications über relevante Ereignisse ermöglicht.

5.1 Anforderungen an den Fachdienst

Der anwendungsspezifische Fachdienst verwaltet die Push Notifications für den jeweiligen Anwendungsfall. Der Fachdienst erstellt Push Notifications für abonnierte Ereignisse und übermittelt diese an das zuständige Push Gateway. Er bietet Schnittstellen für Versicherte zur Registrierung und Konfiguration von Pushern. Ein Pusher bezieht sich auf eine FdV-Instanz und ist eine Konfiguration im Fachdienst, in der die Informationen zur Adressierung der Push Notifications hinterlegt werden (u. a. das zu nutzende Push Gateway, Schlüssel zur Verschlüsselung von Nachrichteninhalten). Der Versicherte kann für mehrere Endgeräte Pusher im Fachdienst hinterlegen.

Nicht alle Anforderungen werden für alle Produkttypsteckbriefe Anwendung finden. Abhängig vom Produkt wird Verschlüsselung für Push Notifications notwendig sein oder nicht, entsprechende Afos entfallen daher gegebenenfalls. Es gelten nur die Afos, die auch im Produktsteckbrief zugeordnet sind.

Der anwendungsspezifische Fachdienst muss sich selbst um die Themen kümmern, die hier nicht festgelegt werden. Dazu gehören unter anderem das Festlegen von Triggern, das Bestimmen des Nachrichteninhalts und Autorisierungsthemen.

5.1.1 Pusher registrieren

A_27104 - Fachdienst - Push Notifications - OpenApi_Notification_Fachdienst

Der Fachdienst MUSS eine API mit den Endpunkten GET /pushers und POST /pushers/set anbieten. [Aktensystem_ePA, TI-M_FD_Basis, funkt. Eignung: Test Produkt/FA, <=]

Da ein anwendungsspezifischer Fachdienst jedoch zusätzliche Anforderungen an seine API haben kann, können dieser eigene Anforderung dazu formuliert, und ein einiges OpenApi auf der Basis [OpenApi_Notification_Fachdienst] definiert werden.

A_27154 - Fachdienst - FdV-Instanz registrieren - App-Registrierung anlegen

Der Fachdienst MUSS beim Aufruf der Operation POST /pushers/set prüfen, ob zu pushkey und app_id eine App-Registrierung existiert und bei negativem Ergebnis eine neue App-Registrierung mit den Daten aus dem Aufruf anlegen. [Aktensystem_ePA, TI-M_FD_Basis, funkt. Eignung: Herstellererklärung, <=]

A_27155 - Fachdienst - FdV-Instanz registrieren - App-Registrierung aktualisieren

Der Fachdienst MUSS beim Aufruf der Operation POST /pushers/set prüfen, ob zu pushkey und app_id eine App-Registrierung existiert und bei positivem Ergebnis, wenn kind nicht null ist,

- diese App-Registrierung mit den Daten aus dem Aufruf aktualisieren,

- eventuell gespeichertes kryptographisches Schlüsselmaterial (shared-secret-Jahr-Monat, AES/GCM-Schlüssel-Jahr-Monat) vor der neuen initialen Schlüsselableitung löschen.

[Aktensystem_ePA, TI-M_FD_Basis, funkt. Eignung: Herstellererklärung, <=]

A_27156 - Fachdienst - FdV-Instanz deregistrieren - App-Registrierung löschen

Der Fachdienst MUSS beim Aufruf der Operation POST /pushers/set prüfen, ob zu pushkey und app_id eine App-Registrierung existiert und bei positivem Ergebnis, wenn kind null ist,

- diese App-Registrierung mit den Daten aus dem Aufruf löschen,
- eventuell gespeichertes kryptographisches Schlüsselmaterial (shared-secret-Jahr-Monat, AES/GCM-Schlüssel-Jahr-Monat) löschen

[Aktensystem_ePA, TI-M_FD_Basis, funkt. Eignung: Herstellererklärung, <=]

A_27157 - Fachdienst - FdV-Instanz registrieren - Initiale Schlüsselableitung

Der Fachdienst MUSS beim Aufruf der Operation POST /pushers/set auf Basis des übermittelten initial shared secret (iss) eine Schlüsselableitung zum Jahr und Monat von time_iss_created vornehmen und das kryptographische Material (shared-secret-Jahr-Monat, AES/GCM-Schlüssel-Jahr-Monat) zur App-Registrierung speichern.

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

A_27158 - Fachdienst - Schlüsselableitung shared-secret-Jahr-Monat und AES/GCM-Schlüssel-Jahr-Monat

Der Fachdienst MUSS für die Anwendungsfälle für Push Notifications mit Verschlüsselung eine Schlüsselableitung nach "Hashed Message Authentication Code (HMAC)-based key derivation function" (HKDF) [RFC-5869] per HKDF(shared-secret-Jahr-Monat, IKM, L=64) nutzen und für das Input keying material (IKM) das Format "yyyy-MM" verwenden.

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

5.1.2 Operation Notify

A_27160 - Fachdienst - Push Notification senden - Schlüsselableitung

Der Fachdienst MUSS beim Auftreten eines Triggers für Push Notifications prüfen, ob für den Versicherten eine App-Registrierung existiert, und bei positivem Ergebnis, für jede App-Registrierung prüfen, ob für die App-Registrierung ein Schlüssel zum aktuellen Zeitpunkt (AES/GCM-Schlüssel-Jahr-Monat) gespeichert ist und falls nicht, basierend auf dem jüngsten vorliegenden Geheimnis (shared-secret-Jahr-Monat) schrittweise Schlüsselmaterial zu dessen Folgemonaten ableiten und speichern, bis die Schlüssel für den aktuellen Zeitpunkt vorliegen. [Aktensystem_ePA, Sich.techn. Eignung: Produktgutachten, <=]

A_27405 - Fachdienst - Schlüsselableitung - Alte Schlüssel löschen

Der Fachdienst MUSS nach jeder Schlüsselableitung alle Geheimnisse (shared-secret-Jahr-Monat) und Schlüssel (AES/GCM-Schlüssel-Jahr-Monat) für Push Notifications löschen, die älter als das jüngste Schlüsselmaterial sind. [Aktensystem_ePA, Sich.techn. Eignung: Produktgutachten, <=]

A_27680 - Fachdienst - Push Notification senden - Nachricht kodieren

Der Fachdienst MUSS den Nachrichteninhalte der Push Notifications mit UTF-8 kodieren.

[Aktensystem_ePA, funkt. Eignung: Test Produkt/FA, <=]

A_27161 - Fachdienst - Push Notification senden - Nachricht verschlüsseln

Der Fachdienst MUSS, wenn der Fachdienst Notifications verschlüsselt senden muss, beim Auftreten eines Triggers für Push Notifications prüfen, ob für den Versicherten eine App-Registrierung existiert und bei positivem Ergebnis, für jede App-Registrierung den Nachrichteninhalt mit dem Schlüssel aus der aktuellen Schlüsselableitung nach AES/GCM verschlüsseln und als Base64(IV || Ciphertext || Authentication Code) im Attribut ciphertext beim Erstellen der Push Notification verwenden.
[Aktensystem_ePA, Sich.techn. Eignung: Produktgutachten, <=]

A_27610 - Fachdienst - Push Notification senden - Größe des Nachrichteninhalts verschleiern

Der Fachdienst MUSS den in der Push Notification zu übermittelnden Nachrichteninhalt mit einer Größe von genau 1024 Bytes vor der Verschlüsselung wie folgt kodieren. Es werden folgende Daten konkateniert

1. die Zeichenkette "PNM1" (4 Bytes),
2. zwei Bytes Länge des folgenden Leerzeichenabschnitts im Network-Byte-Order (big-endian) berechnet mit:
maximale_verfügbare_Größe_für_Nachrichteninhalt - 4 - 2 - Länge(eigentliche Nachricht)
3. Anzahl von Leerzeichen (Character 32) wie bei 2 angeführt,
4. eigentliche Nachricht.

Die Konkatenation ist dann der zu verschlüsselnde Klartext.

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

Beispiel zu A_27610-*:

Die maximal verfügbare Größe für den Nachrichteninhalt sind 2048 Bytes. Die eigentliche Nachricht ist "test". Dann ist die Länge des Leerzeichenabschnitts = $1024 - 4 - 2 - 4 = 1014$.

Hexdump der Konkatenation: 504e4d31 07f6 020202...0202 74657374

A_27162 - Fachdienst - Push Notification senden - Einbetten des Zeitstempels

Der Fachdienst MUSS bei der Verschlüsselung einer Push Notification den Zeitpunkt der Schlüsselableitung im Format "yyyy-MM" in den metadaten (time_message_encrypted) der Push Notification einbetten. [Aktensystem_ePA, funkt. Eignung: Herstellererklärung, <=]

A_27163 - Fachdienst - Push Notification senden - Aufruf Push Gateway

Der Fachdienst MUSS beim Auftreten eines Triggers für Push Notifications prüfen, ob für den Versicherten eine App-Registrierung existiert und bei positivem Ergebnis für jede App-Registrierung den gespeicherten Endpunkt des Push Gateways unter Verwendung von [OpenApi_Notification_PushGateway] aufrufen. [Aktensystem_ePA, TI-M_FD_Basis, funkt. Eignung: Herstellererklärung, <=]

A_27652 - Fachdienst - Push Notification senden - Hinterlegte URL

Der Fachdienst MUSS sicherstellen, dass Push Notifications ausschließlich an die in der Registrierung der FdV-Instanz hinterlegte URL (aus: data/url) übermittelt werden.
[Aktensystem_ePA, Sich.techn. Eignung: Produktgutachten, <=]

A_27374 - Fachdienst - Push Notification senden - Aufruf Push Gateway Response verarbeiten

Der Fachdienst MUSS beim Versenden von Push Notification über ein Push Gateway das Ergebnis des Aufrufs verarbeiten und gegebenenfalls ungültig gewordene Pusher löschen.
[Aktensystem_ePA, TI-M_FD_Basis, funkt. Eignung: Herstellererklärung, <=]

Die Details der möglichen Antworten sind auf der OpenAPI-Seite zu finden [OpenApi_Notification_PushGateway].

A_27436 - Fachdienst - Keine personenbezogenen Klartextdaten in Push Notifications

Der Fachdienst DARF NICHT Push Notifications erzeugen und ans Push Gateway übermitteln, die unverschlüsselte personenbezogene Daten enthalten. [Aktensystem_ePA, TI-M_FD_Basis, Sich.techn. Eignung: Produktgutachten, <=]

Hinweis zu A_27436-*: Das Verbot von unverschlüsselten personenbezogenen Klartextdaten bezieht sich auf alle Informationen einer Push Notification, nicht nur auf den Benachrichtigungsinhalt.

A_27166 - Fachdienst - Exponential Back-off bei Fehlern im Versand an Push Gateway

Der Fachdienst MUSS bei Nichtverfügbarkeit des Push Gateways oder Fehlern beim Versand von Push Notifications die zu versendenden Push Notifications puffern und weitere Sendeveruche nach dem Prinzip des "exponential back-off" unternehmen, bis alle Push Notifications versendet wurden. [Aktensystem_ePA, TI-M_FD_Basis, funkt. Eignung: Herstellererklärung, <=]

Hinweis: Es ist zulässig, dass nach einer gewissen Zeit der Push-Versand abgebrochen wird, da davon ausgegangen werden kann, dass eine Push-Nachricht nur für einen gewissen Zeitraum für ein Event von Bedeutung ist.

5.2 Anforderungen an das Push Gateway

Das Push Gateway besitzt einen anwendungsübergreifenden Endpunkt, an den Push Notifications übermittelt werden. Das Push Gateway leitet die Informationen der Push Notification an den Push Provider weiter. Es wird vom Hersteller des FdV bereitgestellt, und es kann weitere Endpunkte für Dienste außerhalb der TI geben, die ebenfalls über dieses Push Gateway Notifications versenden.

A_27164 - Push Gateway - OpenApi_Notification_PushGateway

Das Push Gateway MUSS eine API gemäß [OpenApi_Notification_PushGateway] anbieten. [Push_Gateway, funkt. Eignung: Herstellererklärung, <=]

A_27165 - Push Gateway - Push Notification senden - Aufruf Push Provider

Das Push Gateway MUSS nach dem Aufruf des POST /notify Endpunkts den entsprechenden Push Provider auswählen und einen Request für eine Push Notification an den Push Provider senden, sodass die Notification am FdV empfangen werden kann. [Push_Gateway, funkt. Eignung: Herstellererklärung, <=]

A_27512 - Push Gateway - Direkte Kommunikation mit Push Provider

Das Push Gateway MUSS sicherstellen, dass Push Notifications ausschließlich an den Plattformspezifischen Push Provider gesendet werden. [Push_Gateway, Sich.techn. Eignung: Produktgutachten, <=]

A_27539 - Push Gateway - Keine Verarbeitung unverschlüsselter personenbezogener Daten

Das Push Gateway MUSS sicherstellen, dass keine unverschlüsselten personenbezogenen Daten im Push Gateway verarbeitet werden. [Push_Gateway, Sich.techn. Eignung: Produktgutachten, <=]

A_27611 - Push Gateway - Keine Rückschlüsse auf genutzte Anwendungen

Das Push Gateway MUSS sicherstellen, dass das Push Gateway an den Plattformspezifischen Push Provider keine Informationen zu Fachdiensten bzw. Anwendungen übermittelt. [Push_Gateway, Sich.techn. Eignung: Produktgutachten, <=]

Hinweis zu A_27611-*: Der plattformspezifische Push Provider soll u.a. nicht erkennen können, ob es sich um Push Notifications zur ePA oder zum E-Rezept handelt.

A_27435 - Push Gateway - Unverzügliches Löschen von Push Notification

Das Push Gateway MUSS Push Notifications nach Übermittlung an den Push Provider unverzüglich löschen. [Push_Gateway, Sich.techn. Eignung: Produktgutachten, <=]

A_27167 - Push Gateway - Prio Feld mappen

Das Push Gateway SOLL beim Aufruf des spezifizierten Endpunkts, wenn das Feld notification.prio vorhanden ist, diese Priorität an den Push Provider weitergeben. [Push_Gateway, funkt. Eignung: Herstellererklärung, <=]

Hinweis: Ein Implementierungsleitfaden ist unter [Push_Notification_Generic_Concept#priority] zu finden.

5.3 Anforderung an die FdV-Instanz

Die FdV-Instanz ist ein auf einem mobilen Endgerät installiertes FdV. Push Notifications werden für eine FdV-Instanz registriert und an diese gesendet. Die FdV-Instanz kann mehrere Anwendungen integrieren (ePA, E-Rezept, TI-Messenger, Kassenanwendungen), für die der Versicherte jeweils Push Notifications auswählen kann.

In der jeweiligen Fachdienst-Spezifikation wird geregelt, ob verschlüsselte oder unverschlüsselte Push Notification versendet werden.

Hinweis: Der Anwendungsfall "Push Notifications" ist optional für die FdV-Hersteller. Das wird auch so im Steckbrief stehen. Wenn sich ein FdV-Hersteller entscheidet, Push Notifications zu implementieren, gelten diese Anforderungen.

Da ein anwendungsspezifischer Fachdienst jedoch zusätzliche Anforderungen an seine API haben kann, können dieser eigene Anforderung dazu formuliert, und ein eigenes OpenApi auf der Basis [OpenApi_Notification_Fachdienst] definiert werden.

5.3.1 Schlüsselableitung für Push Notifications

A_27170 - FdV: Push Notifications - Schlüsselableitung shared-secret-Jahr-Monat und AES/GCM-Schlüssel-Jahr-Monat

Das FdV MUSS, wenn einer der Fachdienste verschlüsselte Push Notifications versendet, für die Anwendungsfälle für Push Notifications eine Schlüsselableitung nach "Hashed Message Authentication Code (HMAC)-based key derivation function" (HKDF) [RFC-5869] per HKDF(ISS, IKM, L=64) nutzen und für das Input Keying Material (IKM) das Format "yyyy-MM" verwenden. [FdV_Option_PushNotification, Sich.techn. Eignung: Produktgutachten, <=]

5.3.2 FdV-Instanz Registrieren

A_27168 - FdV: Push Notifications - Instanz registrieren - app_id

Das FdV MUSS im Anwendungsfall "FdV-Instanz registrieren" eine app_id haben, mit der sich das FdV für den Empfang von Push Notifications beim Fachdienst registrieren kann. [FdV_Option_PushNotification, funkt. Eignung: Herstellererklärung, <=]

Die app_id sollte ein "reverse-DNS style identifier" sein (zum Beispiel: "com.example.app.ios"). Wichtig ist, dass der Push Gateway später daraus ableiten kann, wie das FdV zu erreichen ist. Für iOS FdVs könnte hierfür der *Bundle Identifier* verwendet werden, für Android FdVs wäre dies der *Package Name*.

A_27171 - FdV: Push Notifications - Instanz registrieren - pushkey aktualisieren

Das FdV MUSS, wenn eine Einwilligung zum Empfang von Push Notifications vorliegt, nach dem Start der Anwendung überprüfen, ob sich das vom Push Provider zugewiesene pushkey geändert hat und in diesem Fall zuerst den alten pushkey löschen, und anschließend der Anwendungsfall "FdV-Instanz registrieren" durchführen.

[FdV_Option_PushNotification, funkt. Eignung: Test Produkt/FA, <=]

Hinweis: Die Einwilligung wird typischerweise auf dem Endgerät (z.B. iOS oder Android Gerät) lokal im System gespeichert und kann ggf. in den Systemeinstellungen des Betriebssystems widerrufen werden.

A_27172 - FdV: Push Notifications - Instanz registrieren

Das FdV MUSS den Anwendungsfall "FdV-Instanz registrieren" gemäß TAB_FdV_Registrieren umsetzen.

Tabelle 1: TAB_FdV_Registrieren - FdV-Instanz registrieren

Name	FdV-Instanz registrieren
Auslöser	<ul style="list-style-type: none"> Der Versicherte willigt in Push Notifications ein. Erneuerung des pushkey
Akteur	Versicherter
Vorbedingung	<ul style="list-style-type: none"> Der Nutzer hat sich gegenüber dem Fachdienst authentisiert.
Nachbedingung	<ul style="list-style-type: none"> FdV-Instanz ist registriert am Fachdienst zum Empfang von Push Notifications.
Standardablauf	<p>wenn der Fachdienst verschlüsselte Push Notifications versendet:</p> <ol style="list-style-type: none"> pushkey von Push Provider ermitteln initial shared secret (iss) erzeugen Aufruf zum Registrieren Initiale Schlüsselableitung Schlüssel speichern initial shared secret (iss) löschen <p>wenn der Fachdienst keine verschlüsselte Push Notifications versendet:</p> <ol style="list-style-type: none"> pushkey von Push Provider ermitteln Aufruf zum Registrieren

[FdV_Option_PushNotification, funkt. Eignung: Test Produkt/FA, <=]

Hinweis: Wenn sich das FdV bei mehreren Anwendungen registriert, muss der Prozess für jede Anwendung einzeln ausgeführt werden.

A_27173 - FdV: Push Notifications - Instanz registrieren - pushkey ermitteln

Das FdV MUSS im Anwendungsfall "FdV-Instanz registrieren" einen pushkey vom plattformspezifischen Push Provider nach dessen Vorgaben beziehen und speichern. [FdV_Option_PushNotification, funkt. Eignung: Herstellererklärung, <=]

A_27174 - FdV: Push Notifications - Instanz registrieren - initial shared secret (iss) erzeugen

Das FdV MUSS, wenn der Fachdienst verschlüsselte Push Notifications versendet, im Anwendungsfall "FdV-Instanz registrieren" einen HEX-String (32 Byte (256 Bit), 64 Zeichen Hexadecimal) als initial shared secret (iss) mit einer Entropie von mindestens 120 Bit erzeugen und den aktuellen Zeitpunkt im Format "yyyy-MM" als time_iss_created bestimmen. [FdV_Option_PushNotification, Sich.techn. Eignung: Produktgutachten, <=]

A_27175 - FdV: Push Notifications - Instanz registrieren - Aufruf

Das FdV MUSS im Anwendungsfall "FdV-Instanz registrieren" die HTTP-Operation POST/pushers/set des Fachdienstes ausführen. [FdV_Option_PushNotification, funkt. Eignung: Test Produkt/FA, <=]

A_27396 - FdV: Push Notifications - Instanz registrieren - Keine personenbezogenen Daten bei der Registrierung nutzen

Das FdV MUSS im Anwendungsfall "FdV-Instanz registrieren" sicherstellen, dass bei der Geräteregistrierung in den technisch erhobenen und übermittelten Registrierungsdaten keine personenbezogenen oder sicherheitskritischen Daten enthalten sind, insbesondere nicht die KVNR. Dies bezieht sich ausschließlich auf die vom System automatisch erfassten und verarbeiteten Daten.

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

Hinweis: Diese Anforderung betrifft nur die technisch erhobenen Daten. Eine Benennung von Geräten durch Nutzer, die personenbezogene Daten (wie z.B. die KVNR) enthält, kann technisch nicht verhindert werden und fällt nicht unter diese Anforderung.

A_27176 - FdV: Push Notifications - Instanz registrieren - Initiale Schlüsselableitung shared-secret-Jahr-Monat und AES/GCM-Schlüssel-Jahr-Monat

Das FdV MUSS für den Anwendungsfall "FdV-Instanz registrieren", WENN der Fachdienst verschlüsselte Push Notifications versendet, nach erfolgreicher Response des Fachdienstes für das Jahr und den Monat gemäß time_iss_created eine Schlüsselableitung durchführen. [FdV_Option_PushNotification, Sich.techn. Eignung: Produktgutachten, <=]

A_27177 - FdV: Push Notifications - Instanz registrieren - Speichern des kryptographischen Materials

Das FdV MUSS das neue Geheimnis (shared-secret-Jahr-Monat) und den neuen Schlüssel (AES/GCM-Schlüssel-Jahr-Monat) speichern, um diese für die Entschlüsselung von Push Notifications und eine erneute Ableitung nutzen zu können.

[FdV_Option_PushNotification, funkt. Eignung: Herstellererklärung, <=]

A_27375 - FdV: Push Notifications - Instanz registrieren - initial shared secret (iss) löschen

Das FdV MUSS für den Anwendungsfall "FdV-Instanz registrieren" nach erfolgreicher initialer Schlüsselableitung das initial shared secret (iss) löschen.

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

A_27664 - FdV: Push Notifications - Instanz registrieren - Registrierte Instanzen anzeigen

Das FdV MUSS es dem Nutzer ermöglichen, die registrierten Pusher anzuzeigen.

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

A_27665 - FdV: Push Notifications - Instanz löschen

Das FdV MUSS es dem Nutzer ermöglichen, registrierte Pusher zu löschen.
[FdV_Option_PushNotification, Sich.techn. Eignung: Produktgutachten, <=]

5.3.2.1 Push Notifications empfangen

A_27178 - FdV: Push Notifications empfangen

Das FdV MUSS den Anwendungsfall "Push Notifications empfangen" gemäß [gemF_PushNotification#TAB_FdV_Empfangen] umsetzen.

Tabelle 2: TAB_FdV_Empfangen Push Notifications empfangen

Name	Push Notifications empfangen
Auslöser	<ul style="list-style-type: none">Das FdV erhält eine Push Notification vom Push Provider
Akteur	
Vorbedingung	<ul style="list-style-type: none">Der Nutzer hat in den Empfang von Push Notification eingewilligtDas Push Gateway hat eine Push Notification für die FdV-Instanz gesendet
Nachbedingung	<ul style="list-style-type: none">Im FdV ist aktuelles Schlüsselmaterial gespeichert.Das FdV zeigt dem Nutzer eine Nachricht an.
Standardablauf	<ol style="list-style-type: none">Falls kein aktueller Schlüssel vorliegt: SchlüsselableitungPush Notification Nutzdaten entschlüsselnTitel/Text für Push Notification erzeugen (ggf. weitere/andere Inhalte)Nachricht anzeigen

[FdV_Option_PushNotification, funkt. Eignung: Test Produkt/FA, <=]

A_27179 - FdV: Push Notifications empfangen - Schlüsselableitung

Das FdV MUSS für den Anwendungsfall "Push Notifications empfangen" nach Erhalt einer Push Notification time_message_encrypted extrahieren und prüfen, ob hierfür passendes Schlüsselmaterial (AES/GCM-Schlüssel-Jahr-Monat) im FdV vorliegt.

Das FdV MUSS, falls kein zu time_message_encrypted passendes Schlüsselmaterial vorliegt und time_message_encrypted nach dem aktuellsten vorliegenden Geheimnis (shared-secret-Jahr-Monat) liegt, schrittweise neues Schlüsselmaterial basierend auf dem aktuellsten vorliegenden Geheimnis ableiten, bis die Schlüssel passend zu time_message_encrypted vorliegen. [FdV_Option_PushNotification, Sich.techn. Eignung: Produktgutachten, <=]

A_27180 - FdV: Push Notifications empfangen - Löschen alter Schlüssel

Das FdV MUSS nach jeder Schlüsselableitung alle Geheimnisse (shared-secret-Jahr-Monat) und Schlüssel (AES/GCM-Schlüssel-Jahr-Monat) für Push Notifications löschen, die älter als zwei Monate im Vergleich zum abgeleiteten Jahr-Monat sind.

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

A_27181 - FdV: Push Notifications empfangen - Benachrichtigungsinhalt entschlüsseln

Das FdV MUSS für den Anwendungsfall "Push Notifications empfangen" den Push Notification Nutzdaten mit dem Schlüssel (AES/GCM-Schlüssel-Jahr-Monat) passend zu time_message_encrypted nach AES/GCM entschlüsseln.

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

A_27612 - FdV: Push Notifications empfangen - Aktive Bestätigung bei Verlassen des FdVs

Falls Pushnachrichten Links enthalten, die dazu führen, dass das FdV verlassen wird, MUSS das FdV den Nutzer über Risiken informieren und eine aktive Bestätigung einfordern.[FdV_Option_PushNotification, Sich.techn. Eignung: Produktgutachten, <=]

Hinweis zu A_27612-*: Durch die Anforderung sollen z.B. Phishing-Angriffe verhindert werden.

5.3.2.2 Notifications aktivieren und deaktivieren

A_27182 - FdV: Push Notifications - Default deaktiviert

Das FdV MUSS sicherstellen, dass der Erhalt von Push Notifications in der Default-Einstellung nach Installation deaktiviert ist.[FdV_Option_PushNotification, funkt. Eignung: Herstellererklärung, <=]

A_27183 - FdV: Push Notifications - Option aktivieren

Das FdV MUSS dem Nutzer die Möglichkeit bieten das Erhalten von Push Notifications zu aktivieren.[FdV_Option_PushNotification, funkt. Eignung: Test Produkt/FA, <=]

A_27184 - FdV: Push Notifications - Option deaktivieren

Das FdV MUSS dem Nutzer die Möglichkeit bieten das Erhalten von Push Notifications zu deaktivieren und somit die Einwilligung zum Erhalt von Push Notifications zu widerrufen.

[FdV_Option_PushNotification, funkt. Eignung: Test Produkt/FA, <=]

A_27185 - Hersteller FdV: Datenschutzinformationen zu Push Notifications

Der Hersteller des FdV MUSS den Nutzer des FdV (z.B. in der Datenschutzerklärung) über folgende Punkte informieren:

- die Art der Datenübermittlung und die verbleibenden Risiken,
- welche Metainformation verarbeitet bzw. übertragen werden,
- über welchen plattformspezifischen Push Provider die Push Notifications gesendet werden,
- ob für den genutzten plattformspezifischen Push Provider ein der Europäischen Union der Sache nach gleichwertiges Datenschutzniveau besteht und falls dies nicht der Fall ist,
 - typische Risiken (z.B. erschwerte Durchsetzung von Betroffenenrechten, fehlende Kontrolle der Weiterverarbeitung und Übermittlung der Daten, fehlende Datenschutzaufsicht oder Zugriffe durch staatliche Stellen), und
 - spezifische Risiken, die sich konkret mit den übermittelten Daten in dem Drittland realisieren könnten - sofern dem Hersteller Informationen dazu vorliegen.

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

5.4 Optionale Anforderungen

Folgende Anforderungen sind optional in dem Sinne, dass ein Produktsteckbrief diese Anforderungen verwenden kann, sofern das Produkt das Feature verwenden soll.

Unterstützt ein Produkt ein Feature nicht, werden diese Anforderungen auch kein Teil des Produktsteckbriefes und sind somit auch nicht Teil der Anwendung.

5.4.1 Channel/Trigger Konfiguration

5.4.1.1 Fachdienst

A_27190 - Fachdienst - Push Notifications - Channels - OpenApi_Notification_Fachdienst

Der Fachdienst MUSS eine API mit den Endpunkten GET /channels, GET /channels/{pushkey} und POST /channels/{pushkey} anbieten.

[Aktensystem_ePA, funkt. Eignung: Test Produkt/FA, <=]

Da ein anwendungsspezifischer Fachdienst jedoch zusätzliche Anforderungen an seine API haben kann, können dieser eigene Anforderung dazu formuliert, und ein einiges OpenApi auf der Basis [OpenApi_Notification_Fachdienst] definiert werden.

A_27193 - Fachdienst - FdV-Instanz registrieren - Liste der event_ids des Geräts anlegen

Der Fachdienst MUSS beim Aufruf der Operation POST /pushers/set prüfen, ob zu pushkey und app_id eine App-Registrierung existiert und bei negativem Ergebnis eine neue Liste der event_ids, mit den Status not_set für jede event_id, für diese App-Registrierung speichern. [Aktensystem_ePA, funkt. Eignung: Herstellererklärung, <=]

A_27196 - Fachdienst - Push Notification senden - Status der event_id prüfen

Der Fachdienst MUSS beim Auftreten eines Triggers für Push Notifications folgende Schritte durchführen:

1. Prüfen, ob für den Versicherten eine App-Registrierung existiert.
2. Bei positivem Ergebnis: Für jede App-Registrierung prüfen, ob der Status der getriggerten event_id gleich "Enabled" ist.
3. Bei negativem Ergebnis: Die Operation für die geprüfte App-Registrierung ohne weitere Aktivität beenden

[Aktensystem_ePA, funkt. Eignung: Herstellererklärung, <=]

A_27197 - Fachdienst - FdV-Instanz deregistrieren - Liste der event_ids des Geräts löschen

Der Fachdienst MUSS beim Aufruf der Operation POST /pushers/set prüfen, ob zu pushkey und app_id eine App-Registrierung existiert und bei positivem Ergebnis, wenn kind null ist, die Liste der Status der event_ids löschen. [Aktensystem_ePA, funkt. Eignung: Herstellererklärung, <=]

5.4.1.2 FdV

A_27198 - FdV Push Notifications - Instanz registrieren - Channelkonfiguration anlegen

Das FdV MUSS, wenn der Fachdienst den Anwendungsfall "Channels/Trigger Konfiguration" implementiert hat, bei der Registrierung für Push Notifications sicherstellen, dass eine Channelkonfiguration im Fachdienst hinterlegt wird.

[FdV_Option_PushNotification, funkt. Eignung: Test Produkt/FA, <=]

A_27666 - FdV Push Notifications - Channelkonfiguration verwalten

Das FdV MUSS es dem Nutzer ermöglichen, die Channelkonfiguration zu verwalten.

[FdV_Option_PushNotification, funkt. Eignung: Test Produkt/FA, <=]

5.4.2 Push Notification Historie

Durch das Implementieren der Push Notification Historie wird es den FdVs ermöglicht auch nach dem einmaligen Empfang einer Push Notification erneut auf versendete Push Notifications zuzugreifen. Beispiele wie dieses Feature zum Einsatz gebracht werden kann, finden sich unter [Push_Notification_Optional_History].

5.4.2.1 Fachdienst

A_27531 - Fachdienst - Push Notifications - OpenApi_Notification_Fachdienst_History

Der Fachdienst MUSS eine API mit den Endpunkten GET /history/{notification_id} und GET /history/device/{pushkey} anbieten.
[, , <=]

Da ein anwendungsspezifischer Fachdienst jedoch zusätzliche Anforderungen an seine API haben kann, können dieser eigene Anforderung dazu formuliert, und ein eigenes OpenApi auf der Basis [OpenApi_Notification_Fachdienst] definiert werden.

A_27532 - Fachdienst - Push Notification senden - ReferenzID zur Historie mitschicken

Der Fachdienst MUSS beim Senden einer Push Notification eine zufällige und eindeutige ID als notification.identifizier senden und sie zusammen mit dem Inhalt der Push Notification speichern.
[, , <=]

Hinweis: Wenn ein Fachdienst Anforderungen an maximale Speicherdauer von Daten hat, sind diese ggf. auch für die Push Historie zu berücksichtigen.

5.5 Sicherheit

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 Zertifikate der Komponenten-PKI der TI verwendet werden. Aus Sicht der jeweiligen Komponente ist es wichtig mit dem richtigen Partner zu kommunizieren. Der Fachdienst soll sicher sein, die Notifications an den richtigen Push Gateway zu senden und der Push Gateway soll sicher sein, die Notifications vom richtigen Fachdienst zu erhalten.

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

Für die Festlegung von Maßnahmen zum Schutz der Informationen, die im Notification Service verarbeitet werden, erfolgt hier eine Schutzbedarfsfeststellung der maßgeblichen Informationsobjekte. Die Verwendung von Datenklassen erfolgt dabei gemäß der Methodik zur Schutzbedarfsfeststellung der gematik für die TI.

Tabelle 3: Schutzbedarf der Informationsobjekte, die für das Feature Push Notifications benötigt werden

Informationsobjekt	Beschreibung	Personenbezug	Vertraulichkeit	Integrität
FdV -> Fachdienst				
pushkey	FdV-Installationsspezifischer Identifier	nein	mittel Alleine nicht ausreichend, da im Push Gateway noch ein zusätzliches Geheimnis zum endgültigen Versand benötigt wird.	mittel Datenklasse: Daten ohne Sicherheitsrelevanz Eine Verletzung der Integrität würde zu einem Nichtfunktionieren des Features führen.
kind	Art des verwendeten Push Gateways (immer http)	nein	kein Schaden	mittel Datenklasse: Daten ohne Sicherheitsrelevanz Eine Verletzung der Integrität würde zu einem Nichtfunktionieren des Features führen.
app_id	Reverse DNS Style Identifier für das FdV	nein	kein Schaden	mittel Datenklasse: Daten ohne Sicherheitsrelevanz Eine Verletzung der Integrität würde zu einem Nichtfunktionieren des Features führen.

app_display_name	Identifiziert das FdV die den Pusher registriert hat	nein	kein Schaden	niedrig
device_display_name	Name des Gerätes das den Pusher registriert hat	nein	mittel Datenklasse: Daten ohne Sicherheitsrelevanz	mittel Ein falscher device_display_name könnte genutzt werden, um den Nutzer zu täuschen.
profile_tag	Identifiziert	nein	mittel Datenklasse: Daten ohne Sicherheitsrelevanz	mittel Datenklasse: Daten ohne Sicherheitsrelevanz
lang	Sprache	nein	gering	mittel Datenklasse: Daten ohne Sicherheitsrelevanz
data	<i>Dictionary</i>			
data.url	URL des Push Gateway das verwendet werden muss	nein	mittel Datenklasse: Daten ohne Sicherheitsrelevanz Verbindung durch mTLS gegenseitig abgesichert	mittel Datenklasse: Daten ohne Sicherheitsrelevanz Eine Verletzung der Integrität würde zu einem Nichtfunktionieren des Features führen.
data.format	Identifiziert für Form der Notification	nein	mittel Datenklasse: Daten ohne Sicherheitsrelevanz	mittel Datenklasse: Daten ohne Sicherheitsrelevanz Eine Verletzung der Integrität würde zu einem Nichtfunktionieren des Features führen.

data.*	Weitere, FdV spezifische Felder können hinzugefügt werden	nein siehe A_27396-*	mittel Datenklasse: Daten ohne Sicherheitsrelevanz	mittel Datenklasse: Daten ohne Sicherheitsrelevanz Eine Verletzung der Integrität würde zu einem Nichtfunktionieren des Features führen.
encryption	<i>Dictionary</i>			
encryption.method	Identifiziert für die verwendete Verschlüsselung	nein	kein Schaden	mittel Datenklasse: Daten ohne Sicherheitsrelevanz Eine Verletzung der Integrität würde zu einem Nichtfunktionieren des Features führen.
encryption.time_iss_created	Zeitpunkt ("<Jahr>-<Monat>") der Erzeugung des iss	nein	mittel Datenklasse: Daten ohne Sicherheitsrelevanz	mittel Datenklasse: Daten ohne Sicherheitsrelevanz
encryption.iss (Initial Shared Secret)	Basis für die Verschlüsselung von Nachrichten	nein	sehr hoch Das iss dient zum Schutz von med. Informationen	hoch Datenklasse: Daten mit Sicherheitsrelevanz
encryption.key_identifier	Identifiziert für den verwendeten Schlüssel	nein	mittel Datenklasse: Daten ohne Sicherheitsrelevanz	mittel Datenklasse: Daten ohne Sicherheitsrelevanz
append	Ja/Nein ob bestehende Pusher ersetzt werden sollen	nein	niedrig	mittel
Fachdienst -> Push Gateway -> FdV				

Notification	Push Notifications enthalten die verschlüsselte Nachricht, time_message_encrypted	nein	mittel Datenklasse: Daten ohne Sicherheitsrelevanz	mittel Datenklasse: Daten ohne Sicherheitsrelevanz
time_message_encrypted (Notification)	Zeitpunkt ("<Jahr>-<Monat>") der Verschlüsselung einer Push Notification	nein	mittel Datenklasse: Daten ohne Sicherheitsrelevanz	mittel Datenklasse: Daten ohne Sicherheitsrelevanz
Push Gateway				
Push-Provider Secret (Token/API-Key/Private Key)	Push-Provider spezifische Authentisierung für den Versand von Push Notifications für ein bestimmtes FdV	nein	hoch Das Secret erlaubt den Versand von Push Notifications an beliebige Instanzen eines FdV, sofern deren pushkey bekannt ist.	hoch Datenklasse: Daten mit Sicherheitsrelevanz Eine Verletzung der Integrität würde zu einem Nichtfunktionieren des Features führen.

Diese Bewertung lässt eine Verarbeitung der Informationsobjekte im Push Gateway ohne spezielle technische Maßnahmen - wie z. B. eine VAU - zu.

5.6 Betrieb

5.6.1 Betriebliche Steuerung des Push-Gateways

Die Frage, ob es eine betriebliche Steuerung des Push-Gateways geben soll und, wenn ja, in welchem Umfang, ist noch in interner Abstimmung und wird später nachgeliefert.

6 Dokumentenhaushalt

Punkt befindet sich noch in Klärung

angepasst: gemProdT_ePA_FdV Kapitel 4.1

7 Beispiele und Referenzimplementierungen

Beispiele und ggf. Referenzimplementierungen sind in der Dokumentation unter [Push_Notification_Github_Repo] zu finden.

8 Anhang A - Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung
AES	Advanced Encryption Standard
API	application programming interface
ePA	elektronische Patientenakte
FdV	Frontend des Versicherten
GCM	Galois/Counter Mode
HKDF	HMAC-based key derivation function
HMAC	Hashed Message Authentication Code
IKM	Input keying material
iss	initial shared secret
KVNR	Krankenversichertennummer
mTLS	mutual Transport Layer Security
TLS	Transport Layer Security
UTF-8	8-bit Unicode Transformation Format
VAU	Vertrauenswürdige Ausführungsumgebung

8.2 Abbildungsverzeichnis

Abbildung 1: Systemüberblick.....	10
-----------------------------------	----

8.3 Tabellenverzeichnis

Tabelle 1: TAB_FdV_Registrieren – FdV-Instanz registrieren.....	17
Tabelle 2: TAB_FdV_Empfangen Push Notifications empfangen.....	19
Tabelle 3: Schutzbedarf der Informationsobjekte, die für das Feature Push Notifications benötigt werden.....	23

8.4 Referenzierte Dokumente

8.4.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[Push_Notification_Github_Repo]	https://github.com/gematik/gem-push-notifications-concept
[Push_Notification_Generic_Concept]	https://gematik.github.io/gem-push-notifications-concept/#concept/concept.html
[OpenApi_Notification_Fachdienst]	https://gematik.github.io/gem-push-notifications-concept/#fd_openapi.html
[OpenApi_Notification_PushGateway]	https://gematik.github.io/gem-push-notifications-concept/#push_gateway_openapi.html
[Push_Notification_Generic_Concept#priority]	https://gematik.github.io/gem-push-notifications-concept/#concept/concept.html%23_priorit%C3%A4t
[Push_Notification_Optional_History]	https://gematik.github.io/gem-push-notifications-concept/#concept/optional-features.html%23_historie

8.4.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC-5869]	HMAC-based Extract-and-Expand Key Derivation Function (HKDF)

	https://datatracker.ietf.org/doc/html/rfc5869
[RFC2119]	Key words for use in RFCs to Indicate Requirement Levels https://datatracker.ietf.org/doc/html/rfc2119

9 Anhang C - Offene Punkte, Fragen

9.1 Betriebliche Steuerung des Push-Gateways

Die Frage, ob es eine betriebliche Steuerung des Push-Gateways geben soll und, wenn ja, in welchem Umfang, ist noch in interner Abstimmung und wird später nachgeliefert.