Änderung in gemSpec_Aktensystem_ePA4Aall

Abschnitt 2 wird geändert.

A_25149 wird ersetzt durch A_25149-01-01

A_25149 - ePA-Aktensystem - Rollentrennung ePA-Aktensystem und sektoraler IDP
Falls der Betreiber des ePA-Aktensystems auch einen sektoralen IDP betreibt, MUSS der Betreiber sicherstellen, dass die Erstellung oder Änderungen von IDToken beim sektoralen IDP und die Erstellung oder Änderungen der Mailadresse für die Geräteverwaltung sowie die Aktivitäten im Unlock Service im ePA-Aktensystem durch geeignete technische und organisatorische Maßnahmen so wirkungsvoll voneinander getrennt werden, dass ein einzelner Mitarbeiter des Betreibers nicht die Aktivitäten in beiden Diensten durchführen kann.**[<=]**

A_25149-01 - ePA-Aktensystem - Rollentrennung ePA-Aktensystem und sektoraler IDP
Falls der Betreiber des ePA-Aktensystems auch einen sektoralen IDP betreibt, MUSS der Betreiber sicherstellen, dass die Erstellung oder Änderungen von ID-Token beim sektoralen IDP und die Erstellung oder Änderungen der Mailadresse für die Geräteverwaltung im ePA-Aktensystem durch geeignete technische und organisatorische Maßnahmen so wirkungsvoll voneinander getrennt werden, dass ein einzelner Mitarbeiter des Betreibers nicht die Aktivitäten in beiden Diensten durchführen kann.**[<=]**

Es werden die Abschnitte 3.11, 3.15.1 und 3.18.1 geändert.

3.11 Geräteverwaltung

Die Geräteverwaltung ermöglicht ePA-FdVs die Registrierung und Verwaltung der vom Nutzer verwendeten Geräte ~~und wird durch zwei Services realisiert~~. Der Device Management Service stellt das API zum ePA-FdV für die Geräteverwaltung bereit und ist nur in einer VAU/authentisierten User Session erreichbar.

Bei erstmaliger Nutzung des Gerätesinitiiert das ePA-FdV die Geräteregistrierung und erhält dadurch eine DeviceID (bestehend aus deviceIdentifier und deviceToken), welche bei folgenden Verwendungen des ePA-FdV zur Identifizierung des Geräts verwendet wird. Eine neue Geräteregistrierung muss durch den Nutzer bestätigt werden. Der Zugriff auf ein Aktenkonto kann nur mit einem Gerät mit bestätigter Geräteregistrierung erfolgen. ~~wird eine Geräteregistrierung am ePA-Aktensystem im Rahmen der Nutzerauthentisierung gestartet~~ ~~, siehe auch~~ .

Der Device Management Service ermittelt dazu die für den Nutzer im ePA-Aktensystem hinterlegte E-Mail-Adresse und ~~übergibt diese dem Device Unlock Service. Der Device Unlock Service befindet sich außerhalb der VAU,~~ versendet bei der Geräteregistrierung eine E-Mail an den Nutzer ~~zur Verifikation~~ mit ~~dem Bestätigungslink~~ einem generierten Geräteregistrierungsscode. ~~Bestätigt ein Nutzer die Geräteregistrierung mittels Bestätigungslink, so empfängt und verarbeitet der Device Unlock Service diese Freischaltinformation.~~ Der Nutzer sendet den Geräteregistrierungscode unter Verwendung des ePA-FdV zurück an den Device Management Service und bestätigt dadurch die Registrierung des neuen Geräts. Das Gerät kann nach der Bestätigung uneingeschränkt mit einem Aktenkonto genutzt werden

~~**A_24823 - Device Unlock Service - Erreichbarkeit**~~

~~Das ePA-Aktensystem MUSS sicherstellen, dass der Device Unlock Service außerhalb von VAU/User Session erreichbar ist. <=~~

~~A_24824 - Device Unlock Service - Verification Information erzeugen~~

~~Der Device Unlock Service MUSS bei der Geräteregistrierung als Aufruf durch den Device Management Service einen deviceIdentifier (UUID) als eindeutigen Bezeichner für dieses Gerät und einen zugehörigen Verification Link erzeugen, im Device Unlock Service persistieren und an den Device Management Service zurückgeben. Der Verification Link MUSS genau diese Geräteregistrierung eindeutig adressieren und als URL aus dem Internet aufrufbar sein. <=~~

~~A_24974 - Device Unlock Service - Zufälligkeit des Verification Links~~

~~Der Device Unlock Service MUSS sicherstellen, dass der Verification Link eine Zufallszahl (base64-kodiert) mit mindestens 120 Bit Entropie und Erzeugung gemäß [gemSpec_Krypt#GS-A_4367] beinhaltet. <=~~

~~A_24825 - Device Unlock Service - E-Mail versenden~~

~~Der Device Unlock Service MUSS an alle E-Mail-Adressen, die bei der Geräteregistrierung übergeben werden, eine E-Mail für den Nutzer in einer verständlichen Form mit folgenden Informationen versenden:~~

- ~~Verification Link~~
- ~~Zweck der E-Mail.~~
- ~~Zeitpunkt des Starts des Freischaltprozesses. <=~~

~~A_24826 - Device Unlock Service - Device Verification durchführen~~

~~Falls der Device Unlock Service einen gültigen Verification Link als Bestätigung des Nutzers zur Geräteregistrierung empfängt, MUSS das registrierte Gerät im Device Management Service als verifiziert gekennzeichnet werden. Anschließend MUSS der Device Unlock Service den Verification Link löschen. Ein ungültiger Verification Link führt ausschließlich zu einer für den Nutzer verständlichen Fehlermeldung.~~

~~A_25167 - Device Unlock Service - Löschen der E-Mail-Adresse nach Versand Verification Link~~

~~Der Device Unlock Service MUSS die E-Mail-Adresse des Nutzers nach dem Versand der E-Mail mit dem Verification Link löschen. <=~~

~~A_24975 - Geräteverwaltung - Protokollierung der Zugriffe auf Inhalte der Geräteverwaltung~~

~~Die Geräteverwaltung MUSS bei Anlage oder Änderungen von Einträgen zu registrierten Geräten des Versicherten oder eines Vertreters jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:~~

~~Tabelle 25: Device Management Service Protokollierung~~

~~Strukturelement~~	~~Wert~~	~~Erläuterung~~
~~AuditEvent.type~~	~~"rest"~~	~~Bei Änderungen über die Api~~
	~~"object"~~	~~Bei Änderungen durch den Authorization Service oder die~~

			~~Geräteverwaltung selbst (Device Unlock Service)~~
~~AuditEvent.action~~	~~C~~		~~Erzeugen einer neuen Geräteregistrierung~~
~~-~~	~~D~~ ~~-~~		~~Löschen einer Geräteregistrierung durch den assoziierten Nutzer oder Löschen einer Geräteregistrierung nach Ablauf Wartezeit für Bestätigung~~
~~-~~	~~U~~		~~Ändern des Status einer Geräteregistrierung durch den Device Unlock Service~~
~~AuditEvent.entity.name~~	~~"DeviceRegistration"~~		~~Setzen, Löschen und Anpassen von Geräteregistrierungen~~
~~AuditEvent.entity.detail~~	~~**type**~~	~~**value[x]**~~	~~-~~
~~-~~	~~"DeviceStatus"~~	~~<Status der Registrierung>~~	~~Status "pending" oder "verified"~~
~~-~~	~~"UserName"~~	~~<Name des Nutzers>~~	~~DisplayName des zugeordneten Nutzers des Geräts (Versicherter oder Vertreter)~~
~~-~~	~~"UserId"~~	~~<KVNR>~~	~~KVNR des zugeordneten Nutzers des Geräts (Versicherter oder Vertreter)~~

~~**A_24917 - Device Management Service - Registrierung - E-Mail ermitteln**~~

~~Der Device Management Service MUSS bei einer Geräteregistrierung die für diesen Nutzer hinterlegten E-Mail-Adressen ermitteln und an den Device Unlock Service übergeben. <=~~

~~A_24918 - Device Management Service - Registrierung - deviceToken~~

~~Der Device Management Service MUSS bei einer Geräteregistrierung ein deviceToken erzeugen mit:~~

- ~~Zufallszahl als String von 64 Zeichen mit einer Mindestentropie von 120 Bit gemäß [gemSpec_Krypt#GS-A_4367],~~
- ~~eindeutig in der Menge aller für diese KVNR hinterlegten deviceToken.~~

~~<=~~

~~A_24920 - Device Management Service - Registrierung - Registrierung speichern~~

~~Der Device Management Service MUSS bei einer Geräteregistrierung die folgenden Inhalte für diesen Nutzer persistieren:~~

- ~~createdAt (Zeitpunkt der Erzeugung)~~
- ~~deviceToken (gemäß A_24918*)~~
- ~~deviceIdentifier (gemäß A_24824*)~~
- ~~status="pending" (Status der Registrierung als nicht verifiziert gekennzeichnet)~~
- ~~displayName (vom Hersteller vergebener Gerätename)~~

~~<=~~

~~A_14518 - Device Management Service - Freischaltprozess Freischalt-URL Transportsicherheit~~

~~Der Device Management Service MUSS in der generierten Freischalt-URL das https-Protokoll verwenden.~~
~~<=~~

~~A_14522-02 - Device Management Service - Freischaltprozess beenden~~

~~Der Device Management Service MUSS den Vorgang eines Freischaltprozesses zu `DeviceID` und Nutzer nach 6 Stunden Wartezeit beenden. Dieses beinhaltet auch die Löschung des Verification Links. Der ungültige Verification Link führt bei Nutzung ausschließlich zu einer für den Nutzer verständlichen Fehlermeldung. <=~~

neue Anforderungen:

A_25270 - Device Management Service - Erzeugung von Geräteinformationen und Geräteregistrierungscode bei der Geräteregistrierung
Der Device Management Service MUSS bei der Geräteregistrierung für das zu registrierende Gerät eines Nutzers

- einen deviceIdentifier als aktensystemweit eindeutigen Gerätebezeichner (uuid),
- ein deviceToken als eine Zufallszahl als String mit 64 Zeichen mit einer Mindestentropie von 120 Bit gemäß [gemSpec_Krypt#GS-A_4367] und
- eine zufällige sechsstellige natürliche Zahl als Geräteregistrierungscode

erzeugen.**[**<=**]**

A_25271 - Device Management Service - Speicherung der Geräteinformationen
Der Device Management Service MUSS bei einer Geräteregistrierung eines Geräts eines Nutzers folgende Inhalte für den Nutzer verschlüsselt mit einem Schlüssel gemäß A_24853-* persistieren:

- decviceIdentifier
- deviceToken
- createdAt (Zeitpunkt der Erzeugung des deviceTokens)
- lastUse
- status
- displayName
- Geräteregistrierungscode,
- Fehlerzähler.

[<=**]**

A_25272 - Device Management Service - Pseudonyme Speicherung der Geräteinformationen
Der Device Management Service MUSS sicherstellen, dass die Zuordnung der außerhalb der VAU persistierten verschlüsselten Geräteinformationen zum Nutzer eindeutig ist und durch ein Pseudonym erfolgt.**[**<=**]**

A_25273 - Device Management Service - Gültigkeitsdauer des Geräteregistrierungscodes
Der Device Management Service MUSS sicherstellen, dass der bei der Geräteregistrierung erzeugte Geräteregistrierungsscode maximal 6 Stunden nach Erzeugung der DeviceID (createdAt) für die Verifikation eines Gerätes genutzt werden kann.**[**<=**]**

A_25274 - Device Management Service - Löschen nach Gültigkeitsdauer des Geräteregistrierungscodes
Der Device Management Service MUSS sicherstellen, dass dass die Geräteinformationen für eine nicht bestätigte Geräteregistrierung nach Ende der Gültigkeitsdauer des Geräteregistrierungscodes gelöscht werden.**[**<=**]**

A_25275 - Device Management Service - Versenden des Geräteregistrierungscodes per E-Mail
Der Device Management Service MUSS bei der Geräteregistrierung für den Nutzer, für den das Gerät registriert werden soll, alle im Aktensystem hinterlegten E-Mail-Adressen ermitteln und an alle ermittelten E-Mail-Adressen eine E-Mail in einer für den Nutzer verständlichen Form mit folgenden Informationen versenden:

- Zweck der E-Mail,
- Geräteregistrierungsscode,
- Gültigkeitsdauer des Geräteregistrierungscodes.

[<=**]**

A_25276 - Device Management Service - Bestätigung mittels Geräteregistrierungscodes
Der Device Management Service MUSS für einen übergebenen Geräteregistrierungscode und eine übergebene DeviceID (deviceIdentifier und deviceToken) prüfen, ob der vom Device Management Service bei der Geräteregistrierung erzeugte Geräteregistrierungscode für das angebene Gerät (deviceIdentifier, deviceToken) mit

dem übergebenen Geräteregistrierungscode übereinstimmt sowie der Geräteregistrierungscode zeitlich gültig ist und

1. bei Gleichheit und
   a. zeitlicher Gültigkeit
      - den Status für die Geräteregistrierung wechseln, so das die erfolgreiche Bestätigung des Geräts aus dem Status hervorgeht,
      - den Geräteregistrierungscode und den Fehlerzähler aus den Geräteinformationen löschen und
      - den Zeitpunkt der erfolgreichen Bestätigung in lastUsed erfassen,
   b. zeitlicher Ungültigkeit
      - alle Geräteinformationen zu diesem deviceIdentifier löschen,
2. bei Ungleichheit den Fehlerzählerder Geräteinformation um eins erhöhen und
   - falls der Fehlerzähler größer oder gleich fünf ist,
     - alle Geräteinformationen zu diesem Gerät löschen.

[<=]

A_25277 - Device Management Service - Sperrung bei vermehrter Anzahl von abgebrochenen Geräteregistrierungen
Falls für einen Nutzer innerhalb von 1/3 Erdentagen drei Geräteregistrierungen abgebrochen werden mussten, MUSS der Device Management Service sicherstellen, dass dieser Nutzer für 1/3 Erdentage ab dem Zeitpunkt der dritten abgebrochenen Geräteregistrierung keine Geräte mehr registrieren darf.**[<=]**

A_25291 - ePA-Aktensystem - Health Record Context nur mit verifizieren Gerät
Das ePA-Aktensystem MUSS sicherstellen, dass ein Versicherter (auch wenn er als Vertreter agiert) einen Health Record Context ausschließlich mit einem verifizierten Gerät öffnen kann, außer für den Fall, dass sich der Versicherte am ePA-FdV des Vertreters anmeldet (d.h. `x-authorize-representative=True` bei der Operation `I_Authorization_Service::sendAuthorizationRequestFdV`).**[<=]**

3.15.1 Anforderungen an den Authorization Service für die Authentisierung von Versicherten (FdV)

~~Im Rahmen der Authentisierung des Versicherten erfolgt nach einer erfolgreichen Authentisierung, die Prüfung, ob das Gerät des Nutzers registriert ist. Ist dies nicht der Fall, so wird die Geräteregistrierung im Device Management Service gestartet.~~

~~Weitere Anforderungen zum Device Management Service befinden sich in Kapitel ❑ *ML-144543 - Missing cross-reference* .~~

Im Rahmen der Authentisierung des Versicherten erfolgt die Prüfung der Geräteregistrierung (Verifikation) direkt. Das Gerät muss dafür die Geräteparameter eines zuvor ausgeführten und bestätigten Registrierungsprozesses verwenden.

Bisher nicht registrierte Geräte, bzw. Geräteparameter einer bisher nicht bestätigten Geräteregistrierung, können unter Verwendung des Device Management Services registriert, bzw. bestätigt werden <siehe: Verweis auf Geräteverwaltung >

A_25310 ist neue Anforderung

A_25310 - Authorization Service - Einschränkung bei Authentifizierung mit einem unregistrierten Gerät
Falls keine DeviceID übergeben wird und der Nutzer nicht mit `x-authorize-representative=True` authentisiert wurde, MUSS der Authorization Service sicherstellen, dass der Nutzer ausschließlich Zugriff auf den Device Management Service erhält**[<=]**

Hinweis: Ein vollständiger Zugriff eines authentisierten Nutzers auf alle Dienste des Aktensystems kann nur mit einem Gerät erfolgen, dessen Geräteregistrierung bei der Authentifizierung des Nutzers erfolgreich verifiziert wurde.

A_24804 wird ersetzt durch A_24804-01

Hinweis:A_24804-01 wird auch durch den Change C_11682 verändert

A_24804 - Authorization Service - Prüfung auf registriertes Gerät
Der Authorization Service MUSS bei der Authentifizierung eines Versicherten prüfen, ob die in der Operation `I_Authorization_Service::sendAuthCodeFdV` übergebene DeviceID auf den authentifizierten Nutzer registriert und verifiziert ist, wenn der Wert `DeviceID` nicht `AUTHORIZE_REPRESENTATIVE` ist.**[<=]**

A_24804-01 - Authorization Service - Prüfung auf registriertes Gerät
Falls es sich nicht um eine Authentifizierung eines Versicherten am ePA-FdV des Vertreters handelt und im Operationsaufruf `I_Authorization_Service::sendAuthCodeFdV` eine DeviceID (deviceIdentifier und deviceToken) übermittelt wird, MUSS der Authorization Service bei der Authentifizierung eines Versicherten prüfen, ob die übergebene DeviceID auf den authentifizierten Nutzer registriert und bestätigt ist und übereinstimmt.**[<=]**

A_24914 wird ersetzt durch A_24914-01

A_24914 - Authorization Service - Prüfung auf registriertes Gerät - kein registriertes Gerät
Falls keine bzw. unbekannte DeviceID übergeben wurde MUSS der Authorization Service:

- nach der Authentisierung des Nutzers die Geräteregistrierung in Device Management Service starten, welcher eine DeviceID (deviceIdentifier und deviceToken) erzeugt,
- die Operation `I_Authorization_Service::sendAuthCodeFdV` mit dem HTTP-Status 403 (Forbidden) mit ErrorCode = "unknownDevice", DeviceID mit deviceIdentifier und deviceToken abbrechen

[<=]

A_24914-01 - Authorization Service - Prüfung auf registriertes Gerät - kein registriertes Gerät
Falls eine unbekannte DeviceID (deviceIdentifier und deviceToken) übergeben wurde, MUSS der Authorization Service die Operation sendAuthCodeFdV mit einer Fehlermeldung abbrechen und die User Session beenden.**[<=]**

A_24936 wird entfernt (wird auch durch den Change C_11682 verändert)

~~**A_24936 - Authorization Service - keine Geräteregistrierung bei AUTHORIZE_REPRESENTATIVE**~~
~~Falls DeviceID = AUTHORIZE_REPRESENTATIVE übergeben wird MUSS der Authorization Service sicherstellen, dass keine Geräteregistrierung erfolgt.[<=]~~

A_24915 wird ersetzt durch A_24915-01

A_24915 - Authorization Service - Prüfung auf registriertes Gerät - registriertes Gerät nicht verifiziert
Falls eine nicht verifizierte DeviceID in der Operation send_AuthCode übergeben wurde MUSS der Authorization Service die Operation mit HTTP-Status 403 (Forbidden) mit ErrorCode = "pendingDevice" abbrechen.**[<=]**

A_24915-01 - Authorization Service - Prüfung auf registriertes Gerät - registriertes Gerät nicht bestätigt
Falls eine DeviceID (deviceIdentifier und deviceToken) einer unbestätigten Geräteregistrierung übergeben wurde (status == 'pending'), MUSS der Authorization Service die Operation sendAuthCodeFdV mit einer Fehlermeldung abbrechen und die User Session beenden.**[<=]**

3.18.1 Übersicht der Schnittstellen des Aktensystems

abelle 1: Übersicht der Schnittstellen des Aktensystems

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
....	
I_Device_Management_Insurant	
Schnittstelle zur Geräteverwaltung aus der Umgebung des Versicherten	
`getDevice`	Diese Operation ruft eine bestimmte Geräteregistrierung ab.
`getDevices`	Diese Operation ruft alle Geräteregistrierungen ab.
`updateDevice`	Diese Operation ändert den Displayname einer Geräteregistrierung.
`deleteDevice`	Diese Operation löscht eine bestimmte Geräteregistrierung.
`registerDevice`	Diese Operation erzeugt eine neue Geräteregistrierung und neue Geräteparameter
`confirmDevice`	Diese Operation bestätigt eine neue Geräteregistrierung mit einem Geräteregistrierungscode
....	

Änderung in gemSpec_ePA_FdV

Änderung in Kapitel 6.1.4 Geräteregistrierung

Um einen möglichen Missbrauch und Identitätsdiebstahl erkennen zu können, wird eine Berechtigungsprüfung für das Gerät des Nutzers umgesetzt. Hierzu wird bei erstmaliger Nutzung des Gerätes eine Geräteregistrierung am ePA-Aktensystemaufgerufen ~~im~~

~~Rahmen der Nutzerauthentisierung gestartet~~. Als Ergebnis wird an das FdV die DeviceID mit ~~der~~ deviceIdentifier als Gerätekennung und das deviceToken als Sicherheitsmerkmal zurückgegeben. Diese~~s deviceToken~~ DeviceId wird für den Nutzer im FdV persistent gespeichert und ~~muss~~ kann beim Login am ePA-Aktensystem für die Überprüfung der Registrierung des verwendeten Geräts mitgegeben werden. Der Zugriff auf ein Aktenkonto ist erst nach erfolgreicher Prüfung der DeviceID möglich

~~Der Zugriff auf ein Aktenkonto ist zulässig, wenn das Gerät, auf dem das FdV genutzt wird, durch den Nutzer über einen separaten Benachrichtigungskanal (E-Mail mit Freischalt-Link) zur Benutzung eines Aktenkontos autorisiert wurde.~~

Die DeviceID einer neuen Geräteregistrierung muss vor der Verwendung durch den Nutzer in der Geräteverwaltung des Aktensystemseinmalig bestätigt werden. Dafür erhält der Nutzer über einen separaten Benachrichtigungskanal (E-Mail) den Geräteregistrierungscode (Confirmation Code) für dieses Gerät.

Neue Anforderungen in Kapitel 6.2.4.1 Login User

A_25293 - ePA-Frontend des Versicherten: Login - neues Gerät registrieren
Falls das verwendete Gerät des Nutzers noch nicht registriert ist, MUSS das ePA-Frontend des Versicherten im Anwendungsfall "Login User" die Geräteregistrierung unter Verwendung der Operation`registerDevice` gemäß [I_Device_Management_Insurant.yaml] aufrufen.**[<=]**

Neue Anforderungen in Kapitel 6.2.10 Geräteverwaltung

A_25237 - ePA-Frontend des Versicherten: registriertes Gerät bestätigen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, den Geräteregistrierungscode (Confirmation Code) zur Bestätigung einer neuen Geräteregistrierung einzugeben und diesen mit der Operation `confirmDevice` gemäß [I_Device_Management_Insurant.yaml] an das Aktensystem senden**[<=]**

A_25292 - ePA-Frontend des Versicherten - Eingabe eines falschen Geräteregistrierungscodes
Falls der Device Management Service dem ePA-FdV für den vom Versicherten am ePA-FdV eingegebenen Geräteregistrierungscode (Confirmation Code) in einer Fehlermeldung einen Fehlerzähler zurückmeldet, weil der Geräteregistrierungscode nicht zum deviceIdentifier passt, MUSS das ePA Frontend des Versicherten dem Versicherten ermöglichen, erneut einen Geräteregistrierungscode einzugeben und den Versicherten darauf hinweisen, dass sich die Anzahl der erlaubten Versuche zur Eingabe des Geräteregistrierungscodes reduziert hat.
[<=]