Grobkonzept Anbindung von mobilen Devices ans EPD

Serge Bignens

Oliver Egger

Im Auftrag von:

ehealthsuisse

Kompetenz- und Koordinationsstelle
von Bund und Kantonen

Centre de compétences et de coordination
de la Confédération et des cantons

Centro di competenza e di coordinamento
di Confederazione e Cantoni

8. Mai 2019 Version 1.0

Impressum

Realisierung durch	Serge Bignens Consulting Pfingstweidstrasse 98 8005 Zürich ahdis gmbh c/o The Hub Zürich Association Sihlquai 131 8005 Zürich
Autoren	Serge Bignens, Serge Bignens Consulting Oliver Egger, ahdis gmbh
Stand	8. Mai 2019 | Version 1.0
Review	
Dokumentgeschichte	Version 0.7 Erste Version vor Stakeholder-Interview Version 0.8 nach Stakeholder-Interview Version 0.9 Abgabe Auftragsgeber und mHealth Gruppe Version 1.0 Schlussversion
Gender	Überall, wo in diesem Dokument, nur die männliche Form benutzt wird, sind die weibliche und männliche Form zu verstehen.

INHALTSVERZEICHNIS

1 Auftrag

Es soll ein Grobkonzept erarbeitet werden, das Anhand von Anwendungsfällen die technischen und organisatorischen Rahmenbedingungen für die Anbindung von mHealth-Anwendungen ans EPD beschreibt.

Auf der technischen Seite werden u. a. die Authentisierung, das Lesen und Schreiben von Dokumenten der App-Anwender sowie mögliche Schnittstellen thematisiert. Betrachtet werden mobile Gesundheitsapplikationen für Patienten, Applikationen für Gesundheitsfachpersonen sind abgegrenzt. Dabei werden immer die vorgegebenen Rahmenbedingungen, die sich aus dem Gesetz und den Verordnungen ergeben, berücksichtigt.

Das Grobkonzept wird einerseits im Rahmen der Arbeitsgruppe mHealth und bei vier Stakeholdern validiert. Zu Letzteren gehören eine Person von Seiten der Stammgemeinschaft, eine von Seiten Spitäler, ein EPD-Technologie-Anbieter und ein Start-up, welches die App entwickelt.

1.1 Ausgangslage und Vorarbeiten der mHealth-Gruppe von eHealthSuisse

Dieser Konzeptbericht integriert Resultate von Vorarbeiten der Arbeitsgruppe mHealth von eHealth Suisse und basiert auf folgenden Berichten (komplette Referenzen und links zu den elektronischen Versionen sind im Appendix zu finden).

- Empfehlung I zu mHealth [1]
- Empfehlungen zur Nutzung von technischen Normen und Standards im Bereich mHealth [2]
- Juristisches Gutachten zum Thema Datenschutz [3]
- Transparenz schaffen und Orientierung bieten – Methoden und Werkzeuge als Entscheidungshilfe für die Nutzung von Gesundheits-Apps [7]
- Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer [8]

1.2 Ausgangslage Sicht Patient

Für den Patienten (mHealth-Anwender), der eine oder mehrere Gesundheits-Apps mit dem EPD anbinden will, wird Folgendes vorausgesetzt:

- Das EPDG [4] ist in Kraft.
- Mehrere Gemeinschaften und Stammgemeinschaften sind zertifiziert und in Betrieb.
- Mindestens ein eID-Provider (für Patienten-Identifikation) ist zertifiziert und steht für die Stammgemeinschaften zur Verfügung.
- Mehrere Gesundheits-Apps bieten die Anbindung an sein EPD an.
- Der Patient (oder die Patientin) verfügt schon über ein EPD. Das heisst:
    - Er ist bei einer Stammgemeinschaft registriert.
    - Er ist bei (mindestens) einem eID-Provider registriert und kann sich durch die Dienste der eID-Provider identifizieren und authentisieren.
    - Seine Stammgemeinschaft verwaltet die Verknüpfung (mindestens) mit einer eID und einem EPD (via MPI oder einer anderen IT-Komponenten der Stammgemeinschaft).
    - Er nutzt eine oder mehrere Gesundheits-Apps, die mit seinem EPD angebunden ist.
    - Er nutzt das Patienten-Portal der Stammgemeinschaft.

1.3 Anwendungsfälle

Um einerseits die verschiedenen Ziele und Nutzen von mHealth im Auge zu haben und anderseits bei Gesprächen und Konzeptarbeiten sich auf konkrete Beispiele stützen zu können, wurden (ohne Anspruch auf Vollständigkeit) einige repräsentative Anwendungsfälle (siehe Glossar für Definitionen) skizziert:

Anwendungs-fall	Beispiel	Abfragen /Lesen *)	Hochladen /Schreiben *)
Disease Management	Diabetiker-App, Medikationsplan wird gelesen, wöchentliche Verlaufskurven seines glykämischen Indexes werden in seinem EPD geschrieben	ja	ja
Gesundheits-Tagebuch	Monatlicher Bericht mit Gewicht-, Blutdruck- und Schmerztagebuch wird geschrieben	Nicht zwingend	ja
Lifestyle-Tagebuch (quantified self)	Schlafqualität, Anzahlschritte, Blutdruck, Stresslevel werden mit Sensor gemessen und als Bericht oder strukturierte Datensätze geschrieben	Nicht zwingend	ja
Klinische Forschung	Medikationsplan, Diagnostik, Scores, Berichte werden gelesen, PROM (Patient Reported Outcome Measures) können geschrieben werden	ja	Nicht zwingend
Vor- oder Nach-Behandlung	Medikationsplan wird gelesen, Selbstevaluation vom Gesundheitszustand, Medikamenteneinnahmen werden rapportiert und geschrieben	ja	ja

Abbildung 1 Anwendungsfälle

*) Das Lesen (oder Abfragen) und das Schreiben (oder Hochladen) aus dem eigenen respektive ins eigene EPD.

Bei allen diesen Anwendungsfällen sind die Abläufe identisch:

1. Der Anwender öffnet seine mHealth-App (oder startet diese, wenn sie noch nicht gestartet war).
2. Für die Anbindung der App an das EPD authentisiert er sich mit seiner eID.
3. Er kann Dokumente (diese können Datensätze beinhalten) in seinem EPD schreiben/hochladen (diese selber erfassten Daten sind nicht ärztlich validiert).
4. Er kann Dokumente aus seinem EPD lesen/abfragen.

1.4 Abgrenzungen Grobkonzept

Die Themen mHealth, EPD, API, Sicherheit und Semantik sind sehr breit. In diesem Bericht, der sich auf der Stufe Grobkonzept befindet, wurden nachfolgende Abgrenzungen gemacht. Abgegrenzte Themen können je nach Priorität in weiteren Studien bearbeitet bzw. verfeinert werden.

1) IOT (Internet of Things), z. B. ein Vital-Wert-Sensor, der direkt mit dem Internet verbunden wird, wird in diesem Grobkonzept nicht betrachtet. Unter Mobile Devices sind Smartphones und darauf laufende Gesundheits-Apps berücksichtigt.
2) Das Konzept ist limitiert auf mobile Gesundheitsapplikationen für Patienten. Mobile Applikationen für Gesundheitsfachpersonen werden hier nicht behandelt.
3) Das Konzept gilt für mobile Gesundheitsapplikationen, die via eines App Stores (z. B. *Apple App Store* oder *Google Play Store*) herausgegeben werden, nicht aber für Web-Apps oder Web-Portale, die via Browser des Smartphones erreichbar sind.
4) «*Machine-to-Machine*»- oder «*Server to Server*»- oder auch «*Backend*»-Anbindungen für die Integration von Sensor-Messdaten ins EPD (zum Beispiel die Anzahl Schritte direkt von der Fitbit Cloud ins EPD importieren) werden nicht berücksichtigt.
5) Die speziellen Anforderungen an mobile Applikationen, die unter Software als *medical device* klassifiziert werden, werden hier nicht behandelt.
6) Die Semantik (Austauschformate, Dokument- oder Datensatz-Ansatz) wird hier nicht bearbeitet und sollte in einem Folgeschritt angegangen werden.
7) Bei den Anwendungsfällen wurde auf die Funktion Zugriffsrechte verwalten verzichtet. Dies aufgrund der Hypothese, dass in einem ersten Schritt die Funktion Zugriffsrechte verwalten nur von der Stammgemeinschaft zur Verfügung gestellt wird, nicht aber durch Dritte.
8) Die Auswirkung der Anbindung von Gesundheits-Apps ans EPD und die daraus entstehenden Implikationen an das EPD-Gesetz [4] und dessen Ausführungsrecht [5] muss separat analysiert werden. Wo grössere potenzielle Auswirkung identifiziert wurden, wird dies im Bericht erwähnt – ohne Anspruch auf Vollständigkeit und juristische Korrektheit.
9) Die Detailspezifikation und Zertifizierungsbedingungen der für die Anbindung von Gesundheits-Apps ans EPD resultierende neue Schnittstellen sind nicht Bestandteil dieses Konzeptdokuments.

2 Konzept Technische Anbindung

2.1 EPD, Vertrauensraum, Gemeinschaften, Portale und Apps

Aus der in den Kapiteln 1.2 und 1.3 beschriebenen Ausgangslage und den Anwendungsfällen kann man davon ausgehen, dass folgende Vorgänge möglich sind:

- Ein Patient greift via des Patientenportals seiner Stammgemeinschaft auf alle seine EPD-Dokumente zu. Die Dokumente werden in den jeweiligen Gemeinschaften gespeichert und via Vertrauensraum dem Patienten zugänglich gemacht. Der Patient hat auch die Möglichkeit, selbst Dokumente in seinem EPD zur Verfügung zu stellen.
- Diese Funktionalität soll der Patient auch auf einer oder mehreren Gesundheits-Apps zur Verfügung haben, die an sein EPD angebunden sind.
- Aus einer App muss er sich
    a) identifizieren/authentisieren können
    b) Dokumente schreiben und Dokumente lesen können.

Diese Ausgangslage, und insbesondere die drei letzteren Funktionen, sind in der folgenden Abbildung dargestellt:

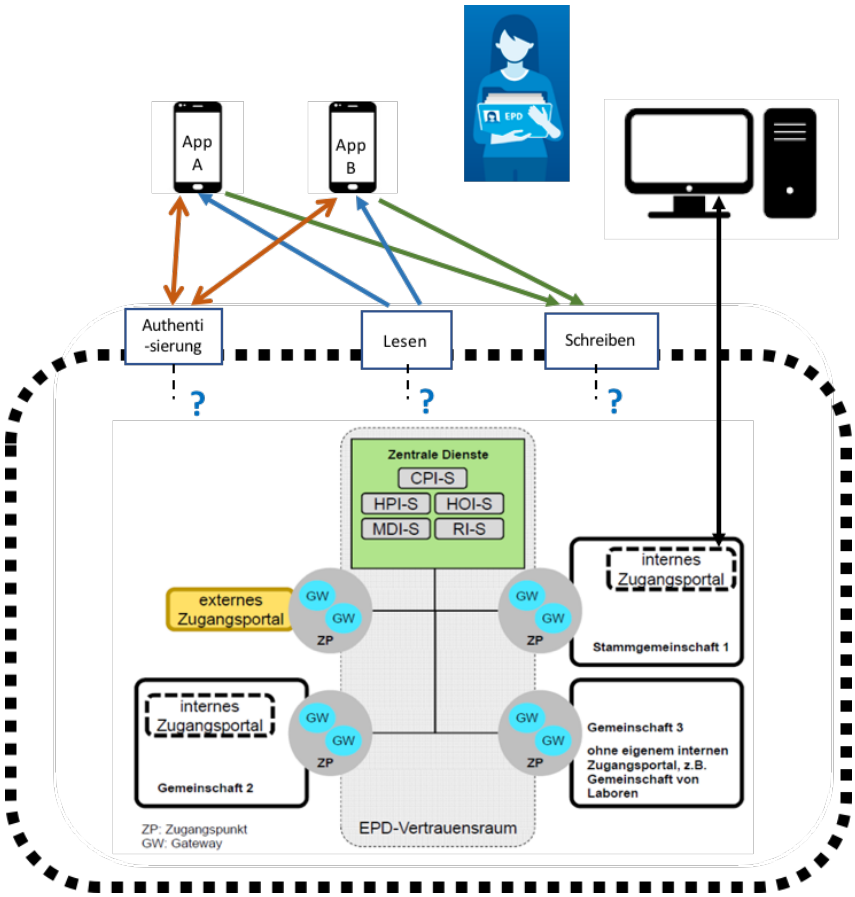


Abbildung 2 Gesundheitsapp Anbindung an EPD

Weiter sind in diesem Bericht Lösungsvorschläge dokumentiert, die es einer Gesundheits-App erlaubt, sich an das EPD anzubinden, um diese Funktionen ausführen zu können.

2.2 Anbindungsvarianten

Für jede der drei Funktionen Authentisierung, Dokument schreiben und Dokument lesen wurden die folgenden Anbindungsmöglichkeiten analysiert (ersichtlich auf der nächsten Abbildung):

A. Anbindung via dem externen Zugangsportal
B. Direkte Anbindung an den Vertrauensraum
C. Anbindung via Stammgemeinschaften

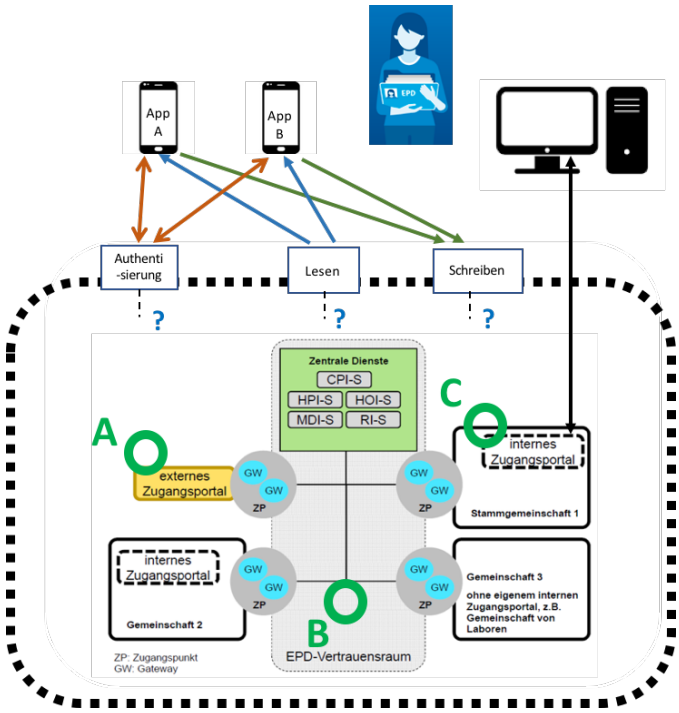


Abbildung 3 Anbindungsmöglichkeiten

2.2.1 Analyse der Variante A, Anbindung via externes Zugangsportal

Ein externes Zugangsportal wäre für nur lesende mHealth-Apps einfacher.

Externe Zugangsportale sind im Gesetz und im Botschaftsbericht [6] zum Gesetz Teil der EPD-Infrastruktur. Sie bieten die Möglichkeit für Patienten, auf ihr EPD zuzugreifen via andere Portale als dem Patientenportal der Stammgemeinschaft. Diese Funktion wurde spezifiziert für das Lesen von Dokument, nicht aber, um Dokumente zu schreiben.

Die Anforderungen für externe Zugangsportale sind bis jetzt aber im Ausführungsrecht nicht präzisiert:

- Das Mapping der eID zu der MPI-ID in den anderen Gemeinschaften müsste realisiert werden. Diese Funktionalität ist in den bestehenden technischen Ergänzungen nicht definiert.
- Ein Assertion Token muss vom Zugangsportal erstellt werden.
- Entsprechende Auditevents müssen generiert werden.

Diese Variante würde Änderungen auf Gesetzesebene (u. a. für das Schreiben via externes Zugangsportal) und auf Aufführungsrechtsebene (u. a. für Schnittstellen-Spezifikationen, ID-Management und allfälligen Zertifizierungsbedingungen) benötigen.

2.2.2 Analyse der Variante B, Direkte Anbindung an den Vertrauensraum

Eine direkte Anbindung an den Vertrauensraum würde der Gesundheits-App erlauben, direkt mit allen Gemeinschaften über ein Gateway und mit den Cross-Community IHE-Profilen zu kommunizieren.

Wie bei der Variante A müssten das Mapping der elektronischen ID, die Assertion Token sowie die Auditevents definiert werden.

Zusätzlich muss ein zentraler Anbindungspunkt (in der Abbildung dargestellt mit dem grünen Kreis bei B) zu Verfügung gestellt werden. Dieser wäre äquivalent wie die Gateways der Gemeinschaften, die auch einen Zugangspunkt mit einem Gateway für einkommende Kommunikation und ein Gateway für ausgehende Kommunikation betreiben müssen. Dieser zentrale Anbindungspunkt müsste eine zusätzliche Aufgabe der zentralen Dienste sein.

Eine weitere Herausforderung gibt es für die Schreiben-Funktion. Wo, in welchem Dokument-Registry und -Repository sollten die Metadaten respektive die Inhalte der vom Patienten via Gesundheits-App, geschriebenen Dokumenten gespeichert und verwaltet werden? Sollte dies in einem zentralen Dokument-Registry und -Repository für mHealth-Dokumente sein, würde dies dem Ansatz der dezentralen Dokumentenverwaltung des EPD widersprechen.

Diese Variante bedingt Änderungen auf Gesetzesebene (u. a. für das Betreiben dieses zusätzlichen Gateways und Dokument-Registry und -Repository) und auf Aufführungsrechtsebene (u.a. für Schnittstellen Spezifikationen, ID Management und allfälligen Zertifizierungsbedingungen).

2.2.3 Analyse der Variante C, Anbindung an die Stammgemeinschaft

Eine Anbindung via Stammgemeinschaften ermöglicht einerseits das Mapping der eID zu der MPI-ID (dies wird im Kapitel 2.4 näher beschrieben) und anderseits das Schreiben von mHealth-Dokumenten des Patienten dezentral in Dokument-Registry und -Repository seiner Stammgemeinschaft.

Dafür müssen die Stammgemeinschaften eine neue Komponente, die in diesen Bericht «*Mobile Access Portal*» oder «*internes mHealth Zugangsportal*» genannt wird, zu Verfügung stellen und höchstwahrscheinlich zertifizieren lassen.

Damit eine App nicht an einzelne Stammgemeinschaft proprietär angebunden werden muss, sollen folgende Interoperabilitätsvorgaben gelten:

- technisch müssen die Schnittstellen (ansprechbar durch ein *internes mHealth-Zugangsportal*) von allen Stammgemeinschaften für die Gesundheits-App die gleichen sein und
- organisatorische und allfällige vertragliche Konditionen, die zwischen den Gesundheits-App-Herausgebern und den Stammgemeinschaften abzumachen sind, sollten nicht dazu führen, dass nur Patienten bestimmter Stammgemeinschaften auf ihre Dokumente via eine bestimmte Gesundheits-App zugreifen können. Dieses Fragmentierungsrisiko wurde auch im Bericht «Datenschutz und Informationssicherheit im Bereich ‘mobile health’ (mHealth)» [3] identifiziert und sollte bei einer Überarbeitung des Aufführungsrechts berücksichtigt werden.

Diese Variante bedingt Änderungen auf Aufführungsrechtsebene [5] (u. a. für Schnittstellen-Spezifikationen, ID-Management und allfällige Zertifizierungsbedingungen) und eventuell auf Gesetzesebene [4].

2.2.4 Schlussfolgerung und Wahl der Variante C

Aus der Analyse der Autoren und bestätigt durch die Gespräche mit den verschiedenen Stakeholdern wurde die Variante C mit einem internen mHealth-Zugangsportal (Mobile Access Portal) gewählt und empfohlen für die weitere Arbeiten.

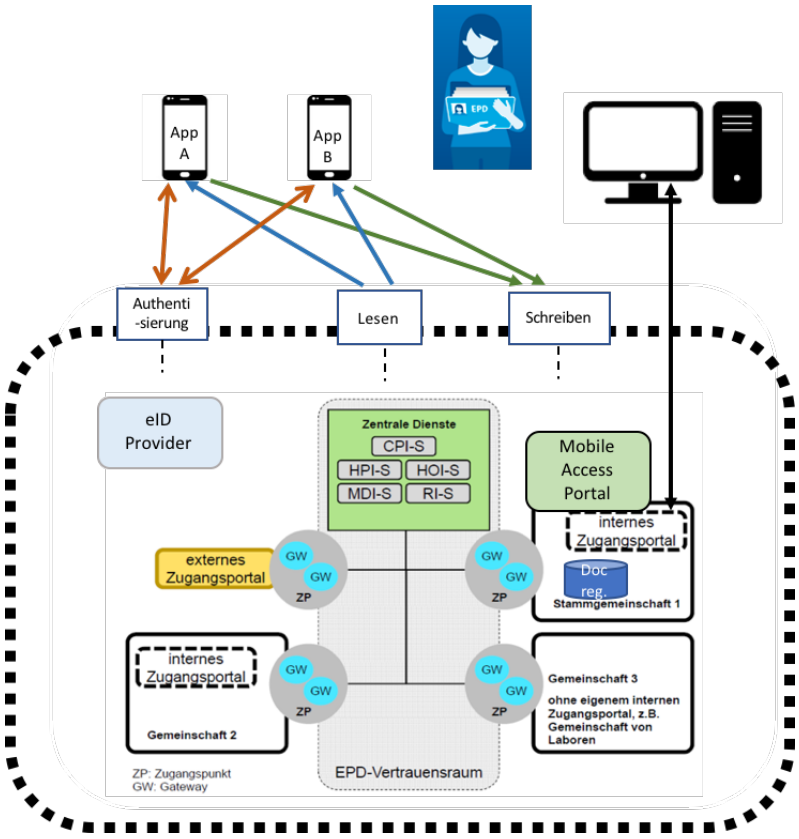


Abbildung 4 Anbindung an die Stammgemeinschaft mit dem Mobile Access Portal

Die Hauptgründe sind:

- Variante A braucht grössere Gesetzänderungen für das Schreiben von Dokumenten, und führt, wie Variante B zu zentralen Dokument-Registry und -Repository.
- Variante B führt zu zentralen Dokument-Registry und -Repository und braucht einen neuen Betreiber für die zusätzlichen Gateways zum Vertrauensraum.

Die Variante C bedingt neue Aufgaben für die Stammgemeinschaften: das Realisieren, Zertifizieren und Betreiben eines «*Mobile Access Portal*». Damit die Gesundheits-App-Landschaft in der Schweiz nicht zerstückelt wird, braucht es Richtlinien für organisationale und vertragliche Anbindungen von Gesundheits-App an allen Stammgemeinschaften.

Empfehlung 1: Die mHealth-Anbindung ans EPD zum Lesen und Schreiben soll via Stammgemeinschaften mit einem *internen mHealth-Zugangsportal* (*Mobile Access Portal*) implementiert werden.

2.2.5 Übergang von Architektur zu Sequenzdiagrammen

Um dem Leser dieses Dokumentes den Übergang vom Lesen dexyr Architektur-Schemen zur Interpretation der Sequenzdiagramme zu erleichtern, wurden die gleichen Farben für die gleichen Schichten angewendet:

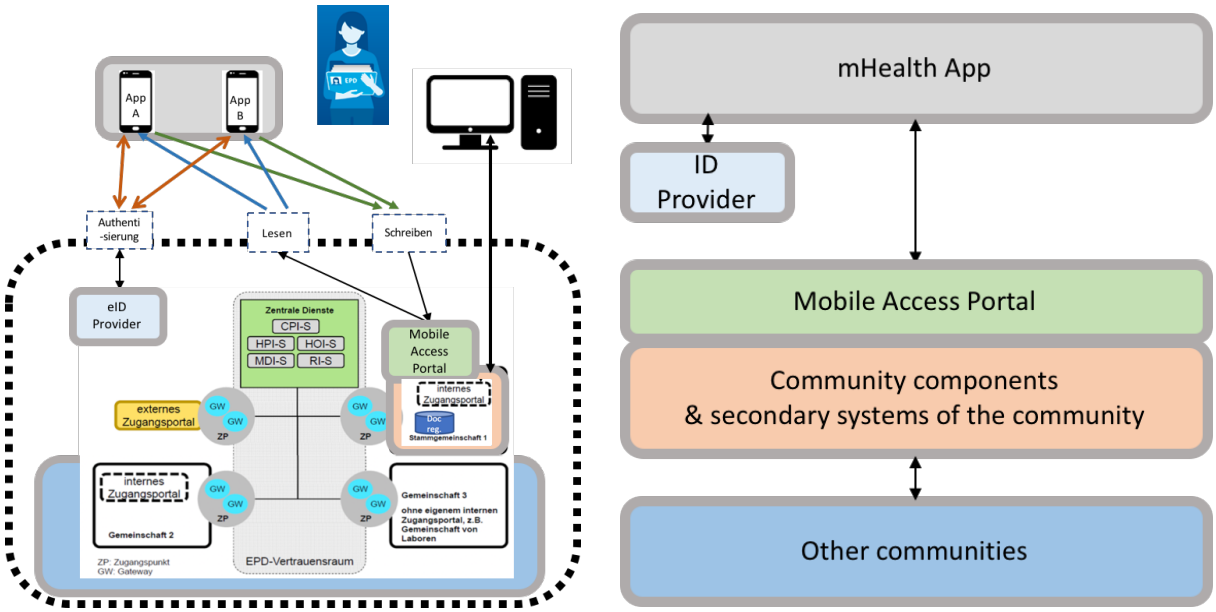


Abbildung 5 Farbecode bei der Architekturschemen

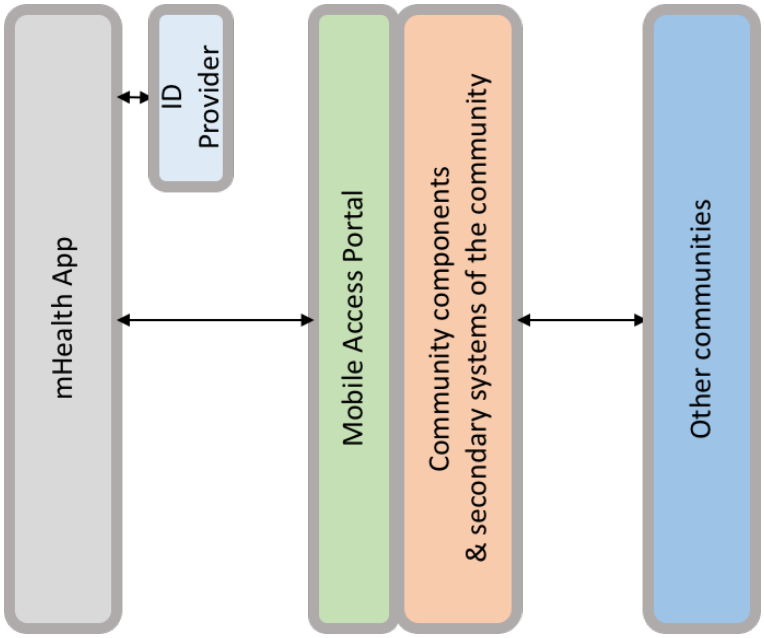


Abbildung 6 Farbecode bei den darunter stehenden Sequenzdiagrammen

2.3 Anbindung einer App ans EPD via Mobile Access Portal

In diesem Kapitel wird eine mögliche Anbindungs-Architektur für das Mobile Access Portal beschrieben, um die verschiedenen Funktionen (Authentifizieren, Lesen und Schreiben) zu definieren. Diese Architektur stützt sich auf die Empfehlungen 2–4 aus dem Dokument «Mobile Health und das elektronische Patientendossier, Empfehlungen zur Nutzung von technischen Standards und Normen» [2] .

2: SMART-on-FHIR-Ansatz verfolgen
Der Smart-on-FHIR-Ansatz ermöglicht es, vom Primärsystem entkoppelte Apps zu entwickeln. Es gibt bereits erste Projekte in der Schweiz, die diesen Ansatz verfolgen. Damit der Ansatz realisiert werden kann, müssen die FHIR-Ressourcen den schweizerischen Vorgaben angepasst werden (Profilierung). Wichtig ist dabei auch, dass die Abbildung auf die Austauschformate des EPD definiert wird, damit keine Integrationshürde zwischen mHealth und EPD entsteht.
3: Erweiterung der EPDV um mobile Web-Technologien
Um das EPD für Mobile Apps attraktiv zu gestalten, soll eine Erweiterung der EPDV um OpenID Connect aufgenommen werden. Das vereinfacht die Authentifizierung an zertifizierten IdP, JSON Web Token für die Autorisierung und die IHE Mobile Integration Profiles. So kann eine höhere Akzeptanz bei den App-Entwicklern erreicht werden.
4: Einsatz der mobilen Integrationsprofile von IHE
Um das EPD für Mobile Apps attraktiv zu gestalten, soll eine Erweiterung der EPDV die mobilen Integrationsprofile von IHE (MHD, PDQm, PIXm) aufnehmen. So kann eine höhere Akzeptanz bei den App-Entwicklern erreicht werden.

Tabelle Empfehlungen aus Mobile Health und das EPD [6]

Mit dem Mobile Access Portal wird eine Gateway-Architektur ermöglicht, mit der die App eine Schnittstelle zum Mobile Access Portal hat, die dem SMART-on-FHIR-Ansatz folgt, mobile Web-Technologien wie OpenID Connect unterstützt sowie mit den mobilen Integrationsprofilen IHE-Dokumente gelesen und geschrieben werden können. Das Mobile Access Portal kann diese Aufrufe dann entsprechend in die gemäss Ausführungsrechts geforderten Profile/Transaktionen umsetzen.

Für die drei Funktionen des Mobile Access Portals (authentisieren, Dokumente lesen und Dokumente schreiben) wird jeweils ein Sequenzdiagramm beschrieben.

2.3.1 Authentisierung

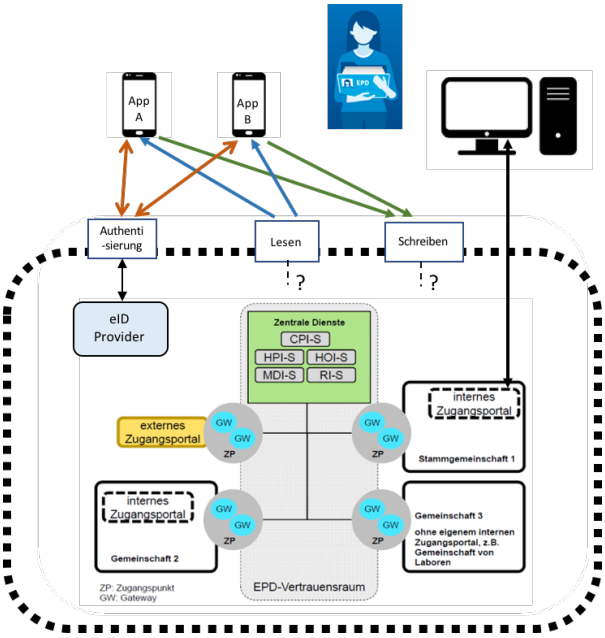
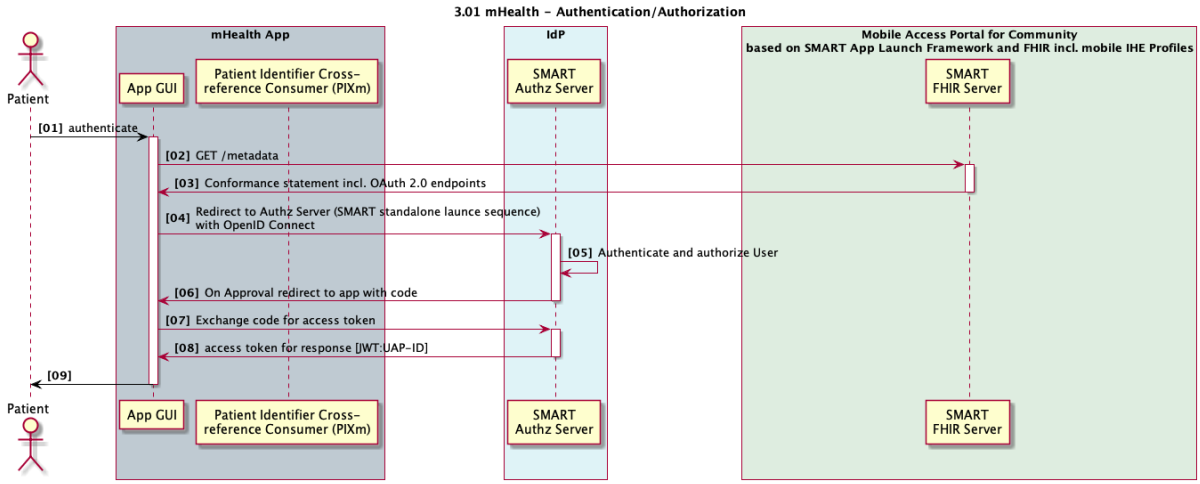


Abbildung 7 Authentisierung

Es wird davon ausgegangen, dass die gleichen eID-Provider für die App benutzt werden, wie sie für das EPDG zertifiziert sind. Somit muss der App-Nutzer für die Anbindung der mHealth-App mit seinem EPD sich mit seiner eID authentisieren. Der Benutzer muss der App den Zugriff entsprechend autorisieren. Eine weitere Voraussetzung ist, dass der Patient sich mit seiner eID in der Stammgemeinschaft schon registriert hat.

Um das EPD für Mobile Apps attraktiv zu gestalten, soll eine Erweiterung des Ausführungsrecht in Anhang 8 OpenID Connect aufnehmen. OpenID Connect basiert auf OAuth 2.0. Das vereinfacht die Authentifizierung an zertifizierten IdP, JSON Web Token für die Autorisierung und für die IHE Mobile Integration Profiles. Das heisst, der eID-Provider müsste entsprechend auch das OpenID-Connect-Verfahren anbieten, gemäss angepasstem Anhang 8.

Das SMART App Launch Framework von HL7[1] definiert verschiedene Arten, wie sich eine App mit einem EHR verbinden kann. Mit dem Anwendungsfall «Provider apps that launch standalone» ist ein Verfahren basierend auf OpenID Connect beschrieben, das auf diesen als Grundlagenarchitektur für die Anbindung einer App ans EPD angewendet werden kann.



[1] http://www.hl7.org/fhir/smart-app-launch/index.html

Abbildung 8 Authentisierung

- Die mHealth-App fragt beim Mobile-Access-Portal der Stammgemeinschaft das Conformance Statetement an (Schritt 2). Im Conformance Statement des FHIR-API müssen die URLs zurückgegeben werden, unter denen sich der Benutzer authentisieren und er die App autorisieren kann (Schritt 3). Damit kann die App die «Standalone launch sequence» verwenden (siehe SMART Application Launch Framework Implementation Guide Release 1.0.0[2]).
- Für die Authentisierung/Autorisierung spezifiziert SMART OpenID Connect. Die eID-Provider müssten dies entsprechend unterstützen. Der eID-Provider gibt für einen Patienten einen entsprechenden Code zurück, und zwar nach der Authentisierung des Users und der Authorisierung der App (Schritt 4-6).
- Die App kann mit dem Code das JWT Access Token vom IdP abfragen (UAP-ID) (Schritt 7-8).

Folgende Punkte sollten in einer Detailspezifikation noch erarbeitetet bzw. geklärt werden:

- Wie weiss die App, welche Stammgemeinschaften es unter welchen Endpunkten gibt? Sollten diese vom zentralen Dienst zu Verfügung gestellt werden oder ist dies der App überlassen?
- Welche zusätzlichen Einschränkungen auf die Funktionalität vom SMART App Launch Framework müssen gemacht werden? Darf ein Offline Access Token (für den Zugriff, falls der User nicht mehr online ist) verwendet werden? Und wenn ja, für wie lange? Siehe dazu auch Empfehlung 3: «Datenschutz und Informationssicherheit im Bereich 'mobile health' (mHealth)» [3])
- Die Apps müssen sich beim SMART Authz Server (IdP) registrieren. Soll dies via OAuth 2.0 Dynamic Client Registration Protocol direkt geschehen? Oder kann dies indirekt via Mobile Access Portal gemacht werden? Siehe dazu auch die Diskussion von ähnlichen Anwendungsfällen[3].
- Die Angaben der eID (UAP-ID) im Token muss festgelegt und ggfs. Müssen weitere Parameter definiert werden. Können ggfs. weitere Claims (wie zum Beispiel die MPI-ID) dem Token hinzugefügt werden?
- Der Aufruf des Conformance Statement (Schritt 2) vom Mobile Access Portal wie auch der IdP müssen über das Internet verfügbar sein.

Empfehlung 2: Detailspezifikation für das SMART App Launch Framework erarbeiten und im Ausführungsrecht festlegen.

[2] http://hl7.org/fhir/smart-app-launch/index.html

[3] https://docs.google.com/document/d/1yMNGDtB2X_6Maj8MAeVVv3ZI4z0X6LZAo5SisPuT_6k/edit

2.3.2 Verknüpfung/Übersetzung Patienten Identitäten zwischen App und EPD

Der App-Anwender authentisiert sich mit seiner eID (UAP-ID). Dies muss die gleiche eID sein, die er für die Authentisierung mit dem Stammgemeinschaftsportal braucht. Für den Zugriff auf die Dokumente im EPD in einer Gemeinschaft wird mit der MPI-ID gearbeitet. Die eID muss in die MPI-ID der Stammgemeinschaft übersetzt werden. Dadurch kann gewährleistet werden, dass die App nicht mit der Patientenidentifikationsnummer (EPRS-PID) verknüpft werden kann (siehe auch Empfehlung 2: «Datenschutz und Informationssicherheit im Bereich 'mobile health' (mHealth)» [3]).

Das Mobile Access Portal bietet die Übersetzung der eID (UAP-ID) zur MPI-ID die in der Gemeinschaft gemäss dem IHE-PIXm-Profil an.

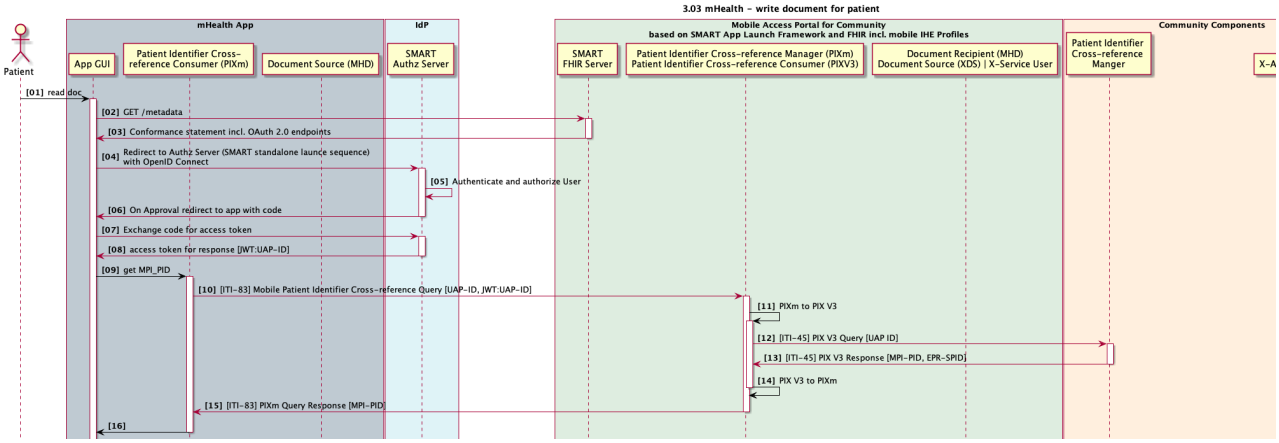


Abbildung 9 Patientenidentität in der Gemeinschaft

Nachdem der Benutzer authentisiert ist (Schritt 2-8), kann die MPI-ID auf Grund der UAP-ID mit der [ITI-83]-Transaktion des IHE PIXm Profils aufgelöst werden (Schritt 8).

Der PIXm Akteur Patient Identifier Cross-reference Manager kann mit dem PIX V3 Akteur Patient Identifier Cross-reference Consumer (PIXV3) gruppiert werden (Schritt 11–14), dies ist im Diagramm zur Verständlichkeit gezeigt, ist aber nicht zwingend.

Folgende Punkte sollten in einer Detailspezifikation noch erarbeitetet bzw. geklärt werden:

- Für IHE PIXm sollte in einer National Extension definiert werden, dass nur die MPI-ID der Gemeinschaft abgefragt werden darf.
- Es muss überlegt werden, ob für die Abfrage ein Policyenforcment auf Grund des Access Tokens gemacht werden muss. Der Inhalt des Access Tokens (Diagram: JWT-UAP-ID) muss definiert werden, zudem muss abgeklärt werden, inwieweit IHE IUA (Internet User Authorization (IUA)) angewendet werden kann (Kompatiblität zu SMART).
- ATNA: Audit Requirements für Serverseite (3.83.5 Security Considerations) muss festgelegt werden.
- Sollte das Mobile Access Portal auch die demographischen Daten des App-Anwender zurückgegeben können für die App? Falls ja, müsste in Erwägung gezogen werden, zusätzlich (oder alternativ) das IHE PDQm Profil einzusetzen.

Empfehlung 3: Das Mobile Access Portal bietet die Übersetzung der eID (UAP-ID) zur MPI-ID die in der Gemeinschaft gemäss dem IHE-PIXm-Profil an.

2.4 Dokumentenzugriff

2.4.1 Dokument schreiben

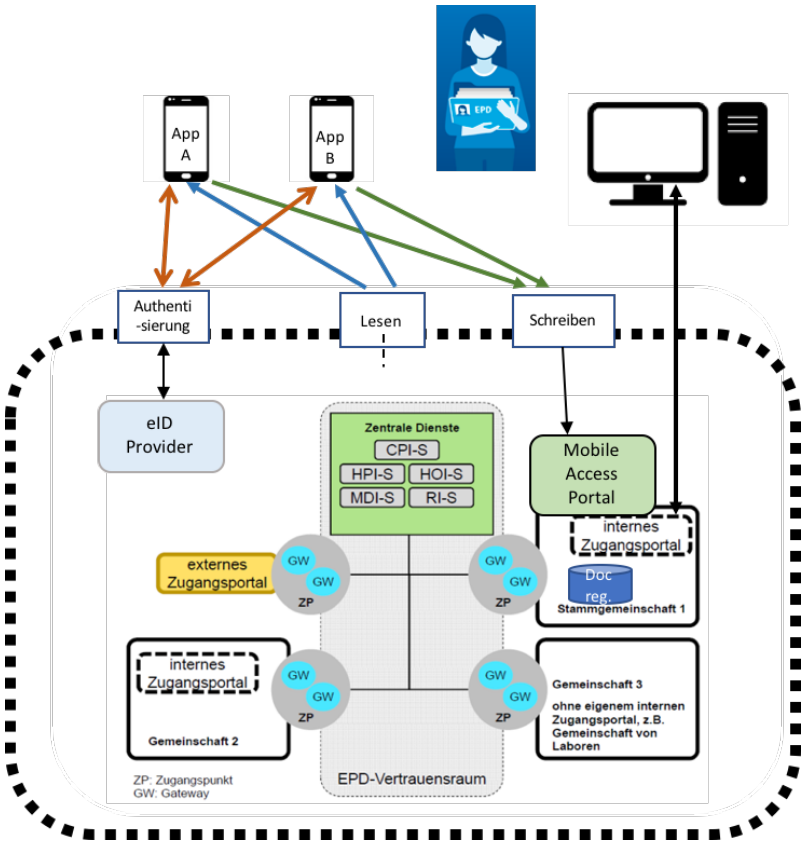


Abbildung 10 Dokument schreiben

Das Mobile-access-to-Health-Documents-Profil (MHD) ermöglicht es, mittels einer RESTful-API auf eine XDS-Infrastruktur zugreifen zu können, wie es für das EPD vorgesehen ist. Diese Funktionalität kann im Mobile Access Portal sowohl für das Dokumentenlesen wie -schreiben verwendet werden.

Für das Dokumenteschreiben muss das Mobile Access Portal den Akteur Document Recipient des MHD-Profils zur Verfügung stellen. Der Akteur kann mit der XDS-on-FHIR Option an die Gemeinschaftskomponenten angebunden werden.

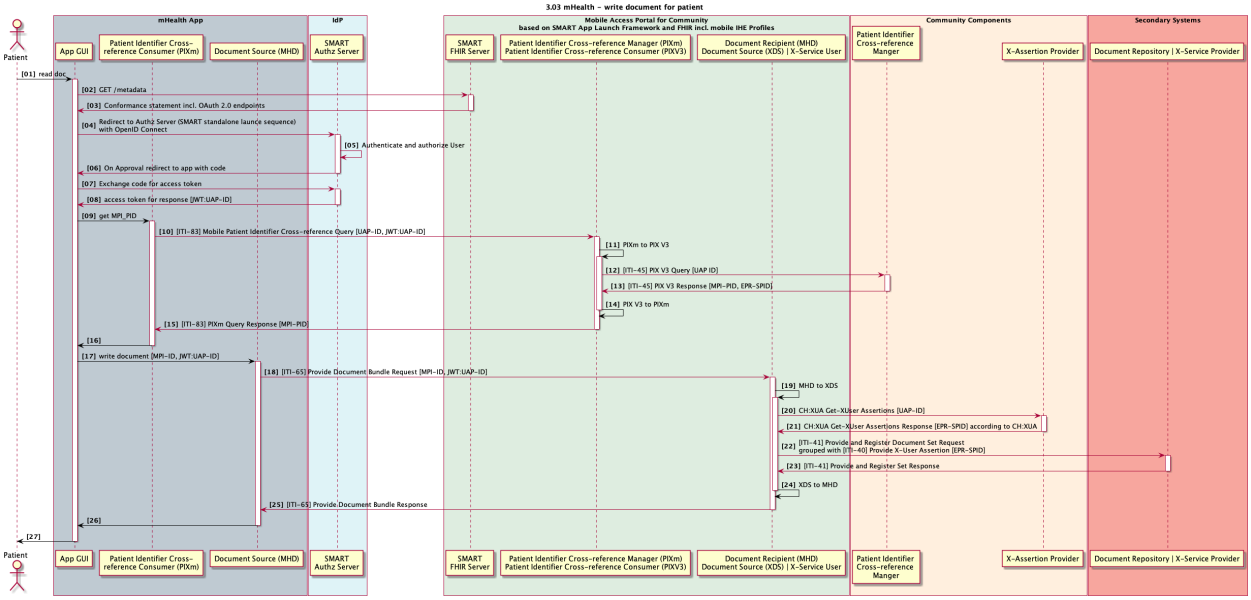


Abbildung 11 Dokument schreiben

Nachdem der Benutzer authentisiert ist (Schritt 2–8) kann die MPI-ID auf Grund der eID (UAP-ID) aufgelöst werden (Schritt 8-16).

Mit der [ITI-68] Provide-Bundle-Transaktion wird das Dokument dem Mobile Access Portal übergeben (Schritt 18). Falls der Akteur mit XDS on FHIR gruppiert ist, kann der Aufruf der Document Source weitergegeben werden (Schritt 19). Da im EPD-Kontext dieser mit dem X-Service User gruppiert sein muss, braucht es ein CH:XUA User Token für die anschliessenden IHE-XDS-Transaktionen. Nachdem das Dokument im Patienten-Repository der Stammgemeinschaft gespeichert wurde, endet die Transaktion im Schritt 26.

Empfehlung 4: Für das Dokumenteschreiben muss das Mobile Access Portal den Akteur Document Recipient des MHD-Profils zur Verfügung stellen.

2.4.2 Dokumente lesen

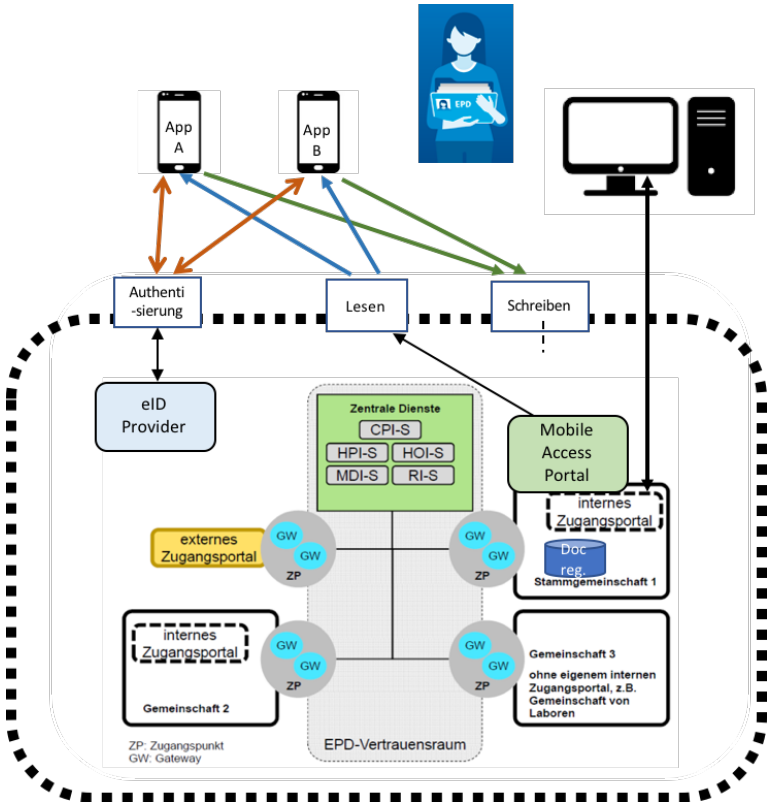


Abbildung 12 Dokument lesen

Zum Lesen der Dokumente muss das Mobile Access Portal den Akteur Document Responder des MHD-Profils zur Verfügung stellen. Der Akteur kann mit der XDS on FHIR Option an die Stammgemeinschaftskomponenten sowie über die Gateways auch an die anderen Gemeinschaften angebunden werden.

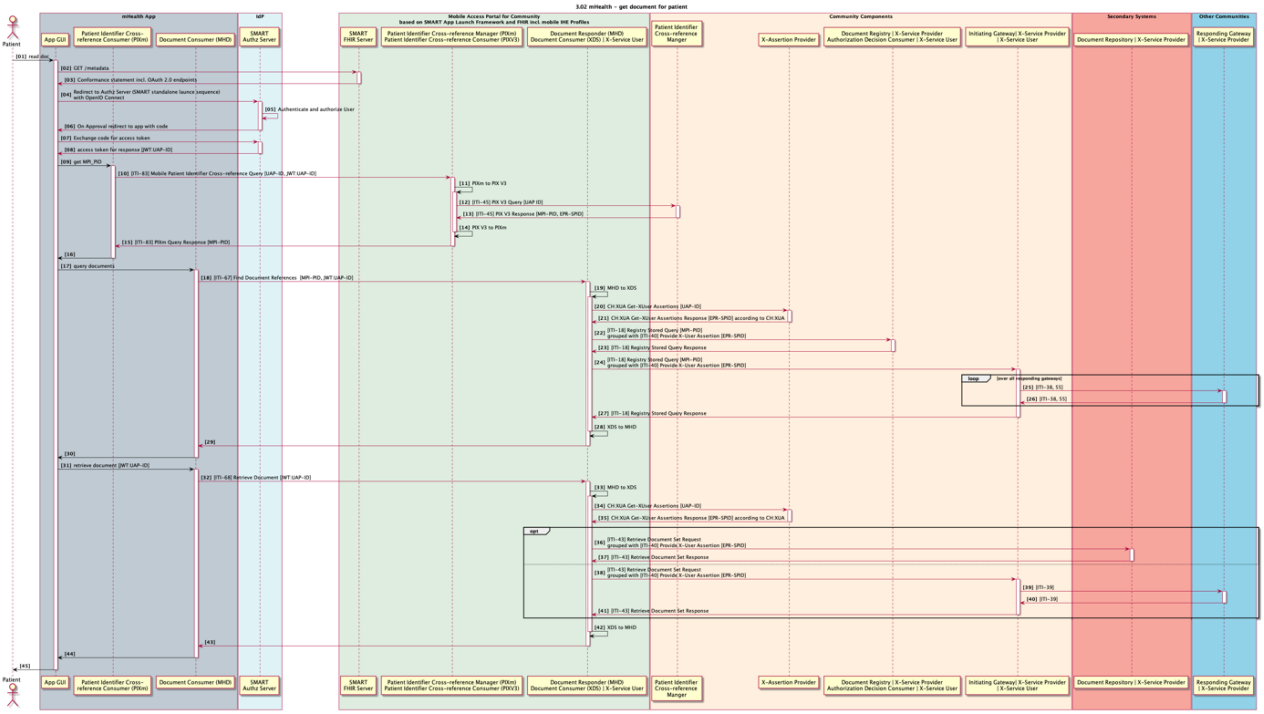


Abbildung 13 Dokument lesen

Nachdem der Benutzer authentisiert ist (Schritt 2–8) kann die MPI-ID auf Grund der eID (UAP-ID) aufgelöst werden (Schritt 8-16).

Mit der [ITI-67] Find Document References Transaktion können die Dokumente des Anwenders gesucht werden (Schritt 18). Falls der Akteur mit XDS on FHIR gruppiert ist, kann der Aufruf dem Document Consumer weitergeben werden (Schritt 19). Da im EPD-Kontext dieser mit dem X-Service User gruppiert sein muss, braucht es ein CH:XUA User Token für die anschliessenden IHE-XDS-Transaktionen. Anschliessend kann mit der [ITI-68] Retrieve-Document-Transaktion ein Dokument heruntergeladen werden.

Folgende Punkte sollten in einer Detailspezifikation noch erarbeitetet bzw. geklärt werden:

- Die CH:XUA Patient Extension (A5E1 1.6.4.2.4.4.6 Patient Extension) muss angepasst werden, dass sie auch mit einem OAuth/JWT Token eine Assertion ausgestellt werden kann.
- Es muss überlegt werden ob eine Policy-Enforcement auf Grund des Access Tokens gemacht werden muss für die Abfrage. Der Inhalt des Access-Tokens (JWT-UAP-ID) muss definiert werden, und es muss abgeklärt werden, inwieweit IHE IUA (Internet User Authorization (IUA) angewendet werden kann (Abklärung Kompatibilität zu SMART).
- Security und ATNA Requirements für das Mobile Access Portal müssen spezifiziert werden, siehe dazu auch die Thematik im IHE-MHD-Profil (33.6.1 MHD Actor grouped with XDS infrastructure: The MHD Document Recipient and Responser, acting as a proxy, would be configured to support only a designated set of mobile devices authorized by the hosting organization and use the security model defined by that hosting organization. The proxy might convert user authentication credentials, and fully implement the ATNA Secure Node or Secure Application Actors.)

Empfehlung 5: Zum Lesen der Dokumente muss das Mobile Access Portal den Akteur Document Responder des MHD-Profils zur Verfügung stellen .

3 Workshop der rechtlichen Aspekte

Bei dem Lösungsvorschlag für die Technische Anbindung, beschrieben im Kapitel 2, wurden neben der Abdeckung der Anwendungsfälle, der Berücksichtigung von anerkannten internationalen Standards und neben der Minimierung der technischen Komplexität die Machbarkeit auf Basis der heutigen Gesetzgebung und die Minimierung von nötigen Änderungen auf Verordnungsrechtebene und allfällig auf Gesetzebene berücksichtigt.

Wie im Kapitel 1.4 abgegrenzt, wird das Identifizieren aller erforderlichen rechtlichen Anpassungen eine ergänzende Analyse benötigen. Innerhalb dieser Konzeptphase haben Vorabklärungen mit dem BAG während einem Workshop bereits Zwischenresultate gebracht, die hier wiedergegeben werden:

1) Die Datenbearbeitung durch Patientinnen und Patienten gemäss EPDG findet ausschliesslich durch die Zugangsportale für Patientinnen und Patienten der Stammgemeinschaften statt.
2) Dokumente aus mobilen Anwendungen gelten als „Eigene Daten“ der Patienten gemäss Art. 8 EPDG. Sie unterstehen den gleichen Regeln wie alle anderen EPD-Dokumente. Falls neue Dokumentenformate notwendig sind, müssen diese im Ausführungsrecht aufgenommen werden.
3) Dabei wird die Datenbearbeitung durch den Patienten oder die Patientin mittels einer mobilen Applikation an die entsprechende neue Komponente «*internes mHealth Zugangsportal*» der Stammgemeinschaft delegiert.
4) Die mobilen Applikationen sind daher nicht Teil des Vertrauensraumes (2. in Verbindung mit 3.) und nicht im Regelungsbereich des EPDG [4] (und deshalb unterliegen keiner Zertifizierung nach EPDG).
5) Damit diese Delegation ein gleichhohes Vertrauensniveau aufweist wie eine Bearbeitung direkt via Zugangsportal, müssen mobile Applikationen ebenfalls auf einer Authentifizierung bei einem nach EPDG zertifizierten IdP aufbauen (siehe Lösungsvorschlag im Kapitel 2.3.1).
6) Auf technischer Ebene unterliegt diese Authentifizierung (mHealth-App -> IdP) zwar nicht den gleichen technischen Vorgaben (SAML) von Anhang 8, muss aber bezüglich Integrität und Authentizität einer Authentifizierung von Personen via Primärsystem oder Zugangsportal gleichwertig sein.
7) Da die Verbindung (mapping) des App-Users, der sich authentisiert hat, mit seinem Dossier durch die Stammgemeinschaft durchgeführt wird, kann die Gesundheits-App nie Kenntnis der EPD-ID des App-Users haben (diese bleibt innerhalb der Vertrauensraum).

4 Appendix

4.1 Referenzen mit Links für Downloads

(Links gültig und verifiziert am 1. März 2019)

[1] «mobile Health (mHealth) Empfehlungen I», 16. März 2017, eHealth Suisse Koordinationsorgan Bund-Kantone

https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2017/D/170316_mHealth_Empfehlungen_I_d.pdf

[2] «Mobile Health und das elektronische Patientendossier Empfehlungen zur Nutzung von technischen Standards und Normen», 27. September 2018, eHealth Suisse Koordinationsorgan Bund-Kantone

https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2018/D/181008-Empfehlungen_mHealth_Standards_d.pdf

[3] «Datenschutz und Informationssicherheit im Bereich „mobile health“ (mHealth)», 19. Januar 2018, Dr.iur. Michael Isler im Auftrag vom eHealth Suisse Koordinationsorgan Bund-Kantone

https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2018/D/180119_Juristisches_Gutachten_mHealth_d.pdf

[4] SR 816.1 Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier (EPDG)

https://www.admin.ch/opc/de/classified-compilation/20111795/index.html

[5] Gesetzgebung Elektronisches Patientendossier (EPDG)

https://www.bag.admin.ch/bag/de/home/gesetze-und-bewilligungen/gesetzgebung/gesetzgebung-mensch-gesundheit/gesetzgebung-elektronisches-patientendossier.html

[6] Botschaft zum Bundesgesetz über das elektronische Patientendossier vom 29. Mai 2013

https://www.admin.ch/opc/de/federal-gazette/2013/5321.pdf

[7] Albrecht UV. Transparenz schaffen und Orientierung bieten – Methoden und Werkzeuge als Entscheidungshilfe für die Nutzung von Gesundheits-Apps. eHealth Suisse, 2019. doi: 10.26068/mhhrpm/20190116-000

https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2019/D/Orientierungshilfe_fuer_Gesundheitsapps_d.pdf

[8] Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer

https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2018/D/180523_Leitfaden_fuer_App_Entwickler_d.pdf

4.2 Glossar

Dieses Glossar stützt sich überall, wo dies möglich ist, auf das Fach-Glossar von eHealthSuisse (https://www.e-health-suisse.ch/header/glossar.html)

Anwendungsfall (Use Case)	Anwendungsfall (Use Case) Ein Use Case definiert eine Interaktion zwischen Akteuren und dem betrachteten System, die stattfindet, um ein bestimmtes fachliches Ziel (engl. business goal) zu erreichen. Ein derartiger Anwendungsfall beschreibt einen Ablauf oder einen Prozess. Ein kommerziell erfolgreicher Use Case wird zum Business Case.
App (Gesundheitsbereich)	App (Gesundheitsbereich) App oder mobile App (Abkürzung vom englischen Wort application) ist eine Anwendungssoftware für Mobilgeräte bzw. mobile Betriebssysteme.
EPD (elektronisches Patientendossier)	Elektronisches Patientendossier (EPD) In der Schweiz versteht man unter dem elektronischen Patientendossier ein virtuelles Dossier, über das dezentral abgelegte behandlungsrelevante Daten einer Patientin oder eines Patienten in einem Abrufverfahren zugänglich gemacht werden können. Das ePatientendossier wird von den Gesundheitsfachpersonen in Absprache mit den Patientinnen und Patienten geführt. Die Inhalte stehen entlang des Behandlungspfades unabhängig von Ort und Zeit zur Verfügung. Die Patienten haben das Recht auf Einsichtnahme und Verwaltung der Zugriffsrechte.
Gateway	Anschlusspunkten der Gemeinschaft und Stammgemeinschaften an dem EPD-Vertrauensraum.
Identity Provider	kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles. (Quelle: EPDV-EDI)
Internes mHealth Zugangsportal (Mobile Access Portal)	Neues, in diesem Konzeptbericht, vorgeschlagenes Komponente der eHealth-Architektur, das die Verbindung von Gesundheits-Apps mit anderen internen Komponenten einer Stammgemeinschaft ermöglicht
mHealth	mHealth (mobile Health) Der Begriff Mobile Health (mHealth) beschreibt medizinische Verfahren sowie Massnahmen der privaten und öffentlichen Gesundheitsfürsorge, die durch Mobilgeräte wie Mobiltelefone, Patientenüberwachungsgeräte, persönliche digitale Assistenten (PDA) und andere drahtlos angebundene Geräte unterstützt werden.
MPI Master Patient Index	Master Patient Index (MPI) Ein Master Patient Index (MPI) ist im Allgemeinen ein Programm / eine Applikation, mit dem/der mehrere Identitäten/Stammdaten

	eines Patienten zu einer einzigen Identität zusammengeführt werden kann. D. h., ein MPI dient dazu, die Patienten-Identitäten aus verschiedenen Quellen (IT-Systeme der Behandelnden) unter einer gemeinsamen Identität zusammenzuführen und einen Index aller erfassten Patienten aufzubauen.
Primärsysteme (Praxis-, Klinik-Informationssysteme)	Primärsysteme (Praxis-, Klinik-Informationssysteme) Als Primärsysteme werden die Praxis- und Klinikinformationssysteme bezeichnet, in denen die interne elektronische Krankengeschichte eines Spitals, einer Arztpraxis oder Apotheke oder Therapeuten geführt wird. Diese interne elektronische Krankengeschichte oder -akte ist die primäre Basis für alle behandlungsrelevanten Entscheidungen. Im Gegensatz dazu wird das elektronische Patientendossier als 'Sekundärsystem' positioniert, welches lediglich als Quelle für weitere medizinische Daten dienen soll.
Quantified Self	Quantified Self Unter «Quantified Self» versteht man eine neue Form der Messung von personenbezogenen Daten. Ein zentrales Ziel stellt dabei der Erkenntnisgewinn u. a. zu persönlichen, gesundheitlichen und sportlichen, aber auch gewohnheitsspezifischen Fragestellungen dar. Quantified Self heisst die Vermessung des Menschen mit Apps und Wearables.
Zugangsportal für Patienten	Zugangsportal für Patienten Internetportal, das Patientinnen und Patienten einen von Ort und Zeit unabhängigen und sicheren Zugriff auf die eigenen Daten ermöglicht. Das Zugangsportal wird von der Stammgemeinschaft des Patienten bereitgestellt. Darüber hinaus kann der Patient über sein Zugangsportal die Zugriffsrechte auf sein elektronisches Patientendossier verwalten.
Zugangspunkt (EPD-Kontext)	Zugangspunkt (EPD-Kontext) Mit Zugangspunkt sind im ePatientendossier-System die technischen Komponenten gemeint, die die Verbindung einer (Stamm-)Gemeinschaft oder externem Zugangsportal mit der «Aussenwelt» herstellt. Das kann die Kommunikation mit anderen (Stamm-)Gemeinschaften oder mit den zentralen Abfragediensten betreffen. In einem logischen Zugangspunkt können mehrere technische 'Gateways' zusammengefasst sein.

4.3 Liste der Interviews

Auftraggeber und Administration:

- Catherine Bugmann, eHealth Suisse und Koordinatorin mHealth Gruppe
- Pero Grgic, eHealth Suisse
- Jürg Bleuer, eHealth Suisse
- Walid Ahmed, BAG

Stammgemeinschaften:

- Thomas Zurkinden, Axsana
- Nicolai Lütschg, Stammgemeinschaft eHealth Aargau

EPD-IT-Betreiber, IT Experten, App Herausgeber:

- Tino Mahn, Swisscom Health AG
- Joël Poyet, Swisscom Health AG
- Tim Dorner, Post CH AG
- Dmytro Rud, Post CH AG
- Patrick Mangesius, ITH icoserve
- Johannes Bachmann, ITH icoserve
- Christian Denk, ITH icoserve
- Urs Stromer, IG eHealth
- Chrysanth Sulzberger, imito AG

Spitäler:

- Nino Theodorovic, Balgrist Uniklinik
- Roland Naef, USZ