Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

EPD - Architektur

Eine ausführliche Beschreibung

Inhalt

SMA
5.09.2023

Schwarzenburgstrasse 157
CH-3003 Bern

www.e-health-suisse.ch

ehealthsuisse
Kompetenz- und Koordinationsstelle
von Bund und Kantonen

1 Einführung

Dieses Dokument gibt eine Übersicht über die die Architektur bzw. die Servicelandschaft des elektronischen Patientendossiers (EPD) der Schweiz.

Aus Benutzersicht ist das EPD ein verteiltes System zum Management von Dokumenten zum Zwecke des Austausches von medizinischen Daten[1] und Dokumenten zwischen Gesundheitsfachpersonen, den Patientinnen und Patienten im Behandlungskontext.

Zu Beginn einer Behandlung sollen Gesundheitsfachpersonen die Krankengeschichte der Patientinnen und Patienten aus dem EPD laden und in ihre Primärsysteme übernehmen. Im Laufe der Behandlung bzw. nach Abschluss der Behandlung sollen Gesundheitsfachpersonen die im Rahmen der Behandlung angefallenen Daten und Dokumente im EPD der Patientinnen und Patienten ablegen und so für die Nachbehandlung oder zur Information der Patientinnen und Patienten verfügbar machen. Patientinnen und Patienten können aber auch eigene Daten und Dokumente im EPD erfassen.

Die Architektur des EPD reflektiert insbesondere die hohen Anforderungen an den Datenschutz im EPD. Patientinnen und Patienten können die Zugriffsrechte feingranular einstellen bis hin zur Freigabe der Dokumente für einzelne Gesundheitsfachpersonen. Alle Benutzer müssen sich stark authentisieren (mindestens zwei Faktoren), alle Zugriffe werden protokolliert und alle am EPD angeschlossenen technischen Systeme müssen im EPD registriert sein und sich auf der Netzwerkschicht oder mittels digitaler Signaturen der Nachrichten authentisieren.

2 Disclaimer

Dieses Dokument dient dem Überblick über die Architektur des EPD für interessierte Leserinnen und Leser, welche sich einen Überblick über die technische Umsetzung des EPD verschaffen wollen. Dieses Dokument konzentriert sich auf die wichtigsten Aspekte, erhebt keinen Anspruch auf eine erschöpfende Behandlung aller Aspekte des EPD und ist insbesondere nicht normativ.

[1] Anders als häufig behauptet, können im EPD auch strukturierte Daten gespeichert werden. (Stamm-)Gemeinschaften müssen die, in den EPDV-EDI geforderten Austauschformte unterstützen, sind aber frei Austauschformate zu definieren und zu nutzen.

3 EPD Architektur

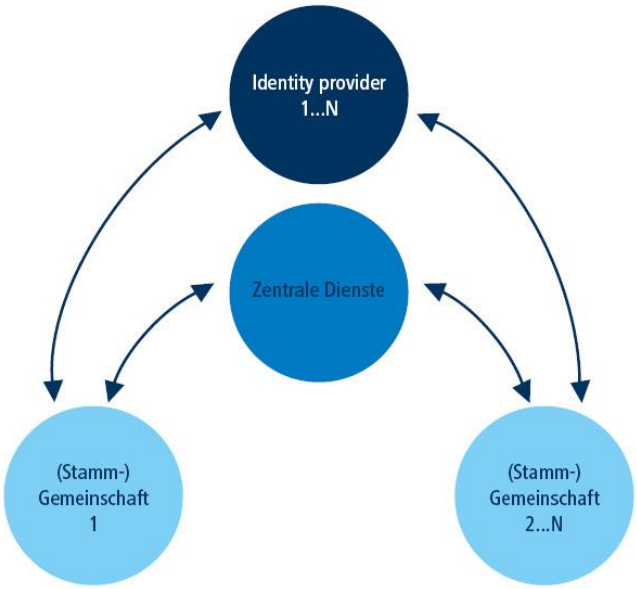

Abb. 1: Übersicht der am EPD beteiligten Systeme.

Das EPD ist ein verteiltes System zum Dokumentenmanagement, welches sich aus den folgenden Systemen zusammensetzt:

- Herausgeber von Identifikationsmitteln (Identity Providern): Services zur Authentisierung von natürlichen Personen im Internet.
- Zentrale Dienste des Bundes: Services zur Bereitstellung von durch alle (Stamm-)Gemeinschaften genutzte Daten, insbesondere die Abfrage von EPD-Metadaten-Definitionen für die Verwendung bei Dokumenten sowie der Suche danach, Verzeichnis von Zugangspunkten der (Stamm-)Gemeinschaften, Verzeichnis der an das EPD angeschlossenen Gesundheitsfachpersonen und Institutionen, Dienst zur Abfrage der Patientenidentifikationsnummer für das EPD (EPR-SPID).
- (Stamm-)Gemeinschaften: Zusammenschluss von Institutionen und Gesundheitsfachpersonen, welche die EPD-Plattformen und die Prozesse zum Betrieb des EPD bereitstellen.
- Angeschlossene Systeme der Gesundheitsfachpersonen und deren Institutionen: Insbesondere die Primärsysteme, Archiv Systeme für Dokumente und Bilddaten (PACS).

3.1 Herausgeber von Identifikationsmitteln

Herausgeber von Identifikationsmitteln, im Folgenden als Identity Provider bezeichnet, stellen für Gesundheitsfachpersonen und ihre Hilfspersonen, Patientinnen und Patienten sowie deren Stellvertretungen und für Administratoreninnen und Administratoren der (Stamm-)Gemeinschaften die Authentisierungsmittel aus, welche für den Zugriff auf das EPD benötigt werden.

Die Identity Provider implementieren die Prozesse zum Ausstellen der Authentisierungsmittel, der rechtgültigen Identifikation, der Revokation, usw. und stellen die Schnittstellen zur Authentisierung von natürlichen Personen bereit.

Die Anforderungen an die Identity Provider sind im Gesetz zum elektronischen Patientendossier (EPDG) und den zugehörigen Verordnungen (EPDV, EPDV-EDI) definiert. Identity Provider müssen

für die Benutzung im EPD zertifiziert werden. Die Zertifizierungskriterien sind im Anhang 8 der EPDV-EDI festgelegt und umfassen sowohl die Anforderungen an die Prozesse, als auch an die Schnittstellen.

Zur Nutzung im EPD schliessen (Stamm-)Gemeinschaften Verträge mit einem oder mehreren Identity Providern ab, welche dann zur Autorisierung der Benutzer in den Portalen der (Stamm-)Gemeinschaften und den angeschlossenen Systemen (Primärsystemen) genutzt werden können.

Das EPD schreibt die zu unterstützenden Schnittstellen vor, macht darüber hinaus aber keine Vorgaben für die Architektur der Identity Provider.

Gemäss Anhang 8 der EPDV-EDI müssen zertifizierte Identity Provider die Schnittstellen der folgenden Integrationsprofile unterstützen:

- SAML 2.0 Artifact Binding mit dem Artifact Resolution Protocol via SOAP Backchannel.
- SAML 2.0 Logout Binding via SOAP Backchannel.
- Renew Protocol mit EPD spezifischen Integrationsprofil (Anhang 8 der EPDV-EDI) auf der Basis des WS Trust Standard.

Optional können zertifizierte Identity Provider Schnittstellen der folgenden Integrationsprofile zur Nutzung im EPD insbesondere für mobile Clients anbieten:

- OpenID Connect Authorization Code Flow mit EPD spezifischen Integrationsprofil (Anhang 8 der EPDV-EDI).
- OpenID Connect Logout Flow mit EPD spezifischen Integrationsprofil (Anhang 8 der EPDV-EDI).

3.2 Zentrale Dienste des Bundes

Der Bund betreibt sogenannte Zentrale Dienste, welche für den korrekten Betrieb der verteilten Architektur benötigt werden:

- Dienst zur Abfrage des sektoriellen Personenidentifikators für das EPD (EPR-SPID)
- EPD Metadaten: Katalog der Value Sets der Dokument-Metadaten und der Value Sets zur Kodierung der strukturierten Daten der Austauschformate.
- Zugangspunkte der (Stamm-)Gemeinschaften: Katalog der Informationen und Daten, welche für die gemeinschaftsübergreifende Kommunikation benötigt werden.
- Verzeichnis der an das EPD angeschlossenen Gesundheitsfachpersonen und Institutionen: Zweckgebundene Sammlung der Institutionen, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen, welche von Patientinnen und Patienten für den Zugriff auf das EPD berechtigt werden können.

3.2.1 Dienst zur Abfrage des sektoriellen Personenidentifikators (EPR-SPID)

Der Dienst zur Abfrage des sektoriellen Personenidentifikators (EPR-SPID) Unique Person Identification Service (UPI) implementiert eine Schnittstelle zur Datenbank der zentralen Ausgleichstelle des Bundes, welche auch die AHV-Nummer (AHVN13) ausgibt und verwaltet.

Die Schnittstelle unterstützt insbesondere die folgenden Funktionen für die (Stamm-)Gemeinschaften:

- Abfrage des sektoriellen Personenidentifikators für das EPD (EPR-SPID) anhand der demographischen Daten oder der AHVN13 der Patientin oder des Patienten.
- Anfrage zur Generierung einer neuen EPR-SPID mit Angabe der demographischen Daten oder der AHVN13 der Patientin oder des Patienten.
- Annullierung bzw. Deaktivierung der EPR-SPID.
- Information über den Status einer EPR-SPID (Aktiv, Inaktiv, Annulliert).

Die Kommunikation mit der UPI erfordert den Betrieb eines SEDEX Clients in der EPD Plattform der (Stamm-)Gemeinschaften. Der SEDEX Client bietet den (Stamm-)Gemeinschaften die folgenden Schnittstellen an:

- SOAP Webservice nach dem eCH-0213 Nachrichtenstandard (query).
- SOAP Webservice nach dem eCH-0213 Nachrichtenstandard (generate, inactivate, cancel).
- File Schnittstelle nach dem eCH-0215 Nachrichtenstandard (broadcast bei Statusänderung).

3.2.2 EPD Metadaten

Der Dienst implementiert eine Schnittstelle zum Abfragen der EPD konformen Dokument-Metadaten und zur Kodierung der strukturierten Daten der Austauschformate.

Die Schnittstelle unterstützt insbesondere die folgenden Funktionen:

- Download der EPD Value Sets von der Web Seite
- Query der EPD Value Sets über einen XML SOAP Webservice gemäss dem IHE Integrationsprofil «Sharing Value Sets (SVS)».

3.2.3 Zugangspunkte der (Stamm-)Gemeinschaften (CPI)

Der Dienst des Verzeichnisses der Zugangspunkte der (Stamm-)Gemeinschaften implementiert Schnittstellen zur Abfrage von Kontaktdaten, welche zur Kommunikation zwischen den (Stamm-)Gemeinschaften benötigt werden. Diese sind insbesondere:

- URL und X.509 Zertifikate der Gateways für den Austausch von Dokumenten.
- URL und X.509 Zertifikate des Endpunktes für die Zugriffsentscheide.
- URL und X.509 Zertifikate des Endpunktes für die Zugriffsprotokolle.

Die Daten werden von den Betriebsverantwortlichen der (Stamm-)Gemeinschaften per Secure E-Mail an das BAG gesendet und den zertifizierten (Stamm-)Gemeinschaften über ein proprietäres Datenformat (siehe EPDV-EDI) auf der Basis des LDAP Protokolls zugänglich gemacht.

3.2.4 Verzeichnis der an das EPD angeschlossenen Leistungserbringer

Der Service implementiert Schnittstellen zum gemeinschaftsübergreifenden Austausch von Daten der Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen, welche von Patientinnen und Patienten zum Zugriff berechtigt werden können.

Die Daten sind zweckgebunden und enthalten nur die im EPD gesetzlich vorgeschriebenen Daten der Gesundheitsfachpersonen, Gruppen von Gesundheitsfachpersonen und Institutionen, insbesondere:

- GLN als Identifikator der Gesundheitsfachperson.
- OID als Identifikator von Gruppen von Gesundheitsfachpersonen sowie Institutionen.
- BUR Nummer der Institutionen.
- Namen und Adressen der Gesundheitsfachpersonen, Gruppen von Gesundheitsfachpersonen sowie Institutionen.
- Relationen zwischen den Gesundheitsfachpersonen, Gruppen von Gesundheitsfachpersonen sowie Institutionen.

Die Daten werden von den (Stamm-)Gemeinschaften erfasst. Die (Stamm-)Gemeinschaften nutzen den Dienst zum gemeinschaftsübergreifenden Austausch der Daten.

Der Service unterstützt dazu die DSML(LDAP) und XML SOAP basierten Schnittstellen des IHE Profils Healthcare Provider Directory (HPD) mit nationalen Anpassungen der EPDV-EDI.

Die Integrität der Daten wird von den (Stamm-)Gemeinschaften verantwortet, welche die Daten erfassen und mit Hilfe des Verzeichnisses an die anderen (Stamm-)Gemeinschaften verteilen.

3.3 (Stamm-)Gemeinschaften

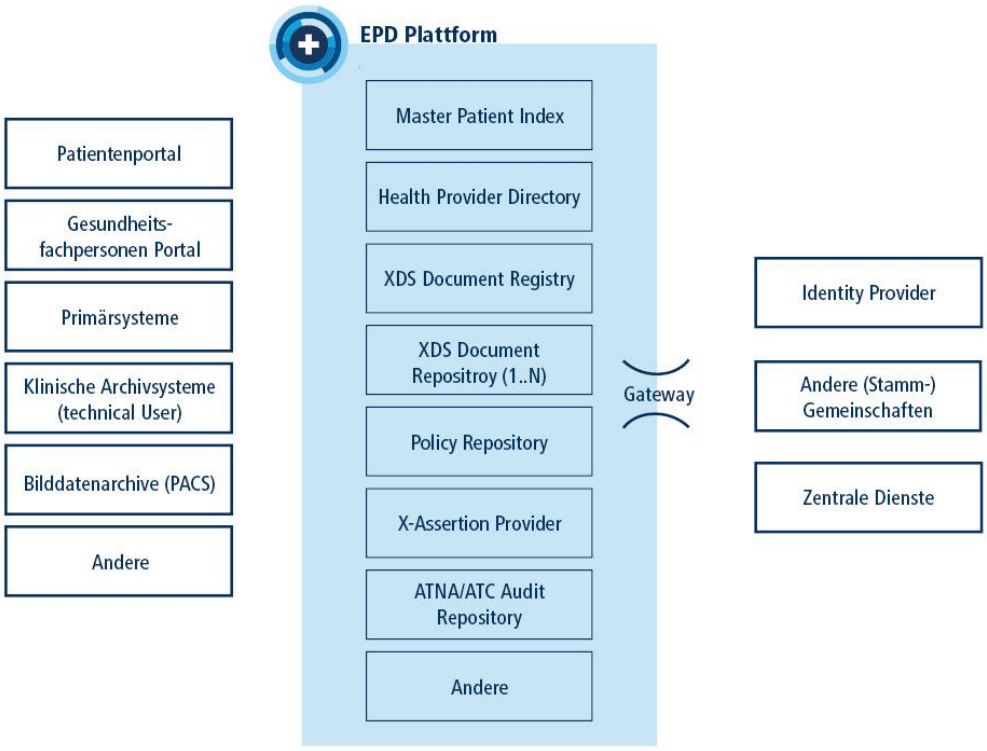

Abb. 2: Übersicht über die Services und Applikationen einer (Stamm-)Gemeinschaft.

Die EPDV-EDI formuliert Anforderungen an die interoperablen Schnittstellen und die Datensicherheit der technischen Infrastruktur der (Stamm-)Gemeinschaften, stellen aber keine weiteren Anforderungen an die Architektur.

(Stamm-)Gemeinschaften und ihre Plattformprovider (Anbieter und Betreiber ihrer EPD-Plattform) können daher die Dienste frei und nach ihren eigenen Anforderungen auf Applikationen aufteilen. Dementsprechend finden sich unter den (Stamm-)Gemeinschaften sowohl monolithische als auch verteilte Service Architekturen.

In der Praxis hat sich aber eine Architektur durchgesetzt, welche die im folgenden beschriebenen Services implementiert (siehe Abb. 2).

3.3.1 Master Patient Index

Service zum Management der Identifikatoren der Patientinnen und Patienten in einer (Stamm-)Gemeinschaft. Der Master Patient Index im EPD ist zweckgebunden und unterstützt alle Funktionen, welche für die systemübergreifende Identifikation der Patientinnen und Patienten für das Dokumentenmanagement erforderlich sind, insbesondere:

- Speicherung und Verwaltung der lokalen Identitäten der Patientinnen und Patienten in den angeschlossenen Systemen (z.B. Primärsysteme, Archive) und dazugehörige demographische Daten.
- Vergabe einer Master Patient ID zur Identifizierung der Patientinnen und Patienten in der (Stamm-)Gemeinschaft.
- Matching der Identifikatoren anhand der demographischen Daten und der EPR-SPID.
- Speicherung der EPR-SPID.

Die Daten werden von den (Stamm-)Gemeinschaften bei der Eröffnung des EPD initial und im laufenden Betrieb von den angeschlossenen Systemen bei der Registrierung von neuen Patientinnen und Patienten (z.B. im Patientendatenmanagementsystem, den Klinik- oder Praxisinformationssystemen, Portalen) erfasst und im Master Patient Index registriert.

Der Master Patient Index speichert alle registrierten Identifikatoren sowie die zugehörigen demographischen Daten und vergibt eine Master Patient ID, welche in den Dokumentenspeichern als Identifikator benutzt werden kann. Der Master Patient Index ermittelt zudem, welche Identifikatoren die gleiche Patientin bzw. den gleichen Patienten identifiziert und führt eine Referenztabelle mit den ermittelten Identifikatoren und der Master Patient ID.

Die angeschlossenen Systeme einer (Stamm-)Gemeinschaften fragen beim Master Patient Index die Master Patient ID der Patientinnen und Patienten ab, welche sie für die Suche und Anfrage von Dokumenten benötigen.

Der Master Patient Index unterstützt dazu die folgenden Schnittstellen nach internationalen Standards auf Basis von HL7 V3 und XML SOAP Webservices mit nationalen Anpassungen der EPDV-EDI:

- Patient Identifier Cross-referencing HL7 V3 (PIXV3),
- Patient Demographics Query HL7 V3 (PDQV3),
- Cross-Community Patient Discovery (XCPD).

Die Einführung von FHIR basierten Schnittstellen ist geplant. Dabei sollen die folgenden FHIR basierten Profile unterstützt werden:

- Patient Identifier Cross-Reference for Mobile (PIXm),
- Patient Demographics Query for Mobile (PDQm).

Alle Aufrufe des Service werden gemäss den Vorgaben der IHE Profile und den nationalen Erweiterungen in einem Standardformat protokolliert und in den ATNA Audit Record Repositories der (Stamm-)Gemeinschaft abgelegt.

Die Zugriffe auf die Daten werden auf dem Netzwerklayer (mTLS) authentisiert. Der Aufbau von Verbindungen und der Zugriff wird nur den Systemen gewährt, welche in den (Stamm-)Gemeinschaften registriert sind und über gültige X.509 Zertifikate verfügen.

Die im Master Patient Index geführten Daten sind minimal auf den Zweck des sytemübergreifenden Austauschs von Dokumenten im EPD ausgelegt. Mit der umfassen Revision des EPD soll der Dienst auch für andere Zwecke genutzt werden können.

Die Integrität der Daten wird von den (Stamm-)Gemeinschaften und den angeschlossenen Systemen (z.B. Primärsysteme) verantwortet, welche die Daten erfassen. Die EPDV-EDI verpflichten die (Stamm-)Gemeinschaften und angeschlossenen Systeme die vertrauenswürdigen demographischen Daten aus dem Dienst zur Abfrage der sektoriellen Personenregisters UPI zu übernehmen und ggf. um die Kontaktdaten oder andere Angaben zu erweitern, welche für den Betrieb des EPDs benötigt werden.

3.3.2 Healthcare Provider Directory (HPD)

Der Service implementiert Schnittstellen zum Austausch von Daten der angeschlossenen Gesundheitsfachpersonen, Hilfspersonen von Gesundheitsfachpersonen, Gruppen von Gesundheitsfachpersonen und Institutionen sowie EPD Administratoren einer (Stamm-)Gemeinschaft.

Die Daten sind zweckgebunden und enthalten nur die per EPDG vorgeschriebenen Daten, insbesondere:

- GLN der Gesundheitsfachpersonen und Hilfspersonen.
- OID der Institutionen und Gruppen von Gesundheitsfachpersonen.
- BUR Nummer der Institutionen.

- Namen und Adressen der Gesundheitsfachpersonen, Gruppen von Gesundheitsfachpersonen und Institutionen.
- Relationen zwischen den Gesundheitsfachpersonen, Gruppen von Gesundheitsfachpersonen und Institutionen.
- Relationen zwischen den Hilfspersonen und den Gesundheitsfachpersonen.

Die Daten werden von den (Stamm-)Gemeinschaften erfasst oder aus den anderen (Stamm-)Gemeinschaften über den zentralen Dienst des Bundes übernommen. Über den zentralen Dienst werden nur die Gesundheitsfachpersonen, Gruppen von Gesundheitsfachpersonen und Institutionen synchronisiert. Einträge von Hilfspersonen und EPD Administratoren werden ausschliesslich in den lokalen Verzeichnissen der (Stamm-)Gemeinschaften geführt.

Die (Stamm-)Gemeinschaften machen die Daten den angeschlossenen Systemen über Standardschnittstellen verfügbar, insbesondere zur Suche nach Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen zur Verwaltung von Zugriffrechten durch die Patientinnen und Patienten.

Der Service unterstützt dazu die DSML (LDAP) und XML SOAP basierten Schnittstellen des IHE Profils Healthcare Provider Directory (HPD) mit nationalen Anpassungen der EPDV-EDI, sowie Benutzeroberflächen zur Verwaltung durch die Administratoren der (Stamm-)Gemeinschaften.

Die Einführung von FHIR basierten Schnittstellen ist geplant. Dazu soll das Profil Mobile Care Services Discovery (mCSD) unterstützt werden.

Die Zugriffe auf die Daten werden auf dem Netzwerk Layer (mTLS) authentisiert. Der Aufbau von Verbindungen wird nur den Systemen gewährt, welche in den (Stamm-)Gemeinschaften registriert sind und über gültige X.509 Zertifikate verfügen.

Die im Verzeichnis geführten Daten sind minimal auf den Zweck des Austauschs von Doku-menten im EPD ausgelegt. Mit der umfassen Revision des EPDG soll der Dienst auch für andere Zwecke genutzt werden können.

Die Integrität der Daten wird von den (Stamm-)Gemeinschaften verantwortet, in denen die Daten erfasst werden.

3.3.3 XDS Document Registry

Das EPD nutzt ein Dokumentenmanagement nach dem Internationalen Standard «Cross-Enterprise Document Sharing» (XDS) von IHE International. Der Document Registry Service implementiert Schnittstellen zur Speicherung der XDS Metadaten zur Registrierung und Suche nach medizinischen Dokumenten in einer verteilten Infrastruktur.

Die Daten in der Document Registry sind zweckgebunden und enthalten nur die für das EPD gesetzlich vorgeschriebenen Daten von Dokumenten, insbesondere:

- Kodierte Werte für Dokumententyp und Klasse.
- Angaben zur Autorin oder dem Autor des Dokuments.
- Kodierte Werte für den Fachbereich der Autorin oder des Autors und der Institution.
- Kodierte Angaben der Vertraulichkeitsstufe.

Die Daten werden von den angeschlossenen Systemen der (Stamm-)Gemeinschaften bei der Speicherung von Dokumenten erfasst und über Schnittstellen registriert.

Die Daten können von allen an das EPD angeschlossenen Systemen über Schnittstellen abgefragt werden, sowohl innerhalb einer (Stamm-)Gemeinschaften als auch gemeinschaftsübergreifend.

Der Service unterstützt dazu die ebXML und SOAP basierten Schnittstellen des IHE Profils Cross-Enterprise Document Sharing (XDS.b) mit nationalen Anpassungen der EPDV-EDI, sowie Benutzeroberflächen zur Verwaltung durch die Administratoren der (Stamm-)Gemeinschaften.

Die Einführung von FHIR basierten Schnittstellen ist geplant. Dazu soll das Profil Mobile access to Health Documents (MHD) unterstützt werden.

Die Zugriffe auf die Daten werden auf dem Netzwerk Layer (mTLS) authentisiert. Der Aufbau von Verbindungen wird nur den Systemen gewährt, welche in den (Stamm-)Gemeinschaften registriert sind und über gültige X.509 Zertifikate verfügen.

Der Zugriff auf die Daten und Dokumente wird durch das Autorisierungssystem des EPD gesteuert. Zugriffsentscheide basieren auf den von Patientinnen und Patienten eingestellten Zugriffsrechten. Der Service nutzt dazu die Daten aus den Security Token und die Services der Zugriffsteuerung im EPD.

Alle Aufrufe des Service werden gemäss den Vorgaben der IHE Profile und den nationalen Erweiterungen in einem Standardformat protokolliert und in den ATNA Audit Record Repositories der (Stamm-)Gemeinschaften abgelegt.

Die Integrität der Daten wird von den Benutzern der (Stamm-)Gemeinschaften und den angeschlossenen Systemen verantwortet, in denen die Daten erfasst werden.

3.3.4 XDS Document Repositories

Das EPD nutzt ein Dokumentenmanagement nach dem Internationalen Standard «Cross-Enterprise Document Sharing» (XDS) von IHE International. Der Document Repository Service implementiert Schnittstellen zur Speicherung und Abfrage der Binärobjekte[2] der XDS Dokumente.

Die Daten werden von den angeschlossenen Systemen der (Stamm-)Gemeinschaften bei der Speicherung von Dokumenten erfasst und über Schnittstellen registriert.

Die Daten können von allen an das EPD angeschlossenen Systemen über Schnittstellen abgefragt werden, sowohl innerhalb einer (Stamm-)Gemeinschaften als auch gemeinschaftsübergreifend.

Der Service unterstützt dazu die ebXML und SOAP basierten Schnittstellen des IHE Profils Cross-Enterprise Document Sharing (XDS.b) mit nationalen Anpassungen der EPDV-EDI.

Die Einführung von FHIR basierten Schnittstellen ist geplant. Dazu soll das Profil Mobile access to Health Documents (MHD) unterstützt werden.

Die Zugriffe auf das EPD werden auf dem Netzwerk Layer (mTLS) authentisiert. Der Aufbau von Verbindungen wird nur den Systemen gewährt, welche in den (Stamm-)Gemeinschaften registriert sind und über gültige X.509 Zertifikate verfügen.

Der Zugriff auf die Daten und Dokumente wird durch das Autorisierungssystem des EPD gesteuert. Zugriffsentscheide basieren auf den von Patientinnen und Patienten eingestellten Zugriffsrechten. Der Service nutzt dazu die Daten aus den Security Token und die Services der Zugriffsteuerung im EPD.

Alle Aufrufe des Service werden gemäss den Vorgaben der IHE Profile und den nationalen Erweiterungen in einem Standardformat protokolliert und in den ATNA Audit Record Repositories der (Stamm-)Gemeinschaften abgelegt.

Die Integrität der Daten wird von den Nutzern der (Stamm-)Gemeinschaften und den angeschlossenen Systemen verantwortet, in denen die Daten erfasst werden.

3.3.5 Assertion Provider (STS)

Zugriffe auf Daten und Dokumente im EPD werden durch Security Token auf der Basis des WS-Trust Protokolls geschützt. Der Assertion Provider Service implementiert den dazu benötigten WS-Trust Secure Token Service mit den zugehörigen Schnittstellen.

Die Daten des Service werden von den (Stamm-)Gemeinschaften erfasst. Der Service nutzt Daten aus anderen Services zur Ausstellung der Security Token, insbesondere die Daten der

[2] Der Dokument Management Standard der OASIS definiert ein Dokument als die Kombination aus dem binären Objekt und den Dokument Metadaten.

Gesundheitsfachpersonen, Gruppen von Gesundheitsfachpersonen und Institutionen aus dem Healthcare Provider Directory (HPD).

Der Service unterstützt die SOAP basierten Schnittstellen aus dem WS-Trust Standard mit nationalen Anpassungen der EPDV-EDI.

Die Einführung von OAuth basierten Schnittstellen ist geplant. Dazu soll das OAuth basierte Profil Internet User Authorization (IUA) unterstützt werden.

Die Zugriffe auf die Daten werden auf dem Netzwerk Layer (mTLS) authentisiert. Der Aufbau von Verbindungen wird nur den Systemen gewährt, welche in den (Stamm-)Gemeinschaften registriert sind und über gültige X.509 Zertifikate verfügen.

Alle Aufrufe des Service werden gemäss den Vorgaben der IHE Profile und den nationalen Erweiterungen in einem Standardformat protokolliert und in den ATNA Audit Record Repositories der (Stamm-)Gemeinschaften abgelegt.

Die Integrität der Daten wird von den (Stamm-)Gemeinschaften verantwortet.

3.3.6 Policy Repository

Das EPD nutzt ein Autorisierungskonzept nach dem XACML 2.0 Standard. Der Service implementiert dabei die Akteure «Policy Repository» und «Policy Administration Point» der XACML Referenzarchitektur mit den zugehörigen Schnittstellen zur Verwaltung der Zugriffsrechte im EPD.

Die Daten werden von den (Stamm-)Gemeinschaften initial erfasst und können von Patientinnen und Patienten über die Portale erweitert bzw. angepasst werden. Im Fall der Delegation können auch Gesundheitsfachpersonen die Einstellungen in ihren Primärsystemen oder im Gesundheitsfachpersonenportal ändern. Die Einstellungen der Zugriffsrechte sind dazu in XACML Policies kodiert, welche von den angeschlossenen Systemen geschrieben werden.

Die Daten können von den Patientinnen und Patienten aus ihrem Portal über Schnittstellen abgefragt werden, bzw. bei Delegation auch von den Primärsystemen oder dem Gesundheitsfachpersonenportal.

Der Service unterstützt dazu die SAML 2.0 und SOAP basierten Schnittstellen des nationalen Integrationsprofils Privacy Policy Query (CH: PPQ) gemäss Spezifikation in der EPDV-EDI.

Die Einführung von FHIR basierten Schnittstellen ist geplant. Dazu soll das nationale Integrationsprofil Privacy Policy Query for Mobile (CH:PPQm) unterstützt werden.

Die Zugriffe auf die Daten werden auf dem Netzwerk Layer (mTLS) authentisiert. Der Aufbau von Verbindungen wird nur den Systemen gewährt, welche in den (Stamm-)Gemeinschaften registriert sind und über gültige X.509 Zertifikate verfügen.

Der Zugriff auf die Daten und Dokumente wird durch das Autorisierungssystem des EPD gesteuert. Zugriffsentscheide basieren auf den von Patientinnen und Patienten eingestellten Zugriffsrechten. Der Service nutzt dazu die Daten aus den Security Token und die Services der Zugriffsteuerung im EPD.

Alle Aufrufe des Service werden gemäss dem nationalen Integrationsprofil in einem Standardformat protokolliert und in den ATNA Audit Record Repositories der (Stamm-)Gemeinschaften abgelegt.

Die Integrität der Daten wird von den Nutzern der (Stamm-)Gemeinschaften und den angeschlossenen Systemen verantwortet, in denen die Daten erfasst werden.

3.3.7 ATNA/ATC Audit Record Repository

Das EPD nutzt ein Protokollierungssystem nach dem IHE Standard, das sogenannte Audit Trail and Node Authentication (ATNA) Profil. Die Transaktionen werden dabei vom aufrufenden sowie vom empfangenden System nach dem Syslog Standard im XML-Format mit dem DICOM Schema mit den nationalen Ergänzungen der EPDV-EDI protokolliert. Damit sich Patientinnen und Patienten über Zugriffe in ihrem EPD informieren können, müssen Protokolldaten gemäss Schweizer

Integrationsprofil Audit Trail Consumption (CH:ATC) in einem für Patientinnen und Patienten verständlicheren Format vom Patientenportal bei allen (Stamm-)Gemeinschaften abgefragt werden können.

Der Service unterstützt dazu die folgenden Integrationsprofile mit den nationalen Ergänzungen der EPDV-EDI:

- IHE Audit Trail and Node Authentication (ATNA),
- Audit Trail Consumption (CH:ATC).

Die Zugriffe auf die Daten werden auf dem Netzwerk Layer (mTLS) authentisiert. Der Aufbau von Verbindungen wird nur den Systemen gewährt, welche in den (Stamm-)Gemeinschaften registriert sind und über gültige X.509 Zertifikate verfügen.

Der Zugriff auf die Daten und Dokumente wird durch das Autorisierungssystem des EPD gesteuert. Zugriffsentscheide basieren auf den von Patientinnen und Patienten eingestellten Zugriffsrechten. Der Service nutzt dazu die Daten aus den Security Token und die Services zur Zugriffsteuerung im EPD.

Die Aufrufe des Service werden gemäss dem nationalen Integrationsprofil in einem Standardformat protokolliert und in den ATNA Audit Record Repositories der (Stamm-)Gemeinschaften abgelegt.

Die Integrität der Daten wird den (Stamm-)Gemeinschaften und den angeschlossenen Systemen verantwortet, welche die Transaktionen protokollieren.

3.3.8 Patientenportal

Zur Erfüllung der Vorgaben des EPDG müssen Stammgemeinschaften mindestens ein Patientenportal implementieren, welche alle Anforderungen der EPDV-EDI erfüllen.

Patientenportale müssen dazu insbesondere die folgenden Funktionen für Patientinnen, Patienten und deren Stellvertretungen zur Verfügung stellen:

- Anzeige von Dokumenten und Dokument-Metadaten,
- Speicherung patienteneigener Dokumente,
- Ansicht und Einstellung der Zugriffsrechte,
- Einsicht in die CH:ATC Protokolle,
- Speicherung und Bearbeitung von administrativen Einstellungen,
- Speicherung von Kontaktdaten (E-Mail, Telefonnummer, usw.).

(Stamm-)Gemeinschaften müssen mindestens ein Patientenportal betreiben, welches über das Internet erreichbar ist und alle im EPDG und in den EPDV-EDI geforderten Funktionen implementiert. Darüber hinaus, können (Stamm-)Gemeinschaften weitere Portale mit ggf. eingeschränkten Funktionsumfang anbieten, z.B. für spezielle ausgewählte Use Cases.

Patientenportale können neben den Funktionen für EPD weitere, kommerzielle Dienste integrieren, wenn diese jederzeit für den Benutzer erkennbar von den Funktionen des EPD getrennt sind.

Alle Zugriffe über das Patientenportal müssen bei einem zertifizierten Herausgeber von Identifikationsmitteln (siehe 3.1) authentisiert werden.

Das Patientenportal muss die oben genannten Dienste und Schnittstellen zum Zugriff auf die Daten und Dokumente nutzen. Das Patientenportal darf insbesondere die Zugriffsrechte nicht umgehen und muss alle Zugriffe im Audit Record Repository der Stammgemeinschaft protokollieren.

3.3.9 Gesundheitsfachpersonenportal

Zur Erfüllung der Vorgaben des EPDG müssen (Stamm-)Gemeinschaften mindestens ein Zugangsportal für Gesundheitsfachpersonen implementieren, welche alle Anforderungen der EPDV-EDI erfüllen.

Gesundheitsfachpersonenportale müssen dazu insbesondere die folgenden Funktionen für Gesundheitsfachpersonen und deren Hilfspersonen implementieren:

- Registrierung von Patientinnen und Patienten,
- Anzeige von Dokumenten und Dokument-Metadaten,
- Speicherung von Dokumenten im EPD,
- Speicherung und Bearbeitung von administrativen Einstellungen,
- Speicherung von Kontaktdaten (E-Mail, Telefonnummer, usw.).

(Stamm-)Gemeinschaften müssen mindestens ein Gesundheitsfachpersonenportal betreiben, welches über das Internet erreichbar ist und alle im EPDG und in den EPDV-EDI geforderten Funktionen implementiert. Darüber hinaus, können (Stamm-)Gemeinschaften weitere Portale mit ggf. eingeschränkten Funktionsumfang anbieten, z.B. für spezielle ausgewählte Use Cases.

Gesundheitsfachpersonenportale können neben den Funktionen für EPD weitere, kommerzielle Dienste integrieren, wenn diese jederzeit für die Benutzer erkennbar von den Funktionen des EPD getrennt sind.

Alle Zugriffe über das Gesundheitsfachpersonenportal müssen bei einem zertifizierten Herausgeber von Identifikationsmitteln (siehe 3.1) authentisiert werden.

Das Gesundheitsfachpersonenportal muss die oben genannten Dienste und Schnittstellen zum Zugriff auf die Daten und Dokumente nutzen. Das Gesundheitsfachpersonenportal darf insbesondere die Zugriffsrechte nicht umgehen und muss alle Zugriffe im Audit Record Repository der (Stamm-)Gemeinschaft protokollieren.

3.3.10 Primärsysteme

Als Primärsystem werden im EPDG Systeme bezeichnet, welche die Gesundheitsfach- und Hilfspersonen zur Unterstützung ihrer täglichen Arbeit in den Spitälern, Heimen und Praxen benutzen.

Primärsysteme implementieren die oben genannten Dienste wie die Gesundheitsfachpersonenportale direkt oder über Intermediäre. Sie unterstützen insbesondere die folgenden Funktionen:

a. Lesen und schreiben von Dokumenten im EPD,
b. Registrierung der Patientenstammdaten in der (Stamm-)Gemeinschaft,
c. Ggf. Lesen und schreiben von Zugriffsrechten für die Delegation (Weitergabe von Zugriffsrechten z.B. für temporäre Stellvertretungen).

Alle Zugriffe auf das EPD müssen bei einem zertifizierten Herausgeber von Identifikationsmitteln (siehe 3.1) authentisiert werden. Darüber hinaus authentisieren sich Primärsysteme auf dem TLS Netzwerk Layer.

Primärsysteme müssen die oben genannten Dienste und Schnittstellen zum Zugriff auf die Daten und Dokumente des EPD nutzen, entweder tief integriert oder über Intermediäre.

Zur Sicherstellung der Rückverfolgbarkeit müssen Primärsysteme alle Zugriffe im Audit Record Repository der (Stamm-)Gemeinschaft protokollieren.

3.3.11 Klinische Archivsysteme

Mit dem Begriff klinische Archivsysteme werden im EPD Systeme bezeichnet, welche die behandlungsrelevanten Dokumente automatisch und nach bestimmten Regeln im EPD speichern. Klinische Archivsysteme werden typischerweise in grösseren Institutionen (Spitäler, Heime, usw.) eingesetzt und zur Archivierung und Verteilung innerhalb der Institution genutzt, sowie zur automatischen Ablage von Dokumenten im EPD. Sie greifen mit einer speziellen Benutzerrolle (Technischer User) und nur schreibend auf das EPD von Patientinnen und Patienten zu.

(Stamm-)Gemeinschaften müssen alle klinischen Archivsysteme registrieren. Die Archivsysteme authentisieren sich auf dem TLS Netzwerk Layer und nutzen digitale Signaturen zur Authentisierung für die Zugriffsteuerung.

Klinische Archivsysteme müssen die oben genannten Dienste und Schnittstellen zum Zugriff auf die Daten und Dokumente des EPD nutzen, entweder tief integriert oder über Intermediäre.

Zur Sicherstellung der Rückverfolgbarkeit müssen klinische Archivsysteme alle Zugriffe im Audit Record Repository der (Stamm-)Gemeinschaft protokollieren.

3.3.12 Bilddatenarchive

Das EPD nutzt eine Integration von Bilddaten für Röntgenbilder, CT-Studien usw. nach dem IHE XDS-I.b Standard. Dabei werden in den Repositories der (Stamm-)Gemeinschaften nicht die Bilddaten selbst, sondern eine Referenz auf die Bilddaten in den Bilddatenarchiven gespeichert. Zur Ansicht der Bilddaten laden die angeschlossenen Primärsysteme und Portale die Referenzudaten (Key Object Selection, KOS) aus den Repositories und erst in einem zweiten Schritt, die Bilddaten aus den Archivsystemen über die von der (Stamm-)Gemeinschaften bereitgestellten Schnittstellen.

Die Bilddatenarchive agieren im EPD daher in zwei Rollen: als Bereitsteller der Referenzen zu den Bilddaten in Form von KOS Objekten und als Bereitsteller der Bilddaten (z.B. DICOM Studien) für die angeschlossenen Primärsysteme und Portale.

Bilddatenarchive müssen bei der Registrierung der Bilddaten die oben genannten Dienste und Schnittstellen zum Zugriff auf das EPD nutzen. Sie müssen sich auf dem TLS Netzwerk Layer authentisieren und digitale Signaturen zur Authentisierung für die Zugriffsteuerung (vgl. 3.3.11) nutzen.

Der Zugriff der Primärsysteme und Portale auf die Bilddaten (z.B. DICOM Studien) wird über die (Stamm-)Gemeinschaften vermittelt, welche auch die Zugriffrechte durchsetzt.

Zur Sicherstellung der Rückverfolgbarkeit müssen auch die Bilddatenarchive alle Zugriffe im Audit Record Repository der (Stamm-)Gemeinschaft protokollieren.

4 Anhang

4.1 Autorisierung im EPD

Das Autorisierungssystem des EPD reflektiert die Anforderungen des EPDG und der EPDV-EDI an Datenschutz und Datensicherheit, insbesondere:

- Jeder lesende und schreibende Zugriff auf das EPD muss stark authentisiert werden.
- Natürliche Personen müssen sich an einem zertifizierten Herausgeber von Authentisierungsmitteln (Identity Provider) authentisieren und technische Systeme müssen sich mit X.509 Zertifikaten ausweisen, welche vorgängig in der (Stamm-)Gemeinschaften registriert wurden.
- Alle (Stamm-)Gemeinschaften müssen die von den Patientinnen und Patienten in ihrer Stammgemeinschaft eingestellten Zugriffrechte durchsetzen.
- Für Notfallzugriffe durch Gesundheitsfachpersonen gelten erweiterte Zugriffsrechte, falls Patientinnen und Patienten den Notfallzugriff nicht ausschliessen.
- Gesundheitsfachpersonen können die Zugriffsrechte von Gruppen von Gesundheitsfachpersonen, bei denen sie Mitglied sind, erben.

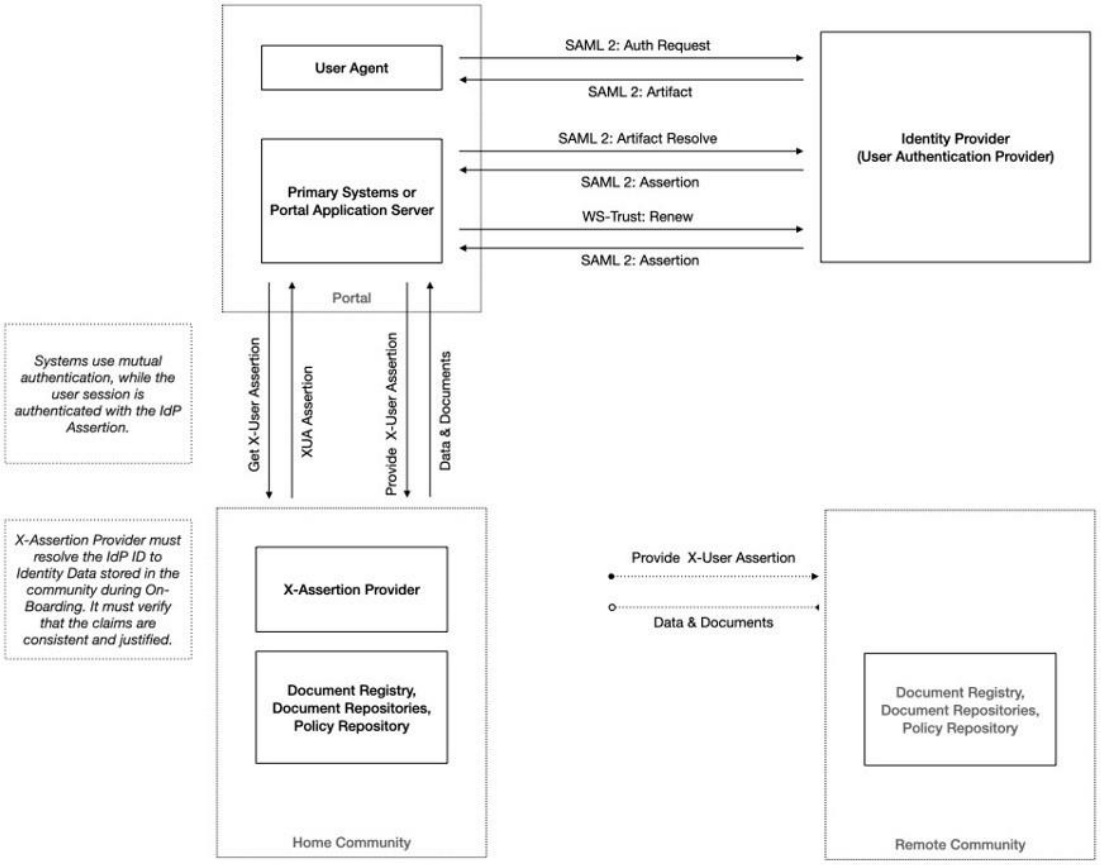

Abb. 3: Authentisierung und Autorisierung von Zugriffen durch natürliche Personen im EPD.

Die Authentisierung und Autorisierung von Zugriffen durch natürliche Personen auf das EPD ist wie folgt (siehe Abb. 3):

- Natürliche Personen, welche über Portale oder Primärsysteme auf das EPD zugreifen wollen, authentisieren sich bei einem zertifizierten Herausgeber von Identifikationsmitteln (Identity Provider (IdP) bzw. IHE XUA User Authentication Provider). Das Portal oder Primärsystem implementiert dazu die Schritte des SAML 2 Artifact Flow oder WS-Trust: Renew Protokoll, jeweils mit den nationalen Ergänzungen der EPDV-EDI.
- Nach erfolgreicher Authentisierung, antwortet der Identity Provider mit einer IdP Assertion im SAML 2 Format, welche die natürliche Person im EPD identifiziert. Die IdP Assertion enthält nur minimale personenidentifizierende Attribute, insbesondere keine Informationen zum Kontext des Zugriffs (z.B. Notfallzugriff).
- Portale oder Primärsysteme tauschen die IdP Assertion gegen einen Autorisierungstoken (X-User Assertion) mit Angaben zum Kontext des Zugriffs und weiteren für die Autorisierung benötigten Attributen (z.B. die verantwortliche Gesundheitsfachperson für Hilfspersonen). Der Zugriff wird dabei durch die beglaubigte Identität des Herausgebers von Identifikationsmitteln (Identity Provider) authentisiert.
- Die Portale und Primärsysteme nutzen den Autorisierungstoken im Security Header der Transaktionen zum Zugriff auf die Dienste (z.B. zur Abfrage von Dokumenten) des EPD.
- Die Services nutzen die Informationen aus dem Autorisierungstoken (X-User Assertion) zur Durchsetzung der Zugriffsrechte. Sie fragen dazu Zugriffsentscheide beim Policy Repository Service der (Stamm-)Gemeinschaften der Patientin bzw. des Patienten ab, ggfs. als gemeinschaftsübergreifende Abfrage.

- Bei allen o.g. Transaktionen authentisieren sich die technischen Systeme gegenseitig auf dem Netzwerk Layer (mTLS).

Hinweis:

- Die Revision der EPDV-EDI erlaubt den Herausgebern von Identifikationsmitteln neu die Nutzung des Open ID Connect Protokolls mit nationalen Ergänzungen der EPDV-EDI zur Authentisierung von natürlichen Personen im EPD. Die o.g. Prozessschritte werden dabei beibehalten, nur das statt SAML 2 auch Open ID Connect unterstützt werden kann.
- Mit der umfassenden Revision soll die Integration von nativen Mobile Apps durch die Einführung von OAuth zur Autorisierung der Zugriffe unterstützt werden.

Weitere Informationen zur Umfassende Revision des EPDG, Übergangsfinanzierung und Jahresrevision