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

Architecture du DEP

Description détaillée

Contenu

SMA
30.01.2024

Schwarzenburgstrasse 157
CH-3003 Berne

www.e-health-suisse.ch

ehealthsuisse
Kompetenz- und Koordinationsstelle
von Bund und Kantonen

1 Introduction

Le présent document donne un aperçu de l'architecture et de l'environnement de services du dossier électronique du patient (DEP) en Suisse.

Du point de vue des utilisateurs, le DEP est un système décentralisé servant à gérer de la documentation en vue d'échanger des données et documents médicaux[1] entre les professionnels de la santé et les patients dans le cadre d'un traitement.

Au début d'un traitement, les professionnels de la santé doivent charger l'anamnèse du patient depuis le DEP dans leurs systèmes primaires. Pendant et après le traitement, les professionnels de la santé doivent enregistrer dans le DEP du patient les données et documents concernant le traitement afin qu'ils soient disponibles pour le suivi ou pour l'information du patient. Les patients peuvent aussi enregistrer eux-mêmes dans leur DEP leurs propres données et documents.

L'architecture du DEP reflète notamment les exigences élevées concernant la protection des données. Les patients peuvent paramétrer les droits d'accès de manière très précise, par exemple en permettant seulement à certains professionnels de la santé d'accéder à des documents. Tous les utilisateurs doivent s'authentifier à l'aide d'au moins deux facteurs, tous les accès sont consignés et tous les systèmes techniques affiliés au DEP doivent être enregistrés et authentifiés sur le réseau ou à l'aide des signatures numériques des messages.

2 Clause de non-responsabilité

Le présent document offre un aperçu de l'architecture du DEP aux lecteurs qui souhaitent en savoir davantage sur la mise en œuvre technique du DEP. Il se concentre sur les principaux aspects, n'aspire pas à l'exhaustivité et n'est pas de nature normative.

[1] Contrairement à ce qui est souvent supposé, le DEP permet aussi d'enregistrer des données structurées. Les communautés (de référence) doivent prendre en charge les formats d'échange tels qu'exigés dans l'ODEP-DFI, mais ont tout loisir de définir et d'utiliser d'autres formats d'échange.

3 Architecture du DEP

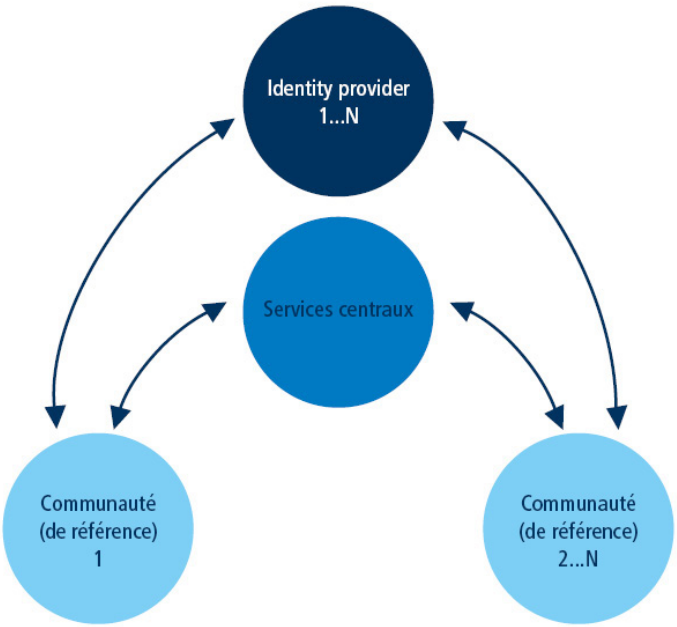

Fig. 1 : Aperçu des systèmes impliqués dans le DEP

Le DEP est un système décentralisé de gestion des documents, composé des systèmes suivants :

- éditeurs de moyens d'identification : services d'authentification de personnes physiques sur Internet ;
- services centraux de la Confédération : services mettant à disposition les données utilisées par toutes les communautés (de référence), notamment la recherche de définitions de métadonnées du DEP pour les utiliser dans des documents, le répertoire des points d'accès des communautés (de référence), le répertoire des professionnels de la santé et des établissements affiliés au DEP, le service de recherche des numéros d'identification des patients pour le DEP (EPR-SPID) ;
- communautés (de référence) : regroupement d'établissements et de professionnels de la santé qui mettent à disposition les plateformes DEP et les processus d'exploitation ;
- systèmes affiliés des professionnels de la santé et de leurs établissements : notamment les systèmes primaires, les systèmes d'archivage pour les documents et les images (PACS).

3.1 Éditeurs de moyens d'identification

Les éditeurs de moyens d'identification, aussi appelés *Identity Provider*, établissent les outils d'authentification nécessaires pour accéder au DEP à l'intention des personnes suivantes : les professionnels de la santé et leurs assistants, les patients et leurs représentants, les administrateurs des communautés (de référence).

Ils installent les processus visant à établir les moyens d'identification, l'identification valable, la révocation, etc. et mettent à disposition les interfaces permettant d'authentifier les personnes physiques.

La loi sur le dossier électronique du patient (LDEP) et les ordonnances y afférentes (ODEP, ODEP-DFI) fixent les exigences posées aux éditeurs de moyens d'identification. Pour pouvoir utiliser le DEP,

ceux-ci doivent avoir reçu une certification. L'annexe 8 de l'ODEP-DFI détermine les critères de certification, qui comprennent les exigences liées aux processus et aux interfaces.

En vue d'une utilisation dans le DEP, les communautés (de référence) concluent des contrats avec un ou plusieurs éditeurs de moyens d'identification qui peuvent être utilisés ensuite pour autoriser les utilisateurs à accéder aux portails des communautés (de référence) et aux systèmes affiliés (systèmes primaires).

Le DEP prescrit les interfaces à prendre en charge, mais pas l'architecture des éditeurs.

En vertu de l'annexe 8 de l'ODEP-DFI, les éditeurs de moyens d'identification certifiés doivent prendre en charge les interfaces des profils d'intégration suivants :

- SAML 2.0 Artifact Binding et protocole de résolution d'artefacts via le backchannel SOAP ;
- SAML 2.0 Logout Binding via le backchannel SOAP ;
- Renew Protocol avec profil d'intégration spécifique au DEP (annexe 8 de l'ODEP-DFI) basé sur le standard WS Trust.

Les éditeurs certifiés de moyens d'identification peuvent proposer, à titre facultatif, les interfaces des profils d'intégration suivants pour une utilisation dans le DEP, notamment pour les clients mobiles :

- OpenID Connect Authorization Code Flow avec profil d'intégration spécifique au DEP (annexe 8 de l'ODEP-DFI) ;
- OpenID Connect Logout Flow avec profil d'intégration spécifique au DEP (annexe 8 de l'ODEP-DFI).

3.2 Services centraux de la Confédération

La Confédération exploite des services centraux nécessaires à l'exploitation correcte de l'architecture décentralisée :

- service de recherche de l'identifiant sectoriel des personnes pour le DEP (EPR-SPID) ;
- métadonnées DEP : catalogue des ensembles de valeurs des métadonnées des documents et des ensembles de valeurs pour le codage des données structurées des formats d'échange ;
- points d'accès des communautés (de référence) : catalogue des informations et des données nécessaires à la communication entre les communautés ;
- répertoire des professionnels de la santé et des établissements affiliés au DEP : liste affectée des établissements, des professionnels de la santé et de leurs groupes que les patients peuvent autoriser à accéder à leur DEP.

3.2.1 Service de recherche de l'identifiant sectoriel des personnes (EPR-SPID)

Le service de recherche de l'identifiant sectoriel des personnes (EPR-SPID) Unique Person Identification Service (UPI) installe une interface vers la banque de données de la Centrale de compensation de la Confédération qui édite et gère le numéro AVS (NAVS13).

L'interface prend notamment en charge les fonctions suivantes pour les communautés (de référence) :

- recherche de l'identifiant sectoriel des personnes pour le DEP (EPR-SPID) à l'aide des données démographiques ou du NAVS13 des patients ;
- demande pour générer un nouvel EPR-SPID en indiquant les données démographiques ou le NAVS13 du patient ;
- annulation ou désactivation de l'EPR-SPID ;
- information sur le statut d'un EPR-SPID (actif, inactif, annulé).

La communication avec l'UPI requiert l'exploitation d'un client SEDEX dans la plateforme DEP des communautés (de référence). Le client SEDEX propose aux communautés (de référence) les interfaces suivantes :

- SOAP Webservice selon la norme eCH-0213 (query) ;
- SOAP Webservice selon la norme eCH-0213 (generate, inactivate, cancel) ;
- interface fichier selon la norme eCH-0215 (broadcast en cas de changement de statut).

3.2.2 Métadonnées du DEP

Le service installe une interface pour rechercher les métadonnées de document conformes au DEP et pour coder les données structurées des formats d'échange.

L'interface prend notamment en charge les fonctions suivantes :

- téléchargement des ensembles de valeur du DEP depuis le site Internet ;
- requête des ensembles de valeur du DEP via un service web XML SOAP selon le profil d'intégration IHE Sharing Value Sets (SVS).

3.2.3 Points d'accès des communautés (de référence) (CPI)

Le service de répertoire des points d'accès des communautés (de référence) installe des interfaces pour rechercher des coordonnées qui peuvent être nécessaires à la communication entre les communautés (de référence). Il s'agit notamment de :

- URL et certificats X.509 des portails pour l'échange de documents
- URL et certificats X.509 du point final pour les décisions d'accès
- URL et certificats X.509 du point final pour les protocoles d'accès

Les responsables de l'exploitation des communautés (de référence) envoient les données à l'OFSP par e-mail sécurisé ; les communautés (de référence) y accèdent via un format de données propriétaire (cf. ODEP-DFI) sur la base du protocole LDAP.

3.2.4 Répertoire des fournisseurs de prestations affiliés au DEP

Le service installe des interfaces pour que les communautés échangent les données des professionnels de la santé ou de leurs groupes auxquels les patients ont octroyé des droits d'accès.

Les données sont affectées et correspondent uniquement aux données des professionnels de la santé, de leurs groupes et des établissements telles que prescrites dans la loi. Il s'agit des données suivantes :

- GLN comme identifiant des professionnels de la santé ;
- OID comme identifiant de groupes de professionnels de la santé et des établissements ;
- numéro REE des établissements ;
- noms et adresses des professionnels de la santé, de leurs groupes et des établissements ;
- relations entre les professionnels de la santé, leurs groupes et les établissements.

Les communautés (de référence) saisissent les données. Elles utilisent le service pour échanger des données entre elles.

Le service prend en charge les interfaces basées sur DSML(LDAP) et XML SOAP du profil IHE Healthcare Provider Directory (HPD) comprenant les adaptations nationales apportées à l'ODEP-DFI.

La responsabilité de l'intégrité des données incombe aux communautés (de référence) qui les saisissent et les transmettent aux autres communautés (de référence) à l'aide du répertoire.

3.3 Communautés (de référence)

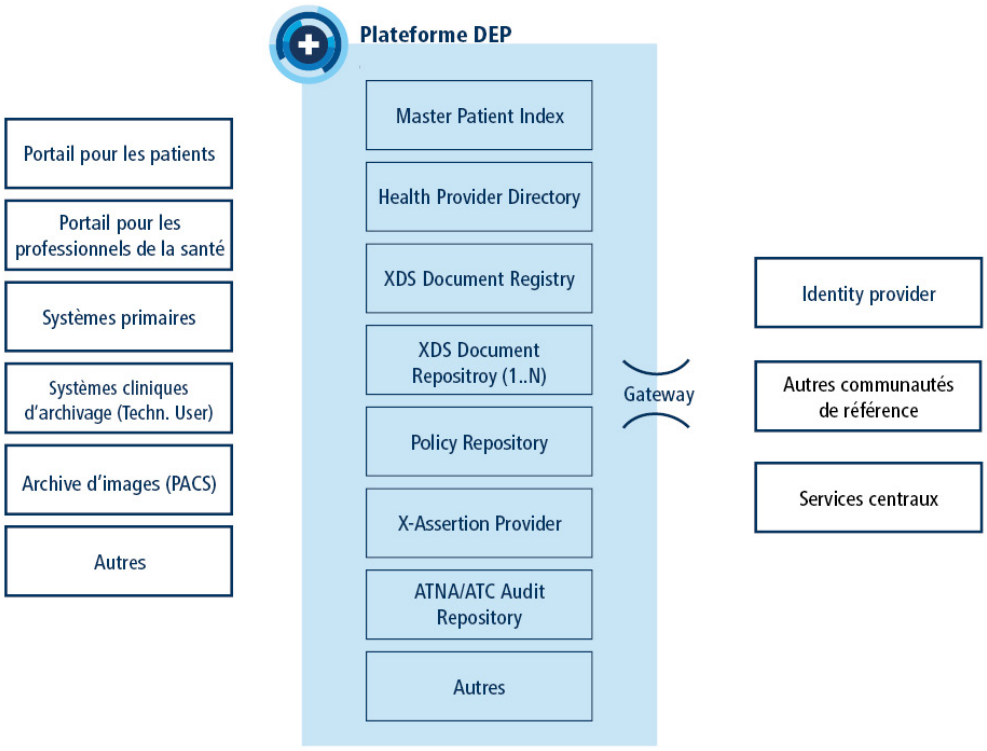

Fig. 2 : Aperçu des services et applications d'une communauté (de référence)

L'ODEP-DFI fixe les exigences liées aux interfaces interopérables et à la sécurité des données de l'infrastructure technique des communautés (de référence), mais aucune exigence quant à l'architecture.

Les communautés (de référence) et leurs fournisseurs de plateforme (fournisseurs et exploitants de leur plateforme DEP) peuvent donc répartir les services sur les applications comme ils l'entendent et selon leurs propres exigences. Par conséquent, on trouve parmi les communautés (de référence) des architectures de service tant monolithiques que décentralisées.

Cependant, dans la pratique, une architecture qui installe les services décrits ci-après s'est imposée (cf. Fig. 2).

3.3.1 Master Patient Index

Ce service permet de gérer les identifiants des patients au sein d'une communauté (de référence). Dans le DEP, le Master Patient Index est affecté et prend en charge toutes les fonctions nécessaires à l'identification des systèmes entre les systèmes, notamment :

- enregistrement et gestion des identités locales des patients dans les systèmes affiliés (p. ex. systèmes primaires, archive) et données démographiques correspondantes ;
- attribution d'un Master Patient ID pour identifier les patients au sein d'une communauté (de référence) ;
- appariement des identifiants à l'aide des données démographiques et du EPR-SPID ;
- enregistrement du EPR-SPID.

Lors de l'ouverture du DEP, les communautés (de référence) enregistrent les données ; en cours d'exploitation, la saisie incombe aux systèmes affiliés lors de l'enregistrement de nouveaux patients

(p. ex. dans le système de gestion des données des patients, dans les systèmes d'information de la clinique ou du cabinet, dans les portails). Elles sont aussi enregistrées dans le Master Patient Index.

Le Master Patient Index saisit tous les identifiants enregistrés ainsi que les données démographiques correspondantes ; il attribue ensuite un Master Patient ID qui peut être utilisé comme identifiant dans les registres de documents. En outre, le Master Patient Index détermine quels identifiants se rapportent au même patient et gère un tableau référençant les identifiants déterminés et le Master Patient ID.

Les systèmes affiliés d'une communauté (de référence) recherchent auprès du Master Patient Index le Master Patient ID des patients dont ils ont besoin pour rechercher des documents.

À cette fin, le Master Patient Index prend en charge les interfaces suivantes conformément aux normes internationales, sur la base des services web HL7 V3 et XML SOAP comprenant les adaptations nationales apportées à l'ODEP-DFI :

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

Il est prévu d'introduire des interfaces basées sur FHIR. Elles permettront de prendre en charge les profils suivants, aussi basés sur FHIR :

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

Conformément aux prescriptions des profils IHE et aux élargissements nationaux, toutes les recherches du service doivent être consignées dans un format standard et enregistrées dans les ATNA Audit Record Repositories de la communauté (de référence).

Les accès aux données sont authentifiés sur la couche de réseau (mTLS). L'établissement de connexions et l'accès sont garantis uniquement aux systèmes enregistrés dans les communautés (de référence) et qui disposent de certificats X.509 valables.

Les données gérées dans le Master Patient Index sont conçues au minimum dans le but de permettre d'échanger des documents dans le DEP. La révision totale de la LDEP conférera d'autres objectifs à l'utilisation du DEP.

Les communautés (de référence) et les systèmes affiliés (p. ex. systèmes primaires) qui saisissent les données sont responsables de l'intégrité des données. En vertu de l'ODEP-DFI, les communautés (de référence) et les systèmes affiliés sont tenus de reprendre les données démographiques fiables du service de recherche des registres sectoriels des personnes UPI et, éventuellement, de les compléter avec les données de contact ou d'autres indications pouvant être utiles pour l'exploitation du DEP.

3.3.2 Healthcare Provider Directory (HPD)

Le service installe des interfaces pour échanger les données des professionnels de la santé, de leurs auxiliaires, des groupes de professionnels de la santé et des établissements affiliés ainsi que des administrateurs DEP d'une communauté (de référence).

Les données sont affectées et correspondent uniquement aux données prescrites par la LDEP, à savoir :

- GLN des professionnels de la santé et des auxiliaires ;
- OID des établissements et des groupes de professionnels de la santé ;
- numéro REE des établissements ;
- noms et adresses des professionnels de la santé, de leurs groupes et des établissements ;
- relations entre les professionnels de la santé, leurs groupes et les établissements ;
- relations entre les auxiliaires et les professionnels de la santé.

Les données sont saisies par les communautés (de référence) ou reprises d'autres communautés (de référence) via le service central de la Confédération. Ce service permet de synchroniser uniquement les professionnels de la santé, leurs groupes et les établissements. Les entrées des auxiliaires et des administrateurs DEP sont saisies exclusivement dans les répertoires locaux des communautés (de référence).

Les communautés (de référence) mettent à disposition les données des systèmes affiliés via les interfaces standard, notamment pour rechercher des professionnels de la santé ou leurs groupes et pour administrer les droits d'accès par les patients.

Le service prend en charge les interfaces basées sur DSML (LDAP) et XML SOAP du profil IHE Healthcare Provider Directory (HPD) comprenant les adaptations nationales apportées à l'ODEP-DFI, ainsi que les interfaces utilisateurs pour la gestion par les administrateurs des communautés (de référence).

Il est prévu d'introduire des interfaces basées sur FHIR. À cette fin, le profil Mobile Care Services Discovery (mCSD) doit être pris en charge.

Les accès aux données sont authentifiés sur le protocole de transport (mTLS). L'établissement de connexions est garanti uniquement aux systèmes enregistrés dans les communautés (de référence) et qui disposent de certificats X.509 valables.

Les documents gérés dans le répertoire sont prévus au minimum pour l'échange de documents dans le DEP. La révision totale de la LDEP conférera d'autres objectifs à l'utilisation du DEP.

Les communautés (de référence) dans lesquelles les données sont enregistrées sont responsables de l'intégrité de ces dernières.

3.3.3 XDS Document Registry

Le DEP utilise un système de gestion des documents basé sur la norme internationale Cross-Enterprise Document Sharing (XDS) d'IHE International. Le service Document Registry installe des interfaces permettant d'enregistrer les métadonnées XDS pour saisir et rechercher des documents médicaux dans une infrastructure décentralisée.

Les données du Document Registry sont affectées et correspondent uniquement aux données de documents que la loi prescrit pour le DEP, à savoir :

- des valeurs codées pour le type de document et la classe ;
- des données sur l'auteur du document ;
- des valeurs codées pour le domaine spécialisé de l'auteur ou de l'établissement ;
- des données codées du niveau de confidentialité.

Les données sont saisies par les systèmes affiliés des communautés (de référence) lors de l'enregistrement des documents et enregistrées via les interfaces.

Tous les systèmes affiliés au DEP peuvent rechercher les données via des interfaces, que ce soit au sein des communautés (de référence) ou entre elles.

À cette fin, le service prend en charge les interfaces basées sur ebXML et SOAP du profil IHE Cross-Enterprise Document Sharing (XDS.b) comprenant les adaptations nationales apportées à l'ODEP-DFI, ainsi que les interfaces utilisateurs pour la gestion par les administrateurs des communautés (de référence).

Il est prévu d'introduire des interfaces basées sur FHIR. À cette fin, le profil Mobile access to Health Document (MHD) doit être pris en charge.

Les accès aux données sont authentifiés sur le protocole de transport (mTLS). L'établissement de connexions est garanti uniquement aux systèmes enregistrés dans les communautés (de référence) et qui disposent de certificats X.509 valables.

Le système d'autorisation du DEP pilote l'accès aux données et aux documents. Les décisions d'accès se basent sur les droits d'accès paramétrés par les patients. Pour cela, le service utilise les données issues du Security Token et les services de pilotage des accès dans le DEP.

Conformément aux prescriptions des profils IHE et aux élargissements nationaux, toutes les recherches du service doivent être consignées dans un format standard et enregistrées dans les ATNA Audit Record Repositories des communautés (de référence).

Les utilisateurs des communautés (de référence) et des systèmes affiliés dans lesquels les données sont enregistrées sont responsables de l'intégrité de ces dernières.

3.3.4 XDS Document Repositories

Le DEP utilise un système de gestion des documents basé sur la norme internationale Cross-Enterprise Document Sharing (XDS) d'IHE International. Le service Document Repository installe des interfaces pour enregistrer et rechercher les objets binaires[2] des documents XDS.

Les données sont saisies par les systèmes affiliés des communautés (de référence) lors de l'enregistrement des documents et enregistrées via les interfaces.

Tous les systèmes affiliés au DEP peuvent rechercher les données via des interfaces, que ce soit au sein des communautés (de référence) ou en dehors.

À cette fin, le service supporte les interfaces basées sur ebXML et SOAP du profil IHE Cross-Enterprise Document Sharing (XDS.b) comprenant les adaptations nationales apportées à l'ODEP-DFI.

Il est prévu d'introduire des interfaces basées sur FHIR. À cette fin, le profil Mobile access to Health Document (MHD) doit être supporté.

Les accès au DEP sont authentifiés sur le protocole de transport (mTLS). L'établissement de connexions est garanti uniquement aux systèmes enregistrés dans les communautés (de référence) et qui disposent de certificats X.509 valables.

Le système d'autorisation du DEP pilote l'accès aux données et aux documents. Les décisions d'accès se basent sur les droits d'accès paramétrés par les patients. Pour cela, le service utilise les données issues du Security Token et les services de pilotage des accès dans le DEP.

Conformément aux prescriptions des profils IHE et aux élargissements nationaux, toutes les recherches du service doivent être consignées dans un format standard et enregistrées dans les ATNA Audit Record Repositories des communautés (de référence).

Les utilisateurs des communautés (de référence) et des systèmes affiliés dans lesquels les données sont enregistrées sont responsables de l'intégrité de ces dernières.

3.3.5 Assertion Provider (STS)

Des Security Token basés sur des protocoles WS-Trust protègent les accès aux données et aux documents dans le DEP. Le service Assertion Provider installe le service WS-Trust Secure Token requis ainsi que les interfaces correspondantes.

Les communautés (de référence) saisissent les données du service. Pour établir le Security Token, le service utilise les données d'autres services, notamment celles des professionnels de la santé, de leurs groupes et des établissements, issues du Healthcare Provider Directory (HPD).

Le service prend en charge les interfaces basées sur SOAP issues de la norme WS-Trust comprenant les adaptations nationales apportées à l'ODEP-DFI.

[2] La norme de gestion des documents du groupe OASIS définit un document comme la combinaison d'un objet binaire et de métadonnées.

Il est prévu d'introduire des interfaces basées sur OAuth. À cette fin, le profil Internet User Authorization (IUA) basé sur OAuth doit être pris en charge.

Les accès aux données sont authentifiés sur le protocole de transport (mTLS). L'établissement de connexions est garanti uniquement aux systèmes enregistrés dans les communautés (de référence) et qui disposent de certificats X.509 valables.

Conformément aux prescriptions des profils IHE et aux élargissements nationaux, toutes les recherches du service doivent être consignées dans un format standard et enregistrées dans les ATNA Audit Record Repositories des communautés (de référence).

Les communautés (de référence) sont responsables de l'intégrité des données.

3.3.6 Policy Repository

Le DEP utilise un concept d'autorisation selon la norme XACML 2.0. Pour gérer les droits d'accès dans le DEP, le service installe les acteurs « Policy Repository » et « Policy Administration Point » de l'architecture de référence XACML avec les interfaces correspondantes.

Les communautés (de référence) saisissent d'abord les données, que les patients peuvent ensuite compléter ou adapter via les portails. En cas de délégation, les professionnels de la santé peuvent également modifier les paramètres dans leurs systèmes primaires ou leur portail. Les paramètres des droits d'accès sont codés dans des composants XACML Policies, écrits par les systèmes affiliés.

Les patients peuvent rechercher les données à partir de leur portail via les interfaces, ou en déléguant cette tâche aux systèmes primaires ou aux portails des professionnels de la santé.

À cette fin, le service prend en charge les interfaces basées sur SAML 2.0 et SOAP du profil d'intégration national Privacy Policy Query (CH:PPQ) en vertu de la spécification figurant dans l'ODEP-DFI.

Il est prévu d'introduire des interfaces basées sur FHIR. À cette fin, le profil d'intégration national Privacy Policy Query for Mobile (CH:PPQm) doit être pris en charge.

Les accès aux données sont authentifiés sur le protocole de transport (mTLS). L'établissement de connexions est garanti uniquement aux systèmes enregistrés dans les communautés (de référence) et qui disposent de certificats X.509 valables.

Le système d'autorisation du DEP pilote l'accès aux données et aux documents. Les décisions d'accès se basent sur les droits paramétrés par les patients. Pour cela, le service utilise les données issues du Security Token et les services de pilotage des accès dans le DEP.

Conformément au profil d'intégration national, toutes les recherches du service doivent être consignées dans un format standard et enregistrées dans les ATNA Audit Record Repositories des communautés (de référence).

Les utilisateurs des communautés (de référence) et des systèmes affiliés dans lesquels les données sont enregistrées sont responsables de l'intégrité de ces dernières.

3.3.7 ATNA/ATC Audit Record Repository

Le DEP utilise un système de procès-verbal basé sur le standard IHE et appelé « profil Audit Trail and Node Authentification (ATNA) ». Les transactions sont consignées par le système émetteur et par le système récepteur selon le standard Syslog au format XML avec le schéma DICOM comprenant les compléments nationaux apportés à l'ODEP-DFI. Pour que les patients puissent s'informer des accès à leur DEP, les données consignées doivent pouvoir être consultées par le portail des patients auprès de toutes les communautés (de référence), conformément au profil d'intégration suisse Audit Trail Consumption (CH:ATC), dans un format plus compréhensible pour les patients.

Pour ce faire, le service prend en charge les profils d'intégration suivants avec les compléments nationaux apportés à l'ODEP-DFI :

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

Les accès aux données sont authentifiés sur le protocole de transport (mTLS). L'établissement de connexions est garanti uniquement aux systèmes enregistrés dans les communautés (de référence) et qui disposent de certificats X.509 valables.

Le système d'autorisation du DEP pilote l'accès aux données et aux documents. Les décisions d'accès se basent sur les droits d'accès paramétrés par les patients. Pour cela, le service utilise les données issues du Security Token et les services de pilotage des accès dans le DEP.

Conformément au profil d'intégration national, les consultations du service doivent être consignées dans un format standard et enregistrées dans les ATNA Audit Record Repositories des communautés (de référence).

Les communautés (de référence) et les systèmes affiliés qui consignent les transactions sont responsables de l'intégrité des données.

3.3.8 Portail pour les patients

Pour satisfaire aux prescriptions de la LDEP, les communautés de référence doivent installer au moins un portail pour les patients répondant à toutes les exigences de l'ODEP-DFI.

Ces portails doivent notamment mettre les fonctionnalités suivantes à la disposition des patients et de leurs représentants :

- affichage de documents et de leurs métadonnées ;
- enregistrement des documents propres aux patients ;
- affichage et réglage des droits d'accès ;
- consultation des protocoles CH:ATC ;
- enregistrement et traitement des paramètres administratifs ;
- enregistrement des données de contact (e-mail, téléphone, etc.).

Les communautés (de référence) doivent exploiter au moins un portail pour patients disponible sur Internet et qui propose toutes les fonctions exigées dans la LDEP et l'ODEP-DFI. Par ailleurs, les communautés (de référence) peuvent mettre à disposition d'autres portails avec des fonctions limitées, par exemple pour certains Use Cases.

En plus des fonctions dédiées au DEP, les portails pour patients peuvent intégrer d'autres services commerciaux, à condition que les utilisateurs puissent les reconnaître et qu'ils soient séparés des fonctions du DEP.

Tous les accès au portail pour les patients doivent être authentifiés auprès d'un éditeur certifié de moyens d'identification (cf. 3.1).

Le portail doit utiliser les services et interfaces susmentionnés pour accéder aux données et aux documents. Il ne doit notamment pas contourner les droits d'accès et doit consigner tous les accès de la communauté de référence à l'Audit Record Repository.

3.3.9 Portail pour les professionnels de la santé

Pour satisfaire aux prescriptions de la LDEP, les communautés de référence doivent installer au moins un portail d'accès pour les professionnels de la santé répondant à toutes les exigences de l'ODEP-DFI.

Ces portails doivent notamment proposer les fonctions suivantes pour les professionnels de la santé et leurs auxiliaires :

- enregistrement des patients ;
- affichage de documents et de leurs métadonnées ;
- enregistrement de documents dans le DEP ;

- enregistrement et traitement de paramètres administratifs ;
- enregistrement des données de contact (e-mail, téléphone, etc.).

Les communautés (de référence) doivent exploiter au moins un portail pour les professionnels de la santé disponible sur Internet et qui propose toutes les fonctions exigées dans la LDEP et l'ODEP-DFI. Par ailleurs, les communautés (de référence) peuvent mettre à disposition d'autres portails avec des fonctions limitées, par exemple pour certains Use Cases.

En plus des fonctions dédiées au DEP, les portails pour les professionnels de la santé peuvent intégrer d'autres services commerciaux, à condition que les utilisateurs puissent les reconnaître et qu'ils soient séparés des fonctions du DEP.

Tous les accès au portail pour les professionnels de la santé doivent être authentifiés auprès d'un éditeur certifié de moyens d'identification (cf. 3.1).

Le portail doit utiliser les services et interfaces susmentionnés pour accéder aux données et aux documents. Il ne doit notamment pas contourner les droits d'accès et doit consigner tous les accès de la communauté (de référence) à l'Audit Record Repository.

3.3.10 Systèmes primaires

La LDEP définit les systèmes primaires comme des systèmes utilisés par les professionnels de la santé et leurs auxiliaires pour les soutenir dans leurs tâches quotidiennes dans les hôpitaux, les homes et les cabinets.

Les systèmes primaires installent les services susmentionnés tels que les portails pour les professionnels de la santé de manière directe ou via des intermédiaires. Ils prennent en charge notamment les fonctions suivantes :

a. lire et modifier les documents dans le DEP ;
b. enregister les données de base des patients dans la communauté (de référence) ;
c. év. lire et modifier les droits d'accès pour la délégation (transmission de droits d'accès, par exemple pour les suppléances temporaires).

Tous les accès au DEP doivent être authentifiés auprès d'un éditeur certifié de moyens d'identification (cf. 3.1). En outre, les systèmes primaires s'authentifient sur la couche de réseau TLS.

Les systèmes primaires doivent utiliser les services et interfaces susmentionnés pour accéder aux données et aux documents du DEP, que ce soit de manière profondément intégrée ou via des intermédiaires.

Pour garantir la traçabilité, les systèmes primaires doivent consigner tous les accès dans l'Audit Record Repository de la communauté (de référence).

3.3.11 Systèmes cliniques d'archivage

Par « systèmes cliniques d'archivage », on entend les systèmes qui enregistrent dans le DEP automatiquement et selon des règles précises les documents relatifs au traitement. Ces systèmes sont utilisés spécifiquement dans les grands établissements (hôpitaux, homes, etc.) pour archiver et distribuer les documents au sein de l'institution et pour les enregistrer automatiquement dans le DEP. Grâce à un rôle utilisateurs spécial (utilisateur technique), ils accèdent au DEP des patients en mode écriture.

Les communautés (de référence) doivent enregistrer tous les systèmes cliniques d'archivage. Les systèmes d'archivage s'authentifient sur la couche de réseau TLS et utilisent les signatures numériques pour l'authentification en vue du pilotage des accès.

Les systèmes cliniques d'archivage doivent utiliser les services et interfaces susmentionnés pour accéder aux données et aux documents du DEP, que ce soit de manière profondément intégrée ou via des intermédiaires.

Pour garantir la traçabilité, les systèmes cliniques d'archivage doivent consigner tous les accès dans l'Audit Record Repository de la communauté (de référence).

3.3.12 Archive des images

Le DEP utilise une intégration d'images pour les radiographies, les examens CT, etc. selon la norme IHE XDS-I.b. Ce faisant, ce ne sont pas les images elles-mêmes qui sont enregistrées dans les répertoires des communautés (de référence), mais une référence aux images dans les archives. Pour afficher les images, les systèmes primaires et portails affiliés chargent les données de référence (Key Object Selection, KOS) depuis les répertoires et, dans un deuxième temps seulement, les images depuis les systèmes d'archivage via les interfaces mises à disposition par les communautés (de référence).

Dans le DEP, l'archive d'images joue donc deux rôles : mettre à disposition les références vers les images sous forme d'objets KOS et mettre à disposition les images (p. ex. études DICOM) pour les systèmes primaires et portails affiliés.

Lors de l'enregistrement des images, les archives doivent recourir aux services et interfaces susmentionnés pour accéder au DEP. Elles doivent s'authentifier sur la couche de réseau TLS et utiliser les signatures numériques pour l'authentification en vue du pilotage des accès (cf. 3.3.11).

L'accès des systèmes primaires et des portails aux images (p. ex. études DICOM) est assuré par la communauté (de référence) qui applique également les droits d'accès.

Pour garantir la traçabilité, les archives d'image doivent consigner tous les accès dans l'Audit Record Repository de la communauté (de référence).

4 Annexe

4.1 Autorisation dans le DEP

Le système d'autorisation du DEP reflète les exigences de la LDEP et de l'ODEP-DFI relatives à la protection et à la sécurité des données, notamment :

- Chaque accès en lecture et en écriture au DEP doit être strictement authentifié.
- Les personnes physiques doivent s'authentifier auprès d'un éditeur certifié de moyens d'authentification, et les systèmes techniques doivent s'identifier avec les certificats X.509, enregistrés au préalable dans les communautés (de référence).
- Toutes les communautés (de référence) doivent appliquer les droits d'accès paramétrés par les patients dans leur communauté de référence.
- Si les professionnels de la santé doivent accéder en urgence au DEP, des droits d'accès élargis s'appliquent, à condition que le patient n'ait pas exclu l'accès d'urgence.
- Les professionnels de la santé peuvent hériter des droits d'accès des groupes dont ils sont membres.

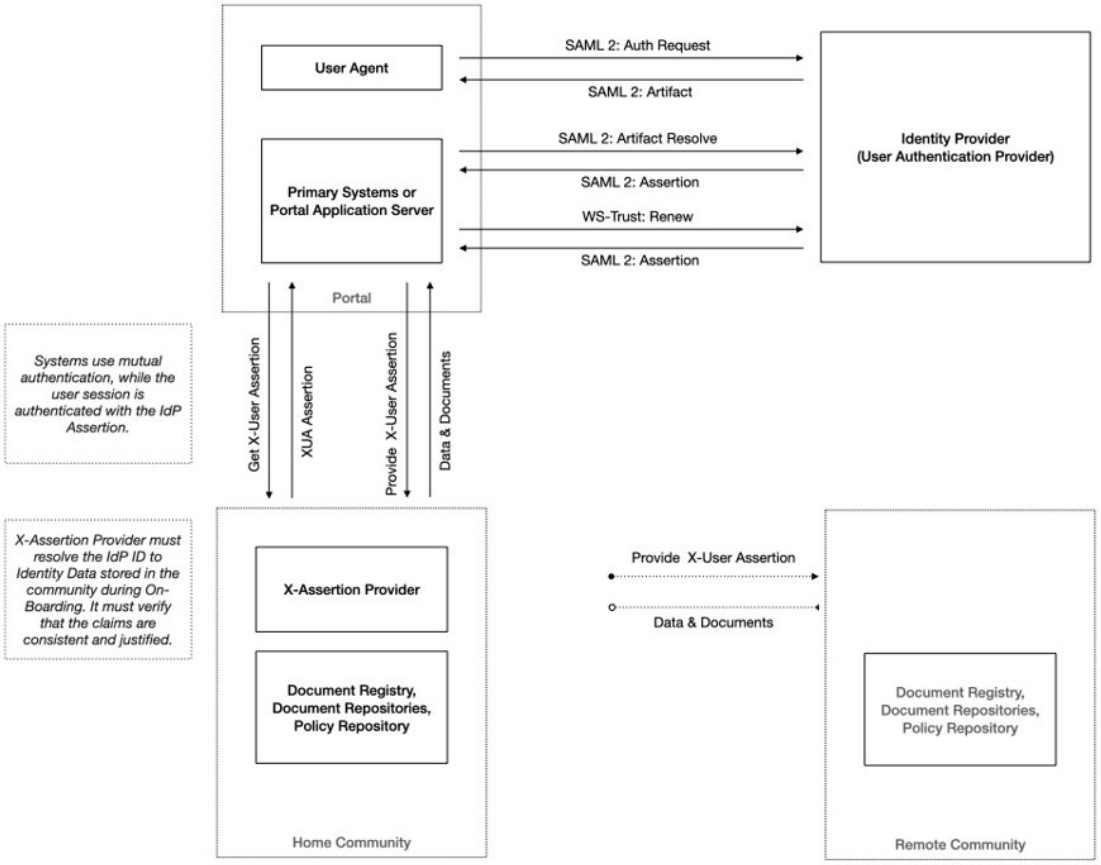

Fig. 3 : Authentification et autorisation des accès au DEP par des personnes physiques

L'authentification et l'autorisation d'accès au DEP par des personnes physiques se déroulent comme suit (cf. Fig. 3) :

- Les personnes physiques qui souhaitent accéder au DEP via les portails ou les systèmes primaires s'identifient auprès d'un éditeur certifié de moyens d'identification (Identity Provider ou IHE XUA User Authentification Provider). À cette fin, le portail ou le système primaire implémente les étapes du protocole SAML 2 Artifact Flow ou WS-Trust: Renew, à chaque fois avec les compléments nationaux apportés à l'ODEP-DFI.
- Après l'authentification, l'éditeur de moyens d'identification répond avec une IdP Assertion au format SAML 2, qui identifie la personne physique dans le DEP. L'IdP Assertion contient un minimum d'attributs permettant d'identifier les personnes, notamment aucune information sur le contexte de l'accès (p. ex., accès d'urgence).
- Les portails ou systèmes primaires échangent l'IdP Assertion avec un token d'autorisation (X-User Assertion) contenant des informations sur le contexte de l'accès et d'autres attributs nécessaires à l'autorisation (p. ex. le professionnel de la santé responsable pour les auxiliaires). L'identité conforme de l'éditeur des moyens d'identification authentifie l'accès.
- Les portails et systèmes primaires utilisent le token d'autorisation dans le Security Header des transactions pour accéder aux services du DEP (p. ex. pour rechercher des documents).
- Les services utilisent les informations issues du token d'autorisation (X-User Assertion) pour appliquer les droits d'accès. Pour cela, ils demandent les décisions d'accès au service Policy Repository des communautés (de référence) du patient ; il peut éventuellement s'agir d'une demande concernant plusieurs communautés.

- Pour toutes les transactions susmentionnées, les systèmes techniques s'authentifient mutuellement sur la couche de réseau (mTLS).

Remarque :

- Pour authentifier les personnes physiques dans le DEP, la révision de l'ODEP-DFI permet aux éditeurs de moyens d'identification d'utiliser le protocole Open ID Connect, qui contient les compléments nationaux apportés à l'ordonnance. Les étapes du processus susmentionnées sont maintenues, à la différence près qu'en plus du SAML 2, l'Open ID Connect est aussi pris en charge.
- La révision complète permettra de prend en charge l'intégration d'applications mobiles natives grâce à l'introduction d'OAuth pour authentifier les accès.

Informations complémentaires sur la révision complète de la LDEP, le financement transitoire et la révision annuelle