# Architecture de référence

Version : 0.1.1

Type : version préliminaire

Date de la version : 17 octobre 2022

Inforoute Santé du Canada

# Table des matières

# 1 Glossaire des termes et abréviations

Le tableau suivant fournit la liste des termes et des abréviations que vous retrouverez dans les spécifications d'interopérabilité pancanadiennes (RDP-CA, CA:FeX) et/ou dans l'information sur le prototypage et la validation.

| Terme/abréviation | Définition |
|---|---|
| Acteurs IHE | Les acteurs IHE (p. ex. professionnel de la santé, DME, DSE, etc.) ont pour rôle de produire et/ou de gérer l'information et/ou d'effectuer une action en fonction de l'information, dans le contexte d'un profil IHE.<br><br>(Source : https://wiki.ihe.net/index.php/Actors) |
| Architecture de référence (AR) | Modèle évolutif de disponibilité des services qui prend en charge un vaste écosystème d'interopérabilité ne se limitant pas aux résumés du dossier du patient. Il a pour but de faciliter le dialogue, la collaboration et la convergence de multiples intervenants vers l'adoption de normes ouvertes communes. Il s'agit d'une vue technique conceptuelle qui fournit un vocabulaire commun ainsi qu'un ensemble d'acteurs et de transactions qui représentent les composantes habituelles d'un écosystème de santé numérique (solutions des secteurs public et privé). L'AR associe des composantes fondamentales provenant d'organismes internationaux d'élaboration de normes à des patrons d'implantation développés au Canada. |
| ATNA | Le profil ATNA (*Audit Trail and Node Authentication*, ou piste d'audit et authentification de nœuds) précise les éléments fondamentaux de toute forme de systèmes sécurisés : authentification des nœuds, authentification des utilisateurs, journalisation des événements (audit) et cryptage des télécommunications. Il est également utilisé pour indiquer que d'autres propriétés de sécurité interne – contrôle d'accès, contrôle de configuration, restriction de privilèges, etc. – sont fournies.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-9.html) |
| Auteur | Professionnel de la santé qui rédige et/ou modifie des données cliniques, p. ex. un résumé du dossier du patient. |
| Base de données sur les produits pharmaceutiques (BDPP) | Base de données qui contient l'information sur les médicaments dont la vente est autorisée par Santé Canada. La BDPP est automatiquement mise à jour tous les soirs et indique la disponibilité des médicaments au Canada. |
| CA:FeX (*Canadian FHIR Exchange*, ou échange FHIR canadien) | Spécification d'interopérabilité visant à faciliter l'implantation de patrons d'échange FHIR RESTful qui ont été développés à partir de la norme de référence FHIR et qui peuvent être appliqués à une infrastructure non FHIR existante tout aussi facilement qu'à des serveurs FHIR. |
| CA:FMT (*Canadian Formatting Service*, ou service de formatage canadien) | Spécification qui permet de convertir des documents en différents formats (p. ex. de FHIR à PDF, à CDA, etc.). |
| Centre de médecine familiale | Le Collège des médecins de famille du Canada définit le centre de médecine familiale (CMF) comme suit :<br><br>« Le CMF est une pratique de médecine de famille définie par ses patients comme l'endroit où ils se sentent le plus à l'aise de parler de leur santé personnelle et familiale, ainsi que de leurs problèmes de santé. (…) Un CMF sert de point central pour la coordination et la continuité des soins liés à tous les |

| Terme/abréviation | Définition |
|---|---|
| | services médicaux que ses patients reçoivent dans la communauté médicale. »<br><br>Ce concept est présenté plus en détail dans le document *Une vision pour le Canada : La pratique de la médecine familiale - Le Centre de médecine de famille*, publié par le Collège des médecins de famille du Canada. |
| Consommateur | Système d'information sur la santé ou de dossiers médicaux (DME, SIS, SIC, DSP, portail-patient, DSE) qui permet à un professionnel de la santé autorisé ou à un patient/sujet de soins d'accéder à un document clinique (p. ex. RDP-CA) ou de le recevoir. |
| Couche d'accès à l'information sur la santé (CAIS) | Spécification d'interface pour l'infostructure de DSE qui définit les composantes des services, les rôles des services, le modèle d'information et les normes de messagerie nécessaires à l'échange de données du DSE et à l'exécution de profils d'interopérabilité entre les services de DSE.<br><br>(Source : https://www.infoway-inforoute.ca/fr/component/edocman/292-architecture-sdse-rapport-complet/view-document, page 360) |
| CT | Le profil d'intégration *Consistent Time* (CT) (synchronisation du temps) permet de bien synchroniser les horloges et les horodateurs des nombreux ordinateurs d'un réseau. Ce profil spécifie une synchronisation comportant une erreur médiane inférieure à 1 seconde. Cela suffit dans la plupart des cas.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-7.html) |
| Dépôt de documents (local ou central) | Voir la définition de Dépôt de données cliniques (local ou central). |
| Dépôt de données cliniques (local ou central) | Aussi appelé « Dépôt de documents cliniques ». Espace de stockage partagé pour les documents cliniques qui peut être hébergé localement (c.-à-d. par le producteur de données) ou dans l'infrastructure centrale et auquel les utilisateurs autorisés peuvent accéder. |
| Dépôt FHIR® | Dépôt basé sur FHIR et utilisé pour le stockage des données cliniques. |
| Domaines IHE | Les domaines IHE sont responsables de l'élaboration et de la tenue à jour des cadres techniques (*IHE Technical Frameworks*) qui décrivent les profils d'intégration. Chaque domaine gère les profils d'intégration dans une discipline particulière des soins de santé (p. ex. les soins virtuels).<br><br>(Source : https://wiki.ihe.net/index.php/Domains) |
| Dossier de santé électronique (DSE) | Solution clinique qui contient un ensemble de données numériques sécurisées et confidentielles sur la santé du patient. Ces données peuvent être partagées entre différents milieux de soins/systèmes cliniques intégrés. Le DSE améliore l'échange et l'interprétation de l'information médicale par les professionnels de la santé qui traitent le patient. Exemples de DSE :<br><br>• CareConnect est le DSE sécurisé et à accès en lecture seule de la Colombie-Britannique. Il offre en tout temps aux professionnels de la santé une vue intégrée à l'échelle provinciale de l'information médicale centrée sur le patient, afin de faciliter la prestation des soins dont il a besoin.<br>• HEALTHe NL est le DSE de Terre-Neuve-et-Labrador. Il fournit des données exactes et fiables qui permettent d'améliorer la prestation des soins, la prise de décisions et l'élaboration des politiques ainsi que d'accroître la reddition de comptes, la stabilité et l'efficacité au sein du réseau provincial de la santé. |

| Terme/abréviation | Définition |
|---|---|
| | • Alberta Netcare est le nom de tous les projets rattachés au DSE provincial, système électronique sécurisé et confidentiel regroupant l'information sur la santé des patients sous la forme de dossiers patients uniques, complets et intégrés.<br>• Autres systèmes cliniques : dans certaines autorités sanitaires, d'autres systèmes cliniques peuvent faire office de DSE, car ils conservent les résumés du dossier du patient. |
| Dossier de santé électronique longitudinal | Dossier patient unique et complet composé de données provenant de nombreuses sources dans le continuum des soins de santé. |
| Échange d'information sur la santé (EIS) | L'échange d'information sur la santé (EIS) permet aux médecins, aux infirmières, aux pharmaciens, aux autres professionnels de la santé et au patient concerné d'accéder de manière appropriée à l'information médicale vitale du patient et de la partager par voie électronique sécurisée, ce qui contribue à améliorer la rapidité, la qualité, la sûreté et le coût des soins.<br><br>Bien que l'EIS ne remplace pas la communication entre le professionnel de la santé et le patient, il améliore grandement l'exhaustivité des dossiers médicaux (ce qui peut avoir un effet important sur les soins), puisque les antécédents, les médicaments pris par le patient et d'autres renseignements sont examinés conjointement pendant les consultations.<br><br>L'échange efficace et rapide de l'information vitale sur le patient permet d'éclairer la prise de décisions au point d'intervention; d'éviter les réadmissions, la répétition inutile des analyses et examens et les erreurs liées aux médicaments; et, enfin, d'améliorer les diagnostics.<br><br>(Source : https://www.healthit.gov/topic/health-it-and-health-information-exchange- basics/what-hie) |
| Ensemble de données extensible du RDP-CA | Contenu du RDP-CA pouvant être augmenté afin de refléter un cas d'utilisation du RDP-CA qui complète les cas d'utilisation primaires.<br><br>*Note : L'ensemble de données est dit « extensible » parce qu'on peut y ajouter des domaines de données, comme les antécédents familiaux. |
| Exigences d'interopérabilité opérationnelle/ juridique | Conditions permettant à des organisations indépendantes les unes des autres d'exécuter un processus ou de fournir un service en collaboration. |
| Exigences d'interopérabilité syntaxique/sémantique | Conditions syntaxiques et sémantiques nécessaires pour que les données échangées entre les systèmes de dossiers médicaux puissent être interprétées correctement et que leur signification puisse être établie sans ambiguïté. |
| Exigences d'interopérabilité technique | Conditions requises pour qu'un système de dossiers médicaux transmette des données à un autre système de dossiers médicaux et pour que le système récepteur accuse réception des données utiles. |
| Exigences opérationnelles non testables | Exigences opérationnelles qui ne sont pas directement rattachées à un profil IHE dans la spécification du RDP-CA (p. ex. exigences à prendre en considération ou destinées à guider les responsables de l'implantation du RDP-CA). |
| Exigences opérationnelles testables | Exigences opérationnelles qui sont directement rattachées à un profil IHE dans la spécification du RDP-CA. |

| Terme/abréviation | Définition |
|---|---|
| Fast Healthcare Interoperability Resources (FHIR®) | Cadre de normes de nouvelle génération créé par HL7. Alliant les meilleures caractéristiques des produits V2, V3 et CDA d'HL7 aux plus récentes normes du Web, FHIR® se distingue par sa grande applicabilité.<br><br>(Source : http://www.hl7.org/implement/standards/fhir/) |
| Gazelle | Gazelle est une suite d'outils virtuels, développée par IHE Europe, qui sert à la réalisation de tests d'interopérabilité. Elle permet aux organisations gouvernementales et aux fournisseurs de valider le rôle qu'ils joueront dans un écosystème et leur capacité à satisfaire aux exigences d'interopérabilité. La suite met à leur disposition plusieurs options en libre-service d'autotest et d'innovation pour tester la conformité de leurs systèmes avec les profils d'intégration représentés. |
| Health Level Seven (HL7) | Fondé en 1987, Health Level Seven (HL7) est un organisme à but non lucratif dont le mandat est de fournir un cadre de travail exhaustif et des normes pour l'échange, l'intégration, la transmission et l'extraction d'information électronique sur la santé pour soutenir la pratique clinique ainsi que la gestion, la prestation et l'évaluation des services de santé.<br><br>(Source : http://www.hl7.org/about/index.cfm?ref=nav) |
| ID | Identifiant (de patient, de client, de ressource, etc.) |
| Infrastructure centrale | Infrastructure qui recueille l'information médicale provenant des organisations participantes et qui la stocke dans un emplacement centralisé. L'infrastructure offre également des mécanismes de contrôle d'accès. En général, l'infrastructure centrale relève de la province ou du territoire. |
| Integrating the Healthcare Enterprise (IHE) | IHE est une initiative menée par des professionnels de la santé et des représentants de l'industrie et qui vise à améliorer le partage de l'information entre les systèmes informatiques du secteur de la santé. IHE préconise l'utilisation coordonnée de normes reconnues, comme DICOM et FHIR, pour répondre aux besoins cliniques de la manière la plus propice à l'optimisation des soins. Les systèmes développés en conformité avec les exigences d'IHE communiquent mieux entre eux, sont plus faciles à implanter et permettent au personnel soignant d'utiliser plus efficacement l'information.<br><br>(Source : https://www.ihe.net/) |
| Interopérabilité | L'interopérabilité permet à l'information de circuler librement entre des solutions et appareils hétérogènes. Lorsque les diverses parties du réseau de la santé sont interopérables, elles « parlent la même langue ». L'interopérabilité améliore la continuité des soins, la collaboration entre les professionnels de la santé et l'accès des patients à leur information médicale. En éliminant le cloisonnement des données, elle réduit l'inefficience et la redondance dans le réseau de la santé.<br><br>Jamais la connexion, la collaboration et la communication n'ont été aussi importantes pour le réseau de la santé. En raison de la hausse de l'utilisation des solutions de santé numériques, il est désormais indispensable d'assurer un partage électronique sûr et efficace de l'information dans tout le cercle des soins. Mais pour continuer à améliorer les soins de santé au Canada, l'interopérabilité s'impose – un réseau connecté est un réseau en meilleure santé.<br><br>Vous trouverez plus d'information à ce sujet sur la page *Interopérabilité* du site Web d'Inforoute. |

| Terme/abréviation | Définition |
|---|---|
| IUA | Le profil *Internet User Authorization* (IUA) (autorisation de l'utilisateur Internet) prend en charge l'autorisation des transactions réseau lors de l'utilisation des transports HTTP RESTful. IHE a créé des profils d'autorisation pour les services Web et les transactions basées sur SOAP, tandis que le profil IUA est un profil d'autorisation pour les transactions HTTP RESTful.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-34.html) |
| Mandataire du patient | Personne ou entité autorisée à agir au nom d'un patient/sujet de soins. Il peut s'agir d'un parent d'enfant à charge, d'un parent d'adulte à charge, d'une personne ayant une procuration, etc. |
| MHD | Le profil *Mobile access to Health Documents* (MHD) (accès mobile aux documents médicaux) définit une interface normalisée (interface de programmation d'application, ou API) pour l'échange de documents cliniques entre appareils mobiles, afin que l'environnement de déploiement des applications mobiles soit homogène et réutilisable.<br><br>(Source : https://profiles.ihe.net/ITI/MHD/index.html) |
| Numéro d'identification de médicament (DIN) | Numéro à huit chiffres, généré par ordinateur, que Santé Canada attribue à chaque produit médicamenteux avant qu'il soit commercialisé au Canada. |
| P et T | Provinces et territoires |
| PDQm | Le profil *Patient Demographics Query for Mobile* (PDQm) (requête de données démographiques de patients pour appareils mobiles) définit une interface RESTful allégée vers un fournisseur de données démographiques de patients qui utilise des technologies facilement accessibles aux applications mobiles et aux applications allégées sur navigateur.<br><br>(Source: https://profiles.ihe.net/ITI/TF/Volume1/ch-38.html) |
| PIXm | Le profil *Patient Identifier Cross-Reference for Mobile* (PIXm) (références croisées des identifiants du patient pour appareils mobiles) fournit des transactions RESTful pour les applications mobiles et les applications allégées sur navigateur, transactions qui permettent de créer, de mettre à jour ou de supprimer des dossiers patients dans un gestionnaire de références croisées des identifiants du patient (*Patient Identifier Cross-Reference Manager*) et d'interroger celui-ci pour la recherche des identifiants interdomaines d'un patient.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-41.html) |
| PMIR | Le profil *Patient Master Identity Registry* (PMIR) (registre de l'identité maîtresse du patient) prend en charge la création, la mise à jour et la dépréciation des données relatives à l'identité maîtresse du patient, ainsi que l'abonnement aux notifications signalant les modifications apportées à l'identité maîtresse, en utilisant les ressources de la norme FHIR et les transactions RESTful.<br><br>(Source : https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_PMIR.pdf) |
| Portail-patient | Point d'accès Web sécurisé qui donne au patient un accès sécurisé à ses renseignements personnels sur la santé (RPS) et à d'autres services de santé numériques en libre-service. Un portail-patient peut être hébergé sur une solution de DME. |

| Terme/abréviation | Définition |
|---|---|
| Producteur | Système (DME, SIS, SIC, DSP ou DSE) qui crée/produit un document clinique (p. ex. RDP-CA) à la suite d'une requête d'un professionnel de la santé autorisé, d'un sujet de soins/patient ou d'un autre système autorisé. |
| Professionnel de la santé (PS) | Personne qui exerce une profession réglementée dans le domaine de la santé (médecin, infirmière, dentiste, pharmacien). |
| Profils d'intégration IHE | Les profils d'intégration IHE apportent une solution aux problèmes d'interopérabilité qui se posent dans les tâches cliniques courantes, représentées dans les cas d'utilisation. Les profils d'intégration décrivent en détail les spécifications techniques qui sous-tendent l'implantation des normes pertinentes en vue d'assurer un flot ininterrompu d'information entre différentes applications logicielles qui interviennent dans un cas d'utilisation spécifique.<br><br>Les profils indiquent comment les systèmes informatiques peuvent fournir un soutien intégré à un flux clairement défini, chaque profil prenant en charge une tâche clinique donnée dans un domaine clinique particulier. Les profils IHE peuvent être utilisés pour une implantation progressive de systèmes dans différents domaines et la mise en place graduelle d'applications de santé électroniques interopérables.<br><br>(Source : https://www.ihe-europe.net/about-us/faq) |
| Projetathon | Étape importante et bonne pratique de mise à l'essai et de validation d'une spécification, où les responsables de l'implantation collaborent pour tester leurs solutions en utilisant une méthodologie et des outils qui accélèrent l'interopérabilité. Un projetathon donne l'occasion aux participants de tester leurs systèmes entre eux et par rapport à un environnement de référence. Il leur permet aussi de mettre en commun leurs connaissances pratiques. |
| Répertoire canadien des médicaments (RCM) | Terminologie relative aux médicaments destinée à être utilisée dans les solutions de santé numériques au Canada, entre autres la solution nationale d'ordonnances électroniques (PrescripTIon$^{MC}$). |
| Résumé du dossier du patient pancanadien (RDP-CA) | Résumé électronique du dossier du patient destiné à être utilisé au point d'intervention et qui comprend un ensemble minimal de données médicales, en conformité avec les spécifications applicables. Le RDP-CA est un extrait du dossier du patient pris à un moment précis et qui contient un ensemble normalisé de données cliniques et contextuelles (rétrospectives, simultanées, prospectives), dont les données minimales nécessaires et suffisantes pour déterminer le traitement d'un patient au point d'intervention. Il est indépendant des problèmes de santé du patient, des spécialités médicales et des traitements. |
| Résumé international du dossier médical du patient (IPS, pour *International Patient Summary*) | Ensemble d'éléments de données minimal et non exhaustif défini par la norme ISO/EN 17269 et implanté à l'aide des normes CDA et FHIR d'HL7. Cet ensemble forme un document de synthèse clinique qui peut être utilisé dans le cadre de soins planifiés ou non, localement ou à l'étranger. Le profil IPS précise les données requises et les critères de conformité nécessaires des cas d'utilisation d'un résumé international du dossier médical du patient.<br><br>(Source : https://wiki.ihe.net/index.php/International_Patient_Summary_(IPS)) |
| SIS | Système d'information sur la santé |
| Soins locaux non planifiés | Soins non planifiés donnés à un résident du Canada dans/par le réseau canadien de la santé. Cela inclut les soins fournis par les organismes gouvernementaux fédéraux, provinciaux et territoriaux, ainsi que les soins pangouvernementaux. |

| Terme/abréviation | Définition |
|---|---|
| Soins locaux planifiés | Soins planifiés donnés à un résident du Canada dans/par le réseau canadien de la santé. Cela inclut les soins fournis par les organismes gouvernementaux fédéraux, provinciaux et territoriaux, ainsi que les soins pangouvernementaux. |
| Soins transfrontaliers non planifiés | Soins non planifiés donnés à un résident du Canada dans/par un autre pays. |
| Soins transfrontaliers planifiés | Soins planifiés donnés à un résident du Canada dans/par un autre pays. |
| Solution clinique | Toute combinaison d'actifs et de processus de technologie de l'information sur la santé qui permet la communication, la gestion et le traitement final des données cliniques entre un producteur et un consommateur. Les solutions cliniques peuvent être constituées de divers systèmes producteurs et consommateurs, notamment le DME, le SIS, le SIC, le DSP, le DSE ou toute combinaison de ceux-ci. |
| Solution de RDP-CA | Toute combinaison d'actifs et de processus de technologie de l'information sur la santé qui permet la création, la communication, la gestion et le traitement final d'un RDP-CA entre un producteur et un consommateur de RDP-CA. Les solutions de RDP-CA peuvent être constituées de divers systèmes producteurs et consommateurs, notamment le DME, le SIS, le SIC, le DSP, le DSE ou toute combinaison de ceux-ci. |
| Spécification du RDP-CA | Spécification implantable et testable basée sur le profil IPS d'IHE et sur le guide d'implantation de l'IPS d'HL7.<br><br>Vous trouverez plus d'information sur la spécification du RDP-CA ici. |
| SUT | Système à tester, système à l'essai |
| SVCM | Le profil *Sharing Valuesets, Codes and Maps* (SVCM) (partage d'ensembles de valeurs, de codes et de mappages) définit une interface allégée par laquelle les systèmes informatiques du réseau de la santé peuvent extraire une nomenclature uniforme gérée de manière centralisée et des mappages entre les systèmes de codes basés sur la spécification FHIR.<br><br>(Source : https://wiki.ihe.net/index.php/Sharing_Valuesets,_Codes_and_Maps_(SVCM)) |
| Système de dossiers de santé | Terme générique qui peut désigner un système de dossiers médicaux, un système d'information sur la santé (SIS), un système d'information clinique (SIC), un système de dossiers de santé électroniques (DSE) ou un système de dossiers de santé personnels (DSP). Il décrit aussi de manière générale les acteurs susceptibles de produire et/ou de consommer un RDP-CA. Les patrons d'implantation adoptés par les provinces et territoires détermineront les types de systèmes utilisés pour la création, la visualisation, la consommation et la gestion des résumés du dossier du patient. |
| Terminologie | Ensemble de concepts identifiables de manière unique et auxquels sont associées des représentations, des désignations et des significations. |
| Test de conformité | Processus d'évaluation structuré visant à garantir qu'une solution ou un système clinique implante correctement une spécification particulière (p. ex. la spécification du RDP-CA), c'est-à-dire que l'implantation a été faite en conformité avec les paramètres indiqués dans la spécification en question. |
| Transactions IHE | Interactions entre des acteurs qui communiquent l'information requise au moyen de messages normalisés (p. ex. requête de recherche de patient, envoi du résumé du dossier du patient). |

| Terme/abréviation | Définition |
|---|---|
| | (Source : https://wiki.ihe.net/index.php/PCC_TF-1/About) |
| XDM | Le profil *Cross-Enterprise Document Media Interchange* (XDM) (échange média de documents entre organisations) assure l'échange de documents à l'aide d'une structure commune de fichiers et de répertoires sur plusieurs types de supports classiques. Ce profil permet au patient d'utiliser un support physique pour transporter ses documents médicaux. Il rend également possible la transmission de documents médicaux de personne à personne par courrier électronique. Le profil XDM prend en charge le transfert de données concernant plusieurs patients au sein d'un même échange de données.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-16.html) |
| XDS | Le profil *Cross-Enterprise Document Sharing* (XDS) (échange de documents entre organisations) facilite l'enregistrement et la distribution des dossiers de santé électroniques des patients et l'accès à ceux-ci dans tous les établissements de santé.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-10.html) |

# 2 Survol

## 2.1 But

L'Architecture de référence (AR), établie dans le but de soutenir l'interopérabilité, sert de guide pour l'application de patrons d'intégration qui permettront d'améliorer la manière dont les systèmes informatiques du réseau de la santé partagent l'information au Canada. Les systèmes qui implantent ces capacités peuvent être représentés par des patrons d'interopérabilité normalisés pouvant être réutilisés dans un vaste éventail de solutions dans l'écosystème. L'AR présente les principaux éléments de normalisation (patrons) qui peuvent être employés dans la conception des solutions à l'échelle du réseau. Ces patrons seront mentionnés dans les guides d'accompagnement et les spécifications d'interopérabilité qui portent sur des aspects prioritaires (p. ex. résumé du dossier du patient, aiguillage électronique des patients, etc.).

Une grande partie des patrons d'intégration présentés dans l'AR sont des profils d'interopérabilité développés par IHE International. Ces patrons sont fondés sur des normes ouvertes et sont testés régulièrement dans le cadre d'événements internationaux de tests d'interopérabilité, les connectathons. Fournisseurs et acheteurs obtiennent ainsi un catalogue de capacités qui peuvent servir pour la conception de solutions dans l'ensemble de l'écosystème. En s'alignant sur les bonnes pratiques et les normes internationales, l'AR pourra évoluer afin de représenter le point de vue pancanadien et de devenir une approche d'interopérabilité.

En plus des profils IHE déjà publiés, l'AR fournit des indications précises sur l'implantation d'éléments qui s'assortissent d'exigences propres au contexte canadien (p. ex. comment utiliser les profils IDP – IUA, indications sur la sécurité et l'audit – ATNA, etc.).

## 2.2 Public cible

Le présent document s'adresse, sans s'y limiter, aux destinataires suivants :

- les services des TI des établissements de santé (gestionnaires de produit technique, gestionnaires en informatique, personnel opérationnel);
- le personnel technique des fournisseurs qui participent à l'initiative IHE;
- les experts qui participent à l'élaboration des normes;
- les personnes et les équipes responsables de l'implantation de solutions logicielles, comme les gestionnaires de projet, les chefs de la technologie, les chefs de la sécurité de l'information, les ingénieurs en logiciels, les gestionnaires de produit technique, les gestionnaires en informatique, le personnel opérationnel et d'autres professionnels du même type.

## 2.3 Survol de l'Architecture de référence

L'AR contient de l'information sur les patrons d'intégration qui favorisent l'interopérabilité du réseau. D'autres spécifications d'interopérabilité (p. ex. RDP-CA, CA:FeX) pourraient contenir des éléments de projets qui renvoient à l'architecture et/ou y renvoyer directement.

**Programmes** : L'AR est un document évolutif qui décrit les profils IHE que l'on recommande aux provinces/territoires et aux fournisseurs d'adopter pour améliorer la façon dont les systèmes informatiques du secteur de la santé échangent l'information au Canada. D'autres profils IHE s'ajouteront au fur et à mesure que de nouvelles priorités verront le jour. L'information sur les programmes de l'AR se trouve ici-même, dans l'espace et sur la page où vous vous trouvez actuellement (voir le diagramme ci-dessous). Cette information a été résumée pour les profils IHE, puis regroupée dans les catégories suivantes :

- profils fondamentaux : liste de profils fondamentaux IHE qui remplissent des fonctions de base dans l'écosystème, comme la connexion autorisée, la journalisation des événements (audit), la synchronisation, etc.
- profils d'échange de documents/données : liste de profils IHE recommandés pour l'échange de documents et de données entre des solutions cliniques
- profils d'identité des patients : liste de profils IHE qui permettent de confirmer l'identité du patient ou du sujet de soins

**Projets** : En plus de l'AR, des documents portant sur des projets particuliers pourraient contenir un sous-ensemble des profils recommandés dans le présent document. Ces guides élaborés pour des projets précis énuméreront les diagrammes de séquence qui répondent aux besoins de ces projets. Les acteurs et les transactions de différents profils peuvent être regroupés pour satisfaire aux exigences opérationnelles des cas d'utilisation de ces projets.

## 2.4 Éléments de l'Architecture de référence

- L'AR présente les acteurs et les transactions des profils IHE qui permettent l'échange sécurisé d'information sur la santé au Canada.
- Les interactions et les transactions normalisées entre les acteurs, qui sont définies par le cadre méthodologique d'IHE, sont indiquées par des lignes noires.
- Les acteurs et les transactions sont regroupés dans deux couloirs : les systèmes cliniques et les systèmes provinciaux/territoriaux. On présume que les fournisseurs joueront les rôles des systèmes cliniques et les provinces et territoires, ceux des systèmes provinciaux/territoriaux, qui peuvent être assumés aussi par les systèmes des fournisseurs (l'AR ne l'empêche pas).
- Dans l'AR, deux options d'implantation ont été mises en évidence, l'option 1 comprenant deux scénarios :
    - Option 1, scénario n$^{o}$ 1 : implantation du profil MHD, pour un dépôt de documents central
    - Option 1, scénario n$^{o}$ 2 : implantation du profil MHD, pour un dépôt de documents local
    - Option 2 : implantation de CA:FeX (échange FHIR canadien)
- L'option privilégiée est assortie d'un astérisque* (c.-à-d. option 1, scénario n$^{o}$ 1)
- Une liste de tous les profils IHE figure dans le bas de l'AR
- Une liste des spécifications et des indications sur l'intégration dans le contexte canadien figure dans le bas de l'AR, où les extensions nationales de profils IHE existants et de nouveaux profils nets pour le Canada sont nommés de façon distincte.
- Une légende dans le bas de l'AR donne des précisions sur le diagramme.

## 2.5 Applications de l'Architecture de référence

Voici un résumé des applications du présent document :

- **Détermination du rôle** : Les provinces/territoires et les fournisseurs devront déterminer leur rôle (c.-à-d. acteurs) dans l'AR et les diagrammes de séquence pour chaque cas d'utilisation inclus.
- **Relevé des lacunes** : Compte tenu du rôle déterminé, il faut procéder à une évaluation pour cerner les lacunes qui nuisent au respect des exigences des acteurs et des transactions normalisés nécessaires à la réalisation de cas d'utilisation.
- **AR provinciale/territoriale** : Les provinces et les territoires pourraient devoir élaborer leur propre version de l'AR en fonction de leurs besoins. Les technologies actuelles, l'architecture existante et les priorités opérationnelles courantes leur seront utiles en ce sens.
- **Évolution du document et rétroaction** : Le présent document est évolutif et sera modifié en fonction des commentaires de tous les intervenants et des améliorations apportées aux cas d'utilisation. Il est publié pour que tous les intervenants puissent le commenter. De plus, de multiples séances seront tenues pour en analyser le contenu et le mettre à jour.
- **Tests de conformité des fournisseurs (connectathon/projetathon)** : Le présent document permettra aux fournisseurs de se préparer aux tests de conformité sur Gazelle, une plateforme de test libre sur le Web développée par IHE qui offre un éventail d'outils de test d'interopérabilité conçus pour valider la conformité de l'interface avec les profils IHE et les spécifications d'interopérabilité fondées sur des normes et spécifiques à chaque projet. Les fournisseurs peuvent valider leurs produits et projets de santé numérique en vue de l'acquisition des interfaces qu'ils déploient. Pour en savoir plus sur Gazelle, consultez la page suivante : IHE Gazelle

*Note : Le lecteur devrait avoir une bonne connaissance des profils IHE, surtout de ceux qui sont mentionnés dans le diagramme général de l'AR (IUA, ATNA, CT, MHD).

## 2.6 Versions des profils IHE

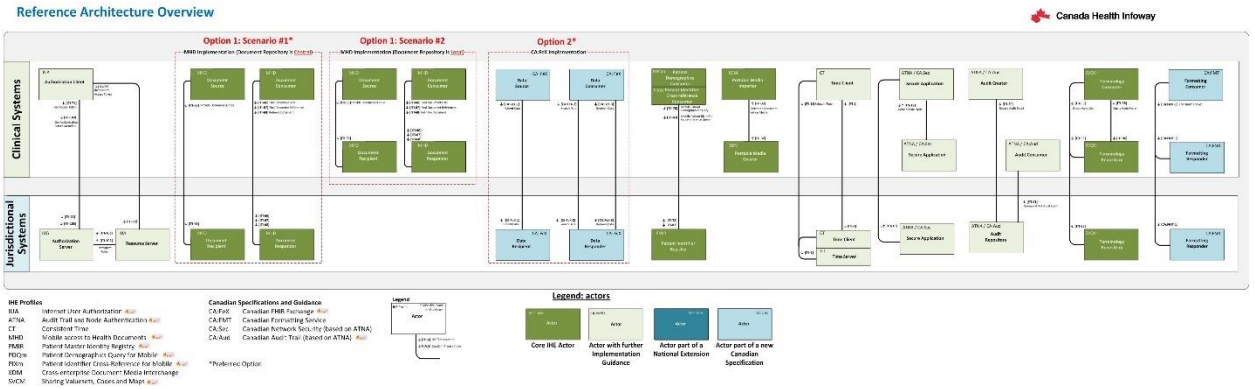
Voici les versions publiées des profils IHE dont il est question dans la présente AR :

- MHD : v4.1.0 – version de mise à l'essai (2022-03-01) basée sur FHIR R4
- IUA : Révision 2.2 – version de mise à l'essai (2022-06-17)
- ATNA : Révision 19.0 – texte final (2022-06-17)
- Supplément RESTful ATNA : Révision 3.3 – version de mise à l'essai (2021-07-02) basée sur FHIR R4
- CT : Révision 19.0 – texte final (2022-06-17)

Pour ce qui est des autres profils IHE qui figurent dans l'AR mais qui ne sont pas mentionnés dans cette liste, il s'agit de la version la plus récente.

## 2.7 Vue d'ensemble de l'Architecture de référence

Voici une vue d'ensemble des profils IHE et des spécifications d'interopérabilité pertinents qui soutiennent l'AR. On y présente un surensemble de profils qui offrent différentes options d'échange de documents et de données, selon le type de service provincial/territorial et sa disponibilité.



# 3 Profils fondamentaux

**Contexte**

Les profils IHE fondamentaux et les spécifications d'interopérabilité pancanadiennes portent sur des composantes essentielles de l'interopérabilité comme l'authentification des utilisateurs (p. ex. IUA), les nœuds de sécurité et les enregistrements d'audit (p. ex. ATNA), la synchronisation des ordinateurs (p. ex. CT), la terminologie (p. ex. SVCM), la conversion/le formatage des documents (p. ex. CA:FMT), et bien d'autres.

**Hypothèse**

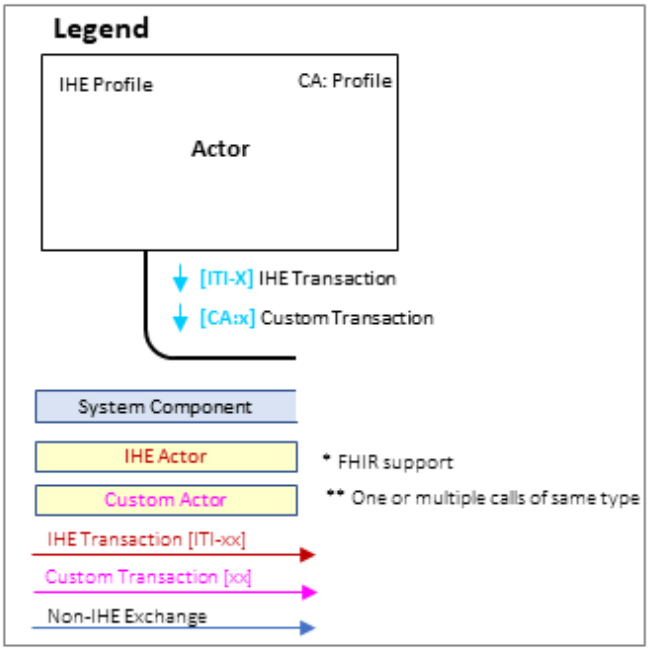
Les fournisseurs et les provinces/territoires qui font partie de l'écosystème peuvent choisir de jouer le rôle des acteurs et d'effectuer les transactions normalisés décrits dans les profils fondamentaux pour la spécification RDP-CA. Des renseignements supplémentaires sur ces profils fondamentaux et les exigences qui y sont liées figurent plus bas. Les fournisseurs et les provinces/territoires peuvent décider de ne pas implanter les profils optionnels énumérés ci-dessous, mais on leur recommande fortement de résoudre les problèmes d'authentification, d'audit et de sécurité en recourant à des solutions qui existent déjà dans leur architecture d'entreprise respective.

**Profils IHE, spécification et indications inclus :**

- Profil ATNA (*Audit Trail and Node Authentication*, ou piste d'audit et authentification de nœuds)
    - Indications sur l'implantation CA:Sec (*Canadian Network Security*, ou sécurité du réseau canadien)
    - Indications sur l'implantation CA:Aud (*Canadian Audit Trail*, ou piste d'audit canadienne)
- Profil IUA (*Internet User Authorization*, ou autorisation de l'utilisateur Internet)
- Profil CT (*Consistent Time*, ou synchronisation du temps)
- Profil SVCM (*Sharing Valuesets, Codes and Maps*, ou partage d'ensembles de valeurs, de codes et de mappages)
- Spécification CA:FMT (*Canadian Formatting Service*, ou service de formatage canadien)

**Légende**

Le diagramme ci-dessous représente la légende des diagrammes de séquence inclus pour les profils, la spécification et les indications.



# 3.1 Profil ATNA

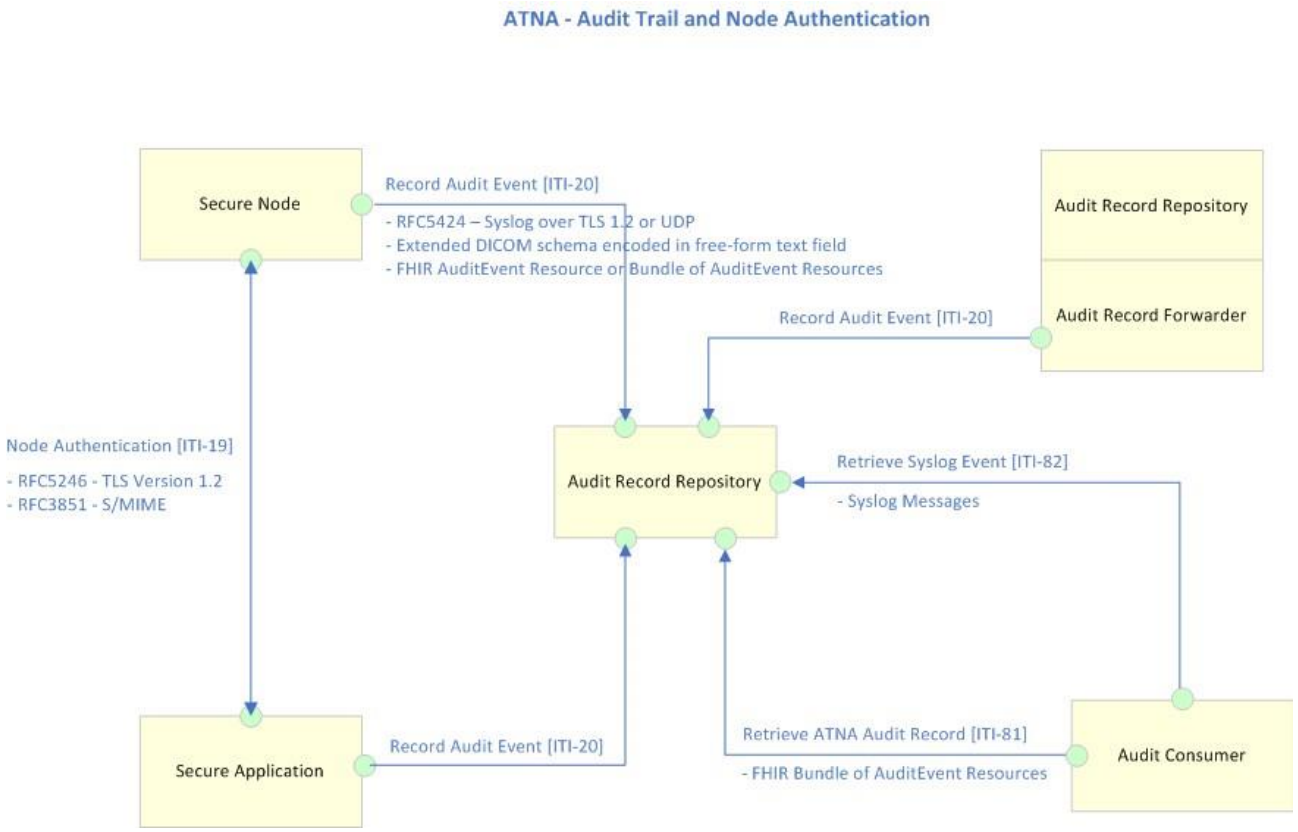
## 3.1.1 Survol

Le profil ATNA (*Audit Trail and Node Authentication*, ou piste d'audit et authentification des nœuds) précise les éléments fondamentaux de toutes les formes de systèmes sécurisés : authentification des nœuds, authentification des utilisateurs, journalisation des événements (audit) et cryptage des télécommunications. Il est également utilisé pour indiquer que d'autres propriétés de sécurité interne telles que le contrôle d'accès, le contrôle de configuration et les restrictions de privilèges sont fournies.

Pour de plus amples renseignements, consultez le profil ATNA et le supplément *Add RESTful ATNA (Query and Feed)* d'IHE.

## 3.1.2 Acteurs et transactions

Le diagramme suivant présente une vue générale des acteurs et des transactions du profil ATNA ainsi que de leurs interactions.



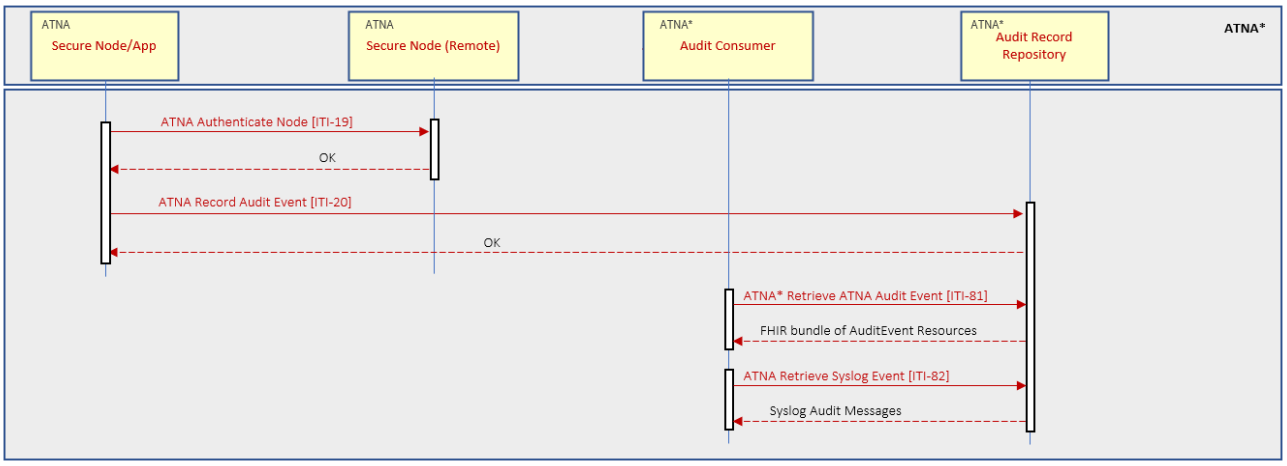

Les transactions relatives à chaque acteur qui intervient directement dans le profil ATNA figurent dans le tableau ci-dessous. Pour être jugé conforme au profil ATNA, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R ») et peut assumer les transactions optionnelles (identifiées par un « O »).

| Acteur | Transaction | Optionalité |
|---|---|---|
| Dépôt d'enregistrements d'audit (Audit Record Repository) | Record Audit Event [ITI-20]<br>Retrieve ATNA Audit Event [ITI-81]<br>Retrieve Syslog Event [ITI-82] | R<br>O<br>O |
| Consommateur d'enregistrements d'audit (Audit Consumer) | Retrieve ATNA Audit Event [ITI-81]<br>Retrieve Syslog Event [ITI-82] | O<br>O |
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder) | Record Audit Event [ITI-20] | R |
| Nœud sécurisé (Secure Node) | Authenticate Node [ITI-19]<br>Record Audit Event [ITI-20] | R<br>R |
| Application sécurisée (Secure Application) | Authenticate Node [ITI-19]<br>Record Audit Event [ITI-20] | R<br>R |

## Transactions

- Authenticate Node [ITI-19] – Dans la transaction *Authenticate Node*, le nœud sécurisé local présente son identité à un nœud sécurisé distant et en valide l'identité. Après cette authentification mutuelle, d'autres transactions sécurisées peuvent s'effectuer dans ce canal sécurisé entre les deux nœuds. Utilise les protocoles RFC5246 - Transport Layer Security (TLS) Protocol Version 1.2 et RFC3851 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification.
- Record Audit Event [ITI-20] – Cette transaction permet de signaler des événements auditables à un dépôt d'enregistrements d'audit. Utilise les protocoles RFC5424 – The Syslog Protocol (TLS ou UDP).
- Retrieve ATNA Audit Event [ITI-81] – Cette transaction permet de chercher des événements ATNA enregistrés dans un dépôt d'enregistrements d'audit ATNA. Le résultat est un *Bundle* FHIR de ressources *AuditEvent* qui correspondent à un ensemble de paramètres de recherche.
- Retrieve Syslog Event [ITI-82] – Cette transaction est employée pour extraire des messages d'enregistrement d'événement du système du dépôt d'enregistrements d'audit selon des paramètres restrictifs.

## 3.1.3 Diagramme de séquence

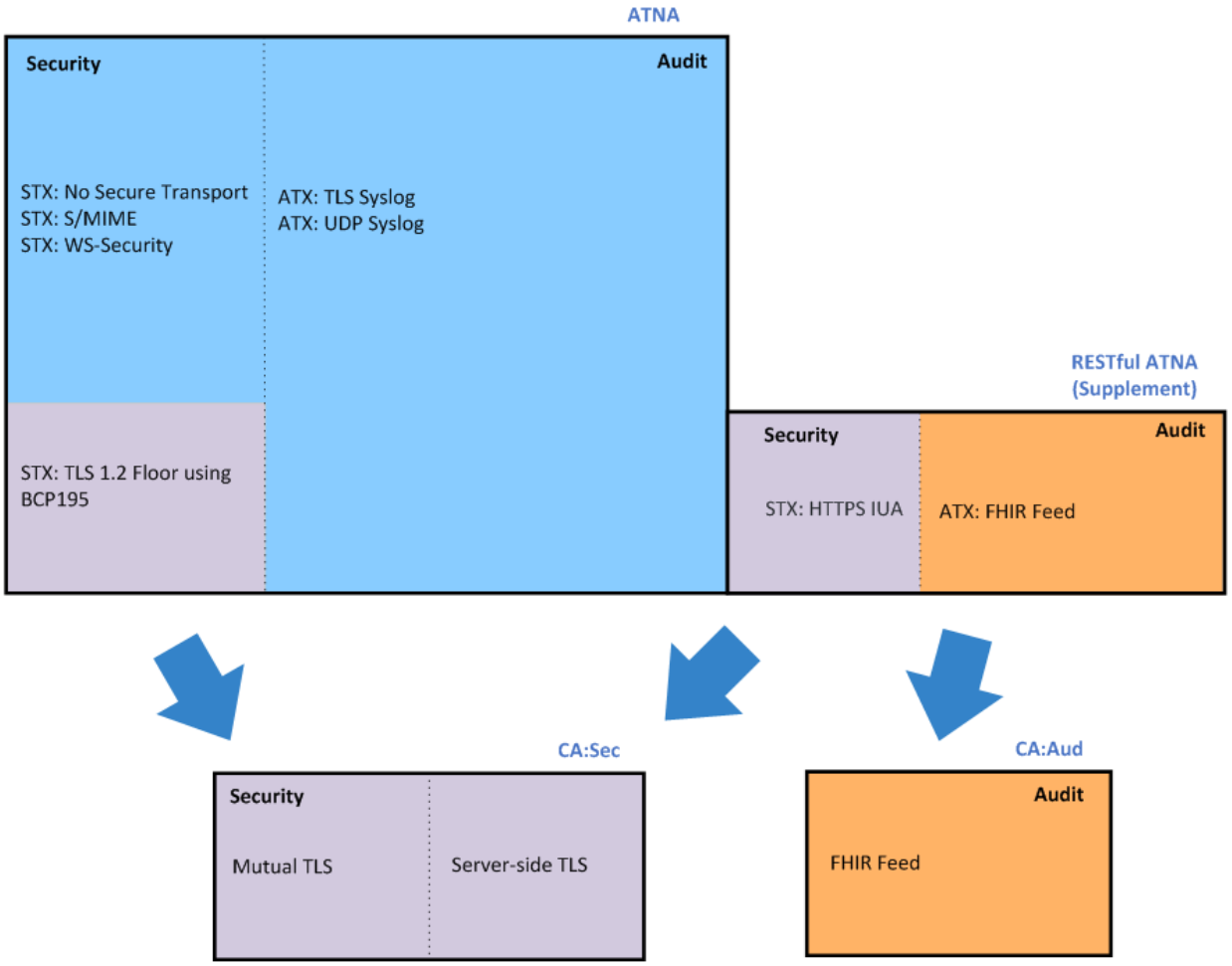



## 3.1.4 Indications sur l'implantation du profil ATNA au Canada – CA:Sec et CA:Aud

Le profil ATNA porte sur deux éléments principaux : la sécurité et la journalisation des événements aux fins d'audit. Comme la sécurité et l'audit sont étroitement liés, tout comme les multiples options offertes pour les deux aspects, le profil ATNA est un profil complexe qui est amplement documenté.

Les indications CA:Sec et CA:Aud ont été créées pour alléger le profil ATNA, apporter des améliorations en séparant les deux principaux aspects du profil (sécurité et audit) et mettre l'accent sur quelques options de formats et de technologies modernes. Ces indications ne remplacent pas le profil ATNA. Une implantation déjà conforme au profil ATNA passera les tests de conformité qui y sont liés.

Le diagramme qui suit présente la segmentation des principaux éléments du profil ATNA selon les indications sur l'implantation en contexte canadien.




La section ci-dessous contient des tableaux de comparaison du profil ATNA et des options sélectionnées pour CA:Sec et CA:Aud.

Les définitions de notation suivantes sont utilisées dans toute la section.

La notation de l'**optionalité** est définie comme suit :

| | |
|---|---|
| **R** | Requis |
| **O** | Optionnel |

La notation du **protocole de transport** est définie comme suit :

| | |
|---|---|
| Préfixe **STX** | Protocole de transport sécurisé |
| Préfixe **ATX** | Protocole de transport d'audit |

## Acteurs/transactions

### ATNA

| Acteurs | Transactions | Optionalité |
|---|---|---|
| Nœud sécurisé (Secure Node) | Authenticate Node [ITI-19] | R |
| | Record Audit Event [ITI-20] | R |
| Application sécurisée (Secure Application) | Authenticate Node [ITI-19] | R |
| | Record Audit Event [ITI-20] | R |
| Dépôt d'enregistrements d'audit (Audit Record Repository) | Record Audit Event [ITI-20] | R |
| | Retrieve ATNA Audit Event [ITI-81] | O |
| | Retrieve Syslog Event [ITI-82] | O |
| Consommateur d'enregistrements d'audit (Audit Consumer) | Retrieve ATNA Audit Event [ITI-81] | O |
| | Retrieve Syslog Event [ITI-82] | O |
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder | Record Audit Event [ITI-20] | R |

### CA:Sec

| Acteur | Transaction | Optionalité |
|---|---|---|
| Application sécurisée (Secure Application) | Authenticate Node [ITI-19] | R |

### CA:Aud

| Acteurs | Transactions | Optionalité |
|---|---|---|
| Créateur d'enregistrements d'audit (Audit Creator) | Record Audit Event [ITI-20] | O (note 1) |
| Dépôt d'enregistrements d'audit (Audit Record | Record Audit Event [ITI-20] | O (note 1) |

| | | |
|---|---|---|
| Repository) | Retrieve ATNA Audit Event [ITI-81] | O (note 2) |
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder) | Record Audit Event [ITI-20] | O (note 1) |
| Consommateur d'enregistrements d'audit (Audit Consumer) | Retrieve ATNA Audit Event [ITI-81] | R |

*Note 1 : Les événements d'audit doivent être enregistrés au moyen de la transaction IHE* Record Audit Event [ITI-20] *avec l'option* FHIR Feed *ou d'autres méthodes (IHE ou autre).*

*Note 2 : Cette transaction est requise si le dépôt d'enregistrements d'audit est central.*

**Notes**

- Le profil ATNA définit deux acteurs ayant un rôle semblable, le nœud sécurisé et l'application sécurisée, qui remplissent des fonctions dans les deux aspects de la sécurité et de l'audit qui répondent à des exigences obligatoires de transaction et qui, par le fait même, sont étroitement liés. Ainsi, pour échanger des communications sécurisées, l'audit doit également être implanté selon le profil ATNA.
  Les messages d'audit doivent être enregistrés avec les moyens définis par le profil ATNA.
- CA:Sec définit un seul acteur et une seule transaction pour la communication sécurisée.
- CA:Aud définit des acteurs qui sont responsables uniquement de l'audit. On recommande de sécuriser les communications en groupant un acteur CA:Aud et un acteur CA:Sec.
  Les messages d'audit peuvent être enregistrés de n'importe quelle façon, au moyen de la transaction IHE ITI-20 et de l'option FHIR ou de toute autre méthode (IHE ou autre). Les messages doivent pouvoir être extraits en format FHIR au moyen de la transaction IHE ITI-81.

## Options liées aux acteurs

**ATNA**

| Acteur | Options |
|---|---|
| Dépôt d'enregistrements d'audit (Audit Record Repository) | *Retrieve Audit Message* (extraire un message d'audit) |
| | *Retrieve Syslog Message* (extraire un message d'enregistrement d'événement du système ) |
| | *ATX: FHIR Feed* (ATX : FHIR Feed) |
| | *ATX: TLS Syslog* (ATX : enregistrement d'événement du système TLS) |
| | *ATX: UDP Syslog* (ATX : enregistrement d'événement du système UDP) |
| Consommateur d'enregistrements d'audit (Audit Consumer) | *Retrieve Audit Message* (extraire un message d'audit) |
| | *Retrieve Syslog Message* (extraire un message d'enregistrement d'événement du système ) |
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder) | *ATX: FHIR Feed* (ATX : FHIR Feed) |

| | |
|---|---|
| | *ATX: TLS Syslog* (ATX : enregistrement d'événement du système TLS) |
| | *ATX: UDP Syslog* (ATX : enregistrement d'événement du système UDP) |
| Nœud sécurisé (Secure Node) | *Radiology Audit Trail* (piste d'audit de radiologie) |
| | *FQDN Validation of Server Certificate* (validation du certificat du serveur selon le nom de domaine complet) |
| | *STX: No Secure Transport* (STX : pas de transport sécurisé) |
| | *STX: TLS 1.2 Floor using BCP195* (STX : plancher TLS 1.2 avec BCP195) |
| | *STX: S/MIME* (STX : protocole S/MIME) |
| | *STX: WS-Security* (STX : protocole WS-Security) |
| | *STX: HTTPS IUA* (STX : IUA avec HTTPS) |
| | *ATX: FHIR Feed* (ATX : FHIR Feed) |
| | *ATX: TLS Syslog* (ATX : enregistrement d'événement du système TLS) |
| | *ATX: UDP Syslog* (ATX : enregistrement d'événement du système UDP) |
| Application sécurisée (Secure Application) | *Radiology Audit Trail* (piste d'audit de radiologie) |
| | *FQDN Validation of Server Certificate* (validation du certificat du serveur selon le nom de domaine complet) |
| | *STX: No Secure Transport* (STX : pas de transport sécurisé) |
| | *STX: TLS 1.2 Floor using BCP195* (STX : plancher TLS 1.2 avec BCP195) |
| | *STX: S/MIME* (STX : protocole S/MIME) |
| | *STX: WS-Security* (STX : protocole WS-Security) |
| | *STX: HTTPS IUA* (STX : IUA avec HTTPS) |
| | *ATX: FHIR Feed* (ATX : FHIR Feed) |
| | *ATX: TLS Syslog* (ATX : enregistrement d'événement du système TLS) |

| | |
|---|---|
| | *ATX: UDP Syslog* (ATX : enregistrement d'événement du système UDP) |

**CA:Sec**

| Acteur | Options | Optionalité |
|---|---|---|
| Application sécurisée (Secure Application) | *Mutual TLS* (authentification TLS mutuelle) | O (note 1) |
| | *Server-side TLS* (authentification TLS côté serveur) | O (note 1) |
| | *FQDN Validation of Server Certificate* (validation du certificat du serveur selon le nom de domaine complet) | O (note 2) |

*Note 1 : L'application sécurisée devra prendre en charge l'une des options suivantes :* Mutual TLS *(authentification TLS mutuelle) ou* Server-side TLS *(authentification TLS côté serveur).*

**CA:Aud**

| Acteur | Options | Optionalité |
|---|---|---|
| Créateur d'enregistrements d'audit (Audit Creator) | *FHIR Feed* | O (note 1) |
| Dépôt d'enregistrements d'audit (Audit Record Repository) | *FHIR Feed* | O (note 1) |
| | *Retrieve Audit Message* (extraire un message d'audit) | O (note 2) |
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder) | *FHIR Feed* | O (note 1) |
| Consommateur d'enregistrements d'audit (Audit Consumer) | *Retrieve Audit Message* (extraire un message d'audit) | R |

*Note 1 : Les événements d'audit doivent être enregistrés au moyen de la transaction IHE* Record Audit Event [ITI-20] *avec l'option* FHIR Feed *ou d'autres méthodes (IHE ou autre).*

*Note 2 : Cette transaction est requise si le dépôt d'enregistrements d'audit est central.*

**Notes :**

- Le profil ATNA offre de nombreuses options pour chaque acteur.
- CA:Sec et CA:Aud se concentrent sur un petit sous-ensemble d'options du profil ATNA.
- Les options CA:Sec améliorent également la sécurité en recommandant des versions supérieures du protocole TLS et des suites cryptographiques plus robustes.

## Groupements d'acteurs requis

**ATNA**

| Acteur ATNA | Acteur avec lequel il est groupé |
|---|---|

| | |
|---|---|
| Dépôt d'enregistrements d'audit (Audit Record Repository) | Synchronisation du temps (Consistent Time) / Client de temps (Time Client) |
| | ATNA / Nœud sécurisé (Secure Node) ou Application sécurisée (Secure Application) |
| Consommateur d'enregistrements d'audit (Audit Consumer) | ATNA / Nœud sécurisé (Secure Node) ou Application sécurisée (Secure Application) |
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder) | Synchronisation du temps (Consistent Time) / Client de temps (Time Client) |
| | ATNA / Nœud sécurisé (Secure Node) ou Application sécurisée (Secure Application) |
| | ATNA / Dépôt d'enregistrements d'audit (Audit Record Repository) |
| Nœud sécurisé (Secure Node) | Synchronisation du temps (Consistent Time) / Client de temps (Time Client) |
| Application sécurisée (Secure Application) | Synchronisation du temps (Consistent Time) / Client de temps (Time Client) |

**CA:Sec et CA:Aud**

Aucun groupement

**Notes :**

- Le profil ATNA exige plusieurs groupements d'acteurs.
- CA:Sec et CA:Aud n'exigent aucun groupement d'acteurs.

Le groupement d'acteurs est optionnel et est recommandé pour l'ajout de fonctionnalités telles que la synchronisation horaire des systèmes ou la sécurité et l'audit.

## 3.1.5 Indications sur l'implantation CA:Sec

**CA:Sec (*Canadian Network Security*, ou sécurité du réseau canadien)** précise les éléments fondamentaux nécessaires pour sécuriser les transactions entre deux systèmes.

Ces indications sont basées sur le profil ATNA et visent à apporter des améliorations en proposant un couplage lâche et une grande cohésion, le tout dans le but de sécuriser les communications.

Pour de plus amples renseignements, consultez le profil ATNA, le supplément Add RESTful ATNA (Query and Feed) et la documentation sur la transaction ITI-19.

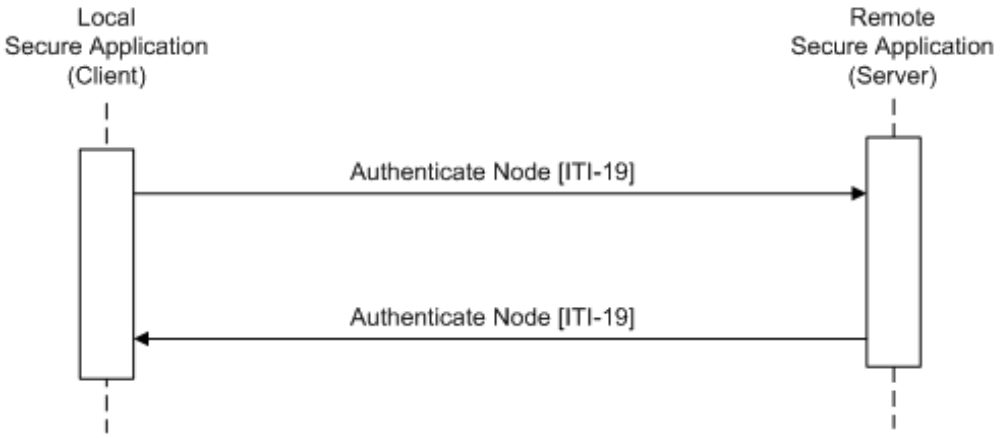
**Note** : Outre la sécurisation des communications dont il est question dans CA:Sec, d'autres aspects critiques doivent être implantés pour assurer un haut degré de cybersécurité. Pour en savoir plus, consultez la section Principes de sécurité.

### But de CA:Sec

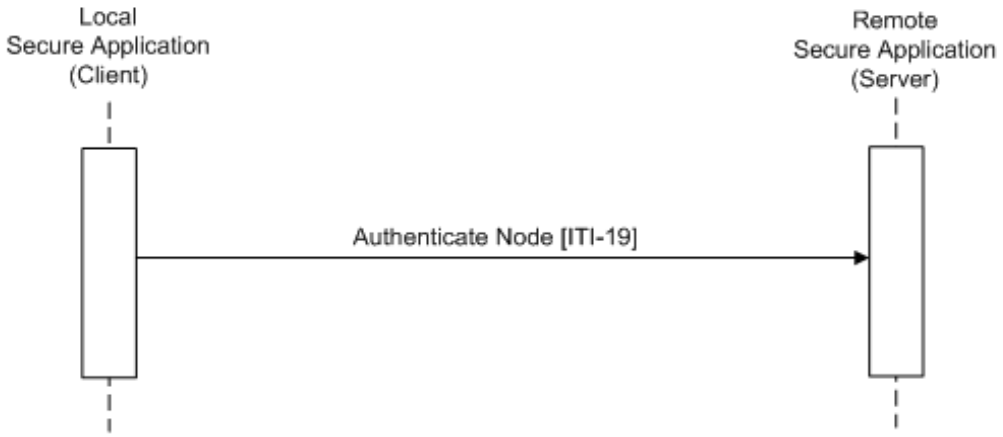
L'objectif est de définir les acteurs et les transactions CA:Sec, ainsi que les options et les groupements des acteurs CA:Sec avec des profils IHE.

**Acteurs/transactions CA:Sec**

Le diagramme ci-dessous montre les acteurs qui sont directement visés par CA:Sec et les transactions pertinentes entre eux.




*Mutual authentication (both client and server authenticate themselves)*




*Server-side authentication (only the server authenticates itself)*

Le tableau ci-dessous présente la transaction liée à chacun de ces acteurs.

Pour être jugé conforme à CA:Sec, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R »).

| **Acteur** | **Transaction** | **Optionalité** |
|---|---|---|
| Application sécurisée (Secure Application) | Authenticate Node [ITI-19] | R |

## Description des acteurs et exigences connexes

Application sécurisée

Une application sécurisée fournit des services de sécurité et de confidentialité (authentification des utilisateurs, sécurisation des communications, enregistrement d'audit de sécurité et application des politiques de sécurité) pour des acteurs IHE groupés et les fonctionnalités des logiciels et des services régis par ladite application sécurisée. En général, les responsabilités d'une application sécurisée n'incluent pas la sécurité de son environnement, comme le système d'exploitation et les bases de données, sur lesquels elle n'a aucun contrôle.

Une application pour téléphone intelligent est un exemple d'application sécurisée qui peut assurer la sécurité de l'application, mais pas des autres composantes logicielles ou matérielles de l'appareil mobile.

À noter qu'un acteur « application sécurisée » peut être un client ou un serveur, et qu'il peut donc s'agir d'un agent de serveur exécuté sur une plateforme nuagique.

Un nœud sécurisé est un cas spécial d'application sécurisée qui contrôle toutes les composantes d'un système informatique, du matériel à l'interface utilisateur en passant par les communications externes. Un échographe est un exemple de nœud sécurisé.

L'application sécurisée devra :

1. utiliser la transaction *Authenticate Node* pour toutes les connections entre le réseau et l'application susceptibles d'exposer des renseignements confidentiels, tel qu'il est précisé à la section Authenticate Node [ITI-19];
2. fournir suffisamment de méthodes d'authentification pour garantir que seuls les utilisateurs autorisés accèdent à l'application sécurisée.

**Options liées aux acteurs CA:Sec**

Pour chaque acteur CA:Sec, les options identifiées par un « R » doivent être sélectionnées.

| Acteur | Options | Optionalité |
|---|---|---|
| Application sécurisée (Secure Application) | *Mutual TLS* **(**authentification TLS mutuelle) | O (note 1) |
| | *Server-side TLS* (authentification TLS côté serveur) | O (note 1) |
| | *FQDN Validation of Server Certificate* (validation du certificat du serveur selon le nom de domaine complet) | R |

*Note 1 : L'application sécurisée devra prendre en charge l'une des deux options suivantes :* Mutual TLS *(authentification TLS mutuelle) ou* Server-side TLS *(authentification TLS côté serveur).*

**Option *Mutual TLS* (authentification TLS mutuelle)**

L'option *Mutual TLS* est un mécanisme d'authentification mutuelle selon lequel le serveur et les applications clientes s'identifient au moyen du protocole Transport Layer Security (TLS) en utilisant des certificats numériques.

Les acteurs qui prennent en charge cette option peuvent :

- utiliser le plus haut degré de cyberprotection du canal de communication protégé par TLS conformément aux normes actuelles et à la meilleure pratique courante de l'IETF (BCP195, RFC5246 au moment de la rédaction – TLS 1.2 ou version supérieure et suites cryptographiques sélectionnées), et
- utiliser seulement la version courante de TLS (1.2 au moment de la rédaction) [RFC5246] ou une version supérieure, et prendre en charge de la version 1.3 [RFC8446] (fortement recommandé).

Note : La recommandation de prise en charge des versions supérieures de TLS (1.3 au moment de la rédaction) deviendra obligatoire ultérieurement.

Un acteur qui prend en charge cette option doit pouvoir se conformer aux normes en vigueur et à la meilleure pratique courante de l'IETF (BCP195, RFC5246 au moment de la rédaction) et aux restrictions supplémentaires énumérées dans Authenticate Node [ITI-19], section Option *Mutual TLS* (authentification mutuelle TLS)/*Server-side TLS* (authentification TLS côté serveur).

Pour plus de précisions, consultez la demande de commentaires RFC7525: https://www.rfc-editor.org/rfc/rfc7525.

### Option *Server-side TLS* (authentification TLS côté serveur)

L'option *Server-side TLS* est un mécanisme d'authentification unidirectionnelle selon lequel le serveur s'identifie à l'application cliente au moyen du protocole Transport Layer Security (TLS) en utilisant des certificats numériques. Ce mécanisme d'authentification est utilisé dans le protocole HTTPS.

L'application cliente utilise d'autres moyens d'identification, habituellement OAuth2/OIDC.

Cette option est décrite dans la spécification IUA pour le profil ATNA sous le nom de *STX: HTTPS IUA* (IUS avec HTTPS).

Note : Les capacités et les exigences de conformité d'un acteur qui prend en charge l'option *Server-side TLS* sont les mêmes que celles décrites dans la section Option *Mutual TLS* (authentification TLS mutuelle).

### Option *FQDN Validation of Server* (validation du certificat du serveur selon le nom de domaine complet)

Consultez les sections Authentification de machine à machine et Option *FQDN Validation of Server* (validation du certificat du serveur selon le nom de domaine complet.
Note : La meilleure pratique courante BCP195 de l'IETF recommande mais n'exige pas la validation du nom de domaine complet.
Lorsqu'un acteur implante cette option, il n'a pas besoin de pouvoir fonctionner sans cette validation.

### Groupements CA:Sec requis

Aucun groupement n'est requis pour CA:Sec.

### Survol de CA:Sec

CA:Sec précise les éléments fondamentaux qui portent sur l'aspect sécurité d'un système de sécurité global :

- authentification de nœud
- communications sécurisées

L'**authentification de nœud** permet aux participants aux communications de :

- confirmer que le serveur est le système de serveur autorisé;
- confirmer que l'application cliente est un client autorisé.

Cela permet d'utiliser des contrôles d'accès au niveau système ou machine qui limitent l'accès aux machines autorisées et authentifiées. Les politiques de gouvernance locales détermineront si des règles de contrôle d'accès au niveau machine sont utilisées.

Les **communications** sont **sécurisées** grâce à TLS. Le protocole TLS assure l'authentification mutuelle, le transport fiable des messages et la communication privée grâce au cryptage des données. Différentes formes de cryptage peuvent être négociées pour protéger les données en transit. CA:Sec permet le cryptage des données utiles pour les sites qui souhaitent implanter une couche de protection supplémentaire.

CA:Sec n'oblige pas les responsables de projets d'implantation et de déploiement à se limiter aux méthodes qu'elle recommande. Pour des raisons d'interopérabilité, le protocole TLS doit être implanté et prêt à être configuré. La RFC7525 *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)* aborde un grand nombre d'options de configuration. Les responsables de projets de déploiement suivent souvent ces recommandations et les intègrent à leurs politiques de sécurité. L'analyse de sécurité d'un déploiement peut aboutir à différents choix. Par conséquent, il est important que ces implantations permettent la configuration de différentes versions de protocole, de différents algorithmes, etc.

### Concepts

La cybersécurité englobe une diversité d'activités opérationnelles, techniques et administratives qui, dans certaines régions, sont décrites dans des lois ou des règlements. Toutes les lois et tous les règlements ont ceci de commun qu'ils exigent un modèle de gouvernance général, divers outils techniques et des comportements opérationnels. Les outils techniques exigés comprennent toujours l'authentification des systèmes, l'authentification des utilisateurs, la journalisation des événements (audit) et le cryptage des télécommunications, et les fonctionnalités techniques requises incluent le contrôle de l'accès, la confidentialité, l'administration des utilisateurs, les copies de sauvegarde, etc. Les exigences opérationnelles et administratives sont également assez importantes en général.

CA:Sec donne également des précisions sur l'authentification des nœuds et le cryptage des

télécommunications. Elle prend pour hypothèse que les acteurs CA:Sec seront installés dans un environnement qui respecte toutes les autres exigences en matière de gouvernance. La conformité avec CA:Sec ne suffit pas à elle seule à assurer une cybersécurité adéquate si les autres activités connexes ne sont pas réalisées.

#### Gouvernance

Les exigences précises qu'il faut remplir pour assurer la cybersécurité varient d'une région et d'une utilisation à l'autre. Les objectifs généraux comprennent toujours la protection de la confidentialité des données, l'intégrité des données et des systèmes, et la disponibilité des données et des systèmes. Les exigences influent sur :

- les politiques administratives, comme les politiques qu'il faut suivre pour l'authentification et le provisionnement d'un nouvel utilisateur;
- les capacités techniques telles que le contrôle d'accès en temps réel; et
- les activités opérationnelles, comme le maintien de centres de secours et la préparation de plans de continuité des services.

Il ne serait ni utile ni raisonnable pour CA:Sec de préciser ces exigences, car elles sont trop variées et débordent le cadre de l'interopérabilité des systèmes.

CA:Sec se fonde sur l'hypothèse qu'une gouvernance est établie dans le même esprit que les recommandations formulées dans les cadres du NIST et de l'ISO :

- NIST Cybersecurity Framework PR.PT.1, https://www.nist.gov/cyberframework
- NIST SP 800-53 Rev4 AU Family, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
- ISO 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, https://www.iso.org/fr/standard/27001

#### Authentification

##### Authentification des utilisateurs

L'application sécurisée distante vérifie que l'utilisateur qui demande l'accès a été authentifié (localement ou à distance) et qu'il est autorisé à utiliser le service demandé.

En ce qui concerne les utilisateurs authentifiés localement, l'authentification doit avoir lieu avant la création d'un tunnel sécurisé. Les utilisateurs ne devraient pas pouvoir utiliser de ressources avant l'authentification locale.

CA:Sec ne précise pas de méthode d'authentification des utilisateurs particulière, mais IHE le fait dans certains de ses profils. On peut utiliser les méthodes mentionnées par IHE ou d'autres. Pour en savoir plus à ce sujet, consultez la section Principes de sécurité.

##### Authentification de machine à machine

CA:Sec précise que les connexions entre les machines doivent être authentifiées et utiliser TLS. L'authentification machine TLS est basée sur l'utilisation de certificats de clé publique ou privée. C'est la méthode qu'on utilise pour authentifier de nombreuses transactions sensibles sur Internet.

Contrairement à la configuration d'un navigateur Internet, dans un milieu de soins de santé :

- la comparaison individuelle et directe pour la validation des certificats peut être pratique et appropriée. Par exemple, il peut être raisonnable d'utiliser la comparaison directe et de fournir le certificat de clé publique entre deux applications sécurisées;
- les certificats signés dans une chaîne de confiance peuvent être pratiques et appropriés. Il peut être raisonnable que le système de sécurité d'un hôpital fournisse l'autorité racine de confiance pour attester qu'une machine donnée est un membre authentifié du réseau hospitalier;
- les autorités de certification racines couramment utilisés pour les navigateurs sont beaucoup moins susceptibles de convenir pour une méthode par chaîne de confiance. Leurs politiques relatives aux certificats sont conçues pour réduire les risques financiers et non pour authentifier un système de santé.

Les certificats requis pour une implantation CA:Sec doivent pouvoir être installés de façon que les systèmes puissent être configurés conformément à la gouvernance locale. Une simple liste de certificats racines de navigateur ne suffit pas. Les responsables de l'implantation d'un projet finiront par établir une règle définitive concernant les exigences détaillées qui s'appliquent aux certificats requis pour un système donné.

### Principes de sécurité CA:Sec

La conformité avec CA:Sec ne suffit pas à elle seule pour assurer une cybersécurité adéquate si les autres activités connexes ne sont pas réalisées.

De nombreux aspects liés à la sécurité jouent un rôle important dans la protection des systèmes informatiques, comme l'authentification des utilisateurs, l'autorisation, le contrôle de l'accès, la confidentialité/le consentement, la journalisation, l'audit, la gouvernance, et bien d'autres. Bien que ces activités de cybersécurité soient primordiales, elles ne constituent pas le principal sujet de CA:Sec. Par contre, plusieurs de ces aspects sont abordés dans d'autres profils IHE spécialisés en la matière.

Pour renforcer la cybersécurité, on peut grouper les acteurs de divers profils IHE lorsque cela est possible. Sinon, on peut utiliser d'autres méthodes qui ne sont pas recommandées expressément par IHE.

### Considérations sur les groupements CA:Sec

#### CA:Aud

CA:Aud permet de journaliser les événements d'audit. Pour générer cette fonctionnalité, on peut grouper un acteur CA:Sec avec un acteur CA:Aud.

Une fois groupé, l'acteur CA:Sec implantera les transactions et/ou les modules de contenu requis dans CA:Sec, ***en plus de toutes*** les transactions exigées pour l'acteur avec lequel il est groupé (deuxième colonne).

| Acteur CA:Sec | Acteur avec lequel il est groupé |
|---|---|
| Application sécurisée (Secure Application) | CA:Aud / Créateur d'enregistrements d'audit (Audit Creator) |

Lorsqu'il est groupé avec l'acteur « créateur d'enregistrements d'audit », l'acteur CA:Sec utilisera la transaction *Record Audit Event* [ITI-20] pour envoyer des messages de journalisation d'événement d'audit à un dépôt d'enregistrements d'audit.

Il est possible d'utiliser d'autres méthodes qui ne sont pas recommandées expressément par IHE pour enregistrer des messages d'audit qui n'exigent pas de groupement avec des acteurs CA:Aud.

#### IUA

Le profil IUA facilite l'authentification des utilisateurs et des applications ainsi que les décisions d'autorisation connexes. Pour générer cette fonctionnalité, on groupe les acteurs CA:Sec avec des acteurs du profil IUA.

Une fois groupé, l'acteur CA:Sec implantera les transactions et/ou les modules requis dans CA:Sec, ***en plus de toutes*** les transactions exigées pour l'acteur avec lequel il est groupé (deuxième colonne).

| Acteur CA:Sec | Acteur avec lequel il est groupé |
|---|---|
| Application sécurisée locale (Local Secure Application) – client | IUA / Client d'autorisation (Authorization Client) |
| Application sécurisée distante (Remote Secure Application) – serveur | IUA / Serveur de ressources (Resource Server) |

Dans la section relative au profil ATNA du supplément *Internet User Authorization* d'IHE, cette option est décrite sous le nom de STX: HTTPS IUA (IUS avec HTTPS).

Les acteurs qui prennent en charge cette option utilisent l'authentification TLS côté serveur (aussi appelée HTTPS) pour attester l'identité du serveur au client et assurer l'intégrité et le cryptage des communications.

Cette configuration utilise l'option d'authentification TLS côté serveur (HTTPS) du profil ATNA pour attester l'identité du serveur au client et assurer l'intégrité et le cryptage des communications et le profil IUA pour attester l'identité de l'application cliente au serveur (IUA / Serveur de ressources).

- La connexion TLS doit être authentifiée par le serveur et pourrait l'être par le client
- La connexion TLS doit être conforme à la BCP195

- Le nœud sécurisé local ou l'application sécurisée locale devra rejeter les connexions qui ne sont pas « HTTPS » et pourrait appliquer d'autres politiques
- Le nœud sécurisé distant ou l'application sécurisée distante devra rejeter les connexions qui ne portent pas de jeton IUA valide et pourrait appliquer d'autres politiques

## Transactions CA:Sec

La présente section décrit les particularités et les contraintes des transactions directement visées par CA:Sec.

### Authenticate Node [ITI-19]

La transaction *Authenticate Node* correspond à la transaction [19] de l'ITI Technical Framework d'IHE. Elle est utilisée par l'acteur « application sécurisée ».

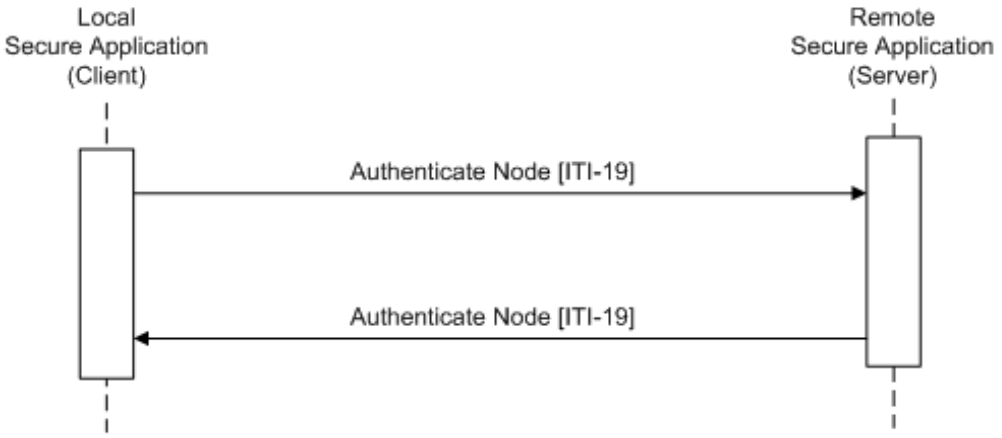
#### Portée

Dans la transaction *Authenticate Node*, une application sécurisée s'identifie à une autre application sécurisée. Cette authentification peut être :

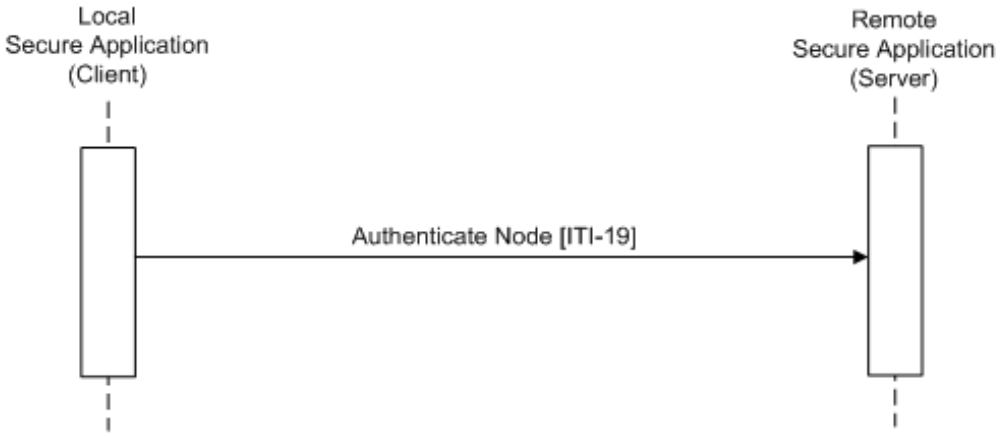
- mutuelle (bidirectionnelle), auquel cas le serveur et le client s'identifient via la transaction *Authenticate Node* [ITI-19]. Après cette authentification mutuelle, d'autres transactions sécurisées pourraient avoir lieu dans le tunnel sécurisé ainsi créé entre les deux nœuds. De plus, l'application sécurisée valide l'identité de l'utilisateur qui demande l'accès au nœud. Cette authentification de l'utilisateur est une opération locale qui ne suppose pas de communication avec un nœud distant;
- côté serveur (unidirectionnelle), auquel cas seul le serveur s'identifie au moyen de la transaction *Authenticate Node* [ITI-19]. L'application cliente utilise d'autres moyens d'identification, habituellement OAuth2/OIDC.

#### Messages

*Note : Le diagramme suivant n'illustre pas la séquence des transactions* Authentication Node *et* Local User Authentication*.*




*Mutual authentication (both client and server authenticate themselves)*




*Server-side authentication (only the server authenticates itself)*

Événement déclencheur

- Authentification mutuelle

L'application sécurisée locale (client) amorce le processus d'authentification bidirectionnelle avec l'application sécurisée distante lorsqu'un échange d'information entre les deux nœuds est demandé. La première transaction sera *Authenticate Node*, et toutes les transactions de RPS subséquentes effectuées par des acteurs IHE seront sécurisées. Ce processus d'authentification est nécessaire lorsqu'une connexion sécurisée est établie.

L'application sécurisée doit toujours appliquer le processus *Authenticate Node* à toutes les connexions.

- Authentification côté serveur

L'application sécurisée locale (client) amorce le processus d'authentification côté serveur avec l'application sécurisée distante lorsqu'un échange d'information entre les deux nœuds est demandé.

## Sémantique du message

La transaction *Authenticate Node* consiste à échanger des certificats qui représentent l'identité des nœuds.

Les suites cryptographiques précisées dans le présent document constituent la base qui permet de réaliser l'interopérabilité. Cette base ne doit pas empêcher l'utilisation de configurations plus sûres. Les suites cryptographiques proprement dites seront négociées dans l'ordre et conformément aux politiques locales, et on

privilégiera les configurations les plus sûres.

#### Validation des certificats

L'organisation locale choisira la formule qui sera utilisée pour l'authentification et l'autorisation des communications en recourant aux méthodes de la chaîne de confiance et de la comparaison directe. Cette formule pourrait être basée uniquement sur une chaîne de confiance composée d'autorités de certification (AC) sélectionnées, ou être fondée entièrement sur l'émission de certificats de nœuds pour une comparaison directe, ou être une combinaison des deux.

*Note : Les AC utilisées pour la chaîne de confiance CA:Sec ne seront pas les mêmes que celles qui figurent sur la liste de confiance du navigateur par défaut et qui servent à authentifier les serveurs Web. De façon générale, on ne fait pas confiance à une AC mondiale comme VeriSign pour déterminer les nœuds d'une organisation qui devraient et ne devraient pas communiquer des renseignements permettant d'identifier le patient.*

Lorsqu'elle authentifie l'application sécurisée distante, l'application sécurisée locale :

- doit pouvoir valider le certificat selon la signature d'une AC de confiance (voir la section Chaîne vers une autorité de certification de confiance) et
- doit pouvoir effectuer une validation directe du certificat par rapport à une série de certificats de confiance (voir la section Validation directe de certificat)

L'application sécurisée locale peut rejeter les communications si le certificat n'est pas validé ou les limiter aux seules communications appropriées pour une tierce partie non identifiée.

#### Chaîne vers une autorité de certification de confiance

L'application sécurisée :

- devra fournir le moyen de configurer la liste des AC de confiance pour l'authentification des certificats de nœuds dans une chaîne de confiance. Ces AC doivent être identifiées selon le certificat de signature à clé publique de l'AC qui signe le certificat;
- devra prendre en charge les certificats numériques codés selon les règles de codage distinctives (DER) et les règles de codage de base (BER);
- devra accepter les communications pour lesquelles une AC de confiance reconnue a signé un certificat.

Autres principes de sécurité pour les transactions par API :

- il pourrait y avoir d'autres méthodes d'autorisation (p. ex. clé API ou certificat émis par l'application).

#### Validation directe de certificat

L'application sécurisée :

- devra fournir le moyen d'installer les certificats requis, par exemple avec un support amovible ou un échange réseau (où l'ensemble de certificats de confiance peut contenir des certificats signés par une AC et des certificats auto-signés);
- devra prendre en charge les certificats numériques codés selon les DER et les BER;
- devra accepter les communications pour lesquelles un certificat a été configuré comme étant acceptable pour la validation directe.

#### Autres exigences liées aux certificats

L'application sécurisée ne devra pas exiger de contenu précis sur les attributs du certificat ni rejeter les certificats qui contiennent des attributs inconnus ou d'autres paramètres. Veuillez noter que, en ce qui concerne les certificats de nœuds, le nom usuel (CN) est souvent un nom d'hôte, et que l'utilisation de ce nom d'hôte n'apporte pas plus de sécurité et générera un nouveau mode de défaillance (p. ex. défaillance du système de noms de domaine).

Les certificats utilisés pour l'authentification mutuelle doivent être des certificats X.509 qui satisfont à l'une des exigences suivantes :

- contenir une clé RSA de 2048 à 4096 bits, dont la longueur dépend de la politique du site local et est conforme à la longueur minimale acceptée par les normes en vigueur (NIST SP 800-57, FIPS140-3), ou

- être conformes aux recommandations relatives aux certificats de la BCP195.

La période de validité maximale des certificats devrait être définie dans la politique de sécurité applicable. Le Technical Framework d'IHE recommande une période de validité maximale de deux ans.

La méthode utilisée pour déterminer si un nœud est autorisé à effectuer des transactions n'est pas spécifiée. On pourrait utiliser une série de certificats de confiance selon une valeur d'attribut contenue dans les certificats, des listes de contrôle d'accès, ou une autre méthode. Nous déconseillons fortement de remonter une chaîne de certificats jusqu'à une AC de confiance externe pour déterminer les autorisations accordées.

Option *FQDN Validation of Server Certificate* (validation du certificat du serveur selon le nom de domaine complet)

L'option *FQDN Validation of Server Certificate* applique les règles présentées dans la norme RFC6125 lorsqu'un client authentifie le serveur avec un certificat X.509 dans le contexte du protocole de sécurité de la couche de transport (TLS).

Un client qui valide l'identité d'un serveur devra vérifier que l'identifiant de référence présent dans une entrée « subjectAltName » de type DNS-ID correspond au domaine source du serveur, conformément à la section 6 de la norme RFC6125. Notez que la section 6 exige que la validation soit fondée sur l'entrée source et le nom de domaine complet (DNS-ID).

Dans un environnement où les clients ont implanté cette option, le certificat X.509 d'un serveur devra contenir une entrée « subjectAltName » de type DNS-ID, conformément à la section 4 de la norme RFC6125.

Toutes les connexions transportant des renseignements protégés qui utilisent le protocole TLS

Option *Mutual TLS* (authentification mutuelle TLS)/*Server-side TLS* (authentification TLS côté serveur)

Un acteur qui utilise l'option *TLS Floor* (plancher TLS) :

- devra pouvoir se conformer à la BCP195. Pour ce faire, l'implantation doit :
    - utiliser le cadre et le mécanisme de négociation précisés par le protocole TLS
    - prendre en charge la version courante de TLS ou une version supérieure
- devra aussi pouvoir imposer l'utilisation de la version courante de TLS ou une version supérieure
- devra également prendre en charge les suites cryptographiques suivantes s'il utilise la version 1.2 de TLS :
    - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- devra aussi prendre en charge les suites cryptographiques suivantes s'il utilise la version 1.3 de TLS :
    - TLS_AES_256_GCM_SHA384
    - TLS_AES_128_GCM_SHA256
- devra rejeter la négociation de toute suite cryptographique reconnue pour offrir une faible sécurité ou un chiffrement inférieur à 128 bits. Une suite cryptographique faible est définie comme un algorithme de chiffrement/déchiffrement qui utilise une clé trop courte, habituellement de moins de 128 bits. Exemples d'algorithmes faibles : Data Encryption Standard (DES), Electronic Codebook (ECB) et Cipher Block Chaining (CBC).

D'autres suites cryptographiques de force semblable ou supérieure pourraient être prises en charge.

Normes mentionnées

IETF :

- [RFC6125] - Saint-Andre, P. et J. Hodges, « Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Transport Layer Security (TLS) », RFC 6125, DOI 10.17487/RFC6125, mars 2011, <https://www.rfc-editor.org/info/rfc6125>.
- [RFC5246] Dierks, T. et E. Rescorla, « The Transport Layer Security (TLS) Protocol Version 1.2 », RFC 5246, DOI 10.17487/RFC5246, août 2008, <https://www.rfc-editor.org/info/rfc5246>.
- [RFC7525] Sheffer, Y., R. Holz et P. Saint-Andre, « Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) », BCP 195, RFC 7525, DOI 10.17487/RFC7525, mai 2015, <https://www.rfc-editor.org/info/rfc7525>.
- [RFC8446] Rescorla, E., « The Transport Layer Security (TLS) Protocol Version 1.3 », RFC 8446, DOI 10.17487/ RFC8446, août 2018, <https://www.rfc-editor.org/info/rfc8446>.
- [BCP195] Sheffer, Y., R. Holz et P. Saint-Andre, « Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) », BCP 195, RFC 7525, mai 2015. Moriarty, K. et S. Farrell, « Deprecating TLS 1.0 and TLS 1.1 », BCP 195, RFC 8996, mars 2021. <https://www.rfc-editor.org/info/bcp195>
- ATNA - Audit Trail and Node Authentication https://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication

UIT-T :

- Recommandation X.509 (03/00). « Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire : cadre général des certificats de clé publique et d'attribut »

**Principes d'audit**

Pour la prise en charge des activités d'audit, on peut grouper des acteurs CA:Sec avec des acteurs CA:Aud (voir la section Considérations sur les groupements CA:Sec). Il est également possible d'utiliser des méthodes autres que les profils IHE pour enregistrer des messages d'audit, méthodes qui ne nécessitent pas de groupement avec des acteurs CA:Aud.

Pour permettre les activités d'audit, une application sécurisée doit détecter et signaler les événements définis dans le tableau ci-dessous. D'autres événements pourraient être signalés.

| Déclencheur d'événement d'audit | Description |
|---|---|
| Actor-start-stop | Début et arrêt d'un acteur. S'applique à tous les acteurs. Distinct du démarrage et de l'arrêt du matériel informatique. |
| Mobile-machine-event | Une machine mobile se connecte à un domaine sécurisé ou le quitte. |
| Node-Authentication-failure | L'authentification d'une application sécurisée a échoué durant la négociation TLS (p. ex. certificat invalide). |

| | |
|---|---|
| Alerte de sécurité | Les fonctions d'administration de la sécurité créent, modifient, suppriment, interrogent et affichent les éléments suivants :<br><br>Configuration et autres changements, p. ex. mises à jour de logiciels qui traitent des renseignements protégés. Des changements qui touchent le matériel pourraient aussi être signalés par ce type d'événement.<br><br>1. Attributs de sécurité et événements auditables qui concernent des fonctions d'applications utilisées pour la gestion des patients, les processus cliniques, le registre des objets et méthodes métier (p. ex. WSDL, UDDI), la création et la maintenance de programme, etc.<br><br>2. Domaines de sécurité pour diverses catégories de l'organisation, comme l'ensemble de l'entité, l'établissement, le service, etc.<br><br>3. Catégories ou groupes de sécurité pour des fonctions et des données comme la gestion des patients, les soins infirmiers, les soins cliniques, etc.<br><br>4. Permissions d'accès autorisées associées à des fonctions et des données comme la création, la consultation, la mise à jour, la suppression et l'exécution d'unités fonctionnelles spécifiques ou de méthodes d'accès à des objets/de manipulation d'objets.<br><br>5. Rôles de sécurité relatifs à diverses catégories de groupement de tâches comme l'administration de la sécurité, le bureau de l'admission, le personnel infirmier, les médecins, les spécialistes cliniques, etc. Comprend aussi l'association de permissions avec des rôles pour le contrôle de l'accès fondé sur le rôle.<br><br>6. Comptes d'utilisateur. Comprend l'attribution ou la modification des mots de passe ou d'autres données d'authentification, ainsi que l'association de rôles avec des utilisateurs pour le contrôle de l'accès fondé sur le rôle ou l'association de permissions avec des utilisateurs pour le contrôle de l'accès fondé sur l'utilisateur.<br><br>7. Tentative d'un utilisateur non autorisé d'utiliser des fonctions d'administration de la sécurité.<br><br>8. Activation et désactivation des fonctions d'audit.<br><br>9. Révocation de l'authentification d'un utilisateur.<br><br>10. Accès au mode d'urgence (aussi appelé « bris de glace »)<br><br>Les événements d'administration de la sécurité devraient toujours être audités. |
| Authentification d'un utilisateur | Ce message décrit un événement de connexion ou de déconnexion d'un utilisateur, qu'il soit réussi ou non. Aucun objet « participant » n'est nécessaire pour ce message. |

## 3.1.6 Indications sur l'implantation CA:Aud

**CA:Aud (Canadian Audit Trail, ou piste d'audit canadienne)** précise les éléments fondamentaux nécessaires à la journalisation d'événements aux fins d'audit.

Ces indications sont basées sur le profil ATNA et visent à apporter des améliorations en proposant un couplage lâche et une grande cohésion, et en se concentrant sur la réalisation d'activités d'audit au moyen de formats et de technologies modernes.

CA:Aud définit les capacités d'enregistrement, de stockage et d'extraction de messages d'audit en format FHIR par des opérations RESTful.

Pour de plus amples renseignements, consultez les documents suivants d'IHE : profil ATNA, supplément Add RESTful ATNA (Query and Feed), ATNA ITI-20 et ATNA ITI-81.

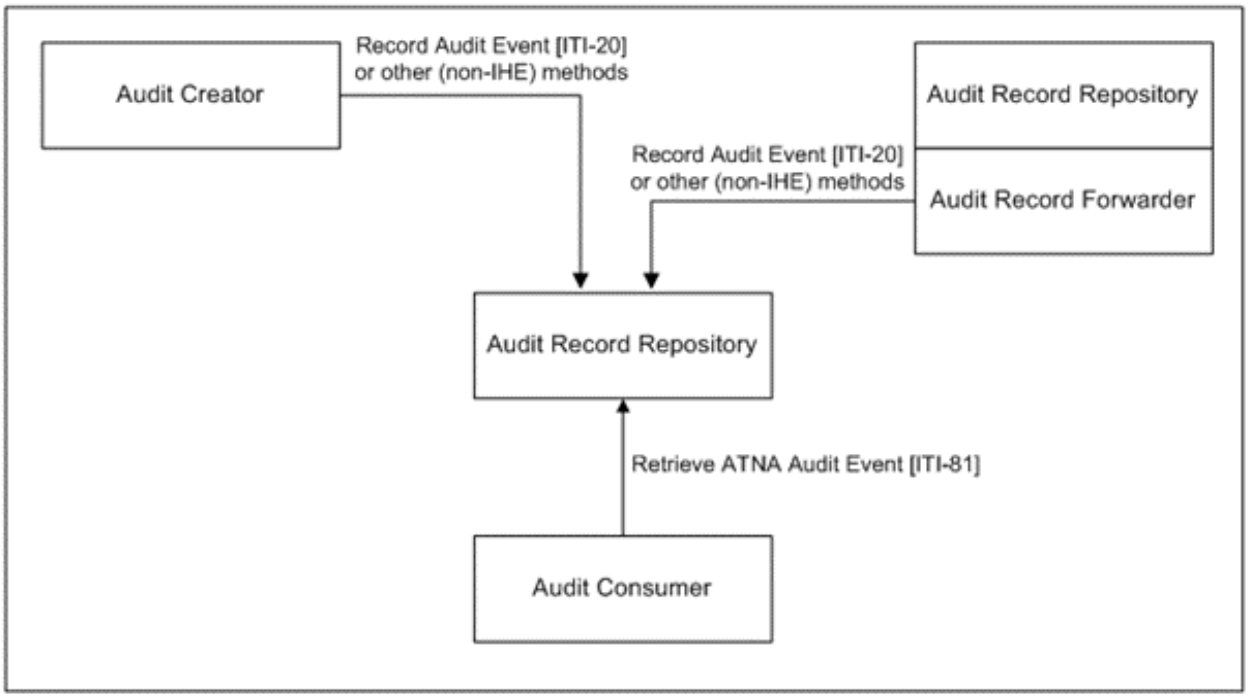
**Note** : CA:Aud a été conçu pour être utilisé dans un environnement sécurisé qui satisfait aux exigences de sécurité et de confidentialité qui, ensemble, assurent une cybersécurité adéquate à toutes les composantes du réseau, telles que la sécurisation des communications, l'authentification des utilisateurs, l'autorisation, le contrôle de l'accès, la confidentialité/le consentement, la gouvernance et bien d'autres. Les journaux d'audit d'autres plateformes comme le serveur Web, le système d'exploitation et les bases de données sont également inclus.

### But de CA:Aud

L'objectif est de définir les acteurs et les transactions CA:Aud, ainsi que les options et les groupements des acteurs avec d'autres profils IHE.

#### Acteurs/transactions CA:Aud

Le diagramme ci-dessous montre les acteurs qui sont directement visés par CA:Aud et les transactions pertinentes entre eux.




Le tableau ci-dessous présente les transactions liées à chacun de ces acteurs.

Pour être jugé conforme à CA:Aud, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R ») et pourrait prendre en charge les transactions optionnelles (identifiées par un « O »).

| Acteurs | Transactions | Optionalité |
|---|---|---|
| Créateur d'enregistrements d'audit (Audit Creator) | Record Audit Event [ITI-20] | O (note 1) |
| Dépôt d'enregistrements d'audit (Audit Record Repository) | Record Audit Event [ITI-20] | O (note 1) |
| | Retrieve ATNA Audit Event [ITI-81] | O (note 2) |
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder) | Record Audit Event [ITI-20] | O (note 1) |
| Consommateur d'enregistrements d'audit (Audit Consumer) | Retrieve ATNA Audit Event [ITI-81] | R |

*Note 1 : Les événements d'audit doivent être enregistrés au moyen de la transaction IHE* Record Audit Event *[ITI-20] avec l'option* FHIR Feed *ou d'autres méthodes (IHE ou autre).*

*Note 2 : Cette transaction est requise si le dépôt d'enregistrements d'audit est central.*

À noter que si d'autres méthodes (IHE ou autre) sont utilisées pour enregistrer les événements d'audit, les messages doivent être convertis dans le format FHIR attendu par le consommateur d'enregistrements d'audit pour la transaction *Retrieve ATNA Audit Event* [ITI-81].

## Descriptions des acteurs et exigences connexes

### Créateur d'enregistrements d'audit

L'acteur « créateur d'enregistrements d'audit » crée des enregistrements *AuditEvent* en format FHIR, comme le précise la transaction *Record Audit Event* [ITI-20], et les envoie au dépôt d'enregistrements d'audit.

L'acteur « créateur d'enregistrements d'audit » :

1. ne devra effectuer que des transactions sécurisées à partir du nœud ou vers celui-ci;
2. devra fournir des méthodes d'authentification suffisantes, en fonction de l'évaluation du risque, pour que seuls les utilisateurs autorisés puissent créer un enregistrement d'audit;
3. devra détecter et déclarer un événement d'enregistrement d'audit comme le précise la transaction *Record Audit Event* [ITI-20] ou par un autre moyen (IHE ou autre), en ce qui concerne :
    - tous les événements liés à une activité pour l'acteur « créateur d'enregistrements d'audit »
    - tous les événements liés à une transaction pour l'acteur « créateur d'enregistrements d'audit »

### Dépôt d'enregistrements d'audit

Le dépôt d'enregistrements d'audit reçoit des rapports d'audit et les stocke. Il peut faire partie d'un réseau de dépôts. En principe, il doit offrir des capacités d'analyse et de production de rapports, mais ces capacités ne sont pas spécifiées dans CA:Aud. La fonction de dépôt d'enregistrements d'audit n'est pas non plus précisée dans CA:Aud, parce que les besoins en matière de déploiement sont si variés qu'il est inutile d'établir des exigences relatives au volume de rapports d'événements ou à la capacité nécessaire.

Le dépôt d'enregistrements d'audit devra prendre en charge les fonctionnalités suivantes :

- l'enregistrement et le stockage d'événements d'enregistrement d'audit avec la transaction *Record Audit Event* [ITI-20] ou par un autre moyen (IHE ou autre);
- les capacités de recherche décrites dans la transaction *Retrieve ATNA Audit Event* [ITI-81];
- des mesures locales de sécurité et de confidentialité ainsi que des contrôles d'accès des utilisateurs.

Le dépôt d'enregistrements d'audit pourrait prendre en charge les fonctionnalités suivantes :

1. le mécanisme de transport d'audit *FHIR Feed* indiqué dans la transaction *Record Audit Event* [ITI-20];
2. la réception d'un message d'audit dans un format décrit par IHE. À noter que le format du message est extensible et qu'il peut inclure des spécifications IHE futures (p. ex. exigences d'audit relatives à de nouvelles transactions IHE) et des extensions privées;
3. d'autres mécanismes de transport et formats de message (IHE ou autre) pour les enregistrements d'audit.

Transmetteur d'enregistrements d'audit

Le transmetteur d'enregistrements d'audit est groupé avec un dépôt d'enregistrements d'audit et transmet des messages d'audit sélectionnés au dépôt d'enregistrements d'audit. Il peut filtrer ces messages et ne transmettre que ceux qu'il a sélectionnés. Il peut aussi les transmettre à différents dépôts d'enregistrements d'audit.

Le transmetteur d'enregistrements d'audit devra :

1. être groupé avec un dépôt d'enregistrements d'audit;
2. filtrer et transmettre les messages à mesure qu'ils arrivent;
3. être configuré pour transmettre les messages à des dépôts d'enregistrements d'audit.

Consommateur d'enregistrements d'audit

Le consommateur d'enregistrements d'audit interroge un dépôt d'enregistrements d'audit pour obtenir des enregistrements d'audit conformes à CA:Aud qui correspondent à des paramètres de contenu. Le traitement subséquent du résultat de l'interrogation n'est pas défini dans la présente version de CA:Aud.

### Options liées aux acteurs CA:Aud

Pour chaque acteur CA:Aud, les options identifiées par un « R » doivent être sélectionnées, et les options identifiées par un « O » sont optionnelles.

| Acteur | Options | Optionalité |
|---|---|---|
| Créateur d'enregistrements d'audit (Audit Creator) | *FHIR Feed* | O (note 1) |
| Dépôt d'enregistrements d'audit (Audit Record Repository) | *FHIR Feed* | O (note 1) |
| | *Retrieve Audit Message* (extraire un message d'audit) | O (note 2) |
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder) | *FHIR Feed* | O (note 1) |
| Consommateur d'enregistrements d'audit (Audit Consumer) | *Retrieve Audit Message* (extraire un message d'audit) | R |

*Note 1 : L'enregistrement des événements d'audit est obligatoire, mais CA:Aud ne précise pas les moyens qu'il faut utiliser pour enregistrer les événements d'audit dans le dépôt d'enregistrements d'audit. Les enregistrements d'audit doivent être enregistrés avec la transaction IHE* Record Audit Event *[ITI-20] et l'option* FHIR Feed *ou une autre méthode (IHE ou autre). L'option* FHIR Feed *est recommandée.*

*Note 2 : Cette transaction est requise si le dépôt d'enregistrements d'audit est central.*

À noter que si d'autres méthodes (IHE ou autre) sont utilisées pour enregistrer les événements d'audit, les messages doivent être convertis dans le format FHIR attendu par le consommateur d'enregistrements d'audit pour la transaction *Retrieve ATNA Audit Event* [ITI-81].

Option *FHIR Feed*

Le message d'audit est transporté via le *FHIR Feed*, ce qui permet d'envoyer les enregistrements d'audit

CA:Aud en utilisant des ressources RESTful et FHIR.

Le dépôt d'enregistrements d'audit devra implanter deux interactions RESTful, *Send Audit Resource* (envoyer une ressource d'audit) et *Send Audit Bundle* (envoyer un *Bundle* d'audit), comme le définit la transaction *Record Audit Event* [ITI-20].

Un créateur d'enregistrements d'audit ou un transmetteur d'enregistrements d'audit doit prendre en charge au moins une des deux interactions RESTful *Send Audit Resource* et *Send Audit Bundle*, comme le définit la transaction *Record Audit Event* [ITI-20].

*FHIR Feed* est l'option recommandée parce qu'elle fournit le format FHIR approprié qui peut être consommé par le consommateur d'enregistrements d'audit qui utilise la transaction *Retrieve ATNA Audit Event* [ITI-81].

Option *Retrieve Audit Message* (extraire des messages d'audit)

L'option *Retrieve Audit Message* permet de demander des enregistrements d'audit qui correspondent au contenu d'un message. Un dépôt d'enregistrements d'audit qui prend en charge cette option devra implanter la transaction *Retrieve ATNA Audit Event* [ITI-81].

La transaction [ITI-81] est une demande de recherche RESTful d'un consommateur d'enregistrements d'audit à un dépôt d'enregistrements d'audit au moyen de ressources FHIR. La réponse reflétera le contenu du dépôt de données au moment de la recherche. CA:Aud ne précise pas les critères de sélection, d'archivage, d'intervalle de conservation, etc., des messages. Ces critères sont établis par la politique locale et varient souvent d'un dépôt d'enregistrements d'audit à l'autre.

**Groupements CA:Aud requis**

Une fois groupé, l'acteur CA:Aud implantera les transactions et/ou les modules de contenu requis dans CA:Aud, ***en plus de toutes*** les transactions exigées pour l'acteur avec lequel il est groupé (deuxième colonne).

| Acteur CA:Aud | Acteur avec lequel il est groupé |
|---|---|
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder) | CA:Aud / Dépôt d'enregistrements d'audit (Audit Record Repository) |

**Survol de CA:Aud**

CA:Aud précise les éléments fondamentaux qui portent sur l'aspect suivant :

- journalisation d'événements (audit)

Le succès de l'implantation de CA:Aud repose sur l'existence et le soutien des éléments suivants :

- communications sécurisées
- services de sécurité du système
- contrôle de l'accès
- gouvernance de la confidentialité et de la sécurité

Pour la journalisation des événements d'audit, CA:Aud précise :

- un schéma normalisé pour le codage d'un événement déclaré
- les événements normalisés à déclarer
  - événements liés à des activités du système, p. ex. « échec de connexion »
  - événements liés à des transactions IHE. Ces événements sont décrits dans les sections du Technical Framework qui décrivent la transaction.
- les messages de rapport d'événement en format FHIR qui utilisent des opérations RESTful
- un dépôt d'enregistrements d'audit pour la collecte de journaux d'audit et les rapports d'événement

**Concepts**

CA:Aud se fonde sur l'hypothèse que les acteurs seront installés dans un environnement qui respecte toutes

les exigences de sécurité, de confidentialité et de gouvernance.

#### Gouvernance

Les exigences précises pour assurer la cybersécurité varient d'une région et d'une utilisation à l'autre. Les objectifs généraux comprennent toujours la protection de la confidentialité des données, l'intégrité des données et des systèmes, et la disponibilité des systèmes.

Il ne serait ni utile ni raisonnable pour CA:Aud de préciser ces exigences, car elles sont trop variées et débordent le cadre de l'interopérabilité des systèmes.

#### Journalisation d'événements

La journalisation d'audit d'événements CA:Aud remplit une fonction de journalisation de surveillance. Ainsi, elle permet d'enregistrer :

- tous les événements de sécurité qui sont détectés;
- un ensemble complet d'événements d'activité et de transaction qui décrit les opérations courantes. On s'en sert pour déterminer quelles opérations sont normales et quelles opérations divergentes sont à surveiller. Le niveau de détail est laissé à la discrétion des responsables. Les détails qui n'aident pas à distinguer ce qui est normal de ce qui ne l'est pas sont exclus, surtout s'ils révèlent des RPS.

La journalisation d'événements n'est pas conçue pour les activités suivantes :

- analyse judiciaire détaillée, comme celle qu'on effectue lorsque la surveillance révèle une activité douteuse ou après la détection d'un événement de sécurité. Ce genre d'activité exige souvent un niveau de détail qui concerne des aspects techniques précis de produits particuliers. CA:Aud présume qu'il existe un journal de niveau judiciaire pour les produits, et que ceux-ci rendent compte de la conception et de renseignements précis sur leurs rapports d'événements. Le journal judiciaire pourrait également utiliser le schéma et les transactions CA:Aud, ou il pourrait être différent;
- journal d'analyse du rendement du flux de tâches, typique dans le cas de contrôle de systèmes étroitement coordonnés. Les événements CA:Aud ont été choisis pour la surveillance de la confidentialité et de la sécurité, et non pour surveiller le rendement d'un système ou du personnel. Un journal d'analyse du rendement du flux de tâches pourrait également utiliser le schéma et les transactions CA:Aud, ou il pourrait être différent.

#### Événements

##### Activité

CA:Aud définit les événements liés aux activités des acteurs IHE et des composantes du système qui sont groupés avec un acteur sécurisé. Il peut s'agir d'événements comme le démarrage d'un système, la connexion d'un utilisateur (succès et échec), la violation d'un contrôle d'accès, etc. Ces événements doivent être détectés et déclarés.

Ces événements sont décrits dans la transaction *Record Audit Event* [ITI-20] (voir la section Événements déclencheurs, sous la section Interaction *Send Audit Resource Request Message – FHIR Feed*). D'autres événements déclarables sont souvent répertoriés dans d'autres profils IHE. Ils sont décrits dans ces profils ou transactions, ou ils pourraient être précisés par des politiques, des lois ou des règlements locaux.

##### Transaction

Les profils IHE qui définissent des transactions pourraient définir des événements et en préciser la structure de déclaration.

### Principes de sécurité CA:Aud

De nombreux aspects liés à la sécurité jouent un rôle important dans la protection des systèmes informatiques, comme l'authentification des utilisateurs, le contrôle d'accès, la confidentialité/le consentement, la journalisation, l'audit, la gouvernance et bien d'autres. Bien que ces activités de cybersécurité soient primordiales, elles ne constituent pas le principal sujet de CA:Aud . Par contre, plusieurs de ces aspects sont abordés dans d'autres profils IHE spécialisés en la matière.

Pour renforcer la cybersécurité, on peut grouper les acteurs de divers profils IHE lorsque cela est possible. Sinon, on peut utiliser d'autres méthodes qui ne sont pas recommandées expressément par IHE.

Certains concepts de base sont décrits dans la section Survol de CA:Aud.

CA:Aud définit les transactions pour le dépôt d'enregistrements d'audit qui permettent l'échange de renseignements sensibles sur les patients et les systèmes.

Dans de nombreux projets et implantations, les dépôts d'enregistrements d'audit sont considérés comme des « boîtes noires » capables d'enregistrer de l'information pertinente aux fins de sécurité et de surveillance. Ces systèmes n'ont pas été conçus au départ pour donner accès à des enregistrements stockés à des parties externes.

Les agents de sécurité et les architectes de système devraient en tenir compte et analyser les risques que suppose la divulgation de données stockées dans le dépôt d'enregistrements d'audit. La transaction *Retrieve ATNA Audit Event* [ITI-81] explique comment chercher les enregistrements d'audit stockés en format FHIR au moyen de la transaction *Record Audit Event* [ITI-20].

C'est pour cette raison qu'on recommande fortement de soumettre les acteurs et les requêtes CA:Aud à des mécanismes de contrôle d'accès. Le profil IUA devrait être envisagé pour les contrôles d'autorisation. On peut grouper le dépôt d'enregistrements d'audit CA:Aud avec un acteur « serveur de ressources » du profil IUA pour appliquer des politiques et des décisions d'autorisation. Le consommateur d'enregistrements d'audit peut être groupé avec un acteur « client d'autorisation » du profil IUA pour fournir des renseignements d'autorisation au dépôt d'enregistrements d'audit CA:Aud. Les contrôles d'accès devraient imposer des restrictions d'accès appropriées aux enregistrements d'audit.

La transaction *Retrieve CA:Aud Audit Event* [ITI-81] pourrait donner lieu à la divulgation de renseignements sensibles. La journalisation de cette transaction d'extraction en tant qu'événement d'interrogation est appropriée (voir la transaction Retrieve ATNA Audit Event [ITI-81] dans la section Principes de sécurité).

D'autres principes de sécurité sont décrits dans la section Z.8 Mobile Security Considerations du supplément Add RESTful ATNA (Query and Feed).

**Considérations sur les groupements CA:Aud**

CA:Sec

CA:Sec permet de sécuriser les communications. Pour générer cette fonctionnalité, on peut grouper des acteurs CA:Aud avec des acteurs CA:Sec.

Une fois groupé, l'acteur CA:Aud implantera les transactions et/ou les modules de contenu requis dans CA:Aud, ***en plus de toutes*** les transactions exigées pour l'acteur avec lequel il est groupé (deuxième colonne).

| Acteur CA:Aud | Acteur avec lequel il est groupé |
|---|---|
| Créateur d'enregistrements d'audit (Audit Creator) | CA:Sec / Application sécurisée (Secure Application) |
| Dépôt d'enregistrements d'audit (Audit Record Repository) | CA:Sec / Application sécurisée (Secure Application) |
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder) | CA:Sec / Application sécurisée (Secure Application) |

Lorsqu'ils sont groupés avec l'acteur « application sécurisée » CA:Sec, les acteurs CA:Aud utiliseront la transaction *Authenticate Node* [ITI-19] pour sécuriser les communications entre les acteurs.

Profil CT

Le profil CT permet de synchroniser les horloges et les horodateurs des ordinateurs d'un réseau. Pour générer cette fonctionnalité, on peut grouper des acteurs CA:Aud avec des acteurs CT.

Une fois groupé, l'acteur CA:Aud implantera les transactions et/ou les modules de contenu requis dans CA:Aud, ***en plus de toutes*** les transactions exigées pour l'acteur avec lequel il est groupé (deuxième colonne).

| Acteur CA:Aud | Acteur avec lequel il est groupé |
|---|---|
| Créateur d'enregistrements d'audit (Audit Creator) | CT / Client de temps (Time Client) |
| Dépôt d'enregistrements d'audit (Audit Record Repository) | CT / Client de temps (Time Client) |
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder) | CT / Client de temps (Time Client) |

## Transactions CA:Aud

La présente section décrit les particularités et les contraintes des transactions directement visées par CA:Aud.

*Record Audit Event* [ITI-20]

Cette section correspond à la transaction *Record Audit Event* [ITI-20] de l'ITI Technical Framework d'IHE, qui permet de déclarer des événements auditables à un dépôt d'enregistrements d'audit.

Portée

Cette transaction permet de déclarer des événements auditables à un dépôt d'enregistrements d'audit au moyen de l'option *FHIR Feed*.

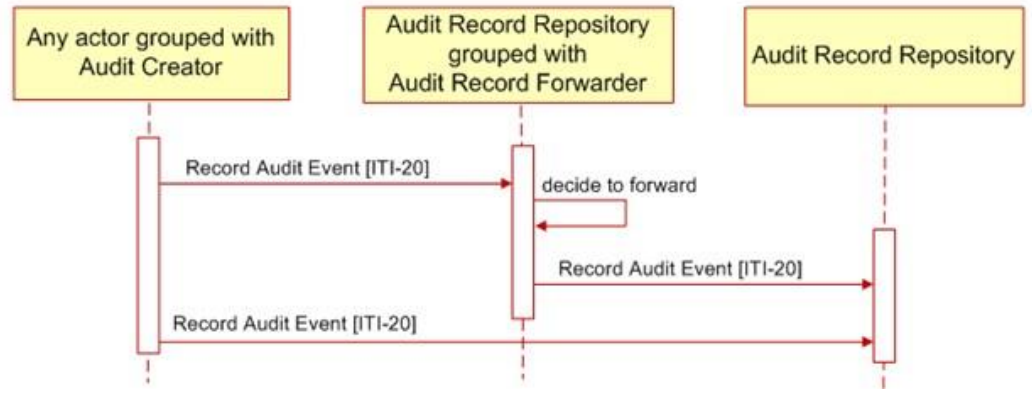
Rôles des acteurs

| Acteur | Rôle |
|---|---|
| Tout acteur groupé avec l'acteur « créateur d'enregistrements d'audit » | Créer un enregistrement d'audit et le transmettre au dépôt d'enregistrements d'audit. |
| Dépôt d'enregistrements d'audit (Audit Record Repository) | Recevoir un enregistrement d'audit du créateur d'enregistrements d'audit et le stocker aux fins d'audit. |
| Transmetteur d'enregistrements d'audit (Audit Record Forwarder) | Transmettre un enregistrement d'audit aux dépôts d'enregistrements d'audit. |

Normes mentionnées

| | |
|---|---|
| HL7 FHIR | Version 4 http://hl7.org/fhir/R4/index.html |
| RFC4627 | The application/json Media Type for JavaScript Object Notation (JSON) d'IETF |

Messages

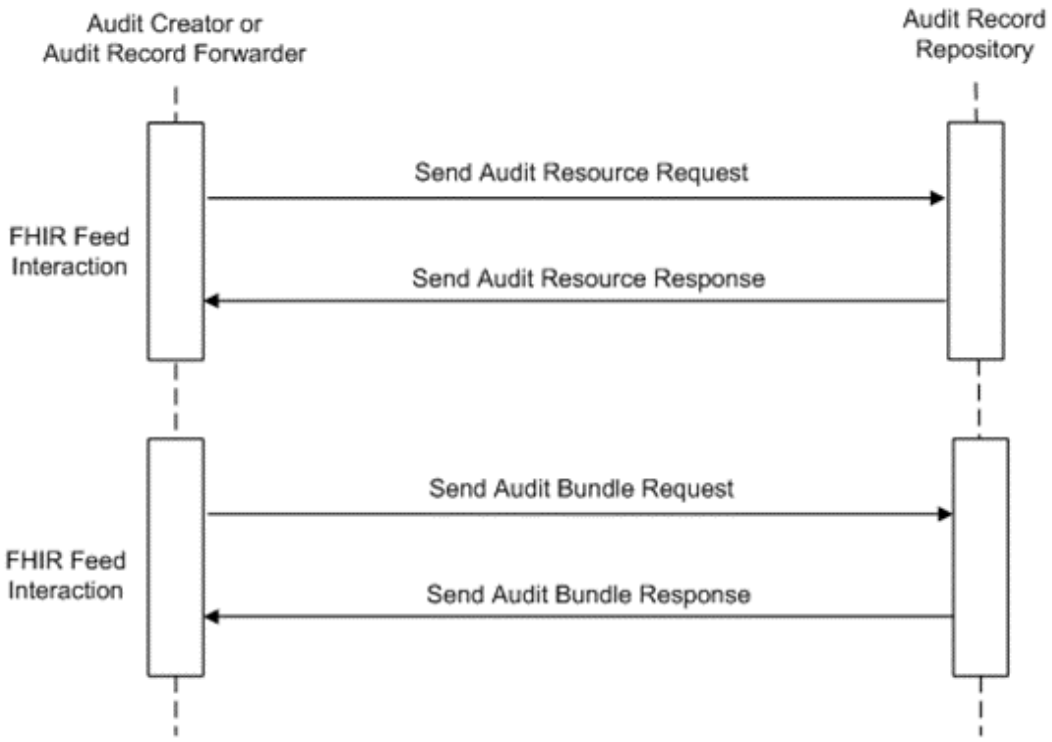



*Note 1 : Tout acteur qui amorce une transaction ITI-20 pourrait envoyer des enregistrements à plusieurs dépôts d'enregistrements d'audit.*

*Note 2 : Le dépôt d'enregistrements d'audit qui reçoit une transaction ITI-20 pourrait ou non être groupé avec un acteur « transmetteur d'enregistrements d'audit ». Le diagramme ci-dessus ne montre pas de chaîne de transmission entre des acteurs.*

Dans le contexte de CA:Aud, la transaction ITI-20 définit deux interactions différentes aux fins d'audit :

1. L'interaction *Send Audit Resource Request Message – FHIR Feed* permet d'auditer une ressource FHIR *AuditEvent* en utilisant un protocole RESTful (voir la section Interaction *Send Audit Resource Request Message – FHIR Feed*).
2. L'interaction *Send Audit Bundle Request Message – FHIR Feed* permet d'auditer un *Bundle* FHIR de ressources *AuditEvent* en utilisant un protocole RESTful (voir la section Interaction *Send Audit Bundle Request Message – FHIR Feed*).




Interaction *Send Audit Resource Request Message – FHIR Feed*

Un acteur groupé avec un acteur « créateur d'enregistrements d'audit » ou « transmetteur d'enregistrements d'audit » détecte un événement qui devrait être déclaré et utilise le message *Send Audit Resource* pour envoyer un rapport sur l'événement à un dépôt d'enregistrements d'audit.

Un créateur d'enregistrements d'audit ou transmetteur d'enregistrements d'audit qui prend en charge l'interaction *FHIR Feed* utilise ce message pour soumettre une ressource *AuditEvent* au dépôt d'enregistrements d'audit au moyen d'une interaction « create » FHIR (voir https://www.hl7.org/fhir/R4/http.html#create).

Événements déclencheurs

Lorsqu'un acteur groupé avec un créateur d'enregistrements d'audit ou transmetteur d'enregistrements d'audit doit soumettre une ressource *AuditEvent* au dépôt d'enregistrements d'audit.

Il y a deux événements déclencheurs :

1. Un créateur d'enregistrements d'audit détecte un événement qui devrait être déclaré au dépôt d'enregistrements d'audit. La présente transaction ne précise pas toutes les politiques et raisons qui touchent la déclaration d'événements. Celles-ci pourraient être mentionnées dans d'autres profils IHE, des lois ou des règlements locaux, ou encore des politiques locales.
2. Un transmetteur d'enregistrements d'audit détermine qu'une ressource *AuditEvent* reçue devrait être envoyée à un autre dépôt d'enregistrements d'audit. La présente transaction ne précise pas quelles règles ou politiques déterminent si une ressource *AuditEvent* devrait être transmise.

Tout acteur d'un profil IHE groupé avec un créateur d'enregistrements d'audit devrait pouvoir déclarer les événements définis dans le tableau ci-dessous. D'autres événements déclarables sont souvent mentionnés dans d'autres profils ou transactions IHE.

**Événements déclencheurs d'un enregistrement d'audit :**

| Événement déclencheur | Description |
|---|---|
| Actor-start-stop | Début et arrêt d'un acteur. S'applique à tous les acteurs. Distinct du démarrage et de l'arrêt du matériel informatique. |
| Audit-Log-Used | Une chose autre qu'un message de piste d'audit a accédé au dépôt de pistes d'audit ou l'a modifié. |
| Begin-storing-instances | Début du stockage d'instances SOP (de différents types ou non) pour un examen. |
| Instances-deleted | Des instances SOP sont supprimées d'un examen spécifique. Un événement englobe toutes les instances supprimées de l'examen. |
| Instances-Stored | Les instances fournies pour un examen particulier ont été stockées dans le système. Un événement englobe toutes les instances stockées pour l'examen. |
| Mobile-machine-event | Une machine mobile se connecte à un domaine sécurisé ou le quitte. |
| Node-Authentication-failure | L'authentification d'une application sécurisée a échoué durant la négociation TLS (p. ex. certificat invalide). |
| Order-record-event | Enregistrement de commande créé, modifié, supprimé ou auquel on a accédé. Acteurs concernés : Order Placer (passeur de commande). Comprend la commande initiale, les mises à jour ou modifications, la livraison, la clôture et l'annulation. Voir la note ci-dessous. |
| Patient-record-event | Dossier de patient créé, modifié ou auquel on a accédé. |

| | |
|---|---|
| PHI-export | Toute exportation de RPS sur un support physique amovible comme un CD-ROM ou le transfert électronique de dossiers comme le courrier électronique. Toute activité d'impression de RPS sur papier ou film, locale ou distante. |
| PHI-import | Toute importation de RPS sur un support physique amovible comme un CD-ROM ou le transfert électronique de dossiers comme le courrier électronique. |
| Procedure-record-event | Dossier d'intervention créé, modifié, supprimé ou auquel on a accédé. |
| Interrogation pour obtenir de l'information | Une interrogation a été reçue, soit dans le cadre d'une transaction IHE, soit dans le cadre d'autres fonctions de produits.<br><br>Par exemple :<br><br>1- Modality Worklist Query (interrogation d'une liste de travail par une modalité)<br>2- Instance or Image Availability Query (interrogation sur la disponibilité d'une instance ou d'une image)<br>3- PIX, PDQ ou XDS Query (interrogation d'un registre PIX, PDQ ou XDS)<br><br>Notes : En général, on recommande de journaliser l'événement d'interrogation en indiquant non pas son résultat, mais plutôt ses paramètres. Le résultat d'une interrogation peut être très long et très peu utile par rapport au temps d'interrogation. Les paramètres peuvent servir à détecter un mauvais comportement et à regénérer le résultat de l'interrogation au besoin. |

| | |
|---|---|
| Alerte de sécurité | Les fonctions d'administration de la sécurité créent, modifient, suppriment, interrogent et affichent les éléments suivants :<br><br>Configuration et autres changements, p. ex. mises à jour de logiciels qui traitent des renseignements protégés. Des changements qui touchent le matériel pourraient aussi être signalés par ce type d'événement.<br><br>1. Attributs de sécurité et événements auditables qui concernent des fonctions d'applications utilisées pour la gestion des patients, les processus cliniques, le registre des objets et méthodes métier (p. ex. WSDL, UDDI), la création et la maintenance de programme, etc.<br><br>2. Domaines de sécurité pour diverses catégories de l'organisation, comme l'ensemble de l'entité, l'établissement, le service, etc.<br><br>3. Catégories ou groupes de sécurité pour des fonctions et des données comme la gestion des patients, les soins infirmiers, les soins cliniques, etc.<br><br>4. Permissions d'accès autorisées associées à des fonctions et des données comme la création, la consultation, la mise à jour, la suppression et l'exécution d'unités fonctionnelles spécifiques ou de méthodes d'accès à des objets/de manipulation d'objets.<br><br>5. Rôles de sécurité relatifs à diverses catégories de groupement de tâches comme l'administration de la sécurité, le bureau de l'admission, le personnel infirmier, les médecins, les spécialistes cliniques, etc. Comprend aussi l'association de permissions avec des rôles pour le contrôle de l'accès fondé sur le rôle.<br><br>6. Comptes d'utilisateur. Comprend l'attribution ou la modification des mots de passe ou d'autres données d'authentification, ainsi que l'association de rôles avec des utilisateurs pour le contrôle de l'accès fondé sur le rôle ou l'association de permissions avec des utilisateurs pour le contrôle de l'accès fondé sur l'utilisateur.<br><br>7. Tentative d'un utilisateur non autorisé d'utiliser des fonctions d'administration de la sécurité.<br><br>8. Activation et désactivation des fonctions d'audit.<br><br>9. Révocation de l'authentification d'un utilisateur.<br><br>10. Accès au mode d'urgence (aussi appelé « bris de glace »)<br><br>Les événements d'administration de la sécurité devraient toujours être audités. |
| Authentification d'un utilisateur | Ce message décrit un événement de connexion ou de déconnexion d'un utilisateur, qu'il soit réussi ou non. Aucun objet « participant » n'est nécessaire pour ce message. |
| Study-Object-Event | Examen créé, modifié, supprimé ou auquel on a accédé. Signale l'ajout de nouvelles instances à des examens existants et la création de nouveaux examens. |
| Study-used | Des instances SOP provenant d'un examen spécifique sont créées, modifiées, ou on y a accédé. Un événement englobe toutes les instances utilisées pour l'examen. |

Sémantique du message

Un créateur d'enregistrements d'audit ou transmetteur d'enregistrements d'audit doit émettre une requête HTTP selon les exigences définies dans la spécification FHIR pour l'interaction « create » (http://hl7.org/fhir/R4/http.html#create). Le message utilise une méthode HTTP POST pour envoyer une ressource FHIR *AuditEvent*.

Le créateur d'enregistrements d'audit ou transmetteur d'enregistrements d'audit doit soumettre la ressource FHIR *AuditEvent* en format XML ou JSON. Les valeurs du type MIME du message de requête sont définies dans ITI TF-2: Appendix Z.6.

Une ressource *AuditEvent* qui répond à la définition de « Audit Message » (message d'audit) fournie dans le Technical Framework d'IHE doit satisfaire aux exigences ci-dessous.

| **Attribut de la ressource FHIR *AuditEvent*** | **Description** |
|---|---|
| type | Identifiant pour une famille de l'événement. Par exemple, un élément de menu, un programme, une règle, une politique, un code de fonction, un nom d'application ou une URL. Identifie la fonction exercée. |
| subtype | Identifie la catégorie d'événement. |
| action | Indique le type d'action exécutée durant l'événement qui a généré l'audit. |
| recorded | Moment où l'événement a été enregistré. |
| outcome | Indique si l'événement a réussi ou échoué. |
| outcomeDesc | Description en texte libre du résultat de l'événement. |
| purposeOfEvent | Le « purposeOfUse » (raison) utilisé durant l'événement enregistré. |
| agent | Acteur qui joue un rôle actif dans l'événement ou l'activité journalisé. |
| agent.type | Spécification du type de participation de l'utilisateur dans l'exécution de l'événement. |
| agent.role | Rôle de sécurité au titre duquel agissait l'utilisateur et qui provient des codes locaux définis par le système de sécurité de contrôle d'accès (p. ex. RBAC, ABAC) et utilisés dans le contexte local. |
| agent.who | Renvoie à qui est l'agent qui était partie à l'événement. |
| agent.altId | Identifiant de rechange de l'agent. Pour un humain, il devrait s'agir d'une chaîne de texte qui constitue l'identifiant de l'utilisateur. Cet identifiant serait connu d'un système d'authentification courant (p. ex. signature unique), le cas échéant. |

| | |
|---|---|
| agent.name | Nom de l'agent significatif pour l'humain. |
| agent.requestor | Indique que l'utilisateur est ou n'est pas l'auteur de la requête relative à l'événement audité. |
| agent.policy | Politique ou programme qui a autorisé l'activité enregistrée. Habituellement, une seule activité peut être visée par plusieurs politiques, comme le consentement du patient, le financement du garant, etc. La politique indiquerait aussi le jeton de sécurité utilisé. |
| agent.media | Type de média en cause. Utilisé lorsque l'événement concerne l'exportation/l'importation dans le média. |
| agent.network.address | Identifiant du point d'accès au réseau de l'appareil de l'utilisateur pour l'événement d'audit. |
| agent.network.type | Identifiant du type de point d'accès au réseau à l'origine de l'événement d'audit. |
| source | Système qui déclare l'événement. |
| source.site | Emplacement source logique dans le réseau de l'entreprise de soins de santé. Par exemple, un hôpital ou l'emplacement d'un autre fournisseur dans un groupe de fournisseurs multiples. |
| source.observer | Identifiant de la source où l'événement a été détecté. |
| source.type | Code qui précise le type de source de l'événement. |
| entity | Instances précises de données ou d'objets auxquelles il y a eu accès. |
| entity.what | Identifie une instance spécifique de l'entité. La référence devrait mentionner explicitement la version. |
| entity.type | Type d'objet en jeu dans l'événement d'audit. |
| entity.role | Code qui représente le rôle que l'entité a joué dans l'événement audité. |
| entity.lifecycle | Identifiant de l'étape du cycle de vie des données pour l'entité. |
| entity.securityLabel | Niveau de confidentialité pour l'entité identifiée. |

| | |
|---|---|
| entity.name | Nom de l'entité dans l'événement d'audit. |
| entity.query | Paramètres d'interrogation pour des entités de type interrogation. |
| entity.detail | Paires de valeurs marquées pour la transmission d'informations supplémentaires sur l'entité. |
| entity.detail.type | Type de renseignement supplémentaire fourni dans la valeur. |
| entity.detail.ValueBase64Binary | Valeur du renseignement supplémentaire Base64Binary. |

#### Actions attendues

Le dépôt d'enregistrements d'audit devra prendre en charge tous les types MIME décrits dans ITI TF-2: Appendix Z.6.

À la réception du message *Send Audit Resource Request*, le dépôt d'enregistrements d'audit devra valider les ressources et envoyer l'un des codes de réponse HTTP présentés dans la section Sémantique du message.

En ce qui concerne la ressource reçue, le dépôt d'enregistrements d'audit pourrait faire ce qui suit :

- rejeter la ressource si elle n'est pas pertinente
- conserver la ressource dans un magasin de données interne
- effectuer d'autres opérations de traitement sur la ressource

Le dépôt d'enregistrements d'audit pourrait appliquer diverses règles de conservation des données au magasin de données, mais ces règles ne sont pas précisées dans la présente transaction. Habituellement, ces règles dépendent de l'affectation du dépôt d'enregistrements d'audit.

Le dépôt d'enregistrements d'audit doit stocker toutes les ressources qui n'ont pas été rejetées et les rendre accessibles pour d'autres recherches faisant intervenir la transaction *Retrieve ATNA Audit Event* [ITI-81].

Lorsque le dépôt d'enregistrements d'audit est groupé avec un transmetteur d'enregistrements d'audit, ce dernier doit :

- appliquer des règles de filtrage à toutes les ressources *AuditEvent* reçues par le dépôt d'enregistrements d'audit, et
- transmettre toutes les ressources *AuditEvent* qui correspondent aux filtres à leurs destinations configurées.

#### Message *Send Audit Resource Response*

Le dépôt d'enregistrements d'audit envoie une réponse au créateur d'enregistrements d'audit ou au transmetteur d'enregistrements d'audit sous la forme d'un message *Send Audit Resource Response* pour informer le client du résultat de l'opération.

#### Événement déclencheur

Lorsque le dépôt d'enregistrements d'audit a fini de stocker la ressource *AuditEvent* reçue, il envoie ce message au client pour l'informer du résultat de sa requête.

#### Sémantique du message

Le dépôt d'enregistrements d'audit envoie un code d'état HTTP qui convient à l'opération, conformément aux exigences de spécification précisées dans https://www.hl7.org/fhir/R4/http.html#create.

Si le résultat est une réussite, le code d'état HTTP de la réponse devrait être un code 2xx. Si par contre c'est

un échec, le dépôt d'enregistrements d'audit devra pouvoir envoyer des codes d'état conformément à ce qui est présenté dans https://www.hl7.org/fhir/R4/http.html#create.

Le dépôt d'enregistrements d'audit peut envoyer d'autres codes d'état 4xx ou 5xx conformément à des règles métier internes qui ne sont pas abordées dans la présente transaction.

Le dépôt d'enregistrements d'audit devrait traiter les erreurs de sorte que les événements d'audit destinés à être enregistrés ne soient pas perdus (p. ex. erreurs attribuables à la validation du format du message).

#### Actions attendues

Le dépôt d'enregistrements d'audit pourrait envoyer des codes d'échec, et le client devra alors décider de ce qu'il en fera.

#### Interaction *Send Audit Bundle Request Message – FHIR Feed*

Un créateur d'enregistrements d'audit ou transmetteur d'enregistrements d'audit qui prend en charge l'option *ATX: FHIR Feed* utilise ce message pour soumettre un *Bundle* de ressources *AuditEvent* au dépôt d'enregistrements d'audit au moyen d'une interaction FHIR « batch » (voir https://www.hl7.org/fhir/R4/http.html#transaction).

#### Événement déclencheur

Lorsqu'un transmetteur d'enregistrements d'audit ou un acteur groupé avec un créateur d'enregistrements d'audit doit envoyer plusieurs événements audités au dépôt d'enregistrements d'audit.

Il existe deux événements déclencheurs :

1. Un créateur d'enregistrements d'audit détecte au moins un événement qui devrait être déclaré au dépôt d'enregistrements d'audit. La présente transaction ne précise pas toutes les politiques et raisons qui touchent la déclaration d'événements. Celles-ci pourraient être mentionnées dans d'autres profils IHE, des lois ou des règlements locaux, ou encore des politiques locales.
2. Un transmetteur d'enregistrements d'audit détermine qu'au moins une ressource *AuditEvent* reçue devrait être envoyée à un autre dépôt d'enregistrements d'audit. La présente transaction ne précise pas quelles règles ou politiques déterminent si une ressource *AuditEvent* devrait être transmise ou non.

Un acteur dans un profil IHE groupé avec un créateur d'enregistrements d'audit devra pouvoir déclarer les événements définis dans la section Événements déclencheurs, sous la section Interaction *Send Audit Resource Request Message – FHIR Feed*. D'autres événements déclarables sont souvent répertoriés pour des événements spécifiques dans d'autres profils IHE. Ils sont décrits dans ces profils ou transactions.

#### Sémantique du message

Un transmetteur d'enregistrements d'audit ou un acteur groupé avec un créateur d'enregistrements d'audit devra émettre une requête HTTP selon les exigences définies dans la spécification FHIR pour l'interaction « batch » (voir https://www.hl7.org/fhir/R4/http.html#transaction).

Le dépôt d'enregistrements d'audit et le client doivent tous les deux prendre en charge l'interaction « batch ». Le message utilise une méthode HTTP POST pour soumettre une ressource FHIR *Bundle*. Le client doit soumettre les ressources FHIR en format XML ou JSON. Les valeurs du type MIME du message de requête sont définies dans ITI TF-2: Appendix Z.6.

La ressource FHIR *Bundle* doit contenir au moins une ressource FHIR *AuditEvent* (https://www.hl7.org/fhir/R4/auditevent.html).

L'élément Bundle.entry.request.method doit être POST.

Les ressources *AuditEvent* incluses dans le *Bundle* qui correspondent à la définition de *Audit Message* donnée dans le Technical Framework d'IHE doivent être conformes aux exigences définies dans la section Sémantique du message , sous la section Interaction *Send Audit Resource Request Message – FHIR Feed*.

**Contraintes relatives aux ressources *Bundle* :**

| Élément et cardinalité | Contraintes |
|---|---|
| type [1..1] | Doit être : batch |
| entry [1..*] | Doit contenir au moins une ressource *AuditEvent* |
| entry.request.method | Doit être : POST |

Actions attendues

Le dépôt d'enregistrements d'audit devra prendre en charge tous les types MIME décrits dans ITI TF-2: Appendix Z.6.

À la réception du message *Send Audit Bundle Resource Request*, le dépôt d'enregistrements d'audit doit valider les ressources et envoyer l'un des codes de réponse HTTP présentés dans la section Sémantique du message, sous la section Interaction *Send Audit Bundle Request Message – FHIR Feed.*

En ce qui concerne la ressource reçue, le dépôt d'enregistrements d'audit pourrait faire ce qui suit :

- rejeter la ressource si elle n'est pas pertinente
- conserver la ressource dans un magasin de données interne
- effectuer d'autres opérations de traitement sur la ressource

Le dépôt d'enregistrements d'audit pourrait appliquer diverses règles de conservation des données au magasin de données, mais ces règles ne sont pas précisées dans la présente transaction. Habituellement, ces règles dépendent de l'affectation du dépôt d'enregistrements d'audit.

Le dépôt d'enregistrements d'audit doit stocker toutes les ressources qui n'ont pas été rejetées et les rendre accessibles pour d'autres recherches faisant intervenir la transaction *Retrieve ATNA Audit Event* [ITI-81].

Lorsque le dépôt d'enregistrements d'audit est groupé avec un transmetteur d'enregistrements d'audit, ce dernier doit :

- appliquer des règles de filtrage à toutes les ressources *AuditEvent* reçues par le dépôt d'enregistrements d'audit, et
- transmettre toutes les ressources *AuditEvent* qui correspondent aux filtres à leurs destinations configurées.

Message *Send Audit Bundle Response*

Le dépôt d'enregistrements d'audit envoie une réponse à une interaction *Send Audit Bundle Request* sous la forme d'un message *Send Audit Bundle Response*.

Événement déclencheur

Lorsque le dépôt d'enregistrements d'audit a fini de stocker les ressources *AuditEvent* reçue dans la ressource *Bundle*, il envoie le message au client pour l'informer du résultat de sa requête.

Sémantique du message

Le dépôt d'enregistrements d'audit envoie un code d'état HTTP qui convient à l'opération, conformément aux exigences de spécification précisées dans https://www.hl7.org/fhir/R4/http.html#transaction-response.

Lorsque le dépôt d'enregistrements d'audit a traité la requête, il doit envoyer une réponse HTTP avec un code d'état général.

Pour permettre au client de connaître le résultat de la transaction et les identités que le dépôt d'enregistrements d'audit a attribuées aux ressources, le dépôt d'enregistrements d'audit doit envoyer un *Bundle* de type « batch-response ». Chaque élément d'entrée doit contenir un élément de réponse avec un code d'état HTTP qui détaille le résultat du traitement de l'entrée de requête.

Si aucun entête « Prefer » n'est spécifié dans la requête, le serveur répondra comme si ses paramètres étaient réglés à « return=minimal »; voir https://www.hl7.org/fhir/R4/http.html#ops.

Si le résultat de l'entrée est une réussite, le code d'état HTTP de la réponse devra être un code 2xx.

Si le résultat de l'entrée est un échec, le dépôt d'enregistrements d'audit devra être capable d'envoyer des codes d'état conformément à ce qui est prévu sur https://www.hl7.org/fhir/R4/http.html#create.

Le dépôt d'enregistrements d'audit peut envoyer d'autres codes d'état 4xx ou 5xx conformément à des règles métier internes qui ne sont pas abordées dans la présente transaction.

Le dépôt d'enregistrements d'audit devrait traiter les erreurs de sorte que les événements d'audit destinés à être enregistrés ne soient pas perdus (p. ex. erreurs attribuables à la validation du format du message).

#### Actions attendues

Le dépôt d'enregistrements d'audit pourrait envoyer un message de réussite partielle concernant le *Bundle* si certaines ressources présentent un échec. Le client devra décider de ce qu'il fait des messages d'échec envoyés par le dépôt d'enregistrements d'audit.

### Principes de sécurité

On recommande d'utiliser le mécanisme de transport TLS ou HTTPS parce que les messages d'événement d'audit contiennent souvent des RPS ou d'autres renseignements sensibles.

Il n'est pas toujours nécessaire de recourir au mécanisme de transport TLS parce qu'il existe d'autres moyens de protection plus appropriés dans certaines situations. La décision d'opter pour le mécanisme de transport UDP devrait être fondée sur une analyse des risques pour la sécurité et la confidentialité.

Le magasin de données du dépôt d'enregistrements d'audit pourrait contenir des renseignements sensibles, et les fonctions d'analyse de ce même dépôt pourraient autoriser des interrogations de données sensibles. Si c'est le cas, le dépôt sera une cible de choix pour les acteurs malveillants et il devrait donc être protégé en conséquence.

Le dépôt d'enregistrements d'audit doit générer des messages d'événement d'audit pour différents types d'utilisation du magasin de données et changements de configuration. Cette procédure est précisée dans la section Événements déclencheurs, sous la section Interaction *Send Audit Resource Request Message – FHIR Feed*.

Si l'option *AuditEvent Message* est prise en charge par le dépôt d'enregistrements d'audit, les interactions de mise à jour, de suppression et de correction des ressources *AuditEvent* devraient être gérées selon des politiques locales.

## *Retrieve ATNA Audit Event* [ITI-81]

Cette transaction permet l'extraction d'un enregistrement d'audit CA:Aud du dépôt d'enregistrements d'audit conformément à une série de paramètres de recherche qui déterminent les rapports d'événement extraits.

Elle permet au consommateur d'enregistrements d'audit de chercher des événements d'audit qu'un dépôt d'enregistrements d'audit a créés au moyen de la transaction *Record Audit Event* [ITI-20] avec l'option *FHIR Feed*. Si le dépôt d'enregistrements d'audit stocke des messages d'audit dans d'autres formats, il devrait alors les convertir au format FHIR pour qu'ils puissent être consommés par la transaction *Retrieve ATNA Audit Event* [ITI-81].

Cette transaction est un profilage d'une recherche FHIR standard de la ressource *AuditEvent*.

### Portée

La transaction *Retrieve ATNA Audit Event* permet de rechercher des événements CA:Aud dans un dépôt d'enregistrements d'audit CA:Aud. Le résultat de cette extraction est un *Bundle* FHIR de ressources *AuditEvent* qui correspondent à une série de paramètres de recherche.

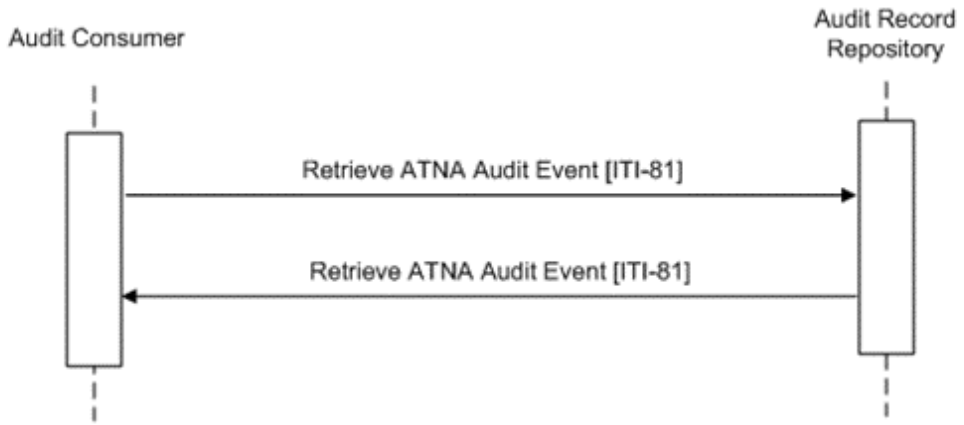
### Rôles des acteurs

| Acteur | Rôle |
|---|---|
| Dépôt d'enregistrements d'audit (Audit Record Repository) | Permet de stocker les événements d'audit CA:Aud et répond aux interrogations pour une partie des enregistrements stockés. |
| Consommateur d'enregistrements d'audit (Audit Consumer) | Interroge un système pour obtenir des enregistrements d'audit CA:Aud. |

Normes mentionnées

| | |
|---|---|
| RFC2616 | Hypertext Transfer Protocol – HTTP/1.1 d'IETF |
| RFC4627 | The application/json Media Type for JavaScript Object Notation (JSON) d'IETF |
| RFC6585 | Additional HTTP Status Codes d'IETF |
| RFC3339 | Date and Time on the Internet: Timestamps d'IETF |
| HL7 FHIR | Version 4 http://hl7.org/fhir/R4/index.html |

Messages




Message de requête *Retrieve ATNA Audit Events*

Ce message consiste en une requête HTTP GET à l'aide de paramètres par un consommateur d'enregistrements d'audit à un dépôt d'enregistrements d'audit. Le dépôt d'enregistrements d'audit a stocké des enregistrements d'audit CA:Aud reçus via des transactions *Record Audit Event* [ITI-20]. Ces messages, qui sont stockés dans un magasin de données, peuvent être extraits conformément à des paramètres de recherche précis.

Événement déclencheur

Le consommateur d'enregistrements d'audit envoie un message *Retrieve ATNA Audit Events* lorsqu'il doit traiter ou analyser des enregistrements d'audit CA:Aud.

Sémantique du message

Le message *Retrieve ATNA Audit Event* doit être une requête HTTP GET qui est envoyée au dépôt d'enregistrements d'audit. Ce message est une recherche FHIR (voir http://hl7.org/fhir/R4/search.html) qui s'applique à des ressources *AuditEvent* (voir http://hl7.org/fhir/ R4/auditevent.html).

Cette cible de recherche est formatée comme ceci :

<scheme>://<authority>/<path>/AuditEvent?date=ge[start-time]&date=le[stop-time]&<query>

où :

- <scheme> sera http ou https. Ce choix relève d'une décision stratégique, mais https est habituellement approprié vu le contenu confidentiel d'un enregistrement d'audit CA:Aud
- <authority> sera représenté comme un hôte (une adresse IP ou un nom de domaine) suivi optionnellement d'un deux-points et d'un numéro de port
- le dépôt d'enregistrements d'audit peut utiliser <path> pour différencier le service de recherche HTTP pour l'implantation *AuditEvent* à partir d'autres services REST
- au moins un paramètre de recherche par date est requis. Voir la section Paramètres de recherche par date
- le caractère « & » est un paramètre conditionnel qui devra être inclus si le paramètre <query> est présent
- le paramètre <query>, s'il est présent, représente une série de paires nom-valeur codées qui constituent les filtres de la recherche. Voir la section Autres paramètres de recherche.

#### Paramètres de recherche par date

Le paramètre de date doit être utilisé pour spécifier une valeur maximale et/ou une valeur minimale pour la recherche. Au moins un paramètre de date doit être présent. On recommande d'inclure deux paramètres de date dans chaque recherche du consommateur d'enregistrements d'audit. Ces paramètres doivent être pris en charge par le dépôt d'enregistrements d'audit pour éviter de surcharger le consommateur d'enregistrements d'audit. Ils permettent au consommateur d'enregistrements d'audit de préciser la période pendant laquelle les enregistrements d'audit qui l'intéressent ont été créés et de limiter le nombre d'enregistrements d'audit envoyés. Les valeurs des paramètres de recherche par date doivent être dans le format prévu par la norme RFC3339.

*Note : Le format prévu par la norme RFC3339 est celui qu'impose le journal d'exploitation pour les horodateurs et est un sous-ensemble du format de données date/heure XML utilisé par FHIR.*

Par exemple, pour faire une recherche de ressources *AuditEvent* créées durant la journée du 5 janvier 2013 :

http://example.com/ARRservice/AuditEvent?date=ge2013-01-05&date=le2013-01-05

Le dépôt d'enregistrements d'audit doit appliquer des critères de correspondance aux ressources *AuditEvent* pour lesquelles la valeur du champ AuditEvent.recorded se situe dans la période précisée dans le message de requête.

Le dépôt d'enregistrements d'audit doit appliquer d'autres critères de correspondance de date selon les règles définies par la spécification FHIR (http://hl7.org/fhir/R4/search.html).

#### Autres paramètres de recherche

Les paramètres de recherche indiqués dans la présente section pourraient être pris en charge par le consommateur d'enregistrements d'audit et devront être pris en charge par le dépôt d'enregistrements d'audit. Le consommateur d'enregistrements d'audit peut utiliser ces paramètres pour raffiner ses requêtes de recherche.

Le consommateur d'enregistrements d'audit devra coder tous les paramètres de recherche conformément aux règles d'encodage-pourcent décrites dans la norme RFC3986. Même si FHIR n'applique pas de contraintes à l'utilisation des opérateurs ET(AND) OU(OR) pour des interrogations de complexité illimitée, cette transaction applique des contraintes aux interrogations autorisées :

- les paramètres de recherche multiples ne devront être combinés qu'avec l'opérateur ET (AND ou &);
- l'opérateur OU (« , ») ne devra être utilisé que dans un paramètre de recherche unique qui contient plusieurs valeurs.

Autres paramètres de recherche :

- « address » est un paramètre de type chaîne qui spécifie l'ID du point d'accès au réseau (NetworkAccessPointID) de l'appareil de l'utilisateur qui crée l'enregistrement d'audit (il pourrait s'agir d'un ID d'appareil, d'une adresse IP ou d'un autre identifiant associé à un appareil).

La valeur de ce paramètre devra contenir la sous-chaîne correspondante. Par exemple : http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&address=192.168.0.1

Le dépôt d'enregistrements d'audit devra trouver la chaîne AuditEvent.agent.network.address qui correspond à ce paramètre.

- « agent.identifier » est un paramètre de type jeton. Ce paramètre identifie l'utilisateur qui a participé à l'événement à l'origine de l'enregistrement d'audit.

Par exemple, pour chercher des ressources *AuditEvent* liées à l'administration des utilisateurs : http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&agent.identifier=admin

Le dépôt d'enregistrements d'audit devra trouver la valeur du champ AuditEvent.agent.who.identifier qui correspond à ce paramètre.

Si un ID de patient est utilisé, le dépôt d'enregistrements d'audit renverra seulement les enregistrements d'audit auxquels le patient a participé en tant qu'utilisateur.

- « patient.identifier » est un paramètre de type jeton. Ce paramètre spécifie l'ID du patient inclus dans l'événement en tant que participant ou utilisateur. La valeur de ce paramètre peut contenir l'URI de l'espace de nommage (qui représente l'autorité d'attribution de l'identifiant) et l'identifiant.

Par exemple :

http://example.com/ARRservice/AuditEvent?
date=ge2013-01-01&date=le2013-01-02&patient.identifier=urn:oid:1.2.3.4|5678

Le dépôt d'enregistrements d'audit devra trouver la chaîne AuditEvent.agent.who.identifier qui correspond à ce paramètre et la chaîne AuditEvent.entity.what.identifier dont la référence est associée à un patient.

- « entity.identifier » est un paramètre de type jeton. Ce paramètre spécifie un identifiant unique pour l'objet. La valeur du paramètre devrait être identifiée conformément au type d'entité.

Exemple :

- ?entity.identifier=urn:oid:1.2.3.4.5|123-203-FJ
- ?entity.identifier=|123-203-FJ.

Le dépôt d'enregistrements d'audit devra associer ce paramètre au champ AuditEvent.entity.what.identifier de type identifiant. Si un ID de patient est utilisé, le dépôt d'enregistrements d'audit enverra uniquement les enregistrements d'audit où le patient est inclus dans l'événement en tant que participant.

- « entity-type » est un paramètre de type jeton. Ce paramètre précise le type de l'objet (p. ex. personne, objet système). La valeur du paramètre devra contenir l'URI de l'espace de nommage http://hl7.org/fhir/audit-entity-type ou http://hl7.org/fhir/resource-types définie par FHIR et une valeur codée. Voir http://hl7.org/fhir/R4/valueset- audit-entitytype.html pour les codes à utiliser.

Le dépôt d'enregistrements d'audit devra associer ce paramètre au champ AuditEvent.entity.type.

- « entity-role » est un paramètre de type jeton. Ce paramètre spécifie le rôle joué par l'entité (p. ex. rapport, emplacement, interrogation). La valeur du paramètre doit contenir l'URI de l'espace de nommage http://hl7.org/fhir/object-role définie par FHIR et une valeur codée. Voir http://hl7.org/fhir/R4/object-role pour les codes à utiliser.

Exemple d'une requête pleinement spécifiée de recherche de tous les enregistrements d'audit liés à l'entité document (rapport = 3) dont l'ID unique est 12345^1.2.3.4.5 : http://example.com/ARRservice/AuditEvent?
date=ge2013-01-01&date=le2013-01-02&entity-role=http://hl7.org/fhir/object-role|3&entity-id=urn:oid:1.2.3.4.5|12345

Le dépôt d'enregistrements d'audit devra associer ce paramètre au champ AuditEvent.entity.role.

- « source.identifier » est un paramètre de type jeton. Ce paramètre identifie la source de l'événement d'audit.

Exemple de requête de recherche de ressources *AuditEvent* produites par l'application source de l'audit dont l'ID unique est 1234 :

http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&source=1234

Le dépôt d'enregistrements d'audit devra associer ce paramètre au champ AuditEvent.source.observer.identifier.

- « type » est un paramètre de type jeton. Ce paramètre représente l'identifiant du type d'événement audité. La valeur du paramètre doit contenir l'URI de l'espace de nommage http://dicom.nema.org/resources/ontology/DCM et une valeur codée. Les codes possibles sont définis par IHE (voir, sous Record Audit Event [ITI-20], la section Événements déclencheurs, sous la section Interaction *Send Audit Resource Request Message – FHIR Feed*.

Exemple de recherche de ressources *AuditEvent* liées à des événements d'exportation de RPS :

http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&type=http://dicom.nema.org/resources/ontology/DCM|110106

Le dépôt d'enregistrements d'audit devra associer ce paramètre au champ AuditEvent.type.

- « subtype » est un paramètre de type jeton. Ce paramètre identifie la transaction IHE à l'origine de l'enregistrement d'audit. La valeur du paramètre peut contenir l'URI de l'espace de nommage urn:ihe:event-type-code pour la recherche de messages d'audit déclenchés par des transactions IHE accompagnées du message d'audit défini. Chaque transaction IHE qui définit des messages CA:Aud précise un code qui identifie la transaction en tant que telle et attribue ce code à l'élément EventTypeCode dans l'enregistrement d'audit ITI-20.

Exemple de recherche de ressources *AuditEvent* liées à des transactions *Retrieve Document Set* [ITI-43] :

http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&subtype=urn:ihe:event-type-code|ITI-43

Le dépôt d'enregistrements d'audit devra associer ce paramètre au champ AuditEvent.subtype :

- « outcome » est un paramètre de type jeton. Ce paramètre représente la réussite ou l'échec de l'événement. La valeur du paramètre doit contenir l'URI de l'espace de nommage http://hl7.org/fhir/audit-event-outcome et un code issu de l'ensemble de valeurs relié. Voir la page http://hl7.org/fhir/R4/valueset-audit-event-outcome.html.

Pour rechercher des ressources *AuditEvent* liées à des événements qui ont échoué :

http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&outcome=http://hl7.org/fhir/audit-event-outcome|4,8,12

Le dépôt d'enregistrements d'audit devra associer ce paramètre au champ AuditEvent.outcome.

La norme FHIR d'HL7 propose d'autres paramètres de recherche. La présente transaction ne définit pas de comportement précis à adopter face à ces paramètres (comme _sort, _include, etc.). Consultez la page http://hl7.org/fhir/R4/search.html pour en savoir plus sur les paramètres possibles.

#### Format de la réponse attendue

La norme FHIR d'HL7 fournit des codages pour des réponses en format XML ou JSON. Le dépôt d'enregistrements d'audit devra prendre en charge les deux formats d'encodage de message. Le consommateur d'enregistrements d'audit devra en prendre au moins un en charge. Pour en savoir plus sur l'encodage de la réponse désiré et la négociation du format, voir ITI TF-2: Appendix Z.6.

#### Actions attendues

Le dépôt d'enregistrements d'audit tient à jour une base de données d'événements d'audit. Il conserve les données conformément aux politiques locales, et certaines données pourraient donc être supprimées.

Le dépôt d'enregistrements d'audit devra envoyer tous les événements d'audit stockés dans sa base de données qui correspondent aux paramètres d'interrogation et que le demandeur est autorisé à visualiser (voir la section Survol de CA:Aud pour en savoir plus).

Lorsqu'il trouve des correspondances selon les paramètres de recherche, le dépôt d'enregistrements d'audit doit :

- sélectionner tous les enregistrements d'audit pour lesquels l'URL de requête contient un intervalle de temps.

Si des paramètres de recherche autres que ceux définis dans la section Autres paramètres de recherche (p. ex. paramètres de résultat de recherche FHIR _sort, _include) sont précisés dans l'URL de requête :

- et que le dépôt d'enregistrements d'audit ne prend pas en charge ces paramètres, ceux-ci seront écartés;
- et que le dépôt d'enregistrements d'audit prend en charge les paramètres, l'opération de correspondance ou tout autre comportement devra respecter les règles de mise en correspondance relatives au type de données dans FHIR.

Le dépôt d'enregistrements d'audit devra envoyer des ressources correspondantes au moyen du message de réponse *Retrieve ATNA Audit Event*. Voir la section Message de réponse *Retrieve ATNA Audit Event*.

#### Message de réponse *Retrieve ATNA Audit Event*

Le dépôt d'enregistrements d'audit envoie le message *Retrieve ATNA Audit Event* en réponse à une interrogation d'un consommateur d'enregistrements d'audit.

#### Événement déclencheur

Le dépôt d'enregistrements d'audit crée ce message quand il reçoit et traite un message *Retrieve ATNA Audit Event*.

#### Sémantique du message

Lorsque le dépôt d'enregistrements d'audit traite la requête de recherche, il doit envoyer les ressources *AuditEvent* correspondantes dans une ressource FHIR *Bundle*.

La valeur « Content-Type » de la réponse dépendra de la négociation du format de la réponse décrite dans ITI TF-2: Appendix Z.6.

S'il n'y a pas de paramètre de recherche par date (voir la section Paramètres de recherche par date), le dépôt d'enregistrements d'audit pourrait envoyer le code de réponse HTTP 400 - Bad Request (requête incorrecte).

Si les paramètres de recherche précisés ne mènent à aucun enregistrement d'audit correspondant, le dépôt d'enregistrements d'audit enverra un code de réponse HTTP 200 (réussite de la requête), avec une ressource FHIR *Bundle* vide.

Si le dépôt d'enregistrements d'audit considère que la taille des données demandées est excessive, il pourrait envoyer les résultats sur plusieurs pages (voir https://www.hl7.org/fhir/R4/http.html#paging).

Le dépôt d'enregistrements d'audit pourrait envoyer d'autres codes de réponse HTTP. Voir, dans ITI TF-2: Appendix Z.7, l'indication Guidance on Access Denied Results.

Le dépôt d'enregistrements d'audit devrait compléter le code d'erreur envoyé par une description de l'erreur dans un langage lisible par l'humain.

Le dépôt d'enregistrements d'audit pourrait envoyer des réponses de redirection HTTP (301, 302, 303 ou 307) à une requête. Le consommateur d'enregistrements d'audit doit suivre la redirection, mais s'il constate une boucle de redirection, il pourrait signaler une erreur.

#### FHIR *Bundle* de messages *AuditEvent*

Lorsque la recherche est réussie, le corps du message de réponse doit contenir un FHIR *Bundle* de ressources *AuditEvent*.

Exemple en format XML :

```
<Bundle>
    <type>searchset</type>
```

```
        <total>3</total>
        <link>
                <relation value="self"/>
                <url value="http://example.com/ARRservice/AuditEvent?
date=&gt;2013-01-01&date=&lt;2013-01-02"/>
        </link>
        <entry>
                <fullUrl value="http://example.com/ARRservice/AuditEvent/23#"/>
                <resource>  <AuditEvent> .....                  </AuditEvent> </resource>
        </entry>
        <entry>
                <fullUrl value="http://example.com/ARRservice/AuditEvent/564#"/>
                <resource>  <AuditEvent> ..... </AuditEvent> </resource>
        </entry>
        <entry>
                <fullUrl value="http://example.com/ARRservice/AuditEvent/3446#"/>
                <resource>  <AuditEvent>           ..... </AuditEvent> </resource>
        </entry>
</Bundle>
```

Actions attendues

Le consommateur d'enregistrements d'audit pourrait analyser davantage les données reçues dans le FHIR *Bundle* de ressources *AuditEvent*.

Principes de sécurité

Voir les Principes de sécurité généraux.

Principes d'audit

Cette transaction pourrait supposer la divulgation de renseignements sensibles. La journalisation de ces transactions d'extraction en tant qu'événement d'interrogation est une pratique appropriée.

Cependant, CA:Aud n'exige pas que le dépôt d'enregistrements d'audit puisse envoyer des enregistrements d'audit via la transaction *Record Audit Event* [ITI-20].

La notation de l'optionalité est définie comme suit :

| | |
|---|---|
| O | Ce champ est obligatoire. |
| NS | L'optionalité de ce champ n'est pas spécialisée. L'optionalité de la norme sous-jacente s'applique. |
| C | Ce champ est obligatoire si une condition spécifiée est vraie (*true*). |

Le dépôt d'enregistrements d'audit devra créer et enregistrer localement un événement d'audit comme suit :

| | **Nom du champ** | **Opt** | **Contraintes de valeur** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **Événement**<br>AuditMessage (message d'audit)/EventIdentification (identification d'événement) | EventID | O | EV (110101, DCM, « journal d'audit utilisé ») |
| | EventActionCode | O | « R » (lecture) |
| | *EventDateTime* | *NS* | *Non spécialisée* |
| | *EventOutcomeIndicator* | *NS* | *Non spécialisée* |
| | EventTypeCode | O | EV (« ITI-81 », « transactions IHE », « Retrieve ATNA AuditEvent ») |
| Source (administrateur de documents) (1) | | | |
| Demandeur humain (0..1) | | | |
| Destination (registre de documents) (1) | | | |
| Source d'audit (administrateur de documents) (1) | | | |
| Message *AuditEvent* (0..n) | | | |

Emplacement :

| | | | |
|---|---|---|---|
| **Source**<br>AuditMessage (message d'audit)/ ActiveParticipant (participant actif) | *UserID* | *NS* | *Non spécialisée* |
| | AlternativeUserID | O | L'ID du processus tel qu'il est utilisé dans les journaux du système d'exploitation local. |
| | *UserName* | *NS* | *Non spécialisée* |
| | *UserIsRequestor* | *NS* | *Non spécialisée* |
| | RoleIDCode | O | EV (110153, DCM, « source ») |
| | NetworkAccessPointTypeCode | O | « 1 » pour le nom (DNS) de la machine, « 2 » pour l'adresse IP |
| | NetworkAccessPointID | O | Le nom de la machine ou l'adresse IP. |
| **Demandeur humain (s'il est connu)** | UserID | O | Identité de l'humain qui a amorcé la transaction. |

| | | | |
|---|---|---|---|
| AuditMessage (message d'audit)/ActiveParticipant (participant actif) | *AlternativeUserID* | *NS* | *Non spécialisée* |
| | *UserName* | *NS* | *Non spécialisée* |
| | *UserIsRequestor* | *NS* | *Non spécialisée* |
| | RoleIDCode | O | Le(s) rôle(s) de contrôle d'accès de l'utilisateur qui permet(tent) cette transaction. |
| | *NetworkAccessPointTypeCode* | *NS* | *Non spécialisée* |
| | *NetworkAccessPointID* | *NS* | *Non spécialisée* |
| **Destination** AuditMessage (message d'audit)/ActiveParticipant (participant actif) | UserID | O | URI de point d'extrémité de SOAP |
| | *AlternativeUserID* | *NS* | *Non spécialisée* |
| | *UserName* | *NS* | *Non spécialisée* |
| | *UserIsRequestor* | *NS* | *Non spécialisée* |
| | RoleIDCode | O | EV (110152, DCM, « destination ») |
| | NetworkAccessPointTypeCode | O | « 1 » pour le nom (DNS) de la machine, « 2 » pour l'adresse IP |
| | NetworkAccessPointID | O | Le nom de la machine ou l'adresse IP |
| **Source d'audit** AuditMessage (message d'audit)/ AuditSourceIdentification (identification de la source d'audit) | *AuditSourceID* | *NS* | *Non spécialisée* |
| | *AuditEnterpriseSiteID* | *NS* | *Non spécialisée* |
| | *AuditSourceTypeCode* | *NS* | *Non spécialisée* |

| | | | |
|---|---|---|---|
| **Message *AuditEvent*** AuditMessage (message d'audit)/ ParticipantObjectIdentification (identification de l'objet participant) | ParticipantObjectTypeCode | O | « 2 » (objet système) |
| | ParticipantObjectTypeCodeRole | O | « 13 » (ressource de sécurité) |
| | *ParticipantObjectDataLifeCycle* | *NS* | *Non spécialisée* |
| | ParticipantObjectIDTypeCode | O | EV (« 12 », « RFC-3881 », « URI ») |
| | *ParticipantObjectSensitivity* | *NS* | *Non spécialisée* |
| | ParticipantObjectID | O | URI du journal d'audit |
| | ParticipantObjectName | O | « journal d'audit de sécurité » |
| | *ParticipantObjectQuery* | *NS* | *Non spécialisée* |
| | *ParticipantObjectDetail* | *NS* | *Non spécialisée* |

# 3.2 Profil IUA

## 3.2.1 Survol

Le profil IUA (*Internet User Authorization*, ou autorisation de l’utilisateur Internet) est un profil d'autorisation pour les transactions HTTP RESTful. Une fois autorisé, l'utilisateur, le patient ou le professionnel de la santé a un accès légitime à ce service HTTP RESTful. L'autorisation comprend l'identification de l'utilisateur et de l'application qui soumet la requête au serveur HTTP RESTful afin que le serveur puisse prendre d'autres décisions en matière de contrôle d'accès.

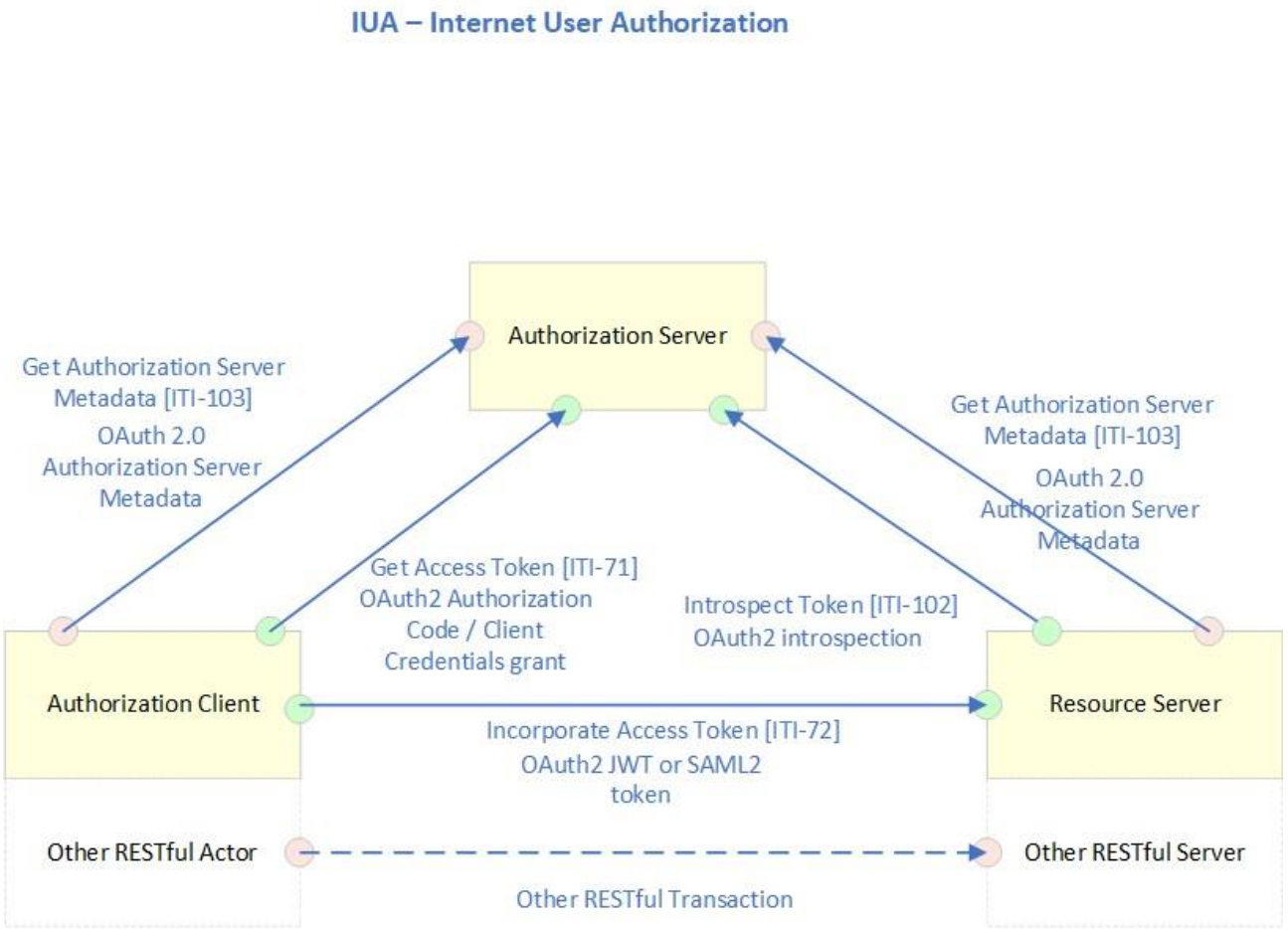
Le profil IUA transmet l'identité, les attributs et les autorisations de l'utilisateur à un service RESTful pour que soit appliquée la politique de sécurité et de confidentialité. Les principaux cas d'utilisation visent l'obtention d'une autorisation d'accès à une ressource à l’aide de transactions HTTP RESTful. Il existe d'autres cas d'utilisation pour la délégation, le provisionnement, etc. qui n'entrent pas dans le champ d'application de ce profil.

Le service d'autorisation est séparé de l'accès HTTP RESTful afin qu'il puisse être fourni par une organisation ou une partie de l'organisation différente du service de ressources. Cela tient au fait que les patients, les professionnels de la santé et les autres utilisateurs souhaitent simplifier les services d'autorisation et en conserver l'autonomie et le contrôle. Un utilisateur peut être amené à interagir avec des dizaines de professionnels de la santé. Il lui serait alors difficile de coordonner différents mécanismes d'autorisation avec chacun de ces professionnels.

Il s'agit là d'un usage courant sur Internet, et il existe déjà des fournisseurs de services d'autorisation habitués à résoudre ce genre de problème, par exemple Facebook, Google et divers autres dans différents secteurs commerciaux et gouvernementaux. Certains pays utilisent la carte d'identité de leurs citoyens pour autoriser l'accès à leurs services gouvernementaux. Cette méthode chevauche celles des fournisseurs de services d'authentification. Ces services permettent au patient d'établir une relation d'authentification et d'autorisation qui nécessite un provisionnement minimal de la part du professionnel de la santé. L'utilisateur peut exiger du professionnel de la santé qu’il utilise un fournisseur en particulier.

## 3.2.2 Acteurs et transactions

Le diagramme suivant présente une vue générale des acteurs et des transactions du profil IUA ainsi que de leurs interactions.




Les transactions relatives à chaque acteur qui intervient directement dans le profil IUA figurent dans le tableau ci-dessous. Pour être conforme au profil IUA, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R ») et peut assumer les transactions optionnelles (identifiées par un « O »).

| Acteur | Transaction | Optionalité |
|---|---|---|
| Client d'autorisation (Authorization Client) | Get Access Token [ITI-71]<br>Incorporate Access Token [ITI-72]<br>Get Authorization Server Metadata [ITI-103] | R<br>R<br>O |
| Serveur d'autorisation (Authorization Server) | Get Access Token [ITI-71]<br>Get Authorization Server Metadata [ITI-103]<br>Introspect Token [ITI-102] | R<br>O<br>O |
| Serveur de ressources (Resource Server) | Incorporate Access Token [ITI-72]<br>Get Authorization Server Metadata [ITI-103]<br>Introspect Token [ITI-102] | R<br>O<br>O |

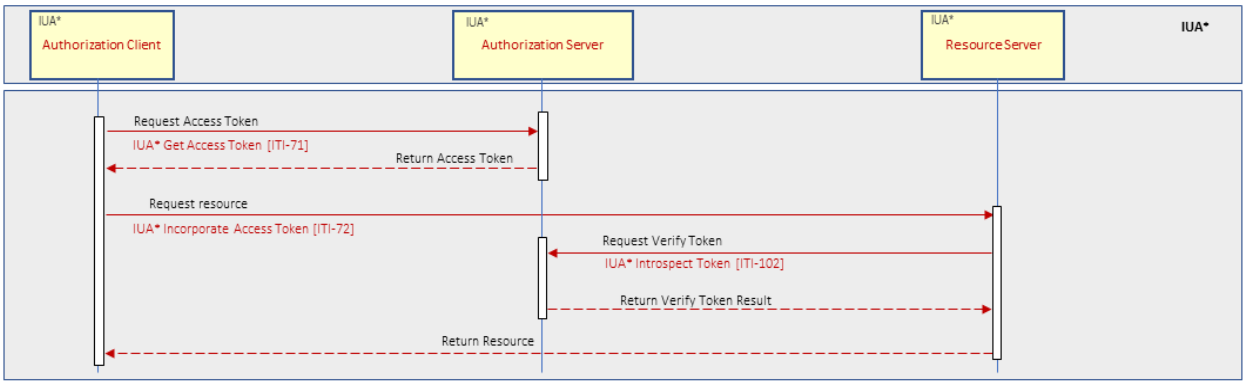
## 3.2.3 Transactions

- Get Access Token [ITI-71] – Cette transaction est utilisée par un client d'autorisation pour obtenir un jeton d'accès conforme à OAuth 2.1. Utilise les protocoles RFC6749 - OAuth 2.0 Authorization Framework, RFC7519 - JSON Web Token et RFC9068 - JSON Web Token (JWT) Profile for OAuth 2.0

Access Tokens.

- Incorporate Access Token [ITI-72] – Cette transaction sert à incorporer l'information d'autorisation dans des transactions HTTP RESTful. Utilise le protocole RFC6749 - OAuth 2.0 Authorization Framework.
- Introspect Token [ITI-102] – Cette transaction définit un protocole permettant aux serveurs de ressources d'interroger le serveur d'autorisation afin de déterminer l'ensemble des réclamations pour un jeton donné qui leur a été présenté par le client d'autorisation. Ces réclamations indiquent notamment si le jeton est actuellement actif et le contexte d'autorisation dans lequel le jeton a été accordé.

## 3.2.4 Diagramme de séquence




## 3.2.5 Indications sur l'implantation du profil IUA au Canada

Les indications sur l'implantation du profil IUA au Canada contiennent des recommandations relatives à l'implantation du profil IUA d'IHE en contexte canadien.

Options liées aux acteurs IUA

| Acteur | Options | Notes |
|---|---|---|
| Serveur d'autorisation (Authorization Server) | JWT Token (jeton Web JSON) | |
| | Token Introspection (introspection du jeton) | (Note 1) |
| | Signature Verification (vérification de la signature) | (Note 1) |
| | Authorization Server Metadata (métadonnées du serveur d'autorisation) | |
| Serveur de ressources (Resource Server) | JWT Token (jeton Web JSON) | |
| | Token Introspection (introspection du jeton) | (Note 1) |
| | Signature Verification (vérification de la signature) | (Note 1) |
| | Authorization Server Metadata (métadonnées du serveur d'autorisation) | |
| Client d'autorisation (Authorization Client) | Authorization Server Metadata (métadonnées du serveur d'autorisation) | |

*Note 1 : L'acteur devra prendre en charge l'une des deux options suivantes :* Token Introspection *(introspection du jeton) ou* Signature Verification *(vérification de la signature) (à l'aide de la clé publique du serveur d'autorisation).*

**Option *JWT Token* (jeton Web JSON)**

L'option *JWT Token* permet d'utiliser un jeton Web JSON encodé comme jeton d'accès émis par le serveur d'autorisation.

**Option *Token Introspection* (introspection du jeton)**

L'option *Token Introspection* permet au serveur de ressources de vérifier l'origine et la validité du jeton d'accès. Le serveur de ressources délègue la vérification du jeton au serveur d'autorisation en accédant au point d'extrémité d'introspection du jeton Le serveur d'autorisation effectuera tous les contrôles applicables à l'état d'un jeton, par exemple la vérification de l'expiration du jeton, la vérification des signatures, etc.

En outre, l'introspection du jeton permet généralement de trouver d'autre information telle que l'utilisateur et les champs d'application associés au jeton. Toutefois, cela n'est pas nécessaire dans le cas d'un jeton JWT, car le serveur de ressources est en mesure d'analyser le jeton et d'effectuer ces vérifications supplémentaires.

**Option *Signature Verification* (vérification de signature)**

Cette option permet au serveur de ressources de vérifier l'origine et la validité du jeton d'accès JWT sans passer par le serveur d'autorisation. Le serveur de ressources utilise la clé publique du serveur d'autorisation pour valider la signature du jeton, puis analyser les réclamations contenues dans le jeton structuré lui-même.

Le point d'extrémité de la clé publique du serveur d'autorisation peut être découvert à l'aide d'URI connu (/ .well-known/) (voir la section Option *Authorization Server Metadata* (métadonnées du serveur d'autorisation). Si l'option de métadonnées du serveur d'autorisation n'est pas prise en charge par le serveur d'autorisation, la clé publique peut être obtenue par d'autres moyens.

**Option *Authorization Server Metadata* (métadonnées du serveur d'autorisation)**

Les point d'extrémités du serveur peuvent être découverts par l'intermédiaire du mécanisme de découverte d'URI connu (/ .well-known). Le client lance une requête HTTP GET au point d'extrémité de métadonnées connu associé au serveur d'autorisation. Voici un exemple d'une telle requête utilisant [RFC8414] :

BASE_URL/.well-known/openid-configuration

où BASE_URL inclut l'information du domaine (locataire).

Exemple pour le serveur d'autorisation Keycloak :

- BASE_URL

  https://<keycloakserver>/realms/<realm>
- Point d'extrémité de découverte de métadonnées du serveur d'autorisation

  BASE_URL/.well-known/openid-configuration
- Point d'extrémité de découverte du certificat du serveur d'autorisation (pouvant être découvert via l'URI connu)

  BASE_URL/protocol/openid-connect/certs

Exemple pour le serveur d'autorisation Amazon Cognito :

- BASE_URL

  https://cognito-idp.<region>.amazonaws.com/<user_pool_id>
- Point d'extrémité de découverte de métadonnées du serveur d'autorisation

  BASE_URL/.well-known/openid-configuration
- Point d'extrémité de découverte du certificat du serveur d'autorisation (pouvant être découvert via l'URI connu)

  BASE_URL/.well-known/jwks.json

## Types d'autorisation

| Acteur | Options | Notes |
|---|---|---|
| Serveur d'autorisation (Authorization Server) | Authorization Code (code d'autorisation) | Doit prendre en charge les deux options |
| | Client Credentials (justificatifs du client) | |
| Client d'autorisation (Authorization Client) | Authorization Code (code d'autorisation) | Doit prendre en charge l'une des deux options |
| | Client Credentials (justificatifs du client) | |

## Principes de sécurité

Recommandations pour un serveur d'autorisation et un client d'autorisation qui utilisent le flux de codes d'autorisation :

- (Clé de preuve pour l'échange de codes) – Mécanismes de protection contre la falsification de requête intersites et l'injection de code
- état – Paramètre de requête qui permet une protection supplémentaire contre la falsification de requête intersites
- nonce – Paramètre de requête qui permet d'imposer l'utilisation d'un code à usage unique et la

protection contre les attaques par réinsertion

## 3.3 Profil CT

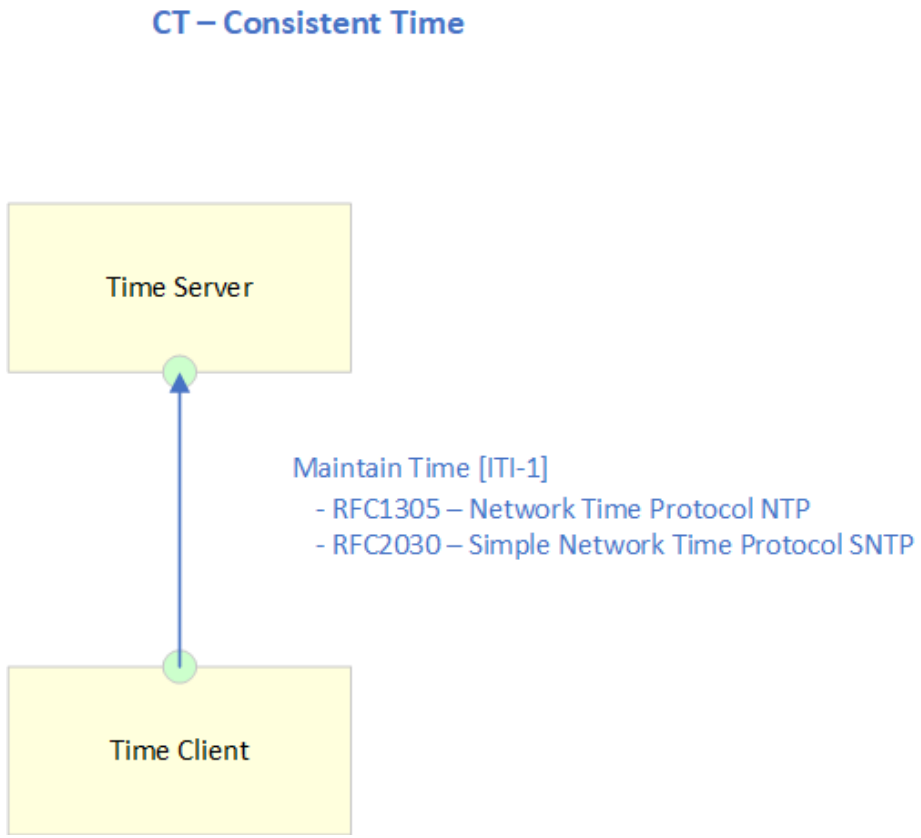
### 3.3.1 Survol

Le profil CT (*Consistent Time*, ou synchronisation du temps) permet de bien synchroniser les horloges et les horodateurs des nombreux ordinateurs d'un réseau. Ce profil spécifie une synchronisation comportant une erreur médiane inférieure à 1 seconde. Cela suffit dans la plupart des cas.

Divers profils d'infrastructure, de sécurité et d'acquisition exigent l'utilisation d'une base de temps synchronisée sur plusieurs ordinateurs, afin de synchroniser les journaux, l'authentification des utilisateurs, la signature numériquement les documents, etc.

### 3.3.2 Acteurs et transactions

Le diagramme suivant présente une vue générale des acteurs et des transactions du profil CT ainsi que de leurs interactions.




Les transactions relatives à chaque acteur qui intervient directement dans le profil CT figurent dans le tableau ci-dessous. Pour être conforme au profil CT, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R »).

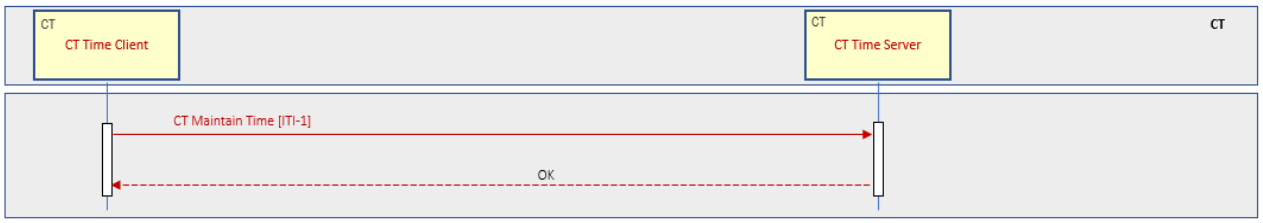
| Acteur | Transaction | Optionalité |
|---|---|---|

| | | |
|---|---|---|
| Client de temps (Time Client) | Maintain Time [ITI-1] | R |
| Serveur de temps (Time Server) | Maintain Time [ITI-1] | R |

### 3.3.3 Transactions

- Maintain Time [ITI-1] – Cette transaction utilise des réponses de service de temps NTP (RFC1305) ou SNTP (RFC4330) pour maintenir la synchronisation avec les serveurs de temps et fixer l'heure de l'horloge système locale.

### 3.3.4 Diagramme de séquence




### 3.3.5 Indications sur l'implantation du profil CT au Canada

Les indications sur l'implantation du profil CT au Canada contiennent des recommandations relatives à l'implantation du profil CT d'IHE en contexte canadien.

#### Serveur de temps

Le serveur de temps doit se synchroniser avec des serveurs de temps de strate 2 ou supérieure.

Le Conseil national de recherche du Canada (CNRC) fournit des services NTP, dont une connexion sécurisée gratuite à ses serveurs NTP de strate 2. Voir le site Web du CNRC pour plus d'information.

Exemples de serveurs de temps NTP du CNRC :

- nrc.ca
- chu.nrc.ca

## 3.4 Profil SVCM

### 3.4.1 Survol

Le profil SVCM (*Sharing ValueSets, Codes and Maps*, ou partage d'ensembles de valeurs, de codes et de mappages) définit une interface allégée par laquelle les systèmes informatiques du réseau de la santé peuvent extraire une nomenclature uniforme gérée de manière centralisée et des mappages entre les systèmes de codes basés sur la spécification FHIR.

Le profil SVCM prend en charge la recherche d'ensembles de valeurs et de systèmes de codes à l'aide des ressources HL7 FHIR. Il permet également de rechercher et de valider des codes, ainsi que d'élargir un ensemble de valeurs afin qu'il liste tous les codes qu'il contient.

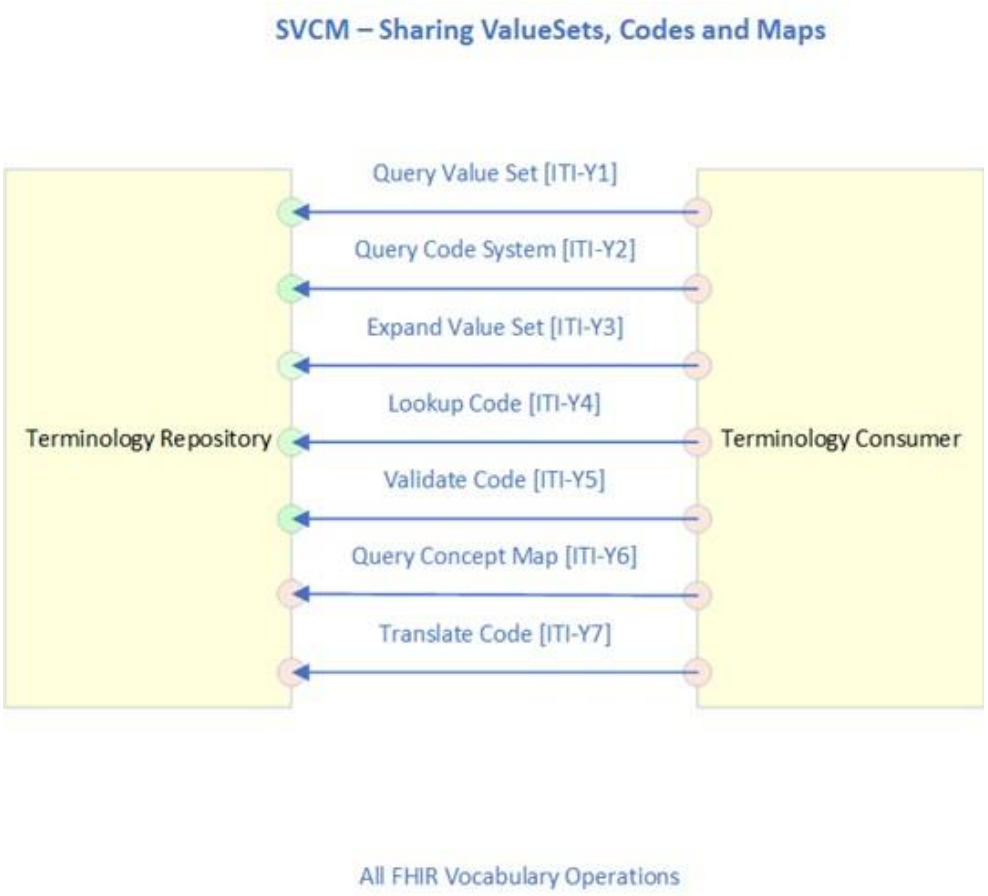
Des mappages conceptuels peuvent également être inclus pour passer d'un système de code ou d'un

ensemble de valeurs à un autre (p. ex. de SNOMED CT à LOINC).

Les terminologies gérées dans les ensembles de valeurs sont particulièrement utiles lorsqu'elles sont largement partagées et normalisées entre les régions et les disciplines, car elles gagnent alors en clarté et en spécificité.

## 3.4.2 Acteurs et transactions

Le diagramme suivant présente une vue générale des acteurs et des transactions du profil SVCM ainsi que de leurs interactions.




Les transactions relatives à chaque acteur qui intervient directement dans le profil SVCM figurent dans le tableau ci-dessous. Pour être conforme au profil SVCM, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R ») et peut assumer les transactions optionnelles (identifiées par un « O »).

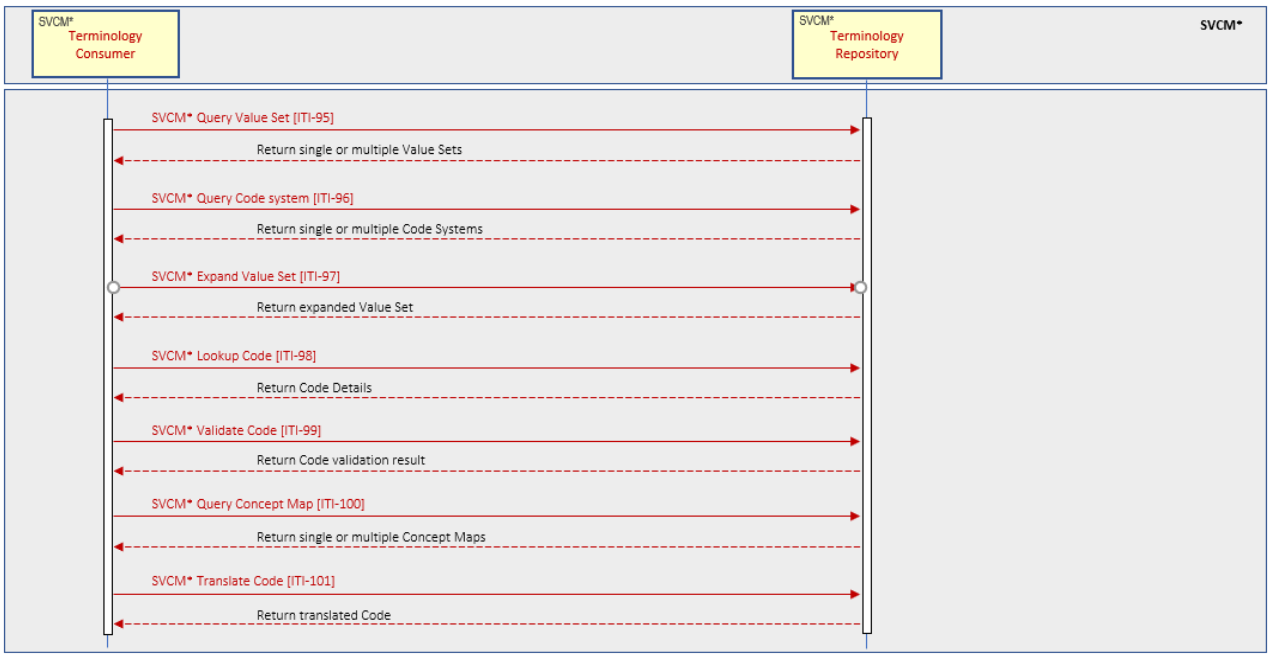
| Acteur | Transaction | Optionalité |
|---|---|---|
| Consommateur de terminologie (Terminology Consumer) | Query Value Set [ITI-95]<br>Query Code System [ITI-96]<br>Expand Value Set [ITI-97]<br>Lookup Code [ITI-98]<br>Validate Code [ITI-99]<br>Query Concept Map [ITI-100]<br>Translate Code [ITI-101] | O (*)<br>O (*)<br>O (*)<br>O (*)<br>O (*)<br>O<br>O |
| Dépôt de terminologie (Terminology Repository) | Query Value Set [ITI-95]<br>Query Code System [ITI-96]<br>Expand Value Set [ITI-97]<br>Lookup Code [ITI-98]<br>Validate Code [ITI-99]<br>Query Concept Map [ITI-100]<br>Translate Code [ITI-101] | R<br>R<br>R<br>R<br>R<br>O<br>O |

(*) Un consommateur de terminologie doit prendre en charge au moins l'une de ces transactions.

## 3.4.3 Transactions

- Query Value Set [ITI-95] – Transaction utilisée par le consommateur de terminologie pour trouver des ensembles de valeurs en fonction des critères qu'il fournit dans les paramètres d'interrogation du message de requête, ou pour extraire un ensemble de valeurs donné. Exécute une opération FHIR d'interrogation d'ensembles de valeurs (*ValueSet Query*).
- Query Code System [ITI-96] – Transaction utilisée par le consommateur de terminologie pour demander de l'information au sujet des systèmes de codes dont les données correspondent aux données fournies dans les paramètres d'interrogation du message de requête. Exécute une opération FHIR d'interrogation de systèmes de codes (*CodeSystem Query*).
- Expand Value Set [ITI-97] – Transaction utilisée par le consommateur de terminologie pour élargir un ensemble de valeurs donné afin d'obtenir la liste complète des concepts inclus dans cet ensemble de valeurs. Exécute une opération FHIR « $expand ValueSet ».
- Lookup Code [ITI-98] – Transaction utilisée par le consommateur de terminologie pour chercher un code donné afin d'en obtenir les détails complets. Exécute une opération FHIR « $lookup» ciblant un ensemble de valeurs (*ValueSet*) ou un système de codes (*CodeSystem*).
- Validate Code [ITI-99] – Transaction utilisée par le consommateur de terminologie pour valider l'existence d'un code donné dans un ensemble de valeurs ou un système de codes. Exécute une opération FHIR « $validate-code » ciblant un ensemble de valeurs (*ValueSet*) ou un système de codes (*CodeSystem*).
- Query Concept Map [ITI-100] – Transaction utilisée par le consommateur de terminologie, qui prend en charge l'option de traduction (*Translate Option*) pour demander de l'information sur des mappages conceptuels dont les données correspondent aux données fournies dans les paramètres d'interrogation du message de requête. Exécute une opération FHIR d'interrogation de mappages conceptuels (*ConceptMap Query*).
- Translate Code [ITI-101] – Transaction utilisée par le consommateur de terminologie qui prend en charge l'option de traduction (*Translate Option*) pour traduire un code donné d'un ensemble de valeurs en un code d'un autre ensemble de valeurs sur la base d'une ressource *ConceptMap*. Exécute une opération FHIR « $translate » ciblant un mappage conceptuel (*ConceptMap*).

### 3.4.4 Diagramme de séquence




### 3.4.5 Terminology Gateway

Les ensembles de valeurs qui font partie des spécifications pancanadiennes sont publiés dans Terminology Gateway. Terminology Gateway offre une API FHIR compatible avec l'acteur « dépôt de terminologie » du profil SVCM et qui permet d'implanter les transactions suivantes :

- Query Value Set [ITI-95]
  - ex. : GET https://fhir.infoway-inforoute.ca/ValueSet?name=*route*
- Expand Value Set [ITI-97]
  - ex. : GET https://fhir.infoway-inforoute.ca/ValueSet/routeofadministration/$expand
- Validate Code [ITI-99]
  - ex. : GET https://fhir.infoway-inforoute.ca/ValueSet/routeofadministration/$validate-code?code=697971008&system=http%3A%2F%2Fsnomed.info%2Fsct
- Query Concept Map [ITI-100]
  - ex. : GET https://fhir.infoway-inforoute.ca/ConceptMap?name=*map*
- Translate Code [ITI-101]
  - ex. : GET https://fhir.infoway-inforoute.ca/ConceptMap/MP-NTP-Mapping/$translate?code=00000817

Pour des raisons de performance, Terminology Gateway ne devrait pas être interrogé en cours d'exécution. On recommande plutôt d'utiliser ses services de notifications pour la mise à jour d'une base de données locale à des fins de validation.

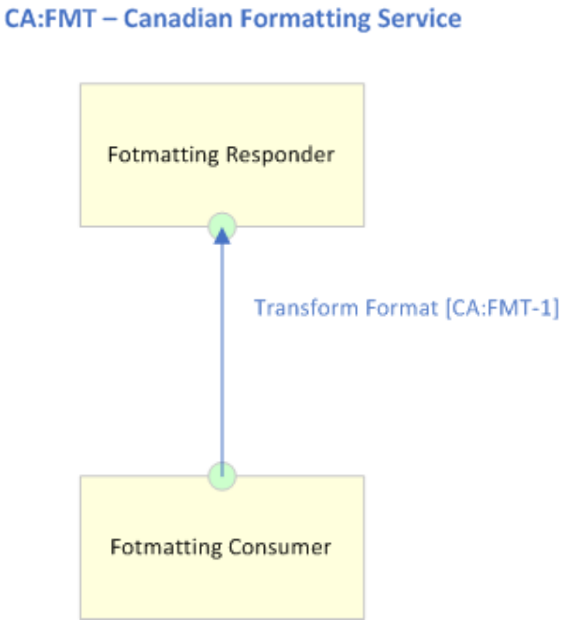
## 3.5 Spécification CA:FMT

### 3.5.1 Introduction

La spécification CA:FMT (*Canadian Formatting Service*, ou service de formatage canadien) est une spécification canadienne qui offre un service de formatage. Plus particulièrement, elle permet de convertir des documents en différents formats (p. ex. de FHIR à PDF, à CDA, etc.).

## 3.5.2 Acteurs et transactions

Le diagramme suivant présente une vue générale des acteurs et des transactions de la spécification CA:FMT ainsi que de leurs interactions.



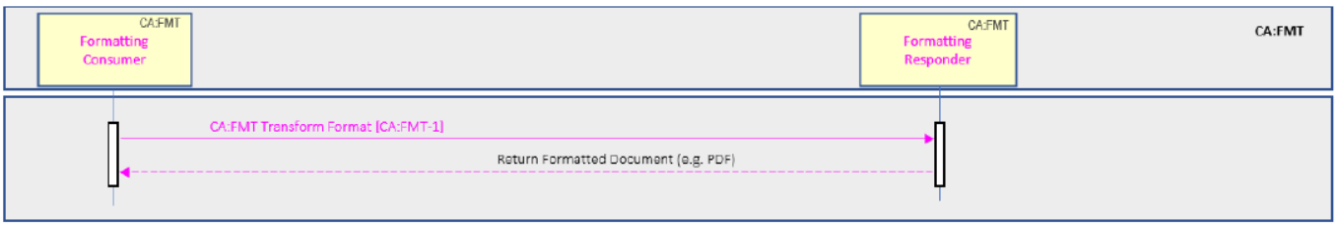

Les transactions relatives à chaque acteur qui intervient directement dans la spécification CA:FMT figurent dans le tableau ci-dessous. Pour être conforme à la spécification CA:FMT, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R »).

| Acteurs | Transactions | Optionalité |
|---|---|---|
| Consommateur de formatage (Formatting Consumer) | Transform Format [CA:FMT-1] | R |
| Répondeur de formatage (Formatting Responder) | Transform Format [CA:FMT-1] | R |

## 3.5.3 Transactions

- Transform Format [CA:FMT-1] : Cette transaction est utilisée pour convertir un document d'un format à un autre (p. ex. FHIR à PDF, à CDA, etc.)

## 3.5.4 Diagramme de séquence



# 4 Profils d’échange de documents

## 4.1 Spécification CA:FeX

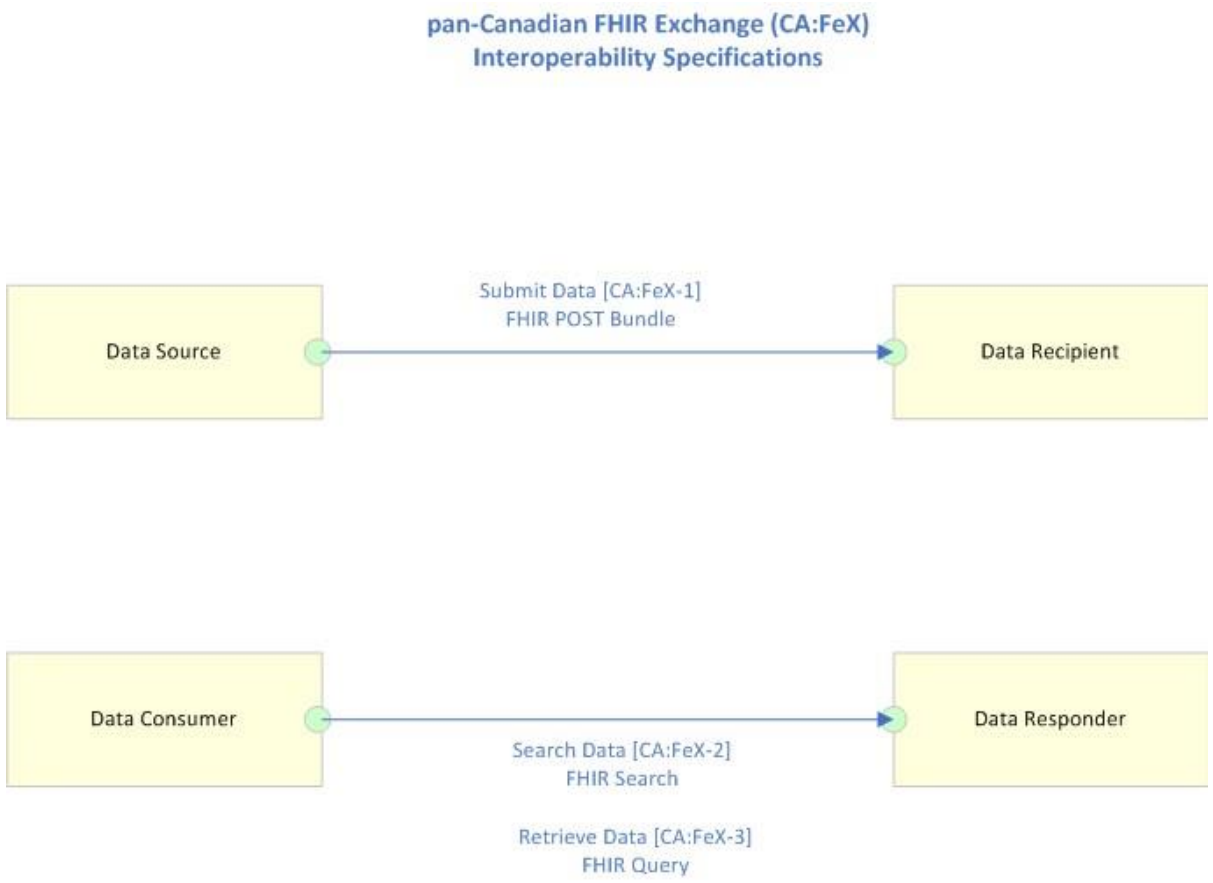
### 4.1.1 Survol

La spécification CA:FeX (*Canadian FHIR Exchange*, ou échange FHIR canadien) est une spécification implantable, testable et dérivée des guides d’implantation FHIR d’HL7. Elle définit les éléments de base qui facilitent l'implantation des patrons FHIR RESTful nécessaires à la création, à la consommation et à l’échange de données cliniques. Voici quelques-uns des avantages de CA:FeX :

- permettre aux professionnels de la santé de créer, de visualiser et de mettre à jour des documents à l’aide d’opérations FHIR normalisées (soumission, recherche et extraction);
- favoriser la prestation sécuritaire de soins planifiés ou non planifiés;
- faciliter la transition des soins ou le transfert des patients dans tout le continuum de soins;
- améliorer la coordination et la collaboration dans l’équipe de soins du patient.

### 4.1.2 Acteurs et transactions

Le diagramme suivant présente une vue générale des acteurs et des transactions de la spécification CA:FeX ainsi que de leurs interactions.



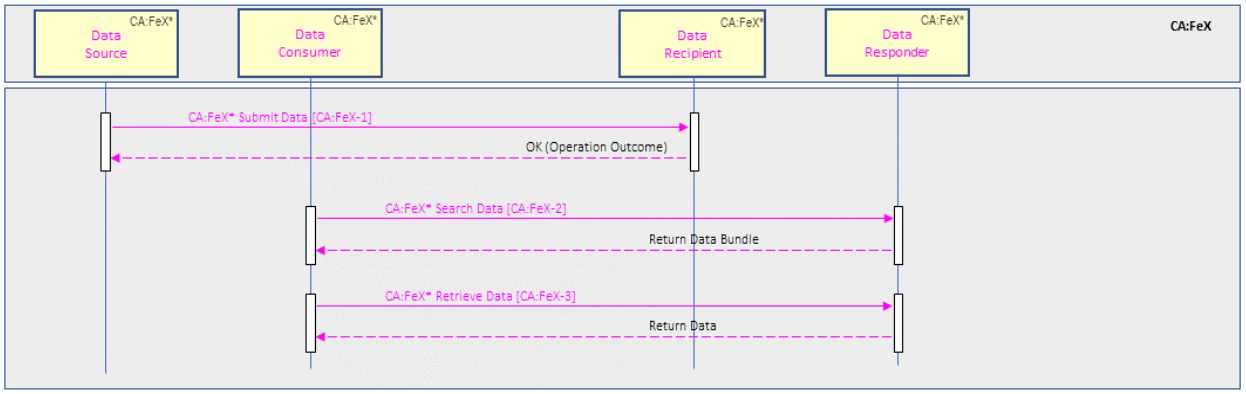
Les transactions relatives à chaque acteur qui intervient directement dans la spécification CA:FeX figurent dans le tableau ci-dessous. Pour être conforme à la spécification CA:FeX, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R »).

| Acteur | Transaction | Optionalité |
|---|---|---|
| Source de données (Data Source) | Soumettre des données [CA:FeX-1] | R |
| Destinataire de données (Data Recipient) | Soumettre des données [CA:FeX-1] | R |
| Consommateur de données (Data Consumer) | Rechercher des données [CA:FeX-2]<br>Extraire des données [CA:FeX-3] | R<br>R |
| Répondeur de données (Data Responder) | Rechercher des données [CA:FeX-2]<br>Extraire des données [CA:FeX-3] | R<br>R |

## 4.1.3 Transactions

- Soumettre des données [CA:FeX-1] – Cette transaction est utilisée par la source de données pour soumettre des données à un destinataire de données. Exécute une requête HTTP POST pour transférer une ressource FHIR ou un *Bundle* de ressources, généralement de type *Document*.
- Rechercher des données [CA:FeX-2] – Cette transaction est utilisée pour trouver des ressources FHIR qui correspondent à un ensemble de paramètres de recherche. La requête est reçue par un répondeur de données qui envoie un *Bundle* contenant des ressources qui correspondent aux paramètres de recherche.
- Extraire des données [CA:FeX-3] – Cette transaction est utilisée par le consommateur de données pour extraire des données d'un répondeur de données. Exécute une requête HTTP GET basée sur un ID de ressource connu. Le répondeur de données envoie un *Bundle* de ressources FHIR dont l'ID avait déjà été utilisé dans une recherche/extraction antérieure.

## 4.1.4 Diagramme de séquence



# 4.2 Profil MHD

## 4.2.1 Survol

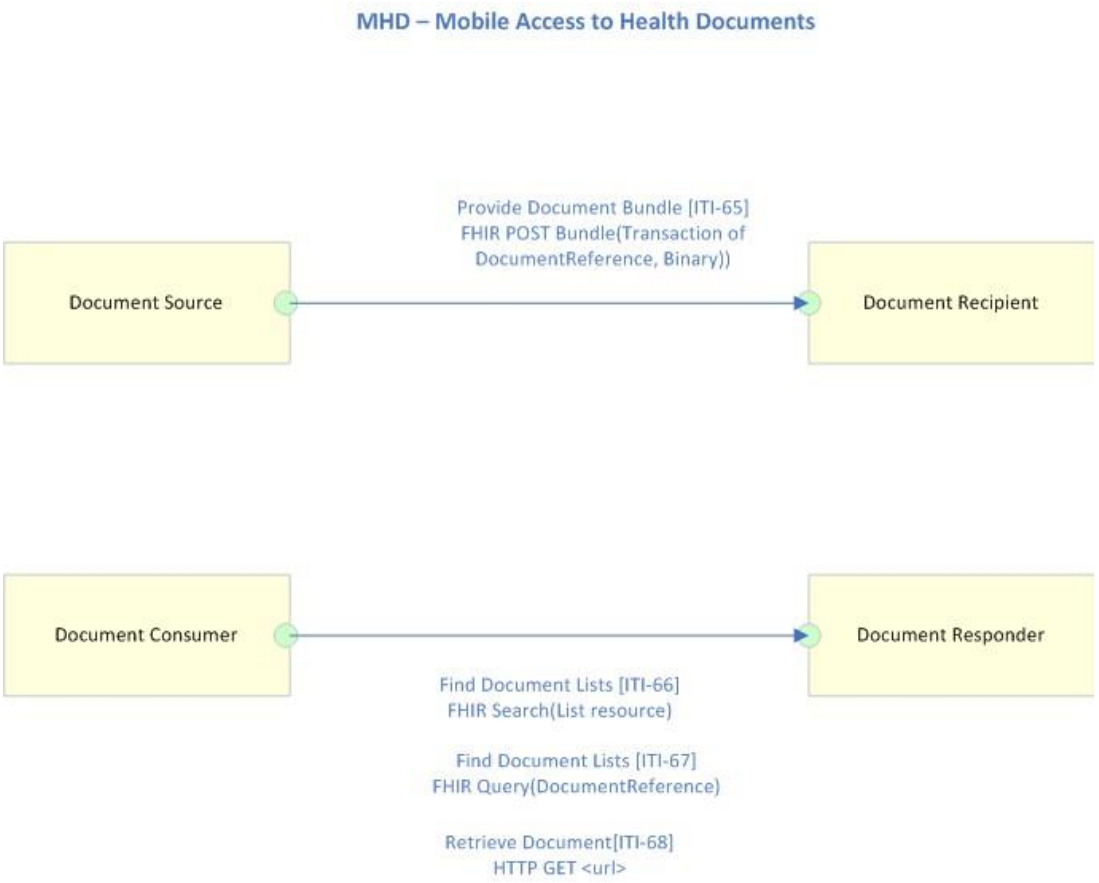
Le profil MHD (*Mobile Access to Health Documents*, ou accès mobile aux documents médicaux) définit une interface normalisée pour l'échange de documents cliniques entre appareils mobiles. Ce profil s'applique aux cas d'utilisation simples, tels que l'extraction du plus récent résumé du dossier du patient pour affichage.

Voici des exemples d'environnements auxquels le profil MHD pourrait convenir :

- dispositifs médicaux, comme ceux visés par le domaine Patient Care Devices (PCD) d'IHE ou la spécification de Continua, qui soumettent des données sous forme de documents;
- kiosques utilisés par les patients dans les services d'enregistrement des hôpitaux, où il est prévu qu'un membre du personnel de l'hôpital examine, modifie et approuve le document avant qu'il soit versé dans le système de l'hôpital;
- publication des données d'un DSP dans l'environnement de simulation pour qu'elles soient ensuite importées dans un système de DSE ou d'EIS;
- application pour patients ou professionnels de la santé configurée pour se connecter de manière sécurisée à un DSP afin de soumettre un document sur les antécédents médicaux (ex. : BlueButton+);
- dispositif de mesure électronique connecté à un flux XDW (*Cross-Enterprise Document Workflow*, ou flux de documents entre organisations) et extrayant des documents sur les antécédents médicaux à partir d'un système d'EIS;
- cabinet de médecins généralistes disposant de capacités informatiques minimales et utilisant une application mobile pour se connecter à un système de DSE ou d'EIS.

## 4.2.2 Acteurs et transactions

Le diagramme suivant présente une vue générale des acteurs et des transactions du profil MHD ainsi que de leurs interactions.




Les transactions relatives à chaque acteur qui intervient directement dans le profil MHD figurent dans le tableau ci-dessous. Pour être conforme au profil MHD, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R »).

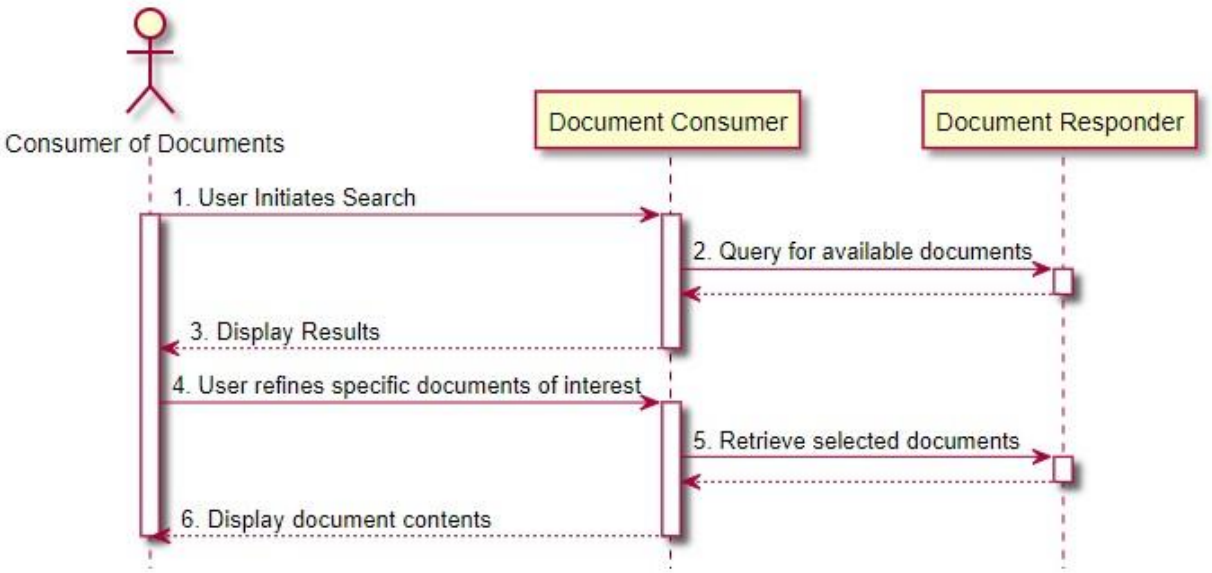
| Acteur | Transaction | Optionalité |
|---|---|---|
| Source de documents (Document Source) | Provide Document Bundle [ITI-65] | R |
| Destinataire de documents (Document Recipient) | Provide Document Bundle [ITI-65] | R |
| Consommateur de documents (Document Consumer) | Find Document Lists [ITI-66]<br>Find Document References [ITI-67]<br>Retrieve Document [ITI-68] | R<br>R<br>R |
| Répondeur de documents (Document Responder) | Find Document Lists [ITI-66]<br>Find Document References [ITI-67]<br>Retrieve Document [ITI-68] | R<br>R<br>R |

## 4.2.3 Transactions

- Provide Document Bundle [ITI-65] – Cette transaction est utilisée par la source de documents pour soumettre un *Bundle* de documents à un destinataire de documents. Exécute une requête HTTP POST ciblant un *Bundle* de ressources de type *DocumentReference* et/ou de ressources au format binaire (*Binary*).

- Find Document Lists [ITI-66] – Cette transaction est utilisée par le consommateur de documents pour rechercher des métadonnées pour les lots ou dossiers de soumission de documents précédemment stockés. Exécute une opération de recherche HTTP pour que le répondeur de documents envoie une liste de ressources.
- Find Document References [ITI-67] – Cette transaction est utilisée par le consommateur de documents pour trouver des ressources de type *DocumentReference* qui correspondent à un ensemble de paramètres de recherche. Exécute une opération de recherche HTTP pour que le répondeur de document envoie un *Bundle* de ressources de type *DocumentReference*.
- Retrieve Document [ITI-68] – Cette transaction est utilisée par le consommateur de documents pour extraire un document d'un répondeur de documents. Exécute une opération HTTP GET pour que le répondeur de documents envoie un seul document.

### 4.2.4 Diagramme de séquence



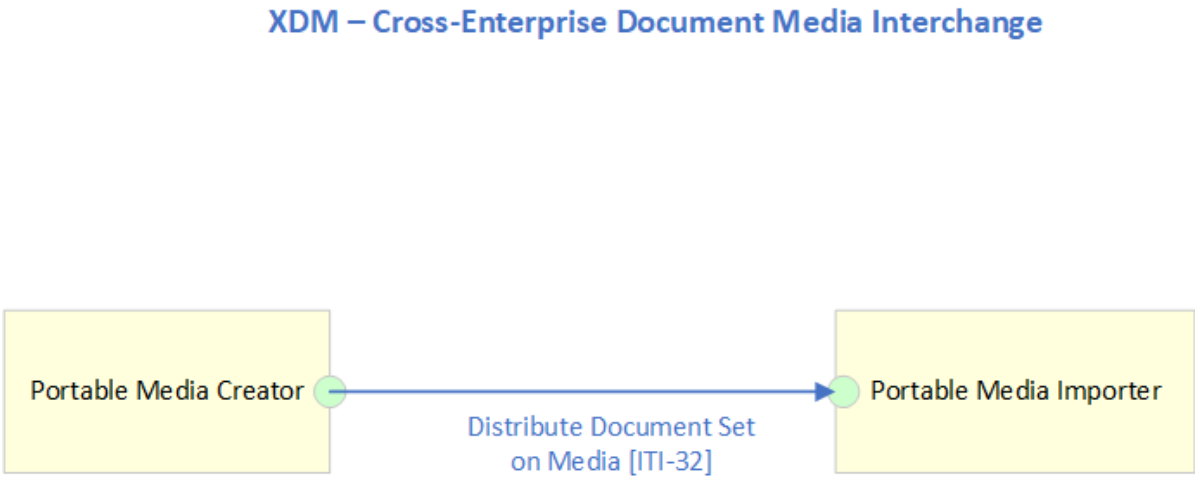

## 4.3 Profil XDM

### 4.3.1 Survol

Le profil XDM (*Cross-Enterprise Document Media Interchange*, ou échange média de documents entre organisations) assure l'échange de documents à l'aide d'une structure commune de fichiers et de répertoires sur plusieurs types de supports classiques. Ce profil permet au patient d'utiliser un support physique pour transporter ses documents médicaux. Il facilite la transmission de documents médicaux de personne à personne par courrier électronique (sous forme de pièce jointe) ou via un support physique (USB et CD-R). Le profil XDM prend en charge le transfert de données concernant plusieurs patients au sein d'un même échange de données.

### 4.3.2 Acteurs et transactions

Le diagramme suivant présente une vue générale des acteurs et des transactions du profil XDM ainsi que de leurs interactions.



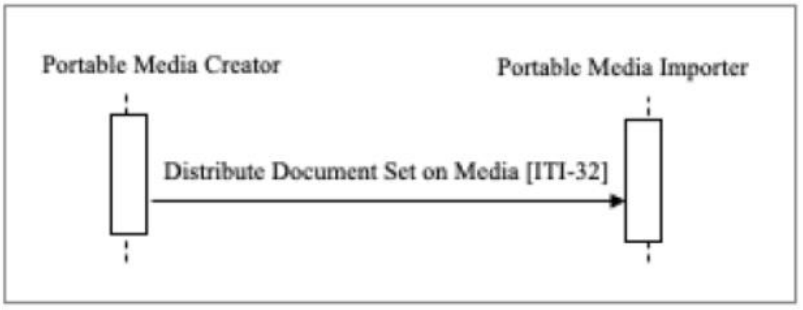

Les transactions relatives à chaque acteur qui intervient directement dans le profil XDM figurent dans le tableau ci-dessous. Pour être conforme au profil XDM, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R »).

| Acteur | Transaction | Optionalité |
|---|---|---|
| Créateur de média portable (Portable Media Creator) | Distribute Document Set on Media [ITI-32] | R |
| Importateur de média portable (Portable Media Importer) | Distribute Document Set on Media [ITI-32] | R |

### 4.3.3 Transactions

- Distribute Document Set on Media [ITI-32] – Le créateur de média portable envoie de l'information à l'importateur de média (acteur qui fera la lecture du média) par l'intermédiaire d'un média (courriel, clé USB, CD/DVD-ROM) qui stocke l'information.

### 4.3.4 Diagramme de séquence



# 5 Profils d’identité du patient

Les profils d’identité du patient inclus dans l’AR sont les suivants :

- PMIR (*Patient Master Identity Registry*, ou registre de l’identité maîtresse du patient)
- PIXm (*Patient Identifier Cross-reference for Mobile*, ou références croisées des identifiants du patient pour appareils mobiles)
- PDQm (*Patient Demographics Query for Mobile*, ou requête de données démographiques de patients pour appareils mobiles)

## 5.1 Profil PMIR

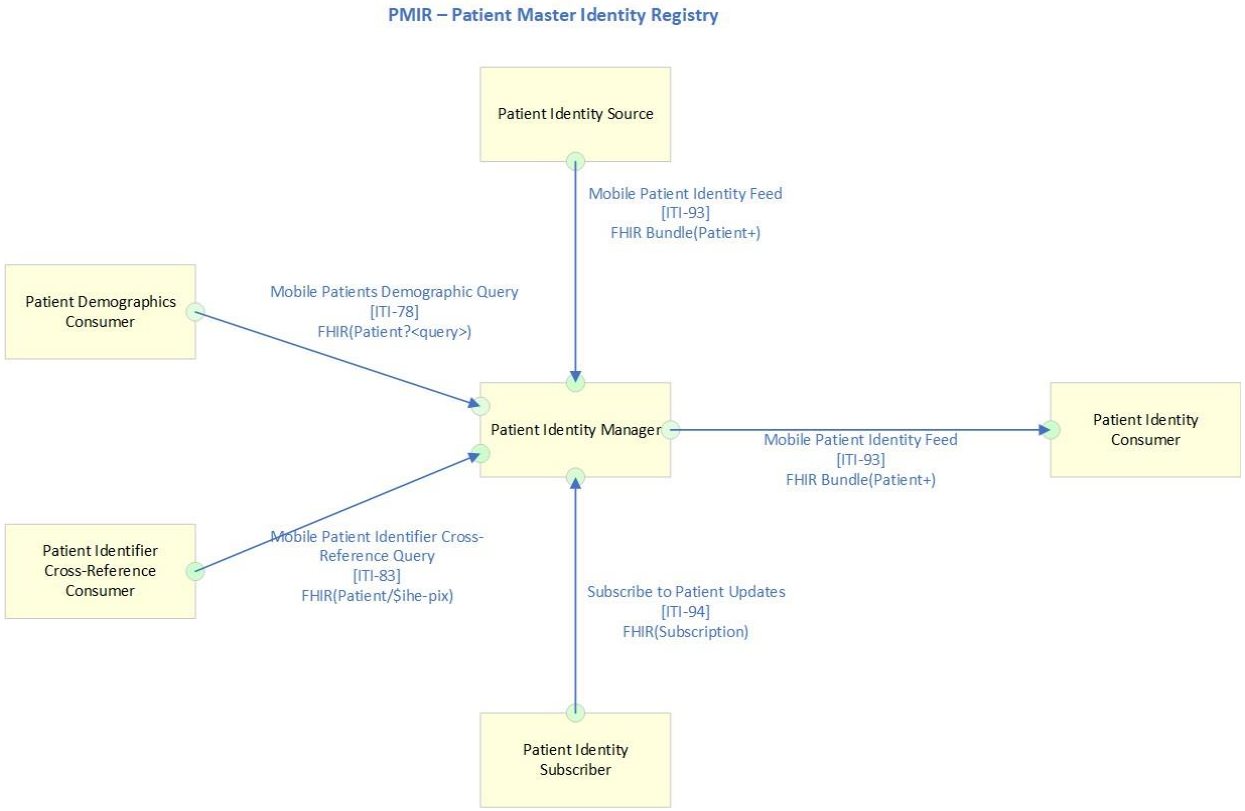
### 5.1.1 Survol

Le profil PMIR (*Patient Master Identity Registry*, ou registre de l’identité maîtresse du patient) prend en charge la création, la mise à jour et la dépréciation des données relatives à l'identité maîtresse du patient/sujet de soins, ainsi que l'abonnement aux notifications signalant les modifications apportées à l’identité maîtresse, en utilisant les ressources FHIR et les transactions RESTful. Ce profil comprend les profils PIXm (*Patient Identifier Cross-reference for Mobile*, ou références croisées des identifiants du patient pour appareils mobiles) et PDQm (*Patient Demographics Query for Mobile*, ou requête de données démographiques de patients pour appareils mobiles). L’identité maîtresse du patient est l’identité *dominante* du patient (ou l’identité *absolue*), dont la gestion est centralisée entre les nombreuses organisations.

Outre les transactions de base (création, extraction, mise à jour et suppression), ce profil permet de résoudre d'importantes questions relatives à la sécurité du patient lorsque deux ou plusieurs identités maîtresses ont été établies pour la même personne et qu'il n'est pas évident de savoir quelle est sa « véritable » identité. Il existe également un risque que des données sur la santé possiblement contradictoires soient associées à chaque identité, et ces données disparates devraient faire l’objet d’un rapprochement avant qu'on puisse dresser un portrait complet et exact de l’état de santé de cette personne. De telles situations peuvent compromettre la sécurité des patients. Ce profil facilite la fusion des différentes identités du patient en une seule identité maîtresse et le flux des données de cette identité maîtresse vers les gestionnaires de données afin qu'ils prennent les mesures appropriées. Le présent profil n'a pas pour objet de définir les modalités de traitement des références à l’identité maîtresse du patient dépréciée que contiennent d’autres données.

## 5.1.2 Acteurs et transactions

Le diagramme suivant présente une vue générale des acteurs et des transactions du profil PMIR ainsi que de leurs interactions.




Les transactions relatives à chaque acteur qui intervient directement dans le profil PMIR figurent dans le tableau ci-dessous. Pour être conforme au profil PMIR, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R »).

| Acteur | Transaction | Optionalité |
|---|---|---|
| Source de données d'identité du patient (Patient Identity Source) | Mobile Patient Identity Feed [ITI-93] | R |
| Consommateur de données d'identité du patient (Patient Identity Consumer) | Mobile Patient Identity Feed [ITI-93] | R |
| Gestionnaire de données d'identité du patient (Patient Identity Manager) | Mobile Patient Identity Feed [ITI-93]<br>Mobile Patient Identifier Cross-Reference Query [ITI-83]<br>Mobile Patient Demographic Query [ITI-78]<br>Subscribe to Patient Updates [ITI-94] | R<br>R<br>R<br>R |
| Consommateur de données démographiques de patients (Patient Demographics Consumer) | Mobile Patient Demographic Query [ITI-78] | R |

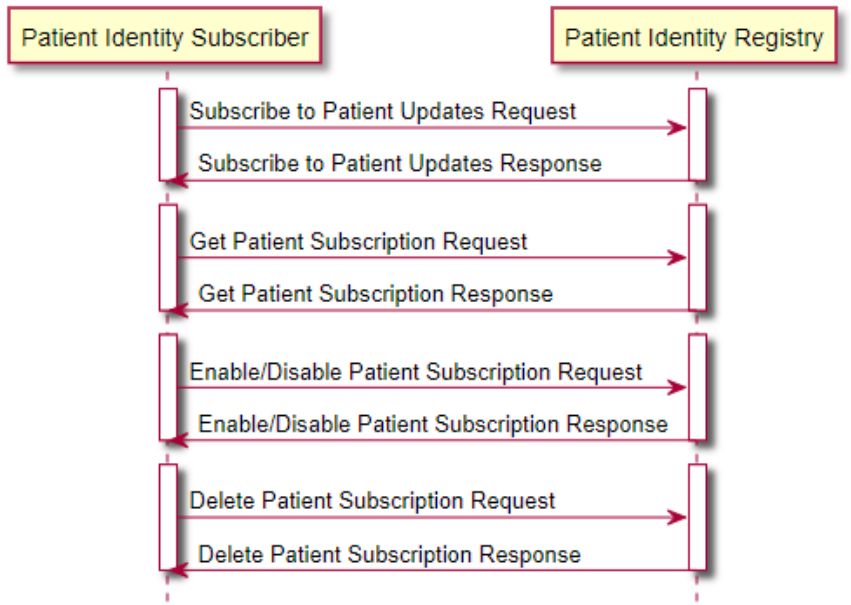
| | | |
|---|---|---|
| Consommateur de références croisées des identifiants du patient (Patient Identifier Cross-Reference Consumer) | Mobile Patient Identifier Cross-Reference Query [ITI-83] | R |
| Abonné aux notifications concernant l'identité du patient (Patient Identity Subscriber) | Subscribe to Patient Updates [ITI-94] | R |

### 5.1.3 Transactions

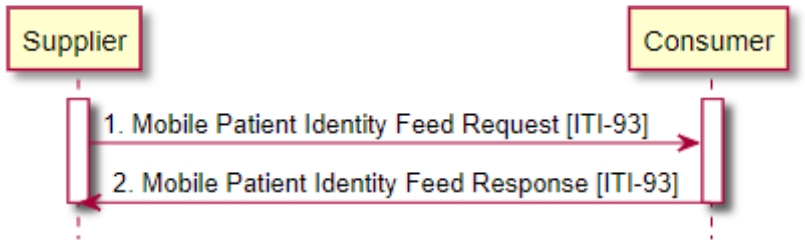
- Mobile Patient Demographic Query [ITI-78] – Transaction utilisée par le consommateur de données démographiques de patients pour demander à un fournisseur de données démographiques de patients une liste de patients correspondant à l'ensemble des critères démographiques fournis (ex. : ID ou nom) dans la requête. Le consommateur de données démographiques de patients peut ensuite compléter ses attributs à partir de l'information reçue. Exécute une requête HTTP GET [base]/Patient?<query>.
- Mobile Patient Identifier Cross-Reference Query [ITI-83] – Transaction utilisée par un consommateur de références croisées des identifiants du patient pour obtenir de l'information sur un patient dont les identifiants présentent des références croisées avec les identifiants fournis dans les paramètres de recherche. La requête est reçue par un gestionnaire de références croisées des identifiants du patient. Celui-ci traite la demande et répond en envoyant aucun ou plusieurs identifiants du patient en question. Exécute une opération FHIR $ihe-pix : GET [base]/Patient/$ihe-pix?<query>.
- Mobile Patient Identity Feed [ITI-93] – Transaction utilisée pour envoyer un *Bundle* FHIR de ressources *Patient* nouvelles ou mises à jour. Exécute une opération POST ciblant un *Bundle* FHIR qui contient au moins une ressource *Patient*.
- Subscribe to Patient Updates [ITI-94] – Transaction qui permet à un abonné aux notifications concernant l'identité du patient de s'abonner à un fil de ressources *Patient* pour appareils mobiles (Mobile Patient Resource Feed [ITI-93]) selon des critères définis. Exécute une opération POST ciblant une ressource FHIR *Subscription*.

### 5.1.4 Diagrammes de séquence

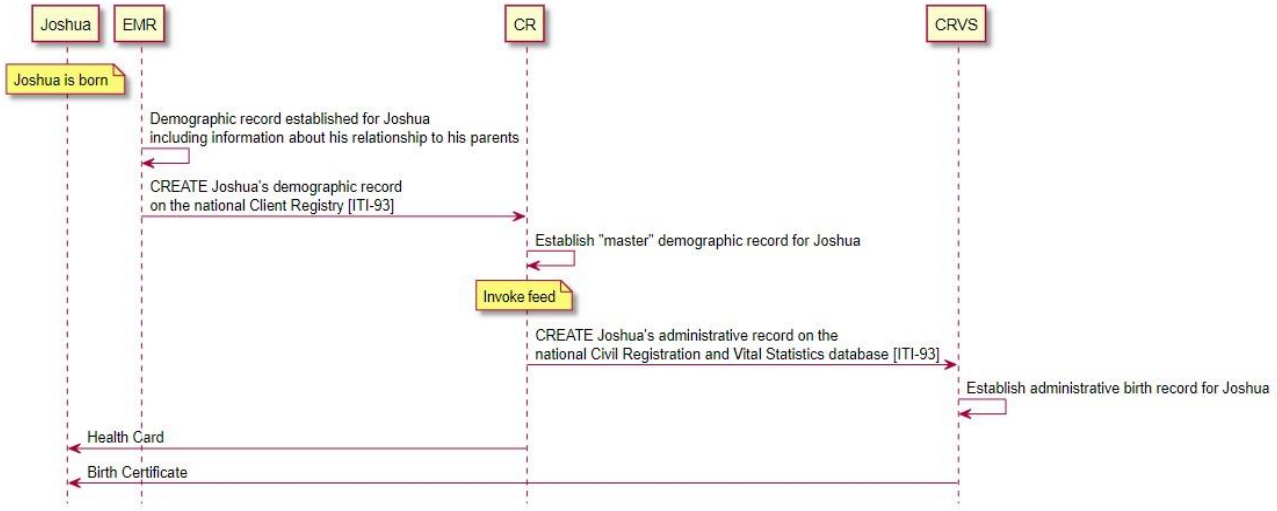
Profil PMIR - abonné et registre



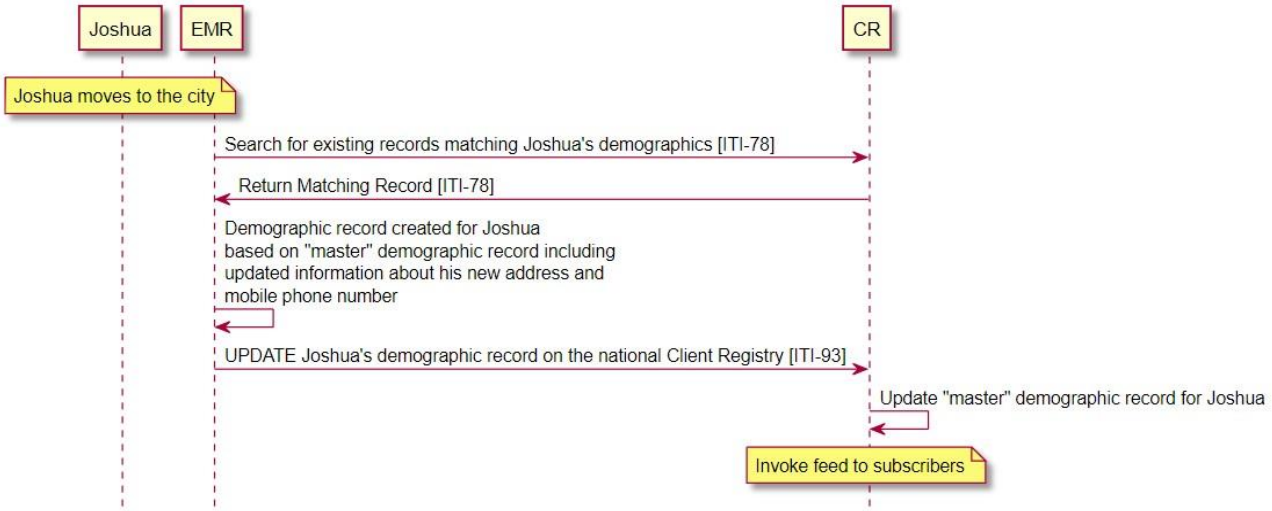
## Profil PMIR - fournisseur et consommateur



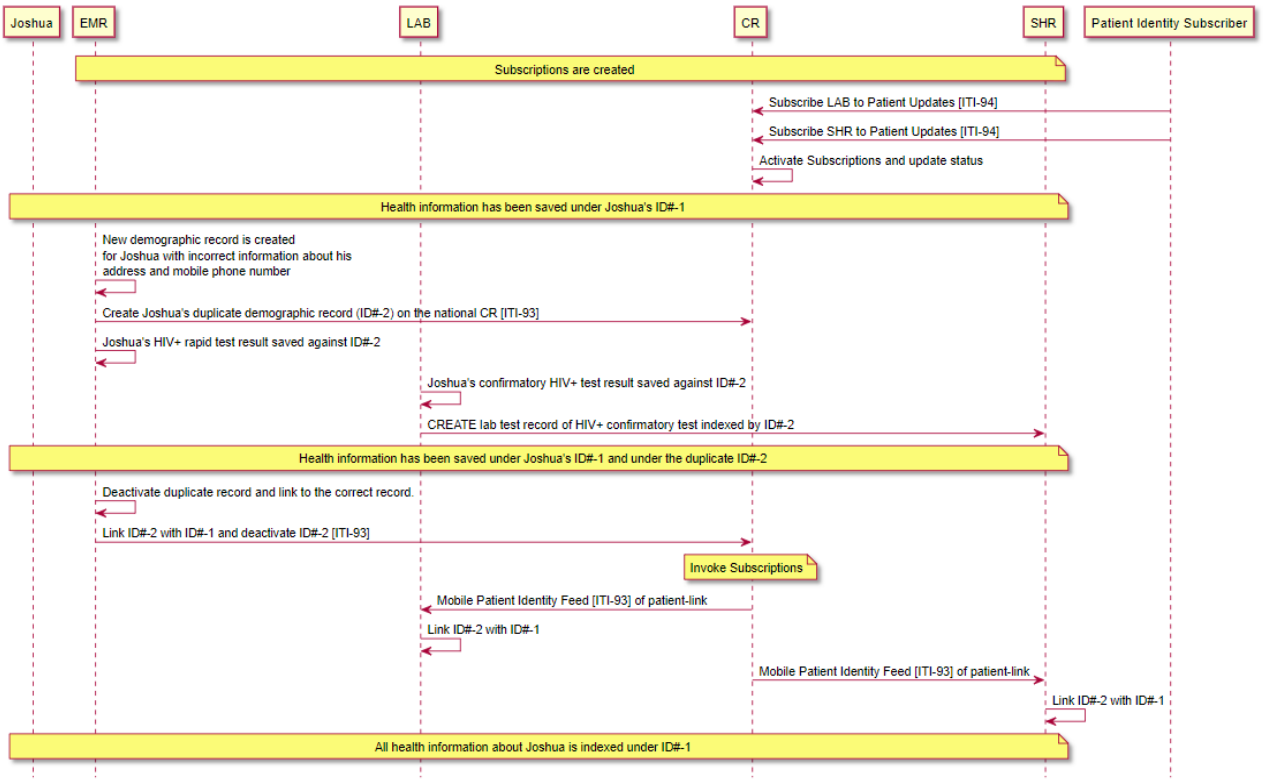

## Profil PMIR – créer l'identité du patient




## Profil PMIR – mettre à jour l'identité du patient



Profil PMIR – fusionner l'identité du patient




# 5.2 Profil PIXm

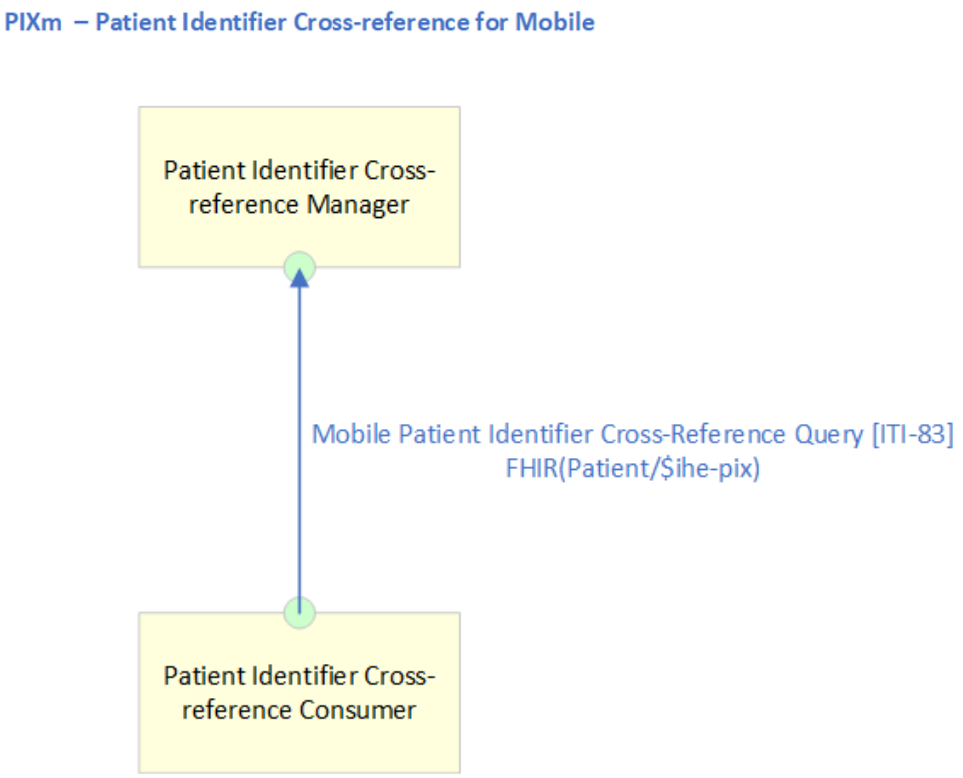
## 5.2.1 Survol

Le profil PIXm (*Patient Identifier Cross-Reference for Mobile*, ou références croisées des identifiants du patient pour appareils mobiles) fournit une transaction qui permet aux applications mobiles et aux applications allégées sur navigateur d'interroger un gestionnaire de références croisées des identifiants du patient pour obtenir une liste d'identifiants du patient à partir de son identifiant dans un domaine différent et d'extraire l'information sur les identifiants interdomaines du patient.

Le profil PIXm est destiné aux applications allégées ou pour appareils mobiles utilisées dans des établissements de santé de toutes tailles (hôpital, clinique, cabinet de médecins, etc.). Il prend en charge l'interrogation croisée d'identifiants du patient provenant de plusieurs domaines en permettant d'accéder à la/aux liste(s) d'identifiants du patient présentant des références croisées, via une interrogation/réponse.

## 5.2.2 Acteurs et transactions

Le diagramme suivant présente une vue générale des acteurs et des transactions du profil PIXm ainsi que de leurs interactions.



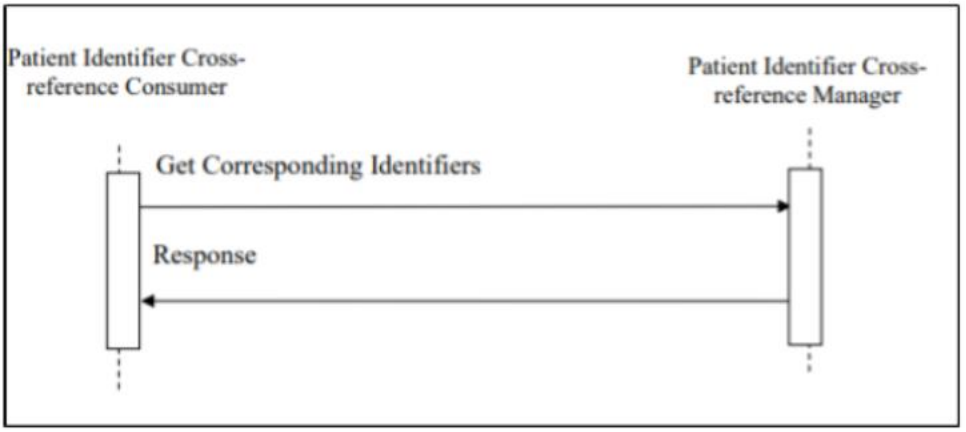

Les transactions relatives à chaque acteur qui intervient directement dans le profil PIXm figurent dans le tableau ci-dessous. Pour être conforme au profil PIXm, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R »).

| Acteur | Transaction | Optionalité |
|---|---|---|
| Gestionnaire de données d'identité du patient (Patient Identity Manager) | Mobile Patient Identifier Cross-Reference Query [ITI-83] | R |
| Consommateur de références croisées des identifiants du patient (Patient Identifier Cross-Reference Consumer) | Mobile Patient Identifier Cross-Reference Query [ITI-83] | R |

## 5.2.3 Transactions

- Mobile Patient Identifier Cross-Reference Query [ITI-83] – Transaction utilisée par un consommateur de références croisées des identifiants du patient pour obtenir de l'information sur un patient dont les identifiants présentent des références croisées avec les identifiants fournis dans les paramètres de recherche. La requête est reçue par un gestionnaire de références croisées des identifiants du patient. Celui-ci traite la demande et répond en envoyant aucun ou plusieurs identifiants du patient pour le patient en question. Exécute une opération FHIR $ihe-pix : GET [base]/Patient/$ihe-pix?<query>.

### 5.2.4 Diagramme de séquence




## 5.3 Profil PDQm

### 5.3.1 Survol

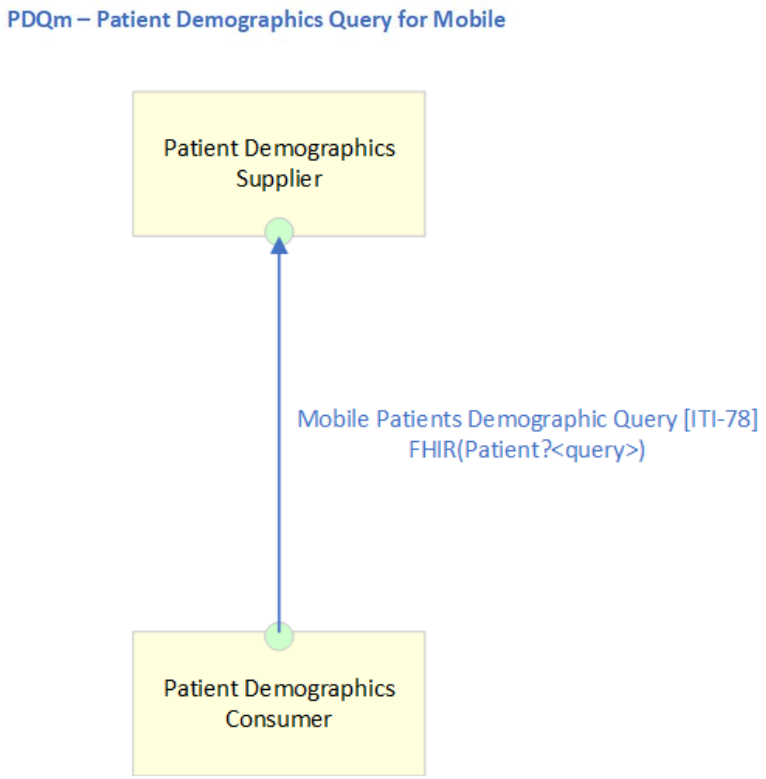
Le profil PDQm (*Patient Demographics Query for Mobile*, ou requête de données démographiques de patients pour appareils mobiles) fournit une transaction qui permet aux applications mobiles et aux applications allégées sur navigateur d'interroger un fournisseur de données démographiques de patients pour obtenir une liste de patients correspondant aux critères de recherche spécifiés par l'utilisateur et extraire les données démographiques de ces patients.

À l'aide de ce patron, le profil PDQm expose la fonctionnalité d'un fournisseur de données démographiques de patients aux applications mobiles et aux applications allégées sur navigateur. Voici des exemples de cas dans lesquels les responsables de l'implantation pourraient utiliser le profil PDQm :

- portail santé qui expose en toute sécurité des données démographiques à des modules d'extension basés sur un navigateur;
- dispositifs médicaux devant accéder à des données démographiques de patients;
- appareils mobiles utilisés par les médecins au chevet qui permettent d'accéder à l'information sur le patient en balayant le code-barres de son bracelet;
- applications Web de DSE/DME qui font une mise à jour dynamique des données démographiques du patient, p. ex. recherche « non postback », information démographique additionnelle, etc.;
- toute application à faibles ressources qui expose la fonctionnalité de recherche de données démographiques de patients;
- toute application utilisant le profil MHD pour accéder à des documents et qui pourrait utiliser PDQm pour trouver un identifiant de patient approprié.

### 5.3.2 Acteurs et transactions

Le diagramme suivant présente une vue générale des acteurs et des transactions du profil PDQm ainsi que de leurs interactions.



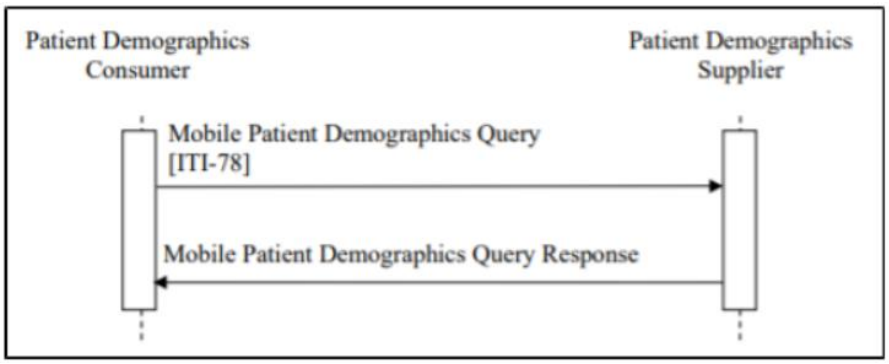

Les transactions relatives à chaque acteur qui intervient directement dans le profil PDQm figurent dans le tableau ci-dessous. Pour être conforme au profil PDQm, un acteur doit prendre en charge toutes les transactions requises (identifiées par un « R »).

| Acteur | Transaction | Optionalité |
|---|---|---|
| Gestionnaire de données d'identité du patient (Patient Identity Manager) | Mobile Patient Demographic Query [ITI-78] | R |
| Consommateur de données démographiques de patients (Patient Demographics Consumer) | Mobile Patient Demographic Query [ITI-78] | R |

## 5.3.3 Transactions

- Mobile Patient Demographic Query [ITI-78] – Transaction utilisée par le consommateur de données démographiques de patients pour demander à un fournisseur de données démographiques de patients une liste de patients correspondant à l'ensemble des critères démographiques fournis (ex. : ID ou nom) dans la requête. Le consommateur de données démographiques de patients peut ensuite compléter ses attributs à partir de l'information reçue du fournisseur de données démographiques de patients. Exécute une requête HTTP GET [base]/Patient?<query>.

## 5.3.4 Diagramme de séquence


Patient Demographics
Consumer
Patient Demographics
Supplier
Mobile Patient Demographics Query
[ITI-78]
Mobile Patient Demographics Query Response