

Programme ROR

Doctrine d'urbanisation

V2.5

Documents de référence

- [Réf. 1] Programme ROR - Doctrine d'urbanisation - présent document
- [Réf. 2] Programme ROR - Doctrine d'urbanisation - Annexe Données issues des référentiels nationaux
- [Réf. 3] Programme ROR - Doctrine d'urbanisation - Annexe Politique d'accès aux données du ROR - situation actuelle
- [Réf. 4] Programme ROR - Doctrine d'urbanisation – Annexe Politique d'accès aux données du ROR - situation cible
- [Réf. 5] Programme ROR - Modèle d'exposition
- [Réf. 6] ROR - Modalités d'accès aux données du ROR
- [Réf. 7] CI-SIS - Cadre d'Interopérabilité des Systèmes d'Information de Santé : site esante.gouv.fr, rubrique « services », rubrique « Cadre d'Interopérabilité des Systèmes d'Information de Santé »
- [Réf. 8] PGSSI-S - Politique Générale de Sécurité des Systèmes d'Information de Santé - site esante.gouv.fr, rubrique « services », rubrique « Politique Générale de Sécurité des Systèmes d'Information de Santé »
- [Réf. 9] Document « ci-sis_transport_volet-synchrone » : CI-SIS - Cadre d'Interopérabilité des Systèmes d'Information de Santé : site esante.gouv.fr, rubrique « services », rubrique « Cadre d'Interopérabilité des Systèmes d'Information de Santé »

Sommaire

1	Objet du document	5
2	Le Répertoire Opérationnel des Ressources (ROR).....	6
2.1	Le référentiel de description de l’offre de santé.....	6
2.2	Une description opérationnelle des activités et des ressources.....	6
2.3	Une architecture distribuée	7
2.4	Un référentiel de données au service des usages métiers.....	8
3	Les espaces de confiance du ROR.....	10
3.1	Les différents espaces de confiance du ROR.....	10
3.2	Conditions et modalités d’accès aux espaces de confiance.....	11
3.2.1	Conditions d’accès à l’espace de confiance	11
3.2.2	Modalités d’intégration à l’espace de confiance	12
3.3	Sécurisation des espaces de confiance	12
3.3.1	Authentification par certificats.....	13
3.3.2	Les certificats à mettre en œuvre dans les échanges	13
3.3.3	Gestion de la liste blanche d’un espace de confiance.....	13
4	Acquisition des données du ROR : adossement du ROR aux référentiels nationaux.....	14
4.1	Contexte de mise en œuvre	14
4.2	Les principes d’adossement	15
4.2.1	Principes généraux	15
4.2.2	Données de référence	15
4.2.3	Identification des structures	16
4.2.4	Identification des professionnels	16
4.3	Accès aux informations des référentiels nationaux.....	16
5	Consommation des données du ROR : typologie des transactions associées	17
5.1	Contexte de mise en œuvre	17
5.2	Les principes de consommation des données du ROR.....	17
5.2.1	Principes généraux	17
5.2.2	Modalités de consommation du ROR.....	18
5.3	Description des modalités de consommation des données du ROR.....	19
5.3.1	Recherche Inter-ROR.....	19
5.3.2	Recherche sur le périmètre national à partir d’une application externe à une solution ROR (à titre prospectif).....	19
5.3.3	Lecture des ressources d’un établissement	20
5.3.4	Lecture d’une organisation interne d’un établissement.....	21
5.3.5	Alimentation et mise à jour d’une application à partir d’une copie partielle ou totale des ROR	22

6	Consommation des données du ROR : politique d'accès aux données du ROR	25
6.1	Contexte de mise en œuvre	25
6.2	Principes d'accès aux données du ROR.....	25
6.2.1	Données en libre accès, données à accès restreint et très restreint	25
6.2.2	Profils d'accès aux données du ROR.....	26
6.3	Mise en œuvre du contrôle d'accès aux données.....	27
6.3.1	Situation actuelle.....	27
6.3.2	Situation en cible	28
7	Annexe : Rappel de la définition d'un référentiel de données	30

Glossaire

Intitulé	Définitions
Champ d'activité	Un champ d'activité caractérise un périmètre d'activités sanitaires ou médico-sociales dans lequel intervient une structure (MCO, PSY, SSR, PA, PH, ...)
Activité opérationnelle	<p>Une activité opérationnelle est un ensemble cohérent d'actions et de pratiques mises en œuvre pour répondre aux besoins en Santé de la personne.</p> <p>Elle peut être d'ordre sanitaire, social ou médico-social.</p> <p>Cet ensemble opérationnel est plus détaillé qu'une activité soumise à autorisation préalable de l'ARS.</p> <p>Dans le secteur médico-social, chaque activité est rattachée à une famille d'activités (prestation niveau 4 de Serafin)</p>
Mode de prise en charge	Un mode de prise en charge précise la durée de prise en charge et le niveau de soins pour un ensemble d'activités opérationnelles
Ressources opérationnelles	Une ressource opérationnelle est une ressource qui contribue à la réalisation d'un ensemble d'activités opérationnelles (professionnels, équipements spécifiques, capacité en lits, ...)
Espace de confiance	L'espace de confiance du ROR, se définit comme l'espace de partage et d'échange des données de description de l'offre de Santé, qui garantit la sécurité des données et les droits des professionnels ressources de cette offre.
Application externe	Dans le contexte du ROR, une application externe correspond à un logiciel non intégré à une solution ROR qui permet la réalisation d'une ou plusieurs tâches dans le cadre d'un processus.
Profil d'accès <ul style="list-style-type: none"> • Accès libre • Accès restreint • Accès très restreint 	<p>Un profil d'accès aux données se définit comme un regroupement de données génériques permettant d'afficher les données aux utilisateurs en cohérence avec leurs habilitations.</p> <p>Les profils d'accès aux données du ROR sont utilisés dans le ROR et dans les applications externes pour exposer les données en libre accès, en accès restreints et très restreints aux utilisateurs en fonction de leurs droits.</p>
Rôle métier Profil utilisateur Couple (Rôle métier/ Profil utilisateur)	<p>Le rôle métier de l'utilisateur correspond à la profession ou spécialité qu'il exerce dans un domaine professionnel (ex : infirmier).</p> <p>Le profil de l'utilisateur dans une application correspond à sa fonction au sein de l'organisation pour laquelle il utilise cette application (ex : gestionnaire de cas).</p> <p>Le profil d'accès ROR est véhiculé dans les échanges sous forme d'un couple d'informations (rôle métier/profil utilisateur). En fonction du contexte d'utilisation, ce couple peut prendre des valeurs qui caractérisent l'application externe (automate/ orientation médicosociale) ou qui caractérise l'utilisateur (médecin/ PS en Centres Antipoison et de Toxicovigilance).</p>

1 Objet du document

Ce document est une partie constitutive du cadre de référence applicable au Répertoire Opérationnel des Ressources (ROR).

Le cadre de référence est un ensemble de documents élaborés en concertation avec les acteurs régionaux et institutionnels. Il permet de spécifier les conditions d'exploitation, de garantir une vision unifiée des ROR.

Ce cadre de référence est constitué :

- d'une doctrine d'urbanisation des flux ;
- d'un modèle d'exposition des données du ROR ;
- d'une spécification des services de consommation des données du ROR ;
- d'un cadre d'homologation (à venir) ;
- d'un cadre juridique de traitement, de diffusion et d'utilisation des données du ROR ;
- de nomenclatures d'échanges.

Le présent document porte sur la doctrine d'urbanisation des ROR. Il a pour objet de :

- présenter le ROR et l'espace de confiance du ROR ;
- de poser les principes d'alimentation du ROR et plus particulièrement l'adossement du ROR aux référentiels nationaux ;
- de poser les principes de consommation des données du ROR en fonction des cas d'usage identifiés à ce jour et de la politique d'accès aux données associée.

2 Le Répertoire Opérationnel des Ressources (ROR)

Le ROR a pour finalités :

1° de disposer d'une vision régionale et nationale de l'offre de santé portée par les établissements, services ou organismes de soins, les cabinets libéraux et les établissements ou services sociaux et médico-sociaux mentionnés dans l'article L. 312-1 du code de l'action sociale et des familles ;

2° de décrire l'ensemble des activités et ressources mises en œuvre par ces acteurs pour participer au rétablissement ou à l'entretien de la santé d'une personne ;

3° de contribuer à une prise en charge efficace et adaptée de l'utilisateur tout au long de son parcours de santé en fournissant une description homogène de l'offre de santé aux applications métiers d'orientation, de régulation et de coordination à destination des professionnels ;

4° de mettre à disposition certaines données du ROR au moyen de portails à destination du public.

2.1 Le référentiel de description de l'offre de santé

Le Répertoire Opérationnel des Ressources (ROR) constitue le référentiel unique de données de description de l'offre de santé portée par les structures qui participent au rétablissement ou à l'entretien de la Santé d'une personne tout au long de son parcours de santé. Une définition de la notion de référentiel de données est présentée en annexe du présent document¹.

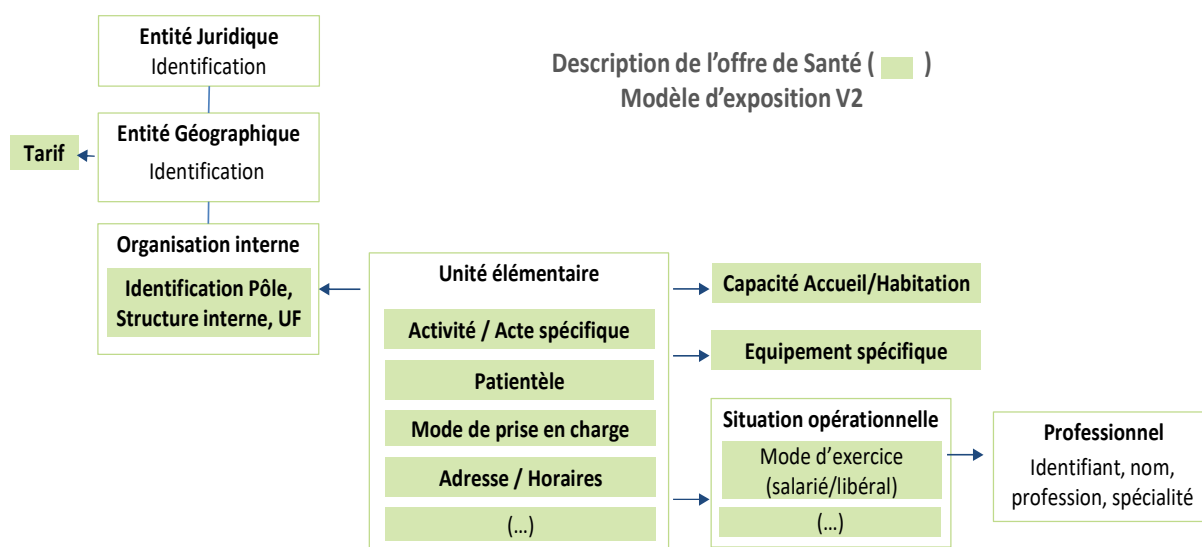
Son périmètre actuel, fixé nationalement, couvre l'offre de santé portée par les établissements sanitaires (MCO, SSR, PSY), par les établissements et services en charge des personnes âgées en perte d'autonomie (PA) et des personnes en situation de handicap (PH) et les structures de ville (cabinets libéraux, maisons de santé, centres de santé).

2.2 Une description opérationnelle des activités et des ressources

L'offre de santé est définie par une ou plusieurs activités opérationnelles, réalisées dans le cadre d'un mode de prise en charge et pour une patientèle, et par les ressources qui permettent la réalisation de ces activités opérationnelles sur un lieu donné. Ces ressources concernent principalement les équipements spécifiques, les capacités d'accueil et les professionnels que l'on souhaite identifier pour cette offre.

¹ Cf l'Annexe Rappel de la définition d'un référentiel de données

Le ROR présente l'offre de santé via un modèle d'exposition des données du ROR commun pour l'ensemble des offres sanitaire et médico-sociale (document [Réf. 5]).



Ce modèle d'exposition présente les données d'identification des structures et des professionnels qui sont issues des référentiels nationaux (FINESS, RPPS/ADELI) lesquels garantissent l'interopérabilité avec de nombreux systèmes.

Ces données d'identification sont complétées par la description des activités et des ressources opérationnelles mises en œuvre par les acteurs de santé pour participer au rétablissement ou à l'entretien de la santé d'une personne.

Ce modèle d'exposition instaure l'homogénéité de description de l'offre de santé portée par les structures et permet désormais à toute application métier de consommer des données du ROR de façon identique sur l'ensemble du territoire et sur le périmètre actuel du ROR.

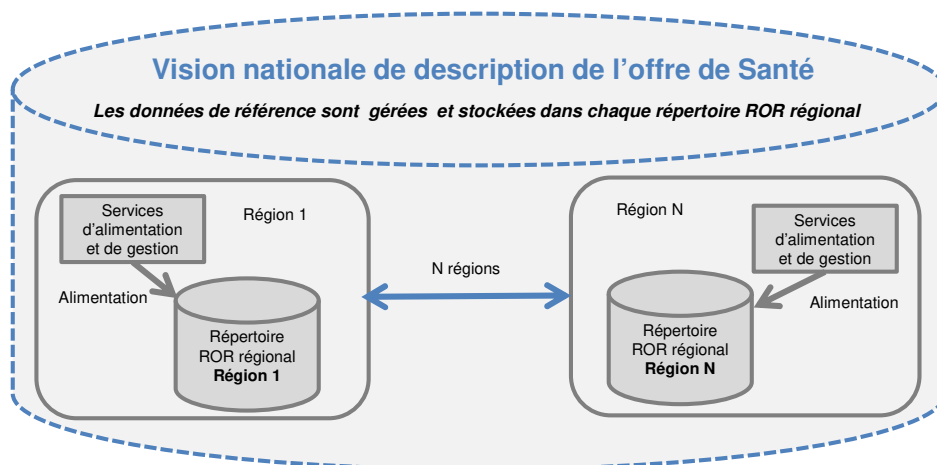
2.3 Une architecture distribuée

Le ROR, en tant que référentiel de description de l'offre de santé (au sens gisement de données), a une couverture nationale. Il doit permettre à toute application autorisée d'accéder à une offre de santé sur l'ensemble du territoire national.

L'architecture actuelle pour déployer le ROR est une architecture distribuée. Deux solutions techniques, appelées solution ROR, coexistent à ce jour et sont implémentées en région. Chaque ARS met en œuvre et exploite une des deux solutions ROR.

L'ARS est responsable de l'alimentation du ROR régional pour le périmètre des ressources mises à disposition dans la région. **Il n'y a pas d'intersection de périmètre entre les régions.** Concernant l'alimentation manuelle du ROR, les modalités fonctionnelles et techniques sont définies dans chaque région. Concernant l'alimentation automatique du ROR (référentiels nationaux, données AMELI, ...), les modalités fonctionnelles sont partagées et déterminées au niveau national, les modalités techniques sont définies régionalement.

L'ensemble des ROR régionaux permet de présenter une vision nationale de l'offre de santé¹.



2.4 Un référentiel de données au service des usages métiers

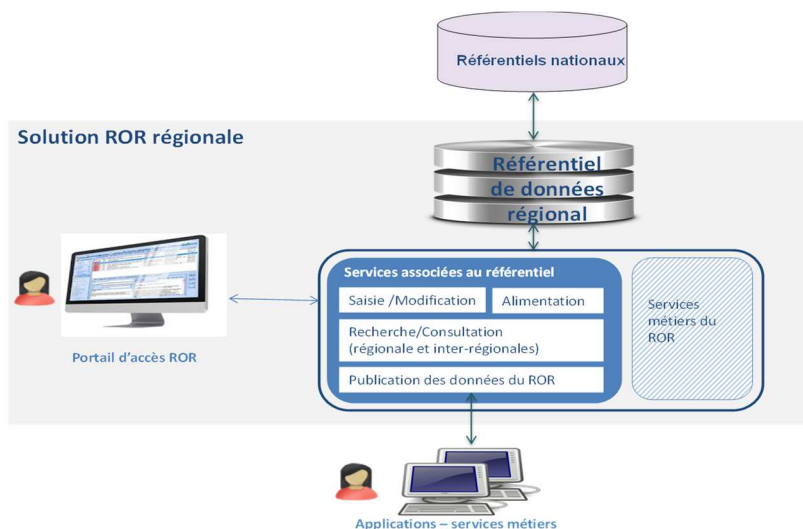
Il est important de distinguer au niveau des solutions ROR² :

- le répertoire ROR en tant que référentiel de données (gisement de données) ;
- les fonctions directes d'alimentation, de recherche, de consultation et de publication associées au référentiel, intégrées à la solution ROR régionale ;
- les fonctions indirectes via des services métiers utilisateurs des données du ROR.

¹ La typologie du ROR en tant que référentiel dans une vision nationale est à rapprocher du « pattern 5 – référentiel hub », tel que défini dans le « Cadre Commun d'Architecture des référentiels de données », publié par la DINSIC en complément au « Cadre Commun d'Urbanisation du Système d'Information de l'état » (<http://references.modernisation.gouv.fr/urbanisation-du-systeme-dinformation-de-letat>).

² Cette précision est nécessaire dans la mesure où, et pour des raisons historiques, l'appellation ROR peut regrouper à la fois le référentiel de données (c'est-à-dire le répertoire et les fonctions associées) et les services métiers.

Le référentiel ROR a vocation à alimenter les applications externes utilisées par des professionnels ou des usagers, qui contribuent à l'orientation des personnes ou à la coordination des parcours de santé.



En termes d'applications externes utilisatrices, on peut citer à titre d'exemple et sans être d'exhaustif :

- au niveau régional :
 - un portail de consultation des ressources régionales ;
 - les services numériques de coordination destinés aux dispositifs d'appui à la coordination et aux professionnels participant aux communautés professionnelles territoriales de santé ;
- au niveau national :
 - un service d'orientation déployé au niveau national type Via trajectoire ;
 - le portail santé.fr du Service Public d'Information en Santé ;
 - le SI-SAMU ;
 - etc.

3 Les espaces de confiance du ROR

3.1 Les différents espaces de confiance du ROR

L'espace de confiance du ROR¹, se définit comme l'espace de partage et d'échange des données de description de l'offre de Santé, qui garantit la sécurité des données et les droits des professionnels ressources de cette offre. L'espace de confiance du ROR est constitué de l'ensemble des acteurs, personnes physiques et personnes morales, reconnus comme étant légitimes à échanger et partager des données opérationnelles de description d'offre en conformité avec la politique d'accès du ROR² et aux conditions de sécurité définies par des référentiels nationaux (la PGSSI-S), notamment en termes d'identification et d'authentification.

On distingue plusieurs espaces de confiance pour le ROR :

- L'espace de confiance Inter-ROR, entre les instances régionales des ROR pour les échanges inter-ROR. Cet espace de confiance n'est pas traité dans ce document.
- L'espace de confiance national qui regroupe les personnes morales responsables d'applications externes qui souhaitent avoir accès aux données de plusieurs ROR ou de tous les ROR sur le territoire national.
- L'espace de confiance régional qui regroupe les personnes morales responsables d'applications externes qui souhaitent avoir accès aux données d'un seul ROR régional. À titre d'exemple, on peut citer les applications intégrées dans l'Espace Numérique Régional de Santé associées à une instance ROR régionale donnée. Il y a donc autant d'espaces de confiance régionaux que d'instances ROR soit 17 espaces de confiance régionaux.

Chaque espace de confiance s'appuie :

- sur une authentification réciproque des entités opérant entre elles, basée sur des certificats électroniques et permettant de mettre en œuvre des sessions sécurisées TLS/SSL,
- sur une liste blanche partagée permettant d'identifier les entités ayant le droit d'inter-opérer au sein de cet espace.

Ce mode de sécurisation permet une reconnaissance mutuelle des entités, garantissant l'origine des données, tout en assurant l'intégrité et la confidentialité des échanges.

Il y a une liste blanche par espace de confiance. Dissocier les listes blanches permet une administration séparée des espaces de confiance :

- L'administration de chaque liste blanche régionale est à la charge de l'ARS gestionnaire du ROR de sa région (ou de son GRADeS par délégation).
- La liste blanche inter-ROR et celle associée à l'espace de confiance nationale des applications consommatrices sont administrées par le programme ROR national.

¹ Cf. Chapitre Objet du document

² [Réf. 3] Programme ROR - Doctrine d'urbanisation - Annexe Politique d'accès aux données du ROR - situation actuelle

3.2 Conditions et modalités d'accès aux espaces de confiance

3.2.1 Conditions d'accès à l'espace de confiance

Les personnes morales responsables d'applications externes qui souhaitent consommer des données du ROR doivent s'inscrire soit dans l'espace de confiance national, soit dans au moins un des espaces de confiance régionaux du ROR.

L'appartenance à l'espace de confiance (national ou régional) du ROR est soumise aux conditions suivantes :

1° Condition d'accès :

- avoir pour finalité de contribuer à une prise en charge efficace et adaptée de l'utilisateur tout au long de son parcours de Santé et outiller des usages dans le cadre de l'orientation, la régulation, la coordination et l'information.

2° Conditions d'usage :

- Respect des finalités et du périmètre pour lesquels il a pu répondre aux critères d'éligibilité à accéder à l'espace de confiance¹.
- Respect du principe de référence selon lequel l'information doit être recherchée dans le respect de son point de vérité au moment où on en a besoin et dans le périmètre de la recherche, autrement dit seule l'information source du référentiel est reconnue.
À titre d'exemple, la duplication des données du ROR en tant que référentiel ne peut que se faire d'en un usage contraint et ponctuel ou éventuellement en synchronisation mais ne constitue pas dans ce cas une preuve de vérité.
- Respect des modalités de sécurisation des échanges avec le ROR par une reconnaissance mutuelle des entités, garantissant l'origine des données, tout en assurant l'intégrité et la confidentialité des échanges (cf. paragraphe 3.3).
- Respect des engagements sur les modalités de consommation des données du ROR ce qui suppose de :
 - mettre en œuvre les flux de consommation du ROR en conformité avec le modèle d'exposition et les spécifications techniques et fonctionnelles des services d'accès aux données du ROR définies dans le document : « ROR - Modalités d'accès aux données du ROR » [Réf. 6] ;
 - mettre en œuvre le profil d'accès ad hoc. L'application externe doit donc être en mesure de créer le VIH (Vecteur d'Identification et d'Habilitation Formelles) pour permettre aux ROR d'appliquer la politique d'accès aux données du ROR [Réf .3] et [Réf .4] ;

Le respect de ces engagements s'impose dès à présent aux personnes morales responsables d'applications externes de l'espace de confiance national et s'inscrit dans une trajectoire adaptée au contexte local pour les applications de l'espace de confiance régional.

¹ Cf le § Modalités d'intégration à l'espace de confiance

- Respect des engagements sur les modalités de diffusion des données du ROR ce qui suppose de :
 - attribuer les droits aux utilisateurs de son application en respectant la politique d'accès aux données du ROR [Réf .3] et [Réf .4] ;
 - ne pas rediffuser les données du ROR à des applications tierces.

3.2.2 Modalités d'intégration à l'espace de confiance

La personne morale responsable de l'application externe peut s'inscrire dans l'espace de confiance du ROR et accéder selon les droits à 3 types de données (données en accès libre, restreint, très restreint)¹ :

- Au niveau national, l'application peut avoir accès à plusieurs ROR ou à tous les ROR et dans ce cas la personne morale responsable de l'application doit demander au programme ROR son intégration dans l'espace de confiance national du ROR.
Après vérification des critères d'éligibilité (finalité, usage), cette demande fait l'objet d'une validation formelle par une instance décisionnaire du programme ROR, le comité de programme stratégique.
Le profil d'accès aux données du ROR est déterminé par l'usage outillé et le profil des utilisateurs de l'application. Ce profil est validé par le comité de programme stratégique du programme ROR.
- Au niveau régional, l'application peut avoir accès au seul ROR régional et dans ce cas la personne morale responsable de l'application doit demander à l'ARS gestionnaire du ROR régional son intégration à l'espace de confiance régional du ROR.
Après vérification des critères d'éligibilité (finalité, usage), cette demande fait l'objet d'une validation formelle de l'ARS gestionnaire du ROR régional.
Le profil d'accès aux données du ROR est déterminé par l'usage outillé et le profil des utilisateurs de l'application. Ce profil est validé par l'ARS gestionnaire du ROR régional.
L'intégration au niveau régional d'une nouvelle application dans l'espace de confiance du ROR et le profil d'accès qui lui a été attribué font l'objet d'une communication trimestrielle au comité de programme stratégique.

3.3 Sécurisation des espaces de confiance

La sécurisation des espaces de confiance s'effectue par une authentification mutuelle par certificats et par la gestion d'une liste blanche associée à ces espaces sécurisés d'échange.

Une application est sous la responsabilité d'une personne morale. L'enrôlement du couple (personne morale, application) passe par l'enregistrement d'un certificat IGC Santé délivré à la personne morale. Le contrôle d'accès au service est assuré au niveau applicatif par rapprochement entre l'identité portée par le certificat et sa présence dans la liste blanche associée à l'espace de confiance.

L'ensemble des modalités de sécurisation décrites ci-dessous s'impose dès à présent aux applications externes de l'espace de confiance national et s'inscrit dans une trajectoire adaptée au contexte local pour les applications de l'espace de confiance régional.

¹ Cf. la définition au chapitre Données en libre accès, données à accès restreint et très restreint

3.3.1 Authentification par certificats

L'utilisation d'une authentification par certificat du système appelant ou client permet de :

- certifier l'identification des entités par l'Autorité de Certification qui délivre les certificats. Ainsi le système destinataire de la transaction (serveur) peut faire confiance à l'identité portée par le certificat présenté par l'entité appelante ou cliente.
- mettre en œuvre des mécanismes de contrôle d'accès indépendant des adresses IP des entités appelantes. L'identification de l'entité appelante est indépendante de l'infrastructure mise en œuvre.

Les entités (ROR et applications externes) s'engagent à informer de tout changement de certificat :

- Le programme national ROR, si elles se sont inscrites dans l'espace de confiance national ;
- L'ARS gestionnaire du ROR (ou son GRADeS par délégation), si elles se sont inscrites dans l'espace de confiance régional.

3.3.2 Les certificats à mettre en œuvre dans les échanges

Dans la mesure où le nombre de systèmes inter-opérant est élevé, il est demandé pour les entités clientes (ROR dans sa fonction de client ou applications consommatrices) d'utiliser des certificats électroniques délivrés par l'ASIP Santé, Autorité de Certification du secteur de la santé, aussi bien sur les web services définis dans le cadre du programme national ROR que pour les échanges régionaux.

Le recours à une autorité de certification commune, pour les certificats clients ou serveurs, permet de rationaliser les opérations de paramétrage sur les infrastructures, et de mettre en œuvre un niveau de sécurité homogène sur tous les échanges.

Ainsi chaque ROR, dans sa fonction serveur, fait confiance aux certificats émis par l'IGC-Santé, présentés par les clients SSL.

Chaque entité, dans sa fonction client (ROR ou application externe), doit faire confiance aux certificats émis par toutes les Autorités de Certification choisies par chacune des instances (serveurs) ROR régionales (IGC-Santé, GoDaddy, GlobalSign, Gandi, Rapid SSL, etc.) et doit paramétrer les chaînes de confiances propres à ces diverses autorités de certification.

3.3.3 Gestion de la liste blanche d'un espace de confiance

L'espace de confiance est matérialisé par 18 listes blanches gérée à deux niveaux :

- Une liste blanche gérée au niveau national par le programme ROR pour les applications qui se sont inscrites dans l'espace de confiance au niveau national ;
- Une liste blanche pour chaque région qui est gérée par l'ARS gestionnaire de son ROR régional (ou son GRADeS par délégation) pour les applications qui se sont inscrites dans l'espace de confiance au niveau régional. Ces listes blanches régionales sont transmises trimestriellement au programme ROR.

La liste blanche consolide l'url de l'application, son certificat et son profil d'accès. Les applications externes s'engagent à informer de tout changement de certificat ou d'Url auprès de l'acteur référent (le programme national ROR pour l'espace de confiance au niveau national, l'ARS gestionnaire du ROR - ou son GRADeS par délégation - pour l'espace de confiance régional).

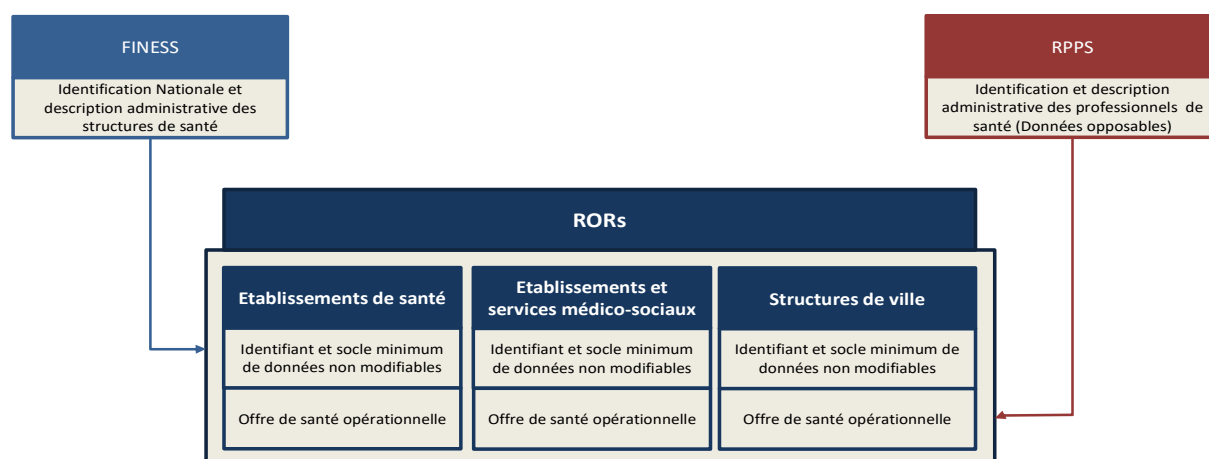
4 Acquisition des données du ROR : adossement du ROR aux référentiels nationaux

4.1 Contexte de mise en œuvre

Parmi les composantes constitutives de l'offre de santé telles que rappelées au paragraphe 2.2, nous distinguons deux types d'informations :

- les informations d'identification enregistrées dans les référentiels nationaux par les autorités d'enregistrement responsables. Les référentiels nationaux sont FINESS, le RPPS et le répertoire ADELI¹ et peuvent notamment concerner, en fonction de la situation, les composantes « structure » et « professionnels de santé » :
 - pour les structures, les informations d'identification (n°FINESS, raison sociale, ...), la catégorie d'établissement, la localisation, ...
 - pour les professionnels de santé, les informations d'identification (n°RPPS ou ADELI, identité d'exercice, état civil), la profession, les qualifications certifiées par les autorités d'enregistrement (spécialité ordinale et autres savoir-faire), ...
 - pour les professionnels de santé libéraux, les informations sur le lieu d'exercice (informations d'identification du cabinet, la localisation, ...).
- les informations à caractère opérationnel enregistrées sous la responsabilité des régions. Ces informations sont complémentaires aux informations mises à disposition par les référentiels nationaux. Il s'agit notamment de la description de l'organisation interne des structures, des activités proposées et des données de description complémentaires permettant de répondre aux besoins opérationnels des utilisateurs (patientèle, capacité d'accueil, ...).

Le ROR est alimenté par des données issues des référentiels institutionnels FINESS pour les structures (situation actuelle) et RPPS/ADELI pour les professionnels de santé (situation cible) et complété par les acteurs régionaux qui saisissent les données opérationnelles.



¹ Cf. « Cadre commun des projets de e-santé », version de mai 2016 et instruction no SG/DSSIS/2016/147 du 11 mai 2016 relative au cadre commun des projets d'e-santé.

4.2 Les principes d'adossement

4.2.1 Principes généraux

Le ROR est adossé aux référentiels socles pour les données d'identification.

- Il récupère un petit nombre de données d'identification de toutes les structures sanitaires et médico-sociales de FINESS : les informations d'identification (n°FINESS, raison sociale, ...), la catégorie d'établissement, l'adresse, ...
- Le ROR n'a pas vocation à intégrer tous les professionnels salariés. Il récupère un nombre limité de données d'identification pour certains professionnels que l'on souhaite identifier dans une organisation interne : informations d'identification (n°RPPS ou ADELI, identité d'exercice, état civil), la profession, les qualifications certifiées par les autorités d'enregistrement (spécialité ordinale et autres savoir-faire) et la structure de rattachement du professionnel.
- Le ROR a vocation à intégrer toutes les structures de ville qui portent une offre de santé ainsi que les professionnels de santé qui y sont rattachés. Il récupère les données sur le professionnel et sa structure de rattachement telles que décrites ci-dessus.

4.2.2 Données de référence

Si un concept est défini dans un référentiel national, alors tout autre concept apparenté qui est utilisé dans le ROR doit avoir un nom et une définition clairement différents pour éviter toute confusion.

Dès lors qu'une information est disponible dans un référentiel national, elle ne doit pas faire l'objet d'une ressaisie locale mais d'une alimentation à partir d'un référentiel national. Ce principe permet d'assurer une cohérence globale avec l'ensemble de la sphère santé, notamment sur les structures et les professionnels.

Certaines données issues des référentiels nationaux ne peuvent donner lieu à aucune correction dans le ROR. Ces données doivent être clairement identifiées, cette liste est présentée dans le document « Programme ROR - Doctrine d'urbanisation - Annexe Données issues des référentiels nationaux » [Réf. 2]. Les autres informations peuvent faire l'objet d'une correction temporaire dans le ROR, sous la responsabilité du gestionnaire du ROR, tant que l'information n'est pas corrigée dans le référentiel national. Toute correction doit faire l'objet d'une signalisation vers l'entité responsable du référentiel concerné.

4.2.3 Identification des structures

Toute structure présente dans le ROR doit être identifiée par un identifiant public à portée nationale :

- les structures (Entités juridiques et établissements) enregistrées dans FINESS doivent être obligatoirement identifiées par leur n° FINESS¹ ;
- les structures ne faisant pas l'objet d'un enregistrement dans FINESS doivent être identifiées par leur numéro SIRET ou SIREN selon le cas² ;
- les associations ne disposant pas d'un SIRET doivent être identifiées par le numéro RNA (Répertoire National des Associations³) ;
- concernant les cabinets libéraux individuels et les cabinets de groupe, à défaut de numéro de SIRET disponible dans le référentiel national, l'identifiant RPPS-rang ou ADELI-rang disponible dans le référentiel national doit être utilisé⁴.

4.2.4 Identification des professionnels

Tout professionnel de santé présent dans le ROR doit être identifié par un identifiant de portée nationale⁵ :

- n° RPPS pour les professions enregistrées dans le RPPS⁶ ;
- n° ADELI pour les autres professions de santé et les assistants de service social ;
- si la personne concernée n'est pas un professionnel enregistré dans un référentiel national, elle doit être identifiée par un identifiant de portée nationale telle que préconisée dans le référentiel d'identification des acteurs de santé de la PGSSI-S⁷, « identifiant public de la structure » / « identifiant privé de la personne physique au sein de la structure ».

L'identification des professionnels devrait évoluer avec la mise en œuvre de la doctrine du numérique en santé qui prévoit notamment la généralisation de l'identification nationale des professionnels des secteurs sanitaire et médico-social.

4.3 Accès aux informations des référentiels nationaux

L'ASIP Santé met à disposition les informations des référentiels nationaux via le service de publication Annuaire Santé qu'elle a mis en œuvre.

¹ Cf. MOS : attribut numFINNESS de la classe EntiteGeographique ou de la classe « EntiteJuridique »

² Cf. MOS : attribut numSIRET de la classe EntiteGeographique ou attribut NumSIREN de la classe EntiteJuridique

³ Cf. <http://www.associations.gouv.fr/le-rna-repertoire-national-des-associations.html>

⁴ Cf. MOS : attribut identifiantEG de la classe Entité Géographique

⁵ Cf MOS : attribut IdPP de la classe Professionnel du MOS

⁶ En janvier 2017 : médecins, chirurgiens-dentistes, sages-femmes, pharmaciens, masseurs-kinésithérapeutes.

⁷ Politique Générale de la Sécurité des Systèmes d'Information de Santé : <http://esante.gouv.fr/> rubrique « Politique Générale de la Sécurité des Systèmes d'Information de Santé »

5 Consommation des données du ROR : typologie des transactions associées

5.1 Contexte de mise en œuvre

À ce jour, les services de consommation des données du ROR sont utilisés dans le cadre de la recherche inter-ROR et dans le cadre d'utilisation des données par des applications intégrées dans un espace de confiance (le concept d'espace de confiance est défini au paragraphe 3.1).

5.2 Les principes de consommation des données du ROR

5.2.1 Principes généraux

Les services de consommation des données du ROR reposent sur des transactions génériques communes à tous les champs d'activités (MCO, SSR, PSY, médico-social, ...).

En termes de représentation des données, ces transactions s'appuient toutes sur le modèle d'exposition des données. Le modèle d'exposition est spécifié dans le document [Réf. 5].

Les données peuvent être à ce jour considérées à la lumière de leur usage :

- les données dites « statiques » relevant des structures et de l'organisation des soins et ne nécessitant pas de modification fréquente ;
- les données dites « dynamiques » nécessitant des modifications fréquentes (par exemple la disponibilité des lits).

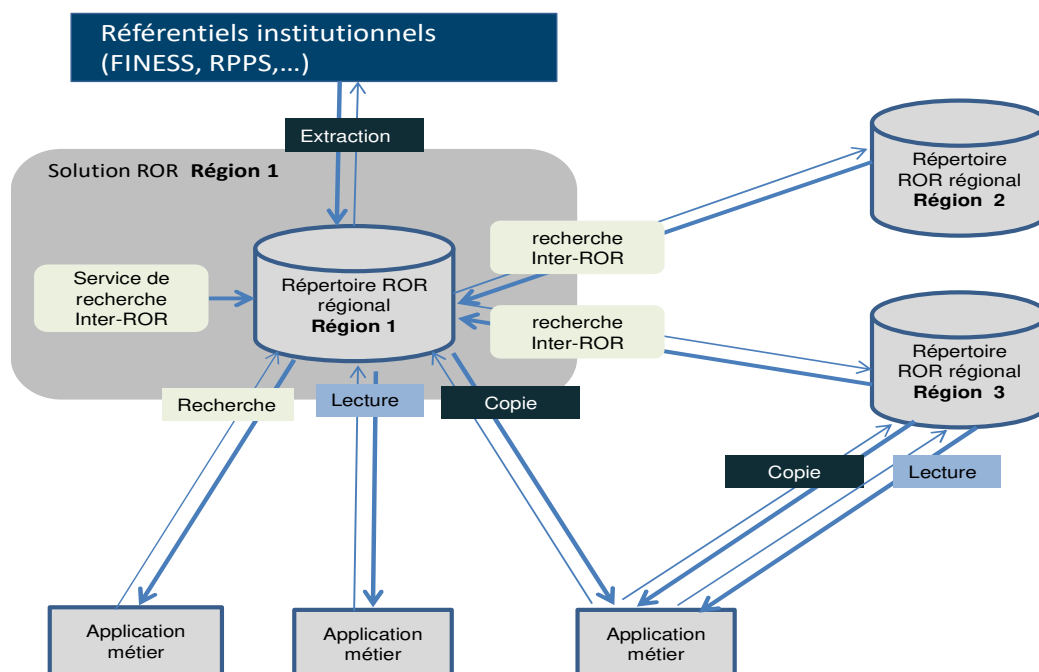
Les transactions sont spécifiées en conformité au profil CSD défini par IHE (Integrating the Healthcare Enterprise).

5.2.2 Modalités de consommation du ROR

À ce jour les modalités d'accès aux données du répertoire ROR régional (gisement de données) identifiées sont les suivantes :

- **recherche Inter-ROR** : à partir d'un service de recherche intégré à une solution ROR mise en œuvre dans une région, il s'agit d'étendre la recherche d'une offre de santé à l'ensemble du territoire national ;
- **recherche sur le périmètre national** (à titre prospectif) : à partir d'une application externe à une solution ROR, il s'agit de rechercher une offre sur un périmètre national ou localisé ;
- **lecture des ressources d'un établissement** : à partir d'une application externe à une solution ROR, il s'agit de consulter les ressources d'un établissement qui a été préalablement identifié ;
- **lecture d'une organisation interne d'un établissement** : à partir d'une application externe à une solution ROR, il s'agit de consulter les informations descriptives d'une organisation interne qui a été préalablement identifiée ;
- **alimentation et mise à jour d'une application à partir d'une copie partielle ou totale des ROR** : une application souhaite disposer d'une copie locale, partielle ou totale, des ROR.

Ces différentes modalités d'accès sont représentées dans le schéma ci-après.



5.3 Description des modalités de consommation des données du ROR

5.3.1 Recherche Inter-ROR

Contexte

À partir d'un service de recherche *intégré* à une solution ROR mise en œuvre dans une région, il s'agit d'étendre la recherche d'une offre à l'ensemble du territoire national.

L'objectif est d'obtenir en temps réel, l'état des informations associées à une offre au moment de la recherche.

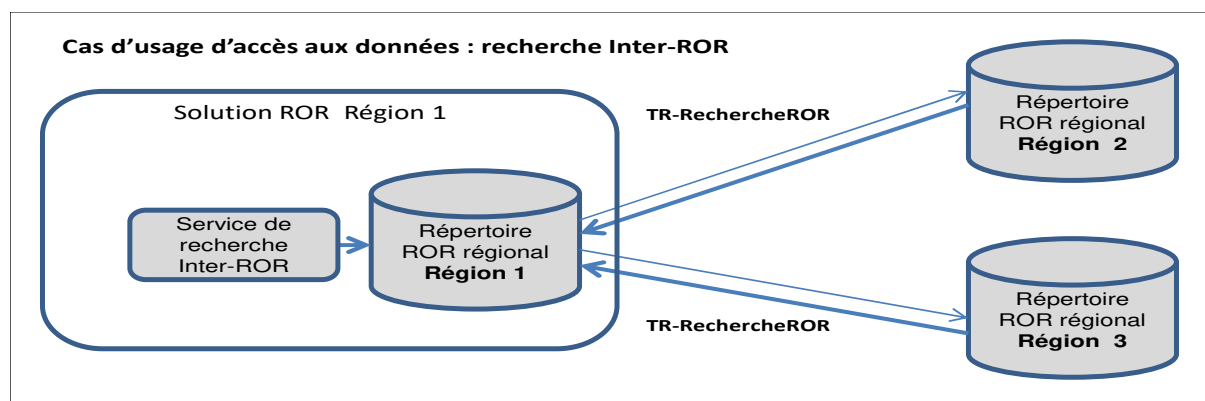
Transaction associée

TR-RechercheROR : Transaction de recherche envoyée à un ROR donné.

La structure de la requête de recherche et la structure de la réponse sont basées sur le profil CSD défini par IHE (Integrating the Healthcare Enterprise).

Principe

Sur la base du critère de recherche « localisation », le ROR local détermine au moyen d'un dispositif de géolocalisation s'il doit consulter d'autres ROR. Le cas échéant, le ROR local utilise la « transaction de recherche ROR » pour interroger chacun des ROR sélectionnés.



Caractéristique

Une solution ROR destinataire de la « transaction RechercheROR » ne propage pas la requête vers d'autres ROR.

5.3.2 Recherche sur le périmètre national à partir d'une application externe à une solution ROR (à titre prospectif)

Préambule

Ce cas d'usage pourra s'avérer opportun à terme, pour la consommation du ROR à partir de certains logiciels de type LPS (Logiciel de Professionnels de Santé).

Contexte

À partir d'une application externe à une solution ROR, il s'agit de rechercher une offre sur un périmètre national ou localisé.

L'objectif est d'obtenir en temps réel, l'état des informations associées à une offre au moment de la recherche. Le système demandeur ne prend pas en charge la détermination des ROR régionaux à interroger.

Transaction associée

TR-RechEtendueROR: Transaction de « recherche sur le périmètre national ».

La structure de la requête de recherche et la structure de la réponse sont basées sur le profil CSD défini par IHE (Integrating the Healthcare Enterprise).

Principe

À étudier lorsque le besoin d'une telle transaction sera confirmé.

5.3.3 Lecture des ressources d'un établissement

Contexte

Cette transaction permet à une application externe de consulter les ressources d'un établissement qui a été préalablement identifié.

Transaction associée

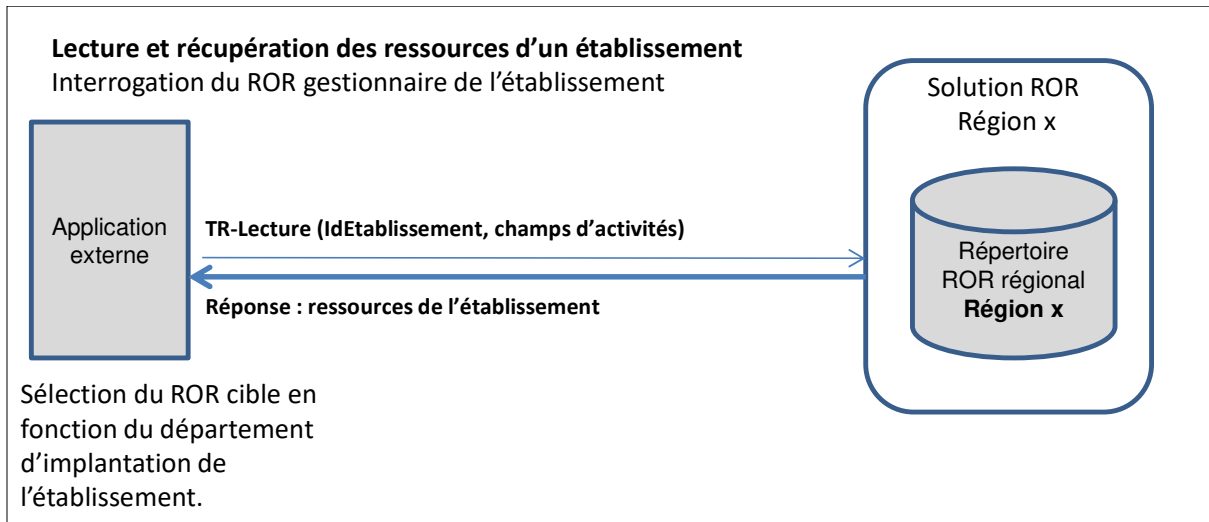
TR-Lecture-OffresSanteEtablissement: Transaction de lecture. L'application externe récupère auprès d'un ROR régional le descriptif des ressources d'un établissement. La demande contient l'identifiant de l'établissement concerné.

Actuellement, la demande de lecture peut être restreinte à un ou plusieurs champs d'activités ; la réponse contient les données associées aux champs d'activités concernés.

En cible, cette transaction exposera toutes les données affichables en fonction du profil d'accès aux données ROR accordé à l'initiateur de la transaction.

Principe

L'application détermine le ROR à atteindre en fonction du département d'implantation de l'établissement. L'application adresse directement la requête de lecture au ROR Régional en charge de la gestion des ressources de l'établissement. Cela implique que l'application dispose d'une table de correspondance région/département.



5.3.4 Lecture d'une organisation interne d'un établissement

Contexte

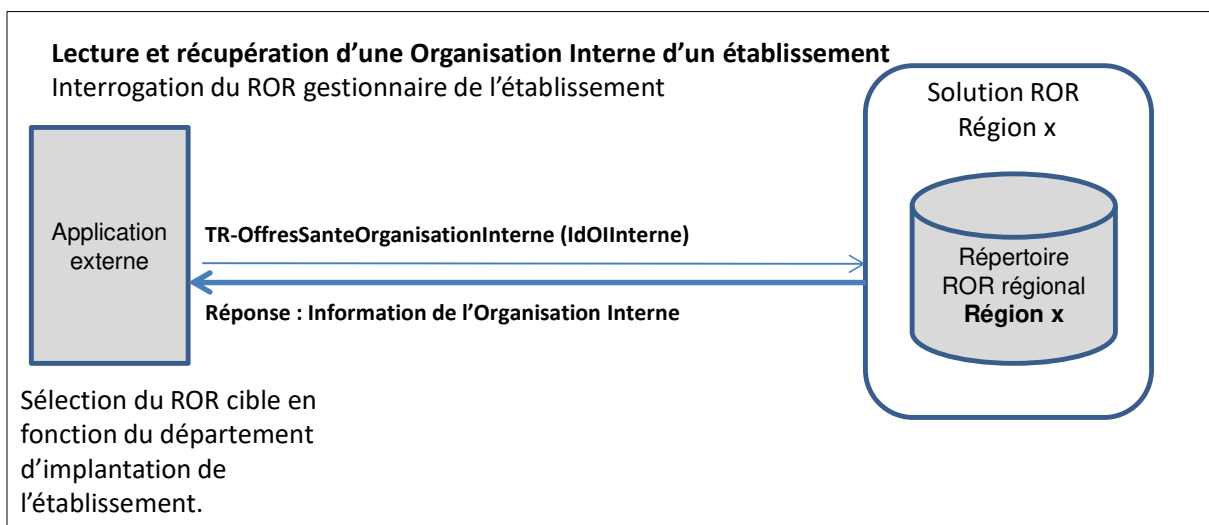
Cette transaction permet à une application externe de consulter les informations descriptives d'une organisation interne qui a été préalablement identifiée.

Transaction associée

TR-Lecture-OffresSanteOrganisationInterne: Transaction de lecture. L'application externe récupère auprès d'un ROR régional le descriptif d'une Organisation Interne d'un établissement. La demande contient l'identifiant de l'Organisation Interne concernée.

Principe

L'application détermine le ROR à atteindre en fonction du département d'implantation de l'établissement. L'application adresse directement la requête de lecture au ROR Régional en charge de la gestion des ressources de l'établissement supportant l'Organisation Interne. Cela implique que l'application dispose d'une table de correspondance région/département.



5.3.5 Alimentation et mise à jour d'une application à partir d'une copie partielle ou totale des ROR

Contexte

Une application souhaite disposer d'une copie locale, partielle ou totale, des ROR.

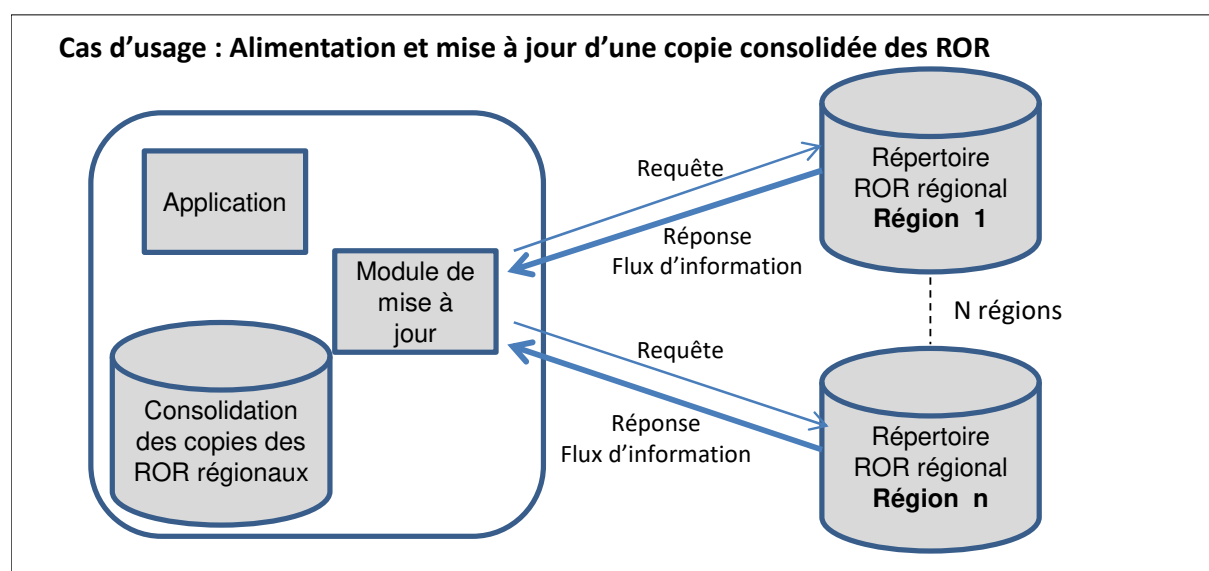
Ce besoin d'une copie locale peut être lié à diverses contraintes : exigences fortes de qualité de service en termes de disponibilité et de performances, contraintes liées à l'existant, etc.

Attention, si l'application utilisatrice nécessite une information temps réel sur la ressource, elle fait appel à l'une des transactions de lecture présentées plus haut.

Principe général

Le protocole d'alimentation et de mise à jour des copies doit être générique. Il ne doit pas être spécifique à une application utilisatrice ni à un champ d'activité.

Le protocole est indépendant des technologies propres aux ROR et aux applications utilisatrices. Il s'appuie sur des standards¹.



N.B : la mise en œuvre de mécanismes de réplique synchrones entre les ROR et les applications utilisatrices n'est pas opportune dans le contexte. Ces mécanismes sont très efficaces au sein d'un parc technologique homogène et faisant l'objet d'une supervision partagée par un nombre réduit d'acteurs.

Transactions associées

Trois transactions sont associées à l'alimentation et la mise à jour d'une copie des données du ROR :

- **TR-Notif-ListeEtablissementsMajAprèsDate**: transaction de notification. L'application externe interroge un ROR Régional afin d'obtenir la liste des structures dans lesquels les ressources ont évolué depuis un instant donné. La demande peut être restreinte à un ou plusieurs champs

¹ Web services SOAP pour les échanges synchrones, Web services REST pour les récupérations d'extractions.

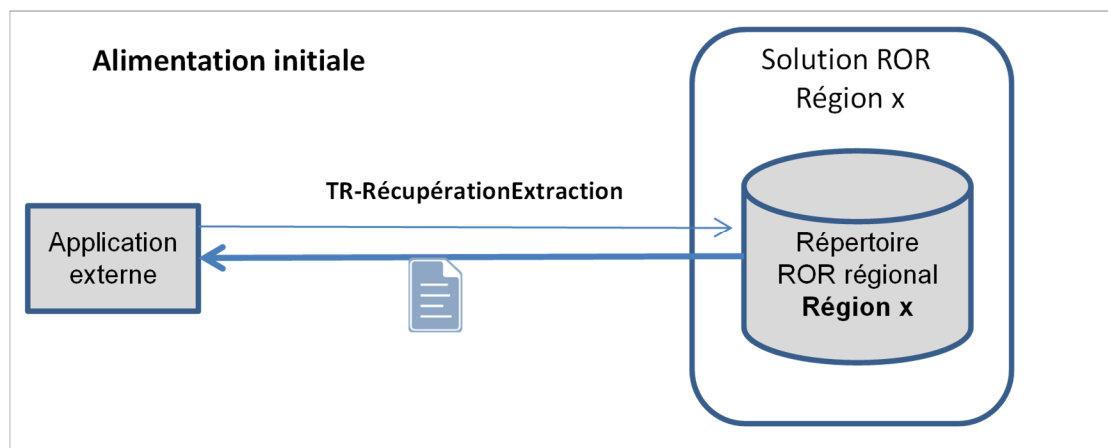
d'activités, auquel cas la réponse ne retiendra que les structures dans lesquels les ressources associées à ces champs d'activités ont évolué.

- **TR-Lecture-OffresSanteEtablissement:** transaction de lecture. Cette transaction est présentée au chapitre précédent.
- **TR-RécupérationExtraction:** chaque ROR met périodiquement à disposition des applications externes des extractions déclinées par champ d'activités (situation actuelle) ou par profils d'accès aux données du ROR contenant tous les champs d'activité (situation cible). La transaction TR-RécupérationExtraction permet à une application externe de récupérer le ou les fichiers d'extraction mis à disposition. Le contenu des fichiers d'extraction n'est pas spécifique à une application cliente. Les fichiers d'extraction sont mis à disposition sur un cadencement donné, ce rythme n'est pas spécifique à chaque application externe.

Principe

- Alimentation initiale de la copie dans l'application externe :

L'application externe utilise la ou les transactions TR-Extraction (une par champs d'activité actuellement, une par profil d'accès en cible).



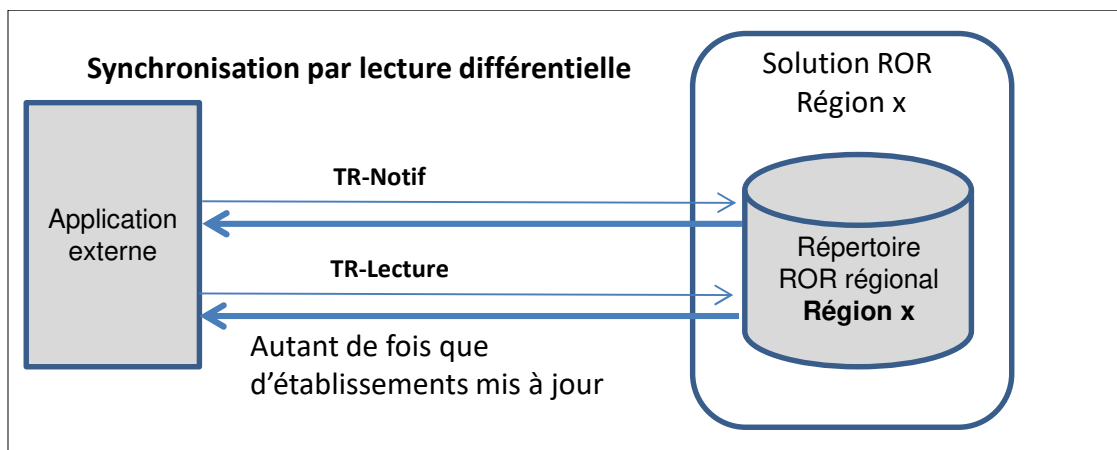
- Mise à jour de la copie dans l'application externe :

Plusieurs principes peuvent être mis en œuvre en fonction des besoins propres à des applications externes.

- Synchronisation par lecture différentielle :

L'application externe invoque la transaction de notification (TR-Notif-ListeEtablissementsMajAprèsDate) à la cadence de son choix vers les ROR de son choix.

L'application externe invoque ensuite des transactions de lecture pour récupérer une copie du descriptif de ressources d'un établissement (ressources actives et ressources désactivées) et l'intégrer dans sa base de données locale selon les processus qui lui sont propres.

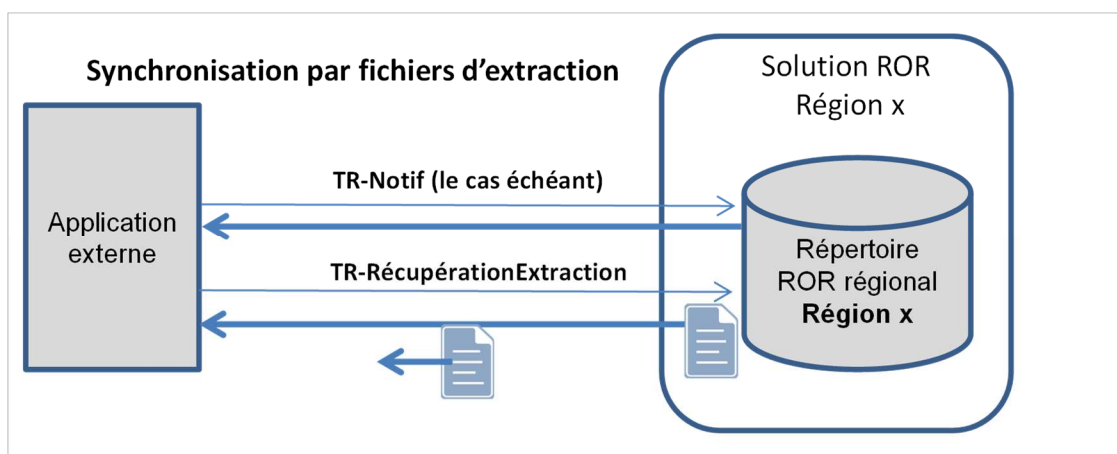


- Synchronisation par fichiers d'extraction :

L'application externe récupère à la cadence de son choix le ou les fichiers d'extraction mis à disposition par les ROR.

Le traitement de mise à jour de la copie locale est sous le contrôle de l'application externe, ce traitement peut se baser à titre d'exemple :

- sur les informations d'horodatage des objets contenus dans le fichier d'extraction,
- sur une utilisation du service de notification pour déterminer les ressources dont il faut tenir compte dans le fichier d'extraction pour la mise à jour.



6 Consommation des données du ROR : politique d'accès aux données du ROR

6.1 Contexte de mise en œuvre

La « politique d'accès aux données du ROR » a pour objet de formaliser les règles, communes à tous les ROR, relatives aux droits d'accès aux données identifiées dans le modèle d'exposition pour l'ensemble des champs d'activités.

Actuellement, les ROR mettent à disposition l'ensemble des données dont ils disposent. La personne morale responsable de l'application qui utilise ces données porte la responsabilité du traitement des données selon la politique d'accès définie dans l'annexe « Programme ROR - Doctrine d'urbanisation - Annexe - Politique d'accès aux données du ROR - situation actuelle » [Réf. 3].

En cible, le ROR mettra à disposition des applications consommatrices les données via des profils d'accès aux données du ROR. La description de ces profils et les règles d'accès aux données par ces profils sont définies dans l'annexe « Programme ROR - Doctrine d'urbanisation - Annexe - Politique d'accès aux données du ROR – situation cible » [Réf. 4].

6.2 Principes d'accès aux données du ROR

6.2.1 Données en libre accès, données à accès restreint et très restreint

Le modèle d'exposition [Réf. 5] décrit les objets utilisés pour exposer l'offre de santé retournée par les ROR lors des échanges entre deux ROR (échanges inter ROR) ou entre un ROR et une application externe (mise à jour d'une application à partir d'un ROR).

Dans le modèle d'exposition, trois types de données distincts sont présents :

- **les données en libre accès** pour le grand public,
- **les données uniquement accessibles en accès restreint** : l'utilisateur est un professionnel identifié, ses droits d'accès dépendent de son rôle métier et de son profil utilisateur,
- **les données uniquement accessibles en accès très restreint** : l'utilisateur est un professionnel identifié, ses droits d'accès dépendent de son rôle métier et de son profil utilisateur.

N.B. : « libre accès » ne signifie pas « obligation de publication ». L'exposition des données en libre accès sur une interface publique par une application utilisatrice des données du ROR dépend de la finalité de cette application et doit être porteuse de sens pour l'utilisateur. Ces données sont par définition accessibles par tout utilisateur.

Les restrictions d'accès aux données par profil d'accès ROR sont établies sur la base des critères suivants :

- La réglementation :
 - la réglementation relative aux données issues des référentiels nationaux ;
 - la réglementation relative à l'interdiction de publicité pour les professionnels de santé libéraux.
- La pertinence de l'accès aux données : un utilisateur ne doit avoir accès qu'à des données qu'il est en mesure de comprendre.

À titre d'exemple, on peut citer les actes spécifiques qui ne sont pas renseignés dans le ROR de façon exhaustive, mais par exception : on ne saisit pas tous les actes que peut réaliser une unité, mais uniquement les actes discriminants, c'est-à-dire ceux qui ne sont pas faits par toutes les unités de même nature, ce qui n'est pas lisible pour un non initié.

- La confidentialité des données : certaines données ne doivent être accessibles qu'aux utilisateurs susceptibles de les utiliser à bon escient.

À titre d'exemple, on peut citer les données à caractère personnel.

Pour rappel, les échanges entre les applications externes et le ROR et les échanges inter-ROR ne contiennent pas de données de santé à caractère personnel.

6.2.2 Profils d'accès aux données du ROR

Un profil d'accès aux données se définit comme un regroupement de données génériques permettant d'afficher les données aux utilisateurs en cohérence avec leurs habilitations.

Les profils d'accès aux données du ROR sont utilisés dans le ROR et dans les applications externes pour exposer les données en libre accès, en accès restreints et très restreints aux utilisateurs en fonction de leurs droits.

Il est prévu 5 profils d'accès aux données :

- Profil 0 - Profil d'accès aux données en libre accès,
- Profil 1 - Accès à toutes les données à accès restreint et très restreint,
- Profil 2 - Accès aux données à accès restreint, hors données très restreintes,
- Profil 3 - Accès aux données à accès restreint sur le champ médico-social (hors données très restreintes) et accès limité aux données en libre accès sur le champ sanitaire,
- Profil 4 - Accès aux données à accès restreint et très restreint d'une structure.

N.B : Accès aux données par les GRADeS

Le GRADeS pilote la mise en œuvre du ROR, l'animation du peuplement et sa mise en qualité. Dans le cadre des missions qui lui sont confiées par l'ARS, les personnels autorisés par le GRADeS peuvent avoir accès à l'ensemble des données dans les limites nécessaires à l'exercice de leur activité.

6.3 Mise en œuvre du contrôle d'accès aux données

6.3.1 Situation actuelle

La politique d'accès est mise en œuvre par le consommateur des données ROR (application externe ou autre ROR).

Les données par profils d'accès aux données du ROR sont décrites dans le document [Réf. 3] Programme ROR - Doctrine d'urbanisation - Annexe Politique d'accès aux données du ROR - situation actuelle.

6.3.1.1 Cas des transactions d'extraction

L'application externe souhaite disposer d'une copie locale, partielle ou totale d'un ROR régional par extraction d'un fichier pour peupler sa base ou vérifier son intégrité.

Chaque ROR met à disposition une extraction par champs d'activité.

L'application externe accède à une ou plusieurs extractions en fonction des champs d'activités inclus dans son périmètre.

Dans ce cas, la politique d'accès est appliquée au niveau de l'application externe.

C'est la personne morale responsable de l'application externe qui a la connaissance de ses utilisateurs et qui porte la responsabilité d'appliquer la politique d'accès. Elle associe un profil d'accès ROR aux utilisateurs de son application conformément à la Politique d'accès aux données du ROR [Réf. 3].

6.3.1.2 Cas des transactions synchrones (notification, lecture)

L'utilisateur final, personne physique, accède au ROR via une application (exemple : consultation du ROR via un SI d'orientation) à travers les transactions synchrones [Réf. 6].

Dans ce cas, la politique d'accès est appliquée au niveau de l'application externe.

C'est la personne morale responsable de l'application externe qui a la connaissance de ses utilisateurs et qui porte la responsabilité d'appliquer la politique d'accès. Elle associe un profil d'accès ROR aux utilisateurs de son application conformément à la Politique d'accès aux données du ROR [Réf. 3].

6.3.1.3 Cas des transactions synchrones recherche inter-ROR

L'utilisateur se connecte directement au ROR.

Dans ce cas, la politique d'accès est appliquée par le ROR auquel se connecte l'utilisateur.

C'est la personne morale, responsable du ROR concerné, qui associe un profil d'accès ROR à l'utilisateur conformément à la Politique d'accès aux données du ROR [Réf. 3].

6.3.2 Situation en cible

La politique d'accès est mise en œuvre par le ROR qui diffuse les données.

Le consommateur des données du ROR (application externe ou autre ROR) envoie le profil d'accès ROR dans les flux d'échange sous forme d'un couple d'informations (rôle métier/profil utilisateur). Ces informations sont définies de la façon suivante :

- Rôle métier de l'utilisateur : le métier de l'utilisateur correspond à la profession ou spécialité qu'il exerce dans un domaine professionnel (ex : infirmier).
- Profil de l'utilisateur : le profil de l'utilisateur dans l'application correspond à sa fonction au sein d'une organisation (ex : gestionnaire de cas).

Les données par profils d'accès aux données du ROR et les couples (rôles métier / profils utilisateurs) associés ainsi que les principes de filtrage sont décrits dans le document [Réf. 4] Programme ROR - Doctrine d'urbanisation - Annexe Politique d'accès aux données du ROR - situation cible.

Le programme ROR gère la matrice [profils d'accès ROR/ couples rôles métier - profils utilisateurs].

6.3.2.1 Cas des transactions d'extraction

L'application externe souhaite disposer d'une copie locale, partielle ou totale d'un ROR régional par extraction d'un fichier pour peupler sa base ou vérifier son intégrité.

Chaque ROR met à disposition une extraction par profil d'accès, tous champs d'activités confondus conformément à la politique d'accès aux données du ROR [Réf. 4].

L'application externe transmet le couple (rôle métier, profil utilisateur) correspondant au profil d'accès aux données du ROR validé au moment de son intégration dans l'espace de confiance ROR (exemple : automate/ orientation médico-sociale) dans une assertion SAML de type VIHF afin que le ROR puisse gérer l'accès aux données sous la forme d'un profil d'accès aux données du ROR.

Le ROR ne transmet en réponse que l'extraction pour ce profil d'accès.

C'est la personne morale responsable de l'application externe qui a la connaissance de ses utilisateurs et qui porte la responsabilité d'appliquer la politique d'accès. Elle associe un profil d'accès ROR aux utilisateurs de son application conformément à la Politique d'accès aux données du ROR [Réf. 4].

6.3.2.2 Cas des transactions synchrones de notification et lecture

L'application externe connaît les informations relatives au rôle métier et au profil de l'utilisateur à l'origine de la transaction (application externe ou utilisateur physique).

Elle transmet le couple (rôle métier, profil utilisateur) dans une assertion SAML de type VIHF afin que le ROR puisse gérer l'accès aux données sous la forme d'un profil d'accès aux données du ROR. Cette association est décrite dans le document [Réf. 4] et plus particulièrement dans la grille d'accès aux données. En fonction du contexte d'utilisation, ce couple peut prendre des valeurs qui caractérisent l'application externe (exemple : automate/ orientation médico-sociale) ou qui caractérise l'utilisateur (exemple : médecin/ PS en Centres Antipoison et de Toxicovigilance).

Le ROR ne transmet en réponse que les données autorisées pour ce profil d'accès.

Il y a là un enjeu de cohérence et de rapidité de mise en application des évolutions de la politique d'accès : l'affectation des couples (rôle métier, profil utilisateur) aux profils d'accès peut évoluer, de même que la définition d'un profil d'accès (données concernées) ou bien le nombre de profils d'accès.

C'est l'application externe qui a la connaissance de ses utilisateurs et qui porte la responsabilité d'appliquer la politique d'accès. Elle associe un profil d'accès ROR aux utilisateurs de son application conformément à la Politique d'accès aux données du ROR [Réf. 4].

6.3.2.3 Cas des transactions synchrones de recherche inter-ROR

L'utilisateur final, personne physique, accède au ROR.

Le ROR appelant a enregistré l'utilisateur et notamment :

- Identité du professionnel,
- Rôle métier,
- Profil utilisateur,
- Moyen d'authentification :
 - id/mot de passe pour un accès via l'IHM des solutions ROR ;
 - certificat CPS (Distinguished Name) si accès via Web service ;
 - e-CPS – Pro Santé Connect.

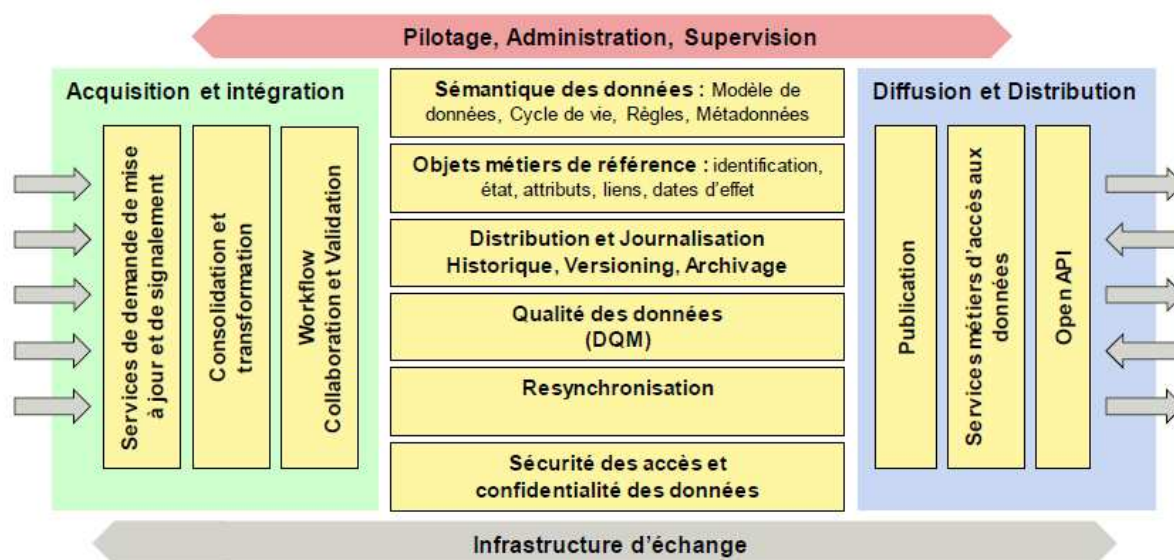
Le ROR appelant transmet le couple (rôle métier, profil utilisateur) dans une assertion SAML de type VIHF afin que le ROR appelé puisse gérer l'accès aux données sous la forme d'un profil d'accès aux données du ROR. Le ROR appelé ne transmet en réponse que les données autorisées pour cet utilisateur.

7 Annexe : Rappel de la définition d'un référentiel de données

Positionner un gisement de données en tant que référentiel de données dans l'urbanisation des systèmes d'information de santé nécessite de partager une définition précise et normée de cette notion. La définition et les caractéristiques du référentiel de données utilisées dans cette annexe font référence au document « *Cadre Commun d'Architecture des référentiels de données* », publié par la DINSIC en complément au « *Cadre Commun d'Urbanisation du Système d'Information de l'état* »¹. Ces concepts sont étendus et complétés dans le contexte des secteurs santé et médico-social.

En première approche, un référentiel de données peut être défini comme un ensemble cohérent d'informations centrales communes à tous. Il répond aux besoins d'établir un langage partagé entre plusieurs acteurs et de fournir une vision commune sur les données constitutives du référentiel et leur utilisation, en respectant des règles de normalisation des données et une certaine qualité.

Le référentiel de données présente une architecture générale, des caractéristiques et des services associés schématisés dans le « *Cadre Commun d'Architecture des référentiels de données* » de la façon suivante :



Les données de référence sont définies par les caractéristiques principales suivantes :

- **la sémantique des données de référence est partagée et stable dans le temps**

La sémantique des données doit être partagée entre les référentiels et les applications qui utilisent les données de référence. Ce modèle est commun en termes d'échange et de partage de données tout en restant neutre technologiquement. La description de la sémantique et des nomenclatures doit être accessible à tous les utilisateurs du référentiel.

Application dans la Santé :

¹ (<http://references.modernisation.gouv.fr/urbanisation-du-systeme-dinformation-de-letat>). DINSIC : direction interministérielle du numérique et du système d'information et de communication de l'Etat.

Le modèle des objets de santé (MOS) et les nomenclatures des objets de santé (NOS) participent à la définition partagée de la sémantique des référentiels de données :

- *le MOS décrit les objets de santé, par exemple un professionnel de santé ;*
- *les NOS correspondent à des listes de valeurs possibles pour les objets du MOS quand les valeurs sont codifiées.*

Le modèle d'exposition des données des ROR régionaux. Ce modèle est commun à tous les ROR et partage une sémantique commune avec le RPPS et FINESS.

- **les objets métiers ont un identifiant unique de référence**

L'entité en charge de la gestion du référentiel est chargée de l'attribution d'un identifiant unique national aux objets du périmètre du référentiel. Cet identifiant permet de faire référence à la description de l'objet dans le référentiel et permet toute logique de rapprochement lors d'échange ou de partage d'information entre les systèmes d'information.

Il est très fortement souhaitable que l'Identifiant soit non signifiant, c'est-à-dire que sa valeur soit sans lien avec des données métier de l'objet concerné, afin d'assurer l'invariance de l'identifiant lors de variation de données métiers.

L'identification des objets est sous la responsabilité du gestionnaire du référentiel, sauf si ces objets disposent déjà d'un identifiant dans un autre référentiel.

Application dans la santé : Dans le ROR, l'identification des unités internes à un établissement est assurée par le gestionnaire du ROR, l'identification de l'établissement est du ressort du référentiel FINESS.

- **Les données de référence ont un point de vérité unique**

Pour une donnée de référence, le référentiel de données est l'unique point de vérité de la donnée.

- **les données de référence ont une durée de vie qui va au-delà des processus opérationnels**

Une donnée de référence ne doit pas être supprimée physiquement, elle doit être supprimée logiquement, elle peut être archivée. Les objectifs de l'historisation sont multiples : analyse des données de référence et de leurs évolutions (pilotage du référentiel), Imputabilité dans le temps de toute opération conditionnée par la valeur de la donnée de référence au moment de son usage. En termes de moyen, l'historique des changements peut être porté par des métadonnées associées à la donnée de référence (date de création, date de modification, date de suppression logique). L'historique des données peut aussi être porté au niveau métier, par exemple la date de fin d'une activité libérale ou salariée d'un professionnel de santé dans le RPPS.

- **la qualité des données de référence est critique pour un grand nombre de processus**

Un processus de contrôle de la qualité des données doit être mis en place en association avec une démarche d'amélioration continue. Un processus de signalement des anomalies doit être proposé aux utilisateurs des données de référence.

- **le référentiel de données doit répondre à une politique de sécurité**

Le référentiel de données respecte des critères de sécurité déclinés notamment sur les axes suivants :

- disponibilité : aptitude du référentiel à remplir sa fonction dans des niveaux de services définis ;
- intégrité : propriété assurant qu'une donnée n'a pas été modifiée ou détruite de façon non autorisée. Non-altération des données pour toute la durée de leur usage, y compris pour les données historisées ;

- confidentialité : seuls les utilisateurs autorisés ont accès aux informations qui leur sont destinées, certaines de ces données peuvent être mises à disposition en libre accès. Des dispositifs de contrôle d'accès adaptés au niveau de sensibilité des informations doivent être mis en œuvre ;
- preuve (ou auditabilité, imputabilité) : garantie de disposer des éléments qui apportent la preuve des traitements ou autres événements relatifs aux informations considérées. Il doit être possible d'imputer à leur auteur toutes opérations sur les données du référentiel. L'auteur peut être une personne physique ou un organisme fournissant des données au référentiel.

Application dans la santé : Les règles du référentiel de sécurité PGSSI-S¹ s'appliquent dès lors qu'un référentiel contient des données de santé à caractère personnel, si nécessaire, les règles peuvent être opportunément réutilisées si les référentiels de données contiennent des informations à accès restreint.

- **les données de référence sont utilisées fréquemment et sont consommées par plusieurs systèmes d'information**

Le processus d'acquisition doit être cadré : les processus et règles d'alimentation des référentiels doivent être clairement explicités. Ils peuvent être définis par voie législative et/ou réglementaire.

- **la facilité d'accès aux données de référence est critique et conditionne l'efficacité et l'efficience globales des solutions utilisatrices**

Les règles et processus d'accès aux données doivent être documentés et mis à disposition des services aux organismes ayant réglementairement le droit d'accès aux données.

Application dans la santé : Le référentiel d'interopérabilité, le CI-SIS², participe le cas échéant à la spécification des protocoles d'accès aux référentiels.

Les référentiels d'homologation sont susceptibles d'être enrichis, notamment pour l'homologation de l'accès des applications aux référentiels.

- **Le référentiel évolue dans un cadre maîtrisé**

Une gouvernance doit être mise en place pour assurer le pilotage d'ensemble du référentiel tant opérationnel que stratégique.

¹ PGSSI-S : Politique générale de Sécurité des Systèmes d'Information de Santé

² CI-SIS : cadre d'interopérabilité des systèmes d'information de santé.