AGENCE
DU NUMÉRIQUE
EN SANTÉ

Volet Transport synchrone pour applications mobiles

CI-SIS

Statut : validé | *Classification : publique* | *Version : 1.1*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1. INTRODUCTION

1.1. Positionnement dans le CI-SIS

Ce document présente les spécifications techniques du volet Transport synchrone pour applications mobiles. Il s'agit d'un volet de la couche transport du cadre d'interopérabilité des systèmes d'information de santé, complémentaire au volet Transport synchrone pour client lourd.

1.2. Lectorat cible

Ce document s'adresse aux développeurs des interfaces interopérables impliquant des échanges synchrones entre applications mobiles et systèmes d'information de santé (SIS) et à toute autre personne intervenant dans le processus de mise en place de ces interfaces.

1.3. Périmètre

Ces spécifications décrivent les mécanismes de transport synchrone pour applications mobiles. Dans le cadre de ce document, on entend par application mobile toute application destinée à être exécutée sur des terminaux mobiles tels que les smartphones et les tablettes. Ces applications sont de deux types: applications mobiles web ou applications mobiles natives.

Ces applications doivent être des applications confidentielles, c'est-à-dire capables de stocker des mots de passe ou des clés de manière sécurisée (dans un serveur applicatif par exemple).

La spécificité de ces applications est qu'elles doivent fonctionner dans un environnement à ressources réduites : processeur, mémoire, batterie et bande passante en réseau mobile. Les dispositions de sécurité doivent aussi être renforcées pour être adaptées à cet environnement exposé.

Ces spécifications sont recommandées pour les implémentations en applications mobiles mais ne sont pas réservées à ces dernières. Le terme « applications mobiles » utilisé par la suite dans le document n'est pas restrictif. Ces spécifications pourraient être mises en œuvre par des applications de type « client lourd ».

1.4. Standards utilisés

Ces spécifications techniques se basent sur les standards suivants:

- **HTTP 1.1** RFC 7230 – 7235 de l'IETF
- **TLS 1.2** (ou supérieur) RFC 5246 de l'IETF
- **JSON** RFC 7159 de l'IETF
- **OpenID Connect 1.0** (OIDC 1.0) de l'OIDF (OpenID Foundation)
- **OAuth 2.0** RFC 6749 et RFC 6750 de l'IETF
- **JWT (JSON Web Token)** RFC 7519, **JWS** RFC 7515, **JWE** RFC 7516, **JWA** RFC 7518 de l'IETF
- **FHIR STU3 Security labels** d'HL7
- **HEART Profile for OAuth 2.0**, **HEART Profile for OpenID Connect 1.0** de l'OIDF

2. SPECIFICATIONS

2.1. Les acteurs

Utilisateur final : Le professionnel, le patient ou une autre personne qui souhaite accéder aux ressources ou services d'un système cible via une application mobile.

Système initiateur : L'application mobile, web ou native, qui assure les interactions avec l'utilisateur final et qui échange avec le système cible.

Système cible : Le fournisseur de ressources et de services abritant les ressources et mettant à disposition les services qui intéressent l'utilisateur final.

> ***N. B. Le système cible est un système tiers différent du serveur applicatif de l'application mobile. Dans le cas d'une application web mobile, par exemple, c'est le couple client/serveur web qui constitue le système initiateur.***

Exemples d'acteurs : Le système initiateur est une application de gestion de cabinet en ligne utilisée par un médecin généraliste sur sa tablette lors d'une consultation à domicile du patient. Le système cible est une plateforme de partage de documents de santé.

2.2. Les flux

Les échanges synchrones entre le système initiateur et le système cible se décomposent en deux types de flux :

- **Les requêtes métier** : le système initiateur fait des appels à des services web permettant de déclencher des actions sur des ressources du système cible. Ces requêtes doivent être dotées d'une autorisation, preuve d'authentification de l'utilisateur final affirmant son identité.
- **Les réponses métier** : Après validation de l'autorisation du système initiateur, le système cible répond à la requête reçue.

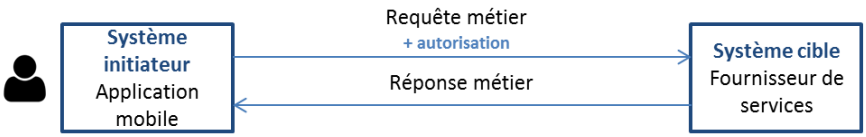

Figure 1 Echanges synchrones entre système initiateur et système cible

Le contenu métier des flux dépend du contexte de mise en place de ces échanges et peut être défini par les volets de la couche services du CI-SIS et de la couche contenu le cas échéant.

2.2.1. Transport

Les échanges se font sur le protocole HTTP 1.1 encapsulé dans une connexion sécurisée TLS (version 1.2, ou supérieure, recommandée).

Les **méthodes** HTTP doivent être utilisées conformément à la sémantique définie par le protocole.

Les **entêtes** HTTP doivent être utilisés conformément à la sémantique définie par le protocole.

- L'entête HTTP *Category*[1] peut être utilisé pour indiquer qu'il s'agit d'un accès en mode bris de glace[2] tel que décrit dans la documentation *FHIR Security Labels*[3]. Exemple :

```
Category: http://hl7.org/fhir/security-label#break-the-glass;
scheme="http://hl7.org/fhir/tag/security"; label="Break The Glass"
```

- De la même manière, l'entête HTTP *Category* peut être utilisé pour indiquer le niveau de restriction d'audience à appliquer aux traces générées par la transaction objet du flux[4].
  Les valeurs possibles pour ce champ doivent être un code provenant de la terminologie de référence suivante :
  - TRE_A07-StatutVisibiliteDocument, OID : 1.2.250.1.213.1.1.4.13

  Les valeurs possibles peuvent être restreintes en fonction du jeu de valeurs correspondant mis à disposition par le projet.
  En l'absence de spécifications complémentaires, le jeu de valeurs suivant peut être utilisé : JDV_J22-RestrictionAudienceVIHF-CISIS.

  Exemple :

```
Category: INVISIBLE_REPRESENTANTS_LEGAUX;
scheme="urn:oid:1.2.250.1.213.1.1.4.13"; label=" Non visible par
les représentants légaux du patient"
```

- L'entête HTTP *User-Agent* peut être utilisé pour indiquer, entre autres, l'identifiant, la version et le nom du système initiateur[5].

Les échanges applicatifs de données structurées peuvent se faire au format JSON ou XML : le système cible, jouant le rôle de fournisseur de services, **doit** supporter les deux formats pour laisser aux systèmes initiateurs le choix du format à adopter.

2.2.2. Autorisation

L'autorisation présentée par le système initiateur au système cible porte la preuve d'authentification de l'utilisateur. Il s'agit d'un **jeton** porté par l'élément d'entête « Authorization » de type « Bearer » tel que défini par le standard OAuth 2.0.

```
Authorization: Bearer <token>
```

Ce jeton doit avoir une validité limitée dans le temps. Pour que le système initiateur soit en possession du dernier jeton valide, ce dernier peut lui être transmis à chaque réponse métier par le système cible.

> ***Cf. la section 3.1 pour avoir plus d'informations sur le processus d'obtention du jeton et la structuration de celui-ci.***

[1] https://tools.ietf.org/html/draft-johnston-http-category-header-02
[2] L'accès en bris de glace permet à un professionnel de santé d'étendre de manière exceptionnelle ses droits d'accès lorsqu'une situation d'urgence le justifie. Par exemple, dans une situation où la vie du patient est en danger, un médecin, ne faisant pas partie de son équipe de prise en charge, peut accéder en mode bris de glace au dossier du patient sans consentement préalable de celui-ci. Cet accès exceptionnel est généralement demandé dans une situation de prise en charge en urgence. Il doit être rigoureusement tracé par le système cible.
[3] https://www.hl7.org/fhir/security-labels.html#break-the-glass
[4] Cette information correspond au champ Confidentiality_Code du VIHF.
[5] Ces informations correspondent aux champs LPS_id, LPS_version et LPS_nom du VIHF.

3. DISPOSITIONS DE SECURITE

3.1. Identification et authentification

Cette section présente le processus d'obtention du jeton qui comporte, entre autres, les étapes d'identification et d'authentification de l'utilisateur.

De nouveaux acteurs, en plus du système initiateur et du système cible peuvent entrer en jeu pour assurer l'identification et l'authentification de l'utilisateur et la création du jeton.

Les nouveaux acteurs :

- **Le serveur d'identification**: Une plateforme d'identification, distincte du système cible, capable d'authentifier l'utilisateur final et de fournir les informations sur le contexte d'authentification et les informations d'identification au système cible auquel le système initiateur veut accéder.
- **Le fournisseur de services annuaires** : Les annuaires nationaux, tel que le RPPS, qui fournissent des informations sur les utilisateurs, notamment sur les professionnels de santé. Ces informations permettent d'affiner les droits d'accès de ces derniers au système cible. Ces informations peuvent être demandées par le serveur d'identification ou par le système cible lui-même. Ces flux ne sont pas spécifiés dans ce volet.

Deux configurations possibles d'authentification de l'utilisateur final sont décrites:

- une configuration avec authentification déléguée ;
- une configuration avec authentification directe.

> ***N.B. Le jeton est appelé jeton d'identification (ID Token d'OpenID Connect) dans la configuration avec authentification déléguée (cf.3.1.1.3.1). Il est appelé jeton d'accès (Access Token du standard OAuth 2.0) dans la configuration avec authentification directe (cf. 3.1.2.3).***

3.1.1. Configuration avec authentification déléguée

Cette configuration met en scène le système initiateur, le système cible, un serveur d'identification et optionnellement un fournisseur de services annuaires. Le système cible délègue l'authentification de l'utilisateur final au serveur d'identification.

Les échanges entre ces différents acteurs permettent de fournir un jeton, appelé jeton d'identification, au système initiateur et **doivent respecter les spécifications du standard OpenID Connect**, flux avec code d'autorisation (*authorization code flow*), lui-même étant basé sur le standard OAuth 2.0. Les exemples donnés dans les sections suivantes sont non normatifs et sont issus des spécifications du standard.

3.1.1.1. Prérequis

Contractualisation entre le système cible et le serveur d'identification

La délégation d'authentification des utilisateurs doit être préalablement formalisée entre le système cible et le serveur d'identification. Dans ce sens, le système cible doit être enregistré auprès du serveur d'identification en tant que client[6]. Il fournit lors de son enregistrement au moins une url de redirection (« redirect_uri ») et le serveur d'identification lui attribue un identifiant client

[6] *Cf.* Documentation OAuth 2.0 sur l'enregistrement des clients, référencée par les spécifications OpenID Connect : https://tools.ietf.org/html/rfc6749#section-2

(« client_id ») et éventuellement ses informations d'authentification (mot de passe « client_secret » à titre d'exemple). Le serveur d'identification lui fournit aussi les URL de ses endpoints.

Le serveur d'identification peut proposer un mécanisme d'enregistrement dynamique de ses clients (systèmes cibles). Dans ce cas les spécifications OpenID Connect sur l'enregistrement dynamique des clients s'appliquent[7].

Un système cible peut contractualiser avec plusieurs serveurs d'identification.

L'enrôlement du système cible peut permettre la déclaration d'un ensemble de systèmes faisant partie du même ensemble applicatif. Le même jeton permettra l'accès à ces différents systèmes déclarés.

Enrôlement de l'utilisateur auprès du serveur d'identification

L'enrôlement initial des utilisateurs auprès du serveur d'identification doit se faire dans le respect des référentiels de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

3.1.1.2. Les flux d'obtention de jetons

Les flux d'obtention de jetons en configuration avec authentification déléguée s'articulent autour de quatre étapes clés :

- **La demande du code d'autorisation** : Le code d'autorisation constitue une procuration d'accès donnée par l'utilisateur à son application et qui est transmise par la suite au système cible. Le code d'autorisation est valable une seule fois. *(Flux en bleu dans* Figure 2*)*
- **L'authentification de l'utilisateur** : L'authentification de l'utilisateur doit être forte et doit passer par un agent distinct de l'application. En s'authentifiant, l'utilisateur consent à donner le code d'autorisation à son application. *(Etape rouge dans Figure 2)*
- **Demande de jeton** : Le jeton est une autorisation d'accès que demande le système cible après s'être authentifié et avoir présenté le code d'accès pour qu'elle soit utilisée par le système initiateur par la suite. Il représente aussi la preuve d'authentification de l'utilisateur. *(Flux en vert dans Figure 2)*
- **Demande d'informations utilisateur** : Les informations utilisateur dont dispose le serveur d'identification permettent au système cible de mettre en œuvre les droits d'accès adéquats. *(Flux en orange dans Figure 2)*

[7] *Cf.* Spécifications OpenID Connect sur l'enregistrement dynamique des clients : http://openid.net/specs/openid-connect-registration-1_0.html

Les flux s'organisent de la manière suivante :

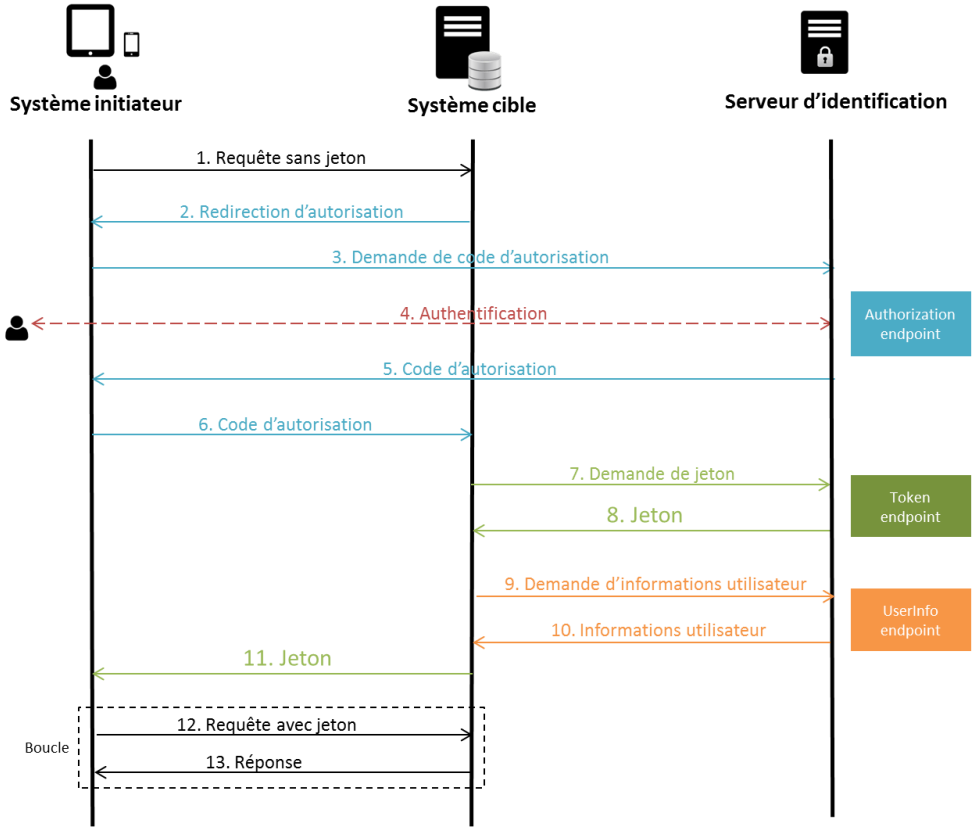

Figure 2 Diagramme de séquence des flux de la configuration avec authentification déléguée

1. Requête sans jeton

L'utilisateur essaie d'accéder via son application, le système initiateur, à une ressource ou un service proposé par le système cible. Une requête HTTP est envoyée sans jeton.

2. Redirection d'autorisation

Le système cible construit la demande de code d'autorisation pour le système initiateur et le redirige vers le serveur d'identification.

La demande d'autorisation doit comporter les paramètres suivants :

- **response_type** : Ce paramètre doit prendre la valeur « **code** » indiquant ainsi qu'il s'agit d'un flux pour l'obtention d'un code d'autorisation.
- **scope** : Ce paramètre permet de spécifier le cadre de l'autorisation demandée via OAuth. Il doit prendre la valeur « **openid** » indiquant ainsi qu'il s'agit d'une requête pour une authentification et un jeton d'identification OpenID Connect.
- **client_id** : L'identifiant du système cible auprès du serveur d'identification.
- **state** : Une valeur envoyée pas le système cible pour maintenir la session entre la première requête du système initiateur et le retour de ce dernier après authentification de l'utilisateur.
- **redirect_uri** : l'URL de retour vers le système cible après l'authentification de l'utilisateur.
- **nonce** : Chaine de caractère associant la session du système cible au jeton. Le nonce sera intégré tel quel au jeton d'identification. Le « nonce » permet d'éviter les attaques par rejeu.

Ce flux peut être une réponse HTTP de redirection (code HTTP 302) spécifiant l'URL de l'endpoint d'authentification.

```
HTTP/1.1 302 Found
  Location: https://serveur.exemple.com/authorize?
    response_type=code
    &scope=openid
    &client_id=s6BhdRkqt3
    &state=af0ifjsldkj
    &redirect_uri=https%3A%2F%2Fsystemecible.exemple.org%2Fcb
```

3. Demande de code d'autorisation

Le système initiateur envoie la demande de code d'autorisation, préparée par le système cible, au serveur d'identification.

```
GET /authorize?
    response_type=code
    &scope=openid
    &client_id=s6BhdRkqt3
    &state=af0ifjsldkj
    &redirect_uri=https%3A%2F%2Fsystemecible.exemple.org%2Fcb HTTP/1.1
  Host: serveur.exemple.com
```

4. Authentification

L'authentification peut se faire à travers des méthodes différentes mais doit respecter les référentiels de la PGSSI-S.

Ce dialogue avec l'utilisateur permet aussi de récupérer les données contextuelles de la demande d'accès, notamment :

- les informations concernant la situation d'exercice du professionnel en lien avec sa demande d'accès (secteur d'activité, nom et identifiant de l'établissement). Ces informations sont portées par le jeton d'informations utilisateur par la suite (cf. section 0),
- la raison de la demande d'un accès exceptionnel le cas échéant.

N.B. Le traitement des données des utilisateurs doivent se conformer aux recommandations de la CNIL en termes respect des libertés, de la vie privée et des droits des utilisateurs sur leurs données.

5. Réponse à la demande de code d'autorisation

Après authentification de l'utilisateur final, le serveur d'identification renvoie le système initiateur vers le système cible en utilisant le paramètre *redirect_uri* du flux 3 et lui fournit le code d'autorisation demandé.

```
HTTP/1.1 302 Found
Location: https://systemecible.exemple.org/cb?
          code=SplxlOBeZQQYbYS6WxSbIA
           &state=af0ifjsldkj
```

6. Transmission du code d'autorisation

Le système initiateur utilise l'URL envoyée par le serveur d'identification pour transmettre au système cible le code d'autorisation ainsi que le statut de session.

7. Demande de jeton

Le système cible envoie une requête au serveur d'identification, sur son endpoint de jetons, pour échanger le code d'autorisation contre un jeton d'identification. Ce flux devrait aussi permettre l'authentification, au niveau applicatif, du système cible auprès du serveur d'identification. Cela peut être assuré, par exemple, par l'élément d'entête « Authorization » contenant un identifiant et un mot de passe encodés[8] ou un jeton JWT.

[8] https://tools.ietf.org/html/rfc6749#section-2.3.1

Tous les échanges entre le système cible et le serveur d'identification doivent se faire dans le cadre d'une connexion TLS avec authentification mutuelle.

Ci-dessous un exemple de requête pour l'obtention d'un jeton d'identification :

```
POST /token HTTP/1.1
  Host: serveur.exemple.com
  Content-Type: application/x-www-form-urlencoded
  Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

  grant_type=authorization_code&code=SplxlOBeZQQYbYS6WxSbIA
    &redirect_uri=https%3A%2F%2Fsystemecible.exemple.org%2Fcb
```

8. Réponse à la demande de jeton

Une fois le système cible authentifié et le code d'autorisation validé, le serveur d'identification fournit au système cible :

- Un jeton d'identification, *id_token* (cf. 3.1.1.3.1),
- Un jeton d'accès, *access_token,* permettant au système cible d'accéder ultérieurement au serveur d'identification sur son endpoint d'informations utilisateur,
- Optionnellement un jeton d'actualisation, *refresh_token*.

La durée de vie du jeton d'identification est définie par le serveur d'identification et/ou le système cible lors de la contractualisation[9]. Par ailleurs, le système cible peut mettre en place un service de révocation de jeton avant son expiration permettant ainsi à l'utilisateur de se déconnecter.

```
HTTP/1.1 200 OK
  Content-Type: application/json
  Cache-Control: no-store
  Pragma: no-cache

  {
   "access_token": "SlAV32hkKG",
   "token_type": "Bearer",
   "refresh_token": "8xLOxBtZp8",
   "expires_in": 3600,
   "id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjFlOWdkazcifQ.ewogImlzc
     yI6ICJodHRwOi8vc2VydmVyLmV4YW1wbGUuY29tIiwKICJzdWIiOiAiMjQ4Mjg5
     NzYxMDAxIiwKICJhdWQiOiAiczZCaGRSa3F0MyIsCiAibm9uY2UiOiAibi0wUzZ
     fV3pBMk1qIiwKICJleHAiOiAxMzExMjgxOTcwLAogImlhdCI6IDEzMTEyODA5Nz
     AKfQ.ggW8hZ1EuVLuxNuuIJKX_V8a_OMXzR0EHR9R6jgdqrOOF4daGU96Sr_P6q
     Jp6IcmD3HP99Obi1PRs-cwh3LO-p146waJ8IhehcwL7F09JdijmBqkvPeB2T9CJ
     NqeGpe-gccMg4vfKjkM8FcGvnzZUN4_KSP0aAp1tOJ1zZwgjxqGByKHiOtX7Tpd
     QyHE5lcMiKPXfEIQILVq0pc_E2DzL7emopWoaoZTF_m0_N0YzFC6g6EJbOEoRoS
     K5hoDalrcvRYLSrQAZZKflyuVCyixEoV9GfNQC3_osjzw2PAithfubEEBLuVVk4
     XUVrWOLrLl0nx7RkKU8NXNHq-rvKMzqg"
  }
```

9. Demande d'informations utilisateur

Le système cible peut déléguer la gestion des informations des utilisateurs au serveur d'identification et plus précisément à son endpoint d'informations utilisateur (User Info endpoint) tel que c'est défini dans les spécifications OpenID Connect.

[9] La durée de vie du jeton ne doit pas dépasser une heure, telle que recommandée dans les spécifications HEART pour les flux avec code d'autorisation.

Le système cible envoie une requête pour demander ces informations et utilise le jeton d'accès (*access_token*) qu'il a reçu à l'étape précédente pour s'authentifier auprès de l'endpoint d'informations utilisateur.

```
GET /userinfo HTTP/1.1
  Host: serveur.exemple.com
  Authorization: Bearer SlAV32hkKG
```

Le support de ce flux est optionnel si le système cible peut disposer, par un autre moyen, des informations nécessaires à la mise en place des droits d'accès de l'utilisateur, en faisant appel à un service annuaire par exemple.

10. Réponse à la demande d'informations utilisateur

Un ensemble d'informations, définies dans la section 3.1.1.2, sont encapsulées dans un jeton JWT sécurisé et sont renvoyées par le serveur d'identification si l'utilisateur a déjà consenti à ce transfert lors de l'authentification. Le content-type de la réponse doit être « application/jwt ».

```
HTTP/1.1 200 OK
  Content-Type: application/jwt

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIyNDgyODk3NjEwMDEiLCJuYW1l
IjoiSmFuZSBEb2UiLCJnaXZlbl9uYW1lIjoiSmFuZSIsImZhbWlseV9uYW1lIjoiRG9lIiwic
HJlZmVycmVkX3VzZXJuYW1lIjoiai5kb2UiLCJlbWFpbCI6ImphbmVkb2VAZXhhbXBsZS5jb2
0iLCJwaWN0dXJlIjoiaHR0cDovL2V4YW1wbGUuY29tL2phbmVkb2UvbWUuanBnIn0.ibiK7a8
EheGjDYbL5-E7oN1gvm6zwm5c7ASvivu4mHY
```

Le support de ce flux, qui constitue la réponse au flux précédent, est aussi optionnel.

Le système cible peut, par railleurs, récupérer des informations d'identité complémentaires des annuaires nationaux tels que le RPPS.

11. Transmission du jeton

Le système cible transmet par la suite le jeton d'identification, *id_token*, au système initiateur.

12. Requête avec jeton

Le système initiateur utilise le jeton d'identification dans ses échanges avec le système cible. Typiquement le jeton d'identification sera porté par l'élément d'entête « Authorization » de type « Bearer » tel que c'est défini par le standard OAuth 2.0.

```
Authorization: Bearer <token>
```

3.1.1.3. Les jetons

3.1.1.3.1. Le jeton d'identification

Le jeton d'identification, ou *id_token*, est un *JWT* signé (*JWS)* dont le *payload* est constitué de l'ensemble des assertions listées ci-dessous. Les assertions sont issues des spécifications de l'ID Token du standard OpenID Connect. Le contenu de certaines assertions a été spécifié et adapté au système de santé français.

> ***Exigences en lien avec la signature du jeton :***
> ***- chiffrement asymétrique,***
> ***- clé RSA 2048 au minimum,***
> ***- algorithmes de chiffrement recommandés : ECDSA P-521 SHA-512 / RSA SHA-512.***

Tableau 1 Assertions du jeton d'identification (id_token)

Assertion	Type[10] et jeu de valeurs	Requis / Optionnel	Description
iss	*StringOrURI*	R	Identité de l'émetteur du jeton. URL de l'endpoint de jetons du serveur d'identification.
sub	*Identifier*[11] ► Pour un **professionnel de santé** : format identifier du *profil fr-practitioner* de la ressource FHIR *Practitioner* (s'appuyant sur le format PS-IdNat[12]) ► Pour un **usager du système de santé** : format identifier du profil *fr-patient* de la ressource FHIR Patient	R	Identifiant de l'utilisateur final, du sujet authentifié.
aud	*Array of StringOrURI* Liste d'URI (URL ou URN:OID par exemple) comportant au moins une entrée	R	Ce champ contient la liste des identifiants des systèmes cibles pour lesquels le jeton a été fourni. La liste doit contenir au moins une entrée. Il doit compter parmi ses valeurs la valeur du champ OAuth 2.0 client_id du système cible.
exp	*NumericDate*	R	Date et heure exprimées en temps universel coordonné (UTC) de fin de validité du jeton.
iat	*NumericDate*	R	Date et heure exprimées en temps universel coordonné (UTC) de création du jeton.
Auth_time	*NumericDate*	O	Date et heure en temps universel coordonné (UTC) auxquelles l'authentification de l'utilisateur final a été réalisée.
jti	*StringOrURI*	R[13]	Identifiant unique du jeton permettant de révoquer le jeton et empêcher le rejeu.
nonce	*StringOrURI*	R[13]	Chaine de caractère associant la session du système cible à l'ID token. Contient la valeur du nonce de la requête d'authentification du système cible. Le « nonce » est nécessaire afin d'éviter les attaques par rejeu.
acr	*StringOrURI*	O	Classe de la méthode d'authentification de l'utilisateur final. Elle prend la valeur « 0 » lorsque la méthode d'authentification ne répond pas aux exigences du niveau 1 de la norme ISO/IEC 29115. Sinon elle prend ses valeurs parmi les contextes d'authentification SAML : « Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 »[14].
amr	*Array of StringOrURI*	O	Liste des méthodes d'authentification de l'utilisateur final. Jeu de valeurs défini par la RFC 8176 : « Authentication Method Reference Values »[15]

[10] Types de données JSON. Les types *NumericDate* et *StringOrURI* sont définis dans les spécifications JWT (*cf.* https://tools.ietf.org/html/rfc7519#section-2)
[11] Type Identifier de FHIR au format JSON: https://www.hl7.org/fhir/datatypes.html#identifier
[12] ANS : CI-SIS – Annexe transversale Sources des données métier pour les personnes et les structures
[13] Contrainte introduite par ces spécifications pour des raisons de sécurité
[14] https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf
[15] https://tools.ietf.org/html/rfc8176

3.1.1.3.2. Le jeton d'informations utilisateur

Les assertions du jeton d'informations utilisateur, *userinfo_token*, proviennent pour la plupart des spécifications des User Info claims d'OpenID Connect et des spécifications du VIHF 3.0 (Vecteur d'Identification et d'Habilitation Formelles) du volet Transport Synchrone pour Client Lourd du CI-SIS.

Le *userinfo_token* est un JWT signé (JWS).

> ***Exigences en lien avec la signature du jeton :***
> ***- chiffrement asymétrique,***
> ***- clé RSA 2048 au minimum,***
> ***- algorithmes de chiffrement recommandés : ECDSA P-521 SHA-512 / RSA SHA-512.***

Le tableau suivant liste les assertions de la version 1.0 du jeton d'informations utilisateur (UITVersion= 1.0).

Tableau 2 Assertions du jeton informations utilisateur (UserInfo Token)

Assertions	Type et jeu de valeurs	Requis / Optionnel	Description
sub	*Identifier*[16] ► Pour un **professionnel de santé** : format identifier du *profil* *fr-practitioner* de la ressource FHIR *Practitioner* (s'appuyant sur le format PS-IdNat[17]) ► Pour un **usager du système de santé** : format identifier du profil *fr-patient* de la ressource FHIR *Patient*	R	Identifiant de l'utilisateur final, du sujet authentifié.
iss	*StringOrURI*	R	Identité de l'émetteur du jeton. URL de l'endpoint d'informations utilisateur du serveur d'identification.
aud	*Array of StringOrURI* Liste d'URI (URL ou URN:OID par exemple) comportant au moins une entrée	R	Ce champ contient la liste des identifiants des systèmes cibles pour lesquels le jeton a été délivré. La liste doit contenir au moins une entrée. Doit contenir parmi ses valeurs le champ OAuth 2.0 client_id du système cible.
family_name	*String*	O	Nom de famille de l'utilisateur. Nom d'exercice pour les professionnels de santé.
given_name	*String*	O	Prénom de l'utilisateur
UITVersion	*String*	R	Version du jeton utilisée.

[16] Type Identifier de FHIR au format JSON : https://www.hl7.org/fhir/datatypes.html#identifier
[17] ANS : CI-SIS – Annexe transversale Sources des données métier pour les personnes et les structures

Assertions	Type et jeu de valeurs	Requis / Optionnel	Description
Palier_Authentification	*String* Valeur : « Code^OID » La valeur utilisée doit être un code provenant de la terminologie de référence suivante : ► TRE_R231-PalierAuthentification, OID : 1.2.250.1.213.1.5.1.1.1 Les valeurs possibles peuvent être restreintes en fonction du jeu de valeurs correspondant mis à disposition par le projet. En l'absence de spécifications complémentaires, le jeu de valeurs JDV_J21-PalierAuthentificationActeurPP peut être utilisé	O	Palier du référentiel d'authentification auquel se situe l'authentification de l'utilisateur tel que défini par la PGSSI-S.
PSI_Locale	*String* Valeur : OID	O	Identifiant de la politique de sécurité mise en œuvre dans le cadre de l'authentification de l'utilisateur.
SubjectRole	*Array of String* Chaque objet de la liste a un codeSystem Chaque valeur de la liste est sous le format « Code^OID » La valeur du code utilisée doit être un code provenant des terminologies de référence suivantes : ► TRE_A00-ProducteurDocNonPS, OID : 1.2.250.1.213.1.1.4.6 ► TRE_G15-ProfessionSante, OID : 1.2.250.1.71.1.2.7 ► TRE_G16-ProfessionFormation, OID : 1.2.250.1.71.1.2.8 ► TRE_R01-EnsembleSavoirFaire-CISIS, OID : 1.2.250.1.71.4.2.5 ► TRE_G05-SousSectionTableauCNOP, OID : 1.2.250.1.71.4.2.6 Les valeurs possibles peuvent être restreintes en fonction du jeu de valeurs correspondant mis à disposition par le projet. En l'absence de spécifications complémentaires, le jeu de valeurs JDV_J05-SubjectRole-CISIS peut être utilisé.	O	Rôle fonctionnel de l'utilisateur, éventuellement multi-valué. *Champ issu d'une option du profil IUA.*
Secteur_Activite	*String* Valeur : « Code^OID » La valeur du code utilisée doit être un code provenant des terminologies de référence suivantes : ► TRE_R02-SecteurActivite, OID : 1.2.250.1.71.4.2.4 Les valeurs possibles peuvent être restreintes en fonction du jeu de valeurs correspondant mis à disposition par le projet.	O	Secteur d'activité dans lequel exerce l'utilisateur. *Donnée contextuelle à demander à l'utilisateur au moment de son authentification.*
SubjectOrganization	*String* Valeur : Texte libre	O	Nom ou description de la personne morale, structure d'exercice de l'utilisateur. *Donnée contextuelle à demander à l'utilisateur au moment de son authentification.* *Champ issu d'une option du profil IUA.*
SubjectOrganizationID	*String*	O	Identifiant de la personne morale, structure d'exercice de l'utilisateur.

Assertions	Type et jeu de valeurs	Requis / Optionnel	Description
	Valeur : valeur de Struct_IdNat identifiant la personne morale[6]		*Donnée contextuelle à demander à l'utilisateur au moment de son authentification.* *Champ issu d'une option du profil IUA.*
Acces_Regulation_Medicale	*Boolean*	O	Accès exceptionnel demandé depuis un centre de régulation médicale. *Donnée contextuelle à demander à l'utilisateur au moment de son authentification.*
Mode_Acces_Raison	*String*	O	Explication de la raison de l'usage d'un accès exceptionnel (Bris de glace ou autre accès exceptionnel) *Donnée contextuelle à demander à l'utilisateur au moment de son authentification.*
Profil_Utilisateur	*String*	O	Profil d'accès au système cible. Les valeurs possibles de ce champ sont définies par le système cible.
Profil_Utilisateur_Perimetre	*String*	O	Périmètre d'application du ProfilUtilisateur. Les valeurs possibles de ce champ sont définies par le système cible.

3.1.1.4. Expiration du jeton

Lorsque le jeton d'identification expire, deux cas de figure peuvent se présenter :

- Un jeton d'actualisation a été fourni par le serveur d'identification à l'étape 8
  Le jeton d'actualisation, ou *refresh_token*, qui a une durée de vie plus longue que celle du jeton d'identification, permet au système cible de demander un nouveau jeton d'identification auprès du serveur d'identification.
  Ci-dessous un exemple de requête d'actualisation de jeton.

```
POST /token HTTP/1.1
Host: serveur.exemple.com
Content-Type: application/x-www-form-urlencoded

client_id=s6BhdRkqt3
  &client_secret=some_secret12345
  &grant_type=refresh_token
  &refresh_token=8xLOxBtZp8
  &scope=openid
```

- Un jeton d'actualisation n'a pas été fourni par le serveur d'identification
  Dans ce cas, une réauthentification de l'utilisateur final est nécessaire. Le système cible doit rediriger le système initiateur vers le serveur d'identification pour reprendre la demande d'autorisation dès le début.

3.1.2. Configuration avec authentification directe

Cette configuration met en scène le système initiateur, le système cible et optionnellement un fournisseur de services annuaires. L'authentification de l'utilisateur se fait directement auprès du système cible.

Le système cible gère lui-même les informations d'identification des utilisateurs et peut s'appuyer optionnellement sur un fournisseur de services annuaires pour demander des informations complémentaires.

Les échanges de cette configuration permettent de fournir un jeton d'accès au système initiateur et **doivent respecter les spécifications OAuth 2.0 flux avec code d'autorisation**[18]. Les exemples donnés dans les sections suivantes sont non normatifs et sont issus de ces dernières.

3.1.2.1. Prérequis

L'enrôlement initial des utilisateurs auprès du système cible doit se faire dans le respect des référentiels de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

3.1.2.2. Les flux d'obtention du jeton

Les flux d'obtention de jeton en configuration avec authentification directe s'articulent autour de trois étapes clés :

- **La demande du code d'autorisation** : Le code d'autorisation constitue une procuration d'accès donnée par l'utilisateur à son application. Le code d'autorisation est valable une seule fois. *(Flux en bleu dans* Figure 3*)*
- **L'authentification de l'utilisateur** : L'authentification de l'utilisateur doit être forte et doit passer par un agent distinct de l'application. En s'authentifiant, l'utilisateur consent à donner le code d'autorisation à son application. *(Etape rouge dans* Figure 3*)*
- **Demande de jeton** : Le jeton est une autorisation d'accès qu'obtient le système initiateur après s'être authentifié et avoir présenté son code d'autorisation. *(Flux en vert dans* Figure 3*)*

Les flux s'organisent de la manière suivante :

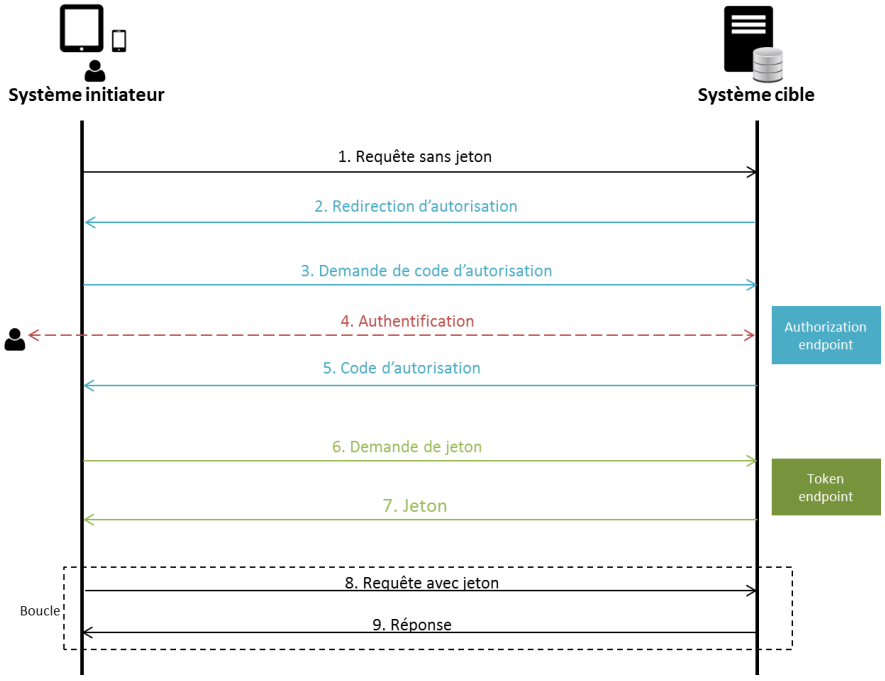

Figure 3 Diagramme de séquence des flux de la configuration avec authentification directe

[18] Ces spécifications adoptent l'option **flux avec code d'autorisation**, une option générique et sécurisée. L'option **flux implicites**, non recommandé pour des considérations de sécurité (*cf.* https://oauth.net/2/grant-types/implicit/), n'est pas adoptée.

1. **Requête sans jeton**

Ce flux est semblable au flux 1 de la configuration en authentification déléguée.

2. **Redirection d'autorisation**

Ce flux est semblable au flux 2 de la configuration en authentification déléguée, sauf qu'il redirige le système initiateur vers l'endpoint d'autorisation du système cible.

La valeur du paramètre *scope* est à définir par le système cible. Le *client_id* est l'identifiant du système initiateur. Le paramètre *nonce* n'est pas requis.

3. **Demande de code d'autorisation**

Ce flux est semblable au flux 3 de la configuration en authentification déléguée.

4. **Authentification**

Comme pour le flux 4 de la configuration en authentification déléguée, ce flux d'authentification dépend du mode d'authentification adopté par le système cible. Il permettra par ailleurs de demander les données contextuelles de la demande d'accès à l'utilisateur.

5. **Réponse à la demande de code d'autorisation**

Ce flux constitue la réponse au flux 3 de demande de code d'autorisation. Il retourne un code d'autorisation et le paramètre *state*.

6. **Demande de jeton**

Ce flux est semblable au flux 7 de la configuration en authentification déléguée. La requête doit inclure en plus l'identifiant du système initiateur. Cette information est portée par le paramètre *client_id*.

7. **Réponse à la demande de jeton**

Une fois le code d'autorisation validé, le système cible fournit au système initiateur un jeton d'accès, *access_token*, et optionnellement un jeton d'actualisation, *refresh_token*.

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
  "access_token":"2YotnFZFEjr1zCsicMWpAA",
  "token_type":"Bearer",
  "expires_in":3600,
  "refresh_token":"tGzv3JOkF0XG5Qx2TlKWIA"
}
```

8. **Requête avec jeton**

Le système initiateur utilise le jeton d'accès dans ses échanges avec le système cible. Typiquement le jeton d'accès sera porté par l'élément d'entête « Authorization » de type « Bearer » tel que c'est défini par le standard OAuth 2.0.

```
Authorization: Bearer <token>
```

3.1.2.3. Le jeton d'accès

Le système cible est libre de choisir le format du jeton d'accès qu'il fournit au système initiateur : une simple chaine de caractères non signifiante ou un jeton porteur d'informations semblable au jeton d'identification de la configuration en authentification déléguée (cf. 3.1.1.3.1).

3.1.2.4. Expiration du jeton

Lorsque le jeton d'accès expire, deux cas de figure peuvent se présenter :

1. Un jeton d'actualisation a été fourni par le système cible
   Le jeton d'actualisation, ou « refresh token », qui a une durée de vie plus longue que celle du jeton d'accès, permet au système initiateur de demander un nouveau jeton d'accès auprès du système cible.
   Ci-dessous un exemple de requête d'actualisation de jeton.

```
POST /token HTTP/1.1
     Host: systemecible.exemple.org
     Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
     Content-Type: application/x-www-form-urlencoded

     grant_type=refresh_token&refresh_token=tGzv3JOkF0XG5Qx2TlKWIA
```

2. Un jeton d'actualisation n'a pas été fourni par le système cible

Dans ce cas, une réauthentification de l'utilisateur final est nécessaire. La demande d'autorisation est reprise dès le début.

3.2. Confidentialité

La confidentialité des échanges au niveau du transport est gérée par l'encapsulation du flux dans une connexion sécurisée TLS version 1.2 ou supérieure. L'usage de SSL version 3.0 ou inférieure est interdit.

3.3. Intégrité

L'intégrité des échanges au niveau du transport est gérée par l'encapsulation du flux dans la connexion sécurisée TLS.

3.4. Disponibilité

Pas de disposition spécifique à ce volet.

3.5. Traçabilité

Il est de la responsabilité du système cible de gérer la traçabilité des accès. Il peut notamment garder les jetons en guise de traces d'accès.

3.6. Imputabilité

Les dispositions d'imputabilité sont gérées au niveau *Service*.

Annexe 1 : Mise en correspondance des acteurs et des flux

Mapping des acteurs

Cette section présente une mise en correspondance entre les acteurs identifiés dans ces spécifications et les acteurs des standards adoptés : OpenID Connect et OAuth.

Configuration avec authentification déléguée

Acteur du volet	Acteur OpenID Connect 1.0
Système initiateur	User agent
Système cible	Relying Party (Client OAuth)
Serveur d'identification	OpenID Provider
Utilisateur final	End user

Configuration avec authentification directe

Acteur du volet	Acteur OAuth 2.0
Système initiateur	Client
Système cible	Resource server
Système cible / endpoint d'authentification	Authorization server
Utilisateur final	Resource owner

Mapping des flux

Cette section présente une mise en correspondance entre les flux identifiés dans ces spécifications et les étapes décrites dans les spécifications des standards adoptés : OpenID Connect et OAuth.

Configuration avec authentification déléguée

Flux du volet	Etapes OpenID Connect (authorization code flow)
1 Requête sans jeton	-
2 Redirection d'autorisation	Authentication Request
3 Demande de code d'autorisation	
4 Authentification	Authorization Server Authenticates End-User
5 Réponse à la demande de code d'autorisation	Successful Authentication Response Authentication Error Response
6 Transmission du code d'autorisation	
7 Demande de jeton	Token Request
8 Réponse à la demande de jeton	Successful Token Response Token Error Response
9 Demande d'informations utilisateur	UserInfo Request
10 Réponse à la demande d'informations utilisateur	Successful UserInfo Response UserInfo Error Response
11 Transmission du jeton	-
12 Requête avec jeton	

Configuration avec authentification directe

Flux du volet	Etapes OAuth 2.0 (authorization code flow)
1 Requête sans jeton	-
2 Redirection d'autorisation	Authorization Request
3 Demande de code d'autorisation	
4 Authentification	-
5 Réponse à la demande de code d'autorisation	Authorization Response
6 Demande de jeton	Access Token Request
7 Réponse à la demande de jeton	Access Token Response
8 Requête avec jeton	-

Annexe 2 : Table des acronymes

Sigle / Acronyme	Signification
API	Application Programming Interface
ASIP Santé	Agence Française de la Santé Numérique (ancienne dénomination de l'ANS)
CI-SIS	Cadre d'interopérabilité des systèmes d'information de santé
CPS	Carte de professionnel de santé
CSS	Cascading Style Sheets
FHIR	Fast Healthcare Interoperability Resources
HEART	Health Relationship Trust
HL7	Health Level Seven International
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IEC	International Electrotechnical Commission
IHE	Integrating the Healthcare Enterprise
ISO	International Organization for Standardization
IUA	Internet User Authorization
JS	JavaScript
JSON	JavaScript Object Notation
JWA	JSON Web Algorithms
JWE	JSON Web Encryption
JWS	JSON Web Signature
JWT	JSON Web Token
OASIS	Organization for the Advancement of Structured Information Standards
OIDC	OpenID Connect
RASS	Référentiel des Acteurs Santé Social
REST	Representational State Transfer
RFC	Requests for comments
RPPS	Répertoire partagé des professionnels de santé
SAML	Security assertion markup language
SIS	Système d'information de santé
SMS	Short Message Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VIHF	Vecteur d'Identification et d'Habilitation Formelles

Annexe 3 : Documents de référence

- Volet CI-SIS : Transport synchrone pour client lourd

Annexe 4 : Historique du document

Version	Rédigé par		Vérifié par		Validé par	
0.1	ASIP Santé	Le 20/11/17	ASIP Santé	Le 20/11/17	ASIP Santé	Le 20/11/17
	Motif et nature de la modification : Publication en concertation publique					
1.0	ASIP Santé	Le 25/07/18	ASIP Santé	Le 25/07/18	ASIP Santé	Le 25/07/18
	Motif et nature de la modification : Publication après intégration des commentaires de concertation et des conclusions de l'analyse sécurité					
1.1	ANS	Le 5/11/20	ANS	Le 5/11/20	ANS	Le 5/11/20
	► Harmonisation des renvois aux nomenclatures en systématisant la référence aux terminologies de référence et aux jeux de valeurs NOS ► Modification du document au format ANS					