SI-SDO - Authentification

Document de spécification

22 décembre 2023

Historique des versions

Date	Version	Auteur	Relecteur(s)	Remarque
06/04/2023	V0.1	James FAURE		Création du document
27/04/2023	V1.0	James FAURE	Franck PILOT	Ajout d'information sur les standards d'échange
21/07/2023	V1.1	James FAURE	Franck PILOT	Ajout des informations concernant le header HTTP « struct_idnat ».
18/12/2023	V1.2	James FAURE		Suppression des mentions SI-MDPH Ajout de précisions sur le client_id.

SOMMAIRE

1 Introduction et objectif du document

Ce document présente les spécifications techniques liées à l'authentification des systèmes d'informations implémentant le volet « SI-ESMS ».

Ces dernières spécifient les mécanismes d'authentification mis en place par le Système d'Information de Suivi des Orientations (SI-SdO) ViaTrajectoire. Il sera dénommé uniquement « ViaTrajectoire » dans la suite de ce document.

1.1 Lectorat cible

Ce document s'adresse aux développeurs des interfaces interopérables des systèmes implémentant le volet « SI-ESMS » ou à toute autre personne intervenant dans le processus de mise en place de ces interfaces.

L'hypothèse est faite que le lecteur est familier du standard OAuth2.

1.2 Utilisation

Les spécifications d'interopérabilité présentées dans ce volet ne présagent pas des conditions de leur mise en œuvre dans le cadre d'un système d'information partagé. Il appartient à tout responsable de traitement de s'assurer que les services utilisant ces spécifications respectent les cadres et bonnes pratiques applicables à ce genre de service (ex. : cadre juridique, bonnes pratiques de sécurité, ergonomie, accessibilité ...).

2 Description générale de l'authentification ViaTrajectoire

2.1 Concept

L'infrastructure de gestion de la confiance du secteur santé-social français, dite « IGC-Santé », est une infrastructure de gestion de clés cryptographiques (IGC) opérée par l'Agence du Numérique en Santé (ANS). Les certificats émis par l'ANS permettent de sécuriser l'identification électronique de personnes morales à des services numériques en santé (DMP, INSi, etc.).

Dans le cadre de l'interopérabilité avec ViaTrajectoire, les certificats IGC-Santé sont considérés comme nécessaire et suffisant pour identifier l'entité juridique d'une structure.

ViaTrajectoire authentifie par le biais des certificats IGC-Santé l'entité juridique. ViaTrajectoire autorise à cette dernière l'exécution des actions décrites dans les spécifications d'interopérabilité du volet « SI-ESMS » sur chaque entité géographique qui lui est associée.

L'annuaire des établissements dans ViaTrajectoire est alimenté par le référentiel FINESS et les ROR régionaux (par le biais du ROR national).

2.2 Standards d'échange employés

2.2.1 Protocole de transport

Le serveur d'autorisation utilise le protocole **HTTP 1.1** encapsulé dans une connexion sécurisée **TLS** 1.2.

2.2.2 Standard d'autorisation OAuth 2.0

Le standard **OAuth 2.0** est un protocole d'autorisation conçu pour accorder l'accès à un ensemble de ressources à une application tierce. Il repose sur un système d'émission et de gestion des jetons d'accès.

Le serveur d'autorisation est un composant essentiel du flux **OAuth 2.0** qui permet de garantir la sécurité et la confidentialité des données de l'utilisateur. Il effectue le contrôle d'accès du client et gère l'envoi et la vérification des jetons d'accès.

2.2.3 Jeton d'accès JWT

Les jetons d'accès sont au format **JSON Web Token (JWT)**. Ils sont signés par le serveur d'autorisation.

Ils contiennent en général les champs suivants :

Champs	Description
iss	Identifiant de l'émetteur du jeton
sub	Identifiant du sujet demandeur du jeton
jti	Identifiant unique du jeton
aud	Identifiant ou liste d'identifiants des ressources qui peuvent être accessibles avec ce jeton
exp	Heure d'expiration du jeton, après laquelle il ne sera plus valide.
iat	Heure à laquelle le jeton a été émis
scope	Périmètre des ressources dont l'accès est autorisé par l'émetteur.

2.2.4 Protocole mTLS

Le protocole mTLS (mutual TLS) est une méthode d'authentification mutuelle où le client et le serveur dispose chacun d'un certificat à présenter à l'autre parti et à vérifier. Il permet de sécuriser les échanges entre le client et le serveur d'autorisation.

Dans le cadre de l'authentification avec ViaTrajectoire, le certificat côté client est celui de l'entité juridique.

3 Fonctionnement de l'authentification ViaTrajectoire

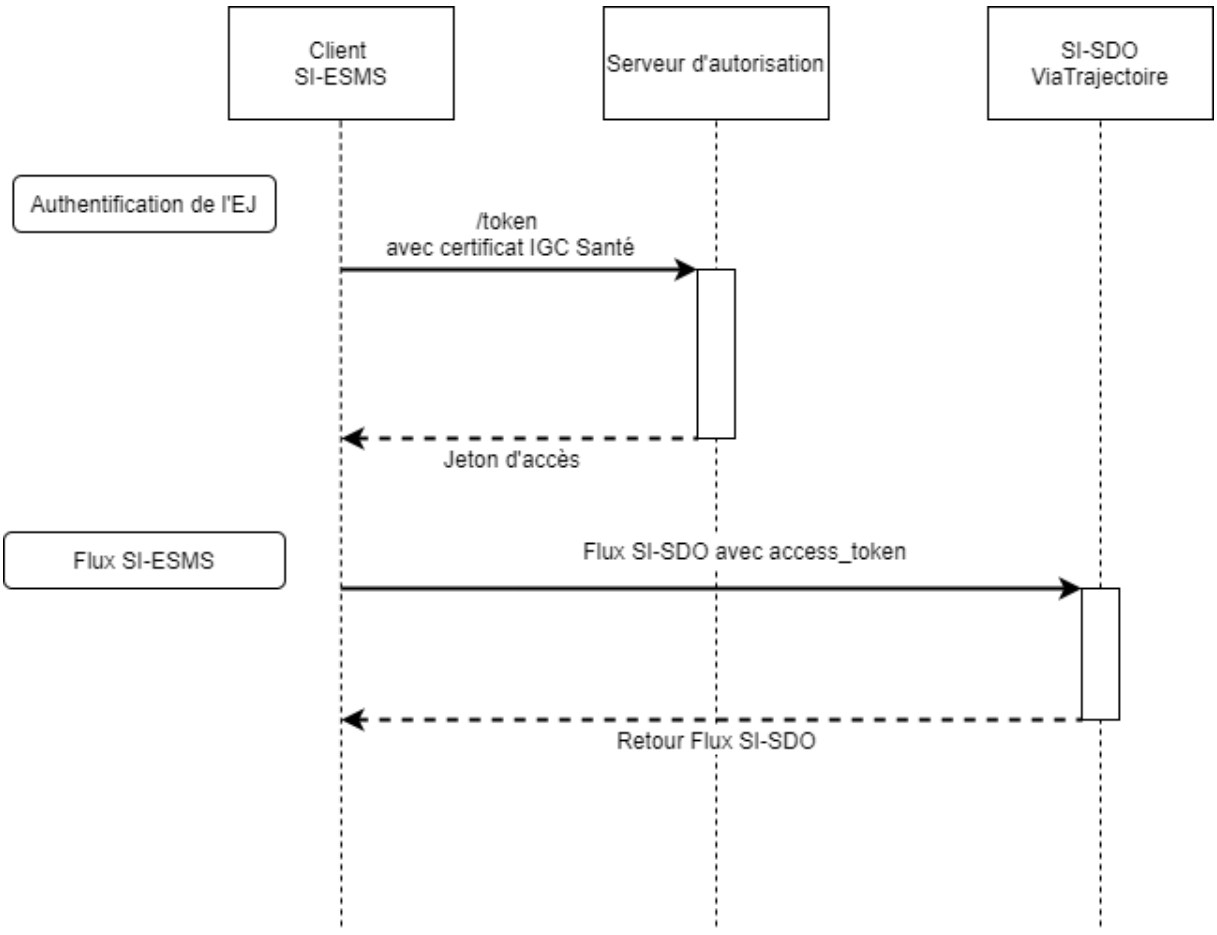
3.1 Description

La sécurisation des appels entre les établissements et ViaTrajectoire est fondée sur un mécanisme d'autorisation OAuth2 en mode Direct Access Token (flux « Resource Owner Password Credentials Grant » sans mot de passe) et sur de l'authentification mutuelle TLS.

L'établissement s'authentifie auprès du serveur d'autorisation ViaTrajectoire grâce à son certificat IGC-Santé. L'authentification s'effectue en passant par un client OAuth2 unique générique. Elle permet de récupérer un jeton d'accès identifiant l'entité juridique de l'établissement.

Pour chaque requête du flux SI-ESMS, le numéro Finess de l'entité géographique de la structure est envoyé dans un header HTTP. ViaTrajectoire utilise le jeton d'accès et ce paramètre afin de confirmer le lien entre l'entité juridique et l'entité géographique et d'autoriser ou non la requête.

3.2 Schéma de principe



3.3 Obtenir un jeton d'accès

3.3.1 Requête

Le système d'information de la structure effectue une requête de type POST vers une URL « /token » du serveur d'autorisation ViaTrajectoire.

Le Content-Type de la requête est : « application/x-www-form-urlencoded »

Les paramètres suivants sont à ajouter à la requête :

Nom du paramètre	Valeur
grant_type	« password »
client_id	Fourni à la demande
client_secret	Fourni à la demande

Les éléments client_id et client_secret changent en fonction de l'environnement appelé. Ils représentent un client unique, commun à tous les établissements.

La requête est sécurisée par authentification mutuelle TLS (mTLS). L'établissement doit présenter de son côté le certificat IGC-Santé. Ce dernier est validé ensuite par le serveur d'autorisation ViaTrajectoire.

Exemple :

```
POST [base]/token?grant_type=password&client_id=si-esms&client_secret=…

Host:
Content-Type: application/x-www-form-urlencoded
```

Où [base] est le point de contact du serveur d'autorisation ViaTrajectoire

3.3.2 Réponse

La réponse est au format JSON. L'attribut « access_token » contient le jeton d'accès permettant de s'identifier auprès de ViaTrajectoire.

Nom de l'attribut	Description
access_token	Jeton d'accès
expires_in	Durée de validité du jeton d'accès
refresh_expires_in	Attribut spécifique au serveur d'autorisation. Durée de validité du jeton de rafraichissement. Valeur par défaut : « 0 »
token_type	Type de jeton. Valeur par défaut : « Bearer »
not-before-policy	Attribut spécifique au serveur d'autorisation.
scope	Périmètre des ressources accessibles par le jeton d'accès.

Exemple :

```
{
  "access_token": "eyJhb…<longue chaîne de caractère représentant le jeton>…",
  "expires_in": 300,
  "refresh_expires_in": 0,
  "token_type": "Bearer",
  "not-before-policy": 0,
  "scope": "ViaTrajectoire"
}
```

En plus des paramètres décrit dans le paragraphe Jeton d'accès JWT, ce jeton d'accès contient le numéro Finess de l'entité juridique associé à l'établissement ayant fait la requête

(attribut « finessEJ »), ainsi que la liste des numéro Finess des entités géographiques appartenant à celle-ci (attribut « listeFinessEG »).

3.4 S'identifier auprès du SI-SDO ViaTrajectoire

3.4.1 Requête

Le cadre d'interopérabilité du volet « SI-ESMS » décrivent le formalisme des requêtes effectuées auprès de ViaTrajectoire.

Le jeton d'accès doit être envoyé dans un header HTTP « Authorization » dont la valeur est la concaténation des chaînes de caractères « Bearer » et du contenu de l'attribut « access_token » du jeton d'accès, séparé par un espace.

Pour chacune de ces requêtes, le numéro Finess de l'entité géographique correspondant à l'établissement appelant doit être communiqué afin de permettre à ViaTrajectoire d'identifier quel établissement de l'entité juridique authentifié est concerné. Le numéro Finess doit être envoyé sous sa forme d'identifiant national, à savoir :

[type structure] + [n° Finess EG] où :

- [type structure] vaut 1
- [n° Finess EG] est le numéro Finess de l'entité géographique.

Les headers HTTP suivant sont à ajouter à la requête :

Nom du header HTTP	Valeur
Authorization	« Bearer » + access_token
struct_idnat	« 1 » + n+ Finess de l'entité géographique

Exemple pour le Flux 1.1 – RecherchePersonneOrienteeDecision du volet « SI-ESMS » :

```
GET [base]/DocumentReference?type=57830-2
&_lastUpdated=gt[dateDernièreRecherche]&_elements=id

Host:
Authorization : Bearer eyJhb…<longue chaîne de caractère représentant le jeton>…
struct_idnat : 1690030051
```

Où [base] est le point de contact FHIR

3.4.2 Réponse

La réponse est celle attendue conformément au cadre d'interopérabilité du volet « SI-ESMS ».

Si l'identité de l'établissement appelant ne peut pas être déterminé, un code d'erreur HTTP 401 est retourné.

L'établissement peut se voir refuser l'accès au SI-SDO si :

- Le jeton d'accès est absent ou non valide (expiré, falsifié, …)
- Le header HTTP « struct_idnat » n'est pas renseigné
- Le header HTTP « struct_idnat » ne contient pas un numéro Finess EG associé à l'entité juridique authentifié par le jeton d'accès.q

Annexe 1 : Glossaire

Terminologie métier :

Sigle / Acronyme	***Signification***
ANS	Agence du Numérique en Santé
CI-SIS	Cadre d'Interopérabilité des Systèmes d'Information de Santé
EG	Entité Géographique
EJ	Entité Juridique
SI-ESMS	Système d'Information des Etablissements et Services Médico-Sociaux
SI-SdO	Système d'Information de Suivi des Orientations

Terminologie technique :

Sigle / Acronyme	***Signification***
API	Application Programming Interface
FHIR	Fast Healthcare Interoperability Resources
HTTP	HyperText Transfer Protocol
JSON	JavaScript Object Notation
JWT	JSON Web Token
mTLS	Mutual TLS
TLS	Transport Layer Security