Abilian
CS LAB

OPEN INTEROP · GT COLLABORATIF

Atelier technique n° 1 : s'intégrer à La Suite numérique

Stefane Fermigier (Abilian SAS) · 10 novembre 2026 · DRAFT

Version 0.2
Licence CC BY 4.0

Le premier atelier technique du groupe de travail collaboratif s'est tenu en visioconférence le 10 novembre 2026. L'équipe de La Suite numérique (DINUM) y a présenté Menshen, son serveur d'autorisation, puis a répondu aux questions des éditeurs sur l'intégration avec Visio et Tchap. Ce compte rendu, établi par l'auteur à partir de l'enregistrement et du support, n'engage pas les participants. Les points rapportés décrivent l'état présenté en séance, sans engagement de calendrier.

Synthèse

- **Menshen** met en œuvre l'échange de jetons OAuth 2.0 (RFC 8693) : un service obtient, pour un utilisateur, un jeton limité à un service de destination et à des permissions précises. Visio l'utilise en production ; d'autres services de La Suite pourraient suivre.
- **De quoi commencer** : le code est libre, avec un client, un exemple d'intégration et une description OpenAPI. Une instance de préproduction est ouverte aux éditeurs, avec des règles d'accès définies au cas par cas.
- **Visio** permet de créer une salle au nom d'un utilisateur. Transcriptions, enregistrements et événements ne sont pas encore accessibles par API.
- **Tchap** s'intègre par l'API client de Matrix, spécifiée publiquement, avec quelques écarts et des règles pour les robots.
- **Deux briques à venir** : « Mon compte », intermédiaire devant ProConnect ; « le Hub », un client web Matrix qui doit relier les produits de La Suite.
- **Les éditeurs** demandent une documentation des ressources ouvertes aux tiers et des ateliers collectifs en amont des choix d'architecture.

1. Menshen et l'échange de jetons

1.1 Le principe

Un service de La Suite doit souvent agir sur un autre au nom d'un utilisateur : Visio range un enregistrement dans Fichiers, par exemple. Transmettre le jeton obtenu de ProConnect oblige le service appelé à interroger ProConnect à chaque requête. Le jeton lui donne en outre les mêmes droits qu'à l'appelant. L'échange de jetons place un serveur d'autorisation entre les services :

1. l'utilisateur s'authentifie auprès de Visio par OpenID Connect, via ProConnect ;
2. Visio présente son jeton au serveur d'autorisation et demande un jeton pour Fichiers ;
3. le serveur d'autorisation valide le jeton d'origine auprès de ProConnect ;
4. il émet un jeton limité à Fichiers et aux permissions demandées ;
5. Visio appelle Fichiers avec ce jeton ;
6. Fichiers le valide auprès du serveur d'autorisation ;
7. Fichiers répond.

1.2 L'API

L'API compte trois points d'accès : échange d'un jeton d'accès contre un jeton d'échange, introspection, révocation. Une demande d'échange contient les paramètres de la RFC 8693 : le jeton présenté et son type (JWT ou jeton opaque), l'audience (le service de destination) et la portée demandée.

Les permissions suivent une nomenclature à trois termes : service, ressource, action. Des portées « d'action » regroupent plusieurs permissions, sur un ou plusieurs services. La documentation de Menshen liste, pour chaque service de La Suite, les ressources accessibles et les actions possibles. Les règles d'accès (quel service source peut obtenir quelles portées sur quel service de destination) sont configurées par l'équipe de La Suite.

1.3 Ressources disponibles

- **Le code**, libre : https://github.com/suitenumerique/menshen, avec le serveur, un client et un *playground*, exemple d'intégration à exécuter en local.
- **La description OpenAPI** : https://menshen-staging.beta.numerique.gouv.fr/auth/token/openapi.json, qui permet de générer un client.
- **Un bac à sable** : l'instance de préproduction, où Visio est déjà raccordé.

Un éditeur qui veut tester demande un identifiant client à l'équipe de Menshen, puis définit avec elle et l'équipe du service visé la ressource, les permissions et le trafic attendu.

2. Visio

Créer une salle. Une salle peut se créer à la première connexion, mais le premier arrivé en devient alors l'organisateur, avec les droits d'enregistrement et de transcription. Il vaut mieux créer la salle à l'avance, au nom de l'utilisateur, en désignant son organisateur ; cette création passe par l'échange de jetons.

Transcriptions et enregistrements. Les transcriptions sont déposées dans Docs, les enregistrements dans Fichiers, dans l'espace de l'organisateur, averti par courriel. Aucune API ne permet encore à un service tiers d'en être averti ni d'en choisir la destination. L'envoi vers d'autres espaces de stockage est prévu, sans date : un webhook signalerait qu'un fichier est prêt, à récupérer par l'échange de jetons.

Événements. Un flux d'événements (appel en cours, participant entré) est prévu, sans date.

Migration. Les intégrations existantes devront passer à l'échange de jetons : Visio fermera à terme les API qui n'y passent pas.

3. Tchap

L'API Matrix. Tchap n'utilise pas l'échange de jetons. Son interface d'intégration est l'API client de Matrix : une fois connecté, un client dispose de toutes les fonctions d'un client Matrix ordinaire. La connexion passe

par ProConnect, bientôt exclusivement. L'authentification de Matrix fondée sur OAuth 2.0 permettrait de restreindre la portée des jetons ; Tchap n'en définit qu'une aujourd'hui.

Écarts à la spécification, que l'équipe cherche à faire remonter dans la spécification Matrix avec d'autres acteurs de l'écosystème :

- un point d'accès propre à Tchap renvoie, pour une adresse électronique, le serveur de rattachement de l'utilisateur ;
- l'annuaire des salons publics s'interroge serveur par serveur ;
- les médias passent, dans les clients de Tchap, par un point d'accès antivirus, que les clients tiers devront sans doute utiliser aussi.

Robots. Un compte automatique doit être identifiable par son adresse électronique. Les actions en masse depuis un compte ordinaire déclenchent les alertes de sécurité et se discutent au préalable. Les *application services* de Matrix, qui donnent un accès direct au serveur, sont exclus.

Fédération. La fédération avec des serveurs Matrix extérieurs, opérés pour des instances publiques, est envisagée, sans date annoncée, sous une charte de sécurité. Les utilisateurs fédérés y auront d'abord un statut d'externe : invités dans des salons, sans conversations directes.

4. Les briques à venir

Mon compte est un intermédiaire placé devant ProConnect, qui donne à La Suite la maîtrise des jetons, des identifiants et des droits. Il servira de fournisseur d'identité aux produits de La Suite ; les services tiers n'y sont pas raccordés.

Le Hub est un client web Matrix, au stade de prototype, qui doit rassembler pour une équipe conversations, fichiers, documents et réunions. Il ajoute la gestion des groupes, absente de Matrix. Il relie aussi les espaces de chaque produit. L'intégration prévue est légère : lister et naviguer dans le Hub, éditer dans le produit d'origine. Il pourrait exposer sa propre API, via Menshen, pour les fonctions absentes de Matrix. Plusieurs éditeurs ont des besoins équivalents (une vue transverse sur les métadonnées des applications) et ont proposé un atelier ouvert sur ce thème.

5. Questions des éditeurs

- **Ressources ouvertes aux tiers.** L'API complète d'un service ne dit pas lesquelles de ses fonctions un service tiers peut obtenir. Ce périmètre n'est pas documenté et se définit au cas par cas.
- **Contributions.** Les produits de La Suite acceptent des contributions. L'équipe, réduite, demande d'ouvrir un ticket et de discuter la conception avant de proposer du code.
- **Instances imposées.** Un éditeur sait intégrer les outils qu'il opère lui-même. Quand un client public lui impose les instances de l'État, ses intégrations dépendent des API que La Suite ouvre. Les éditeurs demandent que ces sujets soient traités collectivement, comme les intégrations avec Docs et Fichiers ; l'équipe de La Suite est prête à organiser des réunions dédiées.

6. Analyse de l'auteur

- **Un standard ouvert.** Menshen s'appuie sur la RFC 8693 et son code est libre : la même mécanique peut relier des services qui ne sont pas ceux de l'État (proposition de doctrine, principes 2 et 3).
- **Un profil à écrire.** La RFC laisse ouverts le format des jetons, la nomenclature des portées, l'introspection. Publier la nomenclature de Menshen comme un profil, avec une suite de tests,

permettrait à d'autres serveurs d'autorisation de tenir le même rôle (principe 4), dans le prolongement du chantier C1 de la fiche collaboratif.

- **Des conditions d'accès publiques.** Un catalogue public des ressources, des portées et des conditions d'accès, par service, rendrait l'intégration prévisible pour tous les éditeurs (principe 8).
- **Les données des réunions.** Le dépôt des transcriptions et enregistrements vers un stockage tiers est à suivre au regard du principe 6.
- **Matrix.** Les écarts de Tchap à la spécification sont des candidats directs au chantier C3.

7. Suites

- Les éditeurs prêts à tester demandent un accès à la préproduction de Menshen.
- Des réunions individuelles sur les intégrations avec Visio, pour les éditeurs qui ont des cas d'usage.
- Des ateliers collectifs : sur le Hub, la gestion des groupes et les métadonnées transverses ; sur les intégrations avec Docs et Fichiers.

Références

- RFC 8693, *OAuth 2.0 Token Exchange*, IETF, janvier 2020. https://www.rfc-editor.org/info/rfc8693/
- Menshen, code source. https://github.com/suitenumerique/menshen
- Spécification Matrix. https://spec.matrix.org/