AGENCE
DU NUMÉRIQUE
EN SANTÉ

COMPTE-RENDU

Task Force MSSanté

Atelier technique #1

Réunion du 10/12/2021

Statut : Validé | *Classification : Publique* | *Version : v1.0*

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

1. OBJET DU COMPTE-RENDU

Objet	TF MSSanté – Atelier technique #1
Date	10 décembre 2021
Organisateur[1]	Mathieu SLOSAR
Type de réunion	Atelier
Rédacteur[2]	Edouard BRIS

Documents de référence
- Support de présentation « **MSS_TF_MSS_Atelier_1_20211210_V1** »

2. INTERVENANTS

Nom	Prénom	Entité	Fonction
BRIS	Edouard	ANS	Régulation espace de confiance
GUEYE	Mike	ANS	Régulation espace de confiance
LAPEYRIE	Jean-Baptiste	DNS	Directeur de projets DNS
SLOSAR[1]	Mathieu	ANS	Responsable de produit MSSanté

[1] Personne à l'origine de la réunion (qui en assure l'animation).
[2] Personne en charge de la rédaction du compte rendu de la réunion

3. COMPTE-RENDU SYNTHETIQUE

Les objectifs de ce premier atelier étaient les suivants :

1. Présenter les enjeux et positionnement de la TF MSSanté dans le Segur
2. Rappeler les objectifs et principes de la nouvelle API Clients – Opérateurs (dont POC CIBA)
3. Présenter les évolutions envisagées des exigences des référentiels
4. Concertation autour des méthodes d'authentification de la nouvelle API

L'objet de ce CR n'est pas de reprendre les éléments partagés par les intervenants lors de l'atelier, mais revenir sur les éléments structurants remontés par les participants via les commentaires et questions partagés en séance.

III. Restitution	Auteur/Emetteur :	Date de la réunion :
	Edouard BRIS / ANS	10/12/2021

III. Relevé d'Informations, de Décisions et d'Actions (RIDA)

#	Nature	Objet	Question	Réponse
1	I	Authentification CPS via l'opérateur	Quel est l'usage de l'authentification CPS en IMAP/SMTP ?	Ce mode d'authentification semble nécessaire principalement pour les LGC qui utilisent déjà ce mode d'authentification.
2	**I**	Authentification pour les BAL applicatives	Peut-on faire en sorte d'utiliser le même certificat que celui dans le cadre de PSC ? pour éviter de multiplier les certificats	Hors réunion : l'EX PSC 24 indique que "Le Fournisseur de Service DOIT communiquer avec Pro Santé Connect via une connexion sécurisée au minimum via TLS 1.2 par un certificat AUTH_CLI de l'offre ORG de l'IGC-Santé". Il s'agit ici d'un certificat de l'opérateur utilisé pour sécuriser les échanges avec PSC. Il ne pourra pas donc être employé pour sécuriser les échanges avec les clients de messagerie, car un certificat ne doit être utilisé que pour une unique finalité.

3	**A**	Authentification eCPS par flux de redirection	Les logiciels référencé Segur ont l'obligation de supporter l'authentification par flux de redirection (par opposition au flux CIBA). Pourquoi ne pas rendre obligatoire cette méthode d'authentification pour les opérateurs MSSanté ? Un éditeur compatible Mailiz précise que l'authentification OTP est vue comme un moyen de secours lorsque le professionnel a oublié sa CPS. Ce mode de secours pourrait être la eCPS à l'avenir.	Le flux par redirection est bien adapté au logiciel en SAAS, par contre l'ergonomie du flux CIBA semble plus adaptée aux les logiciels client lourd et aux application mobiles. Doctrine à définir avec les couloirs Ségur et les autres services socle. Hors réunion : - les éditeurs sont invités à se positionner sur le choix entre les 2 flux PSC dans la v0.1 des exigences transmises le 15/12. - D'après le référentiel PSC v1.8 : **EX PSC 25** : Le Fournisseur de Service de type client lourd DOIT utiliser une autre méthode que l'intégration native d'un composant navigateur à l'intérieur de son applicatif pour le déroulé de la cinématique de connexion Pro Santé Connect **EX PSC 26** : Le Fournisseur de Service de type client lourd DOIT utiliser un navigateur extérieur à son application pour la cinématique "flux code d'autorisation" de Pro Santé Connect
4	**I**	Authentification CIBA	Comme demandé par les DSR vagu1, les éditeurs de clients lourds vont implémenter le flux par redirection via l'ouverture d'un navigateur. Il est probable qu'une fois ce flux implémenté, ils ne voient pas l'intérêt de migrer sur CIBA	L'ANS va reconsidérer l'usage du flux par redirection, versus le flux CIBA. Une approche commune aux différents services nationaux est à considérer
5	**I**	Nombre de moyens d'authentification	« 4 moyens d'authentification est prohibitif. La complexité de validation/certification ne devrait pas être sous-estimée »	Effectivement. Il est souhaitable que nos échanges permettent de réduire ce nombre.
6	**D**	Nombre de FQDN	Pour réduire ne nombre de FQDN, utiliser un unique FQDN pour IMAP et SMTP, ce qui fait un seul FQDN par moyen d'authentification, et donc une seule IP publique	Pris en compte
7	**I**	Position vis-à-vis des API existantes	Si je comprends bien nos usages actuels ne sont pas remis en cause ? Vous voulez jusque ajouter un standard d'authentification supplémentaire ?	Effectivement, l'objectif est que tout opérateur présente l'API standard telle qu'elle aura été spécifiée. Il ne sera pas interdit qu'un opérateur utilise d'autres API avec des clients spécifiques (existant), pour peu que cette dernière respecte les référentiels applicables (sécurité …).
8	**I**	TOTP	Avec l'TOTP, prendre garde à l'heure du serveur : changement d'heure, fuseaux horaires, …	Vu

9	**I**	Messagerie MES	Serait-il envisageable d'échanger sur spécificité des usages de la MSS avec la messagerie sécurisée de MonEspaceSanté ?	La CNAM a produit une note à destination des éditeurs : *Note technico-fonctionnelle sur le client de messagerie Mon Espace Santé*. Elle a été publiée le 03/12 sur https://mssante.fr/is/doc-technique.