AGENCE
DU NUMÉRIQUE
EN SANTÉ

COMPTE-RENDU

Task Force MSSanté

Atelier technique #3

Réunion du 11/02/2022

Statut : Validé | *Classification : Publique* | *Version : v0*

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 #3
Date	11 février 2022
Organisateur[1]	Mathieu SLOSAR
Type de réunion	Atelier
Rédacteur[2]	William TRIEU

Documents de référence
- Support de présentation «MSS_TF_MSS_Atelier_3_20220211»

2. INTERVENANTS

Nom	Prénom	Entité	Fonction
BRIS	Edouard	ANS	Régulation espace de confiance
GUEYE	Mike	ANS	Régulation espace de confiance
SLOSAR[1]	Mathieu	ANS	Responsable de produit MSSanté
DANGIN	Bastien	Capgemini	Architecte solution en appui aux équipes techniques MSSanté de l'ANS

[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 points abordés durant le troisième atelier étaient les suivants :

1. Introduction
    a. Exigences – MAJ récentes
    b. API LPS – Synthèse des concertations à date
2. Présentation des nouvelles exigences hors API LPS
    a. Evolution des indicateurs d'usage MSS côté opérateur
    b. Qualité des BAL présentes dans l'annuaire
    c. Contrat : nouvelles modalités de contrôle et de sanction
3. Focus sur les moyens d'authentification électronique (MIE) de l'API LPS
    a. Cinématique d'authentification PSC pour éditeurs LPS
    b. Cinématique d'authentification PSC pour les opérateurs
    c. Authentification par certificat IGC Santé pour les BAL applicatives
4. Rappels : spécifications ENS disponibles pour les éditeurs

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

III. Restitution	Auteur/Emetteur :	Date de la réunion :
	William TRIEU / Capgemini Invent	11/02/22

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

#	Nature	Objet	Question / Remarque	Réponse
1	A	API LPS (p.6)	EFS : Comment faire si l'opérateur n'a pas d'authentification forte pour l'instant (pour des raisons de coût, planning, ressources) ? Est-ce qu'il est nécessaire de mettre en place une authentification forte vers la MSSanté ou globale EFS pour une mise en conformité de l'établissement ?	ANS : pour les CH, l'API LPS pourra être utile pour se brancher sur des boites applicatives. Concernant l'authentification forte des personnes physiques, l'API LPS répond à un certain nombre de besoins (en particulier en libéral) mais pas à tous. Pour les CH, les référentiels MSSanté permettront toujours d'utiliser une autre API avec les logiciels clients. Mais celle-ci devra respecter les exigences de sécurité décrit dans les référentiels d'identification électroniques .Les modalités seront précisées dans le cadre de la vaque 2 Ségur.
2	I	API LPS (p.6)	Weda : Les protocoles IMAP/SMTP posent des problèmes de scalabilité/performance : est ce qu'il est prévu de mettre en place des webservices ?	ANS : Le choix des protocoles IMAP/SMTP (par rapport aux Webservice) a été fait en concertation avec les industriels. Le principal argument était l'utilisation d'un standard de messagerie existant et grandement éprouvé.

3	I	API LPS (p.6)	Weda / GIP ESEA : Est-ce que les DUI sont concernés ? Est-il possible de faire uniquement du PSC sans back-up ? Quel choix de Back-Up à PSC ? Quel est le calendrier ?	ANS : Les DUI sont bien concernés par l'API LPS. On utilise le terme LPS dans sa définition la plus large incluant les DUI. La cible est PSC pour les personnes physiques et les certificats serveurs pour les personnes morales. Il est cependant judicieux d'avoir une alternative à PSC, le choix est laissé à l'opérateur et ne sera pas imposé nationalement par les référentiels. Pour rappel, les MIE alternatifs à PSC envisagés lors de premiers ateliers ont été écartés : - L'OTP SMS est jugé couteux par les opérateurs et semble disproportionné - La CPS locale est couteuse à maintenir et redondante avec la CPS de PSC et n'apporte pas de cas d'usage supplémentaires intéressant La finalisation et la publication du nouveau référentiel sont prévues au plus tard le **15 avril**, la prochaine version (avant le 11/03) sera la dernière en concertation dans le cadre de la TF.
4		API LPS (p.6)	GIP ESEA : Jusqu'à quand est prévue la tolérance sur l'utilisation de TLS 1.0 sur l'interface entre opérateurs ?	ANS : Il n'y a pas de date précise pour l'instant. Une période de transition suffisante entre les 2 niveaux de TLS sera laissée. Une piste est un retrait du support de TLS 1.0 à la sortie du Référentiel v1.6 qui sera sûrement sur 2023

5	I	Nouvelles exigences hors API LPS - Entêtes spécifiques MSSanté côté client de messagerie (p.9)	ANS : Est-ce que les éditeurs ont des recommandations ou remarques sur les informations à véhiculer dans les entêtes ?	MSI 2000/Pharmagest : Dans l'utilisation des TLSi : seul le nom du logiciel et la version (agréé par le CNDA) sont envoyés, mais pas le nom de l'éditeur ou le numéro agrément TLSi Cas FSE : envoi d'un numéro NIL/NIE (attribué par le CNDA à vie) spécifique agréé pour l'éditeur --> Numéro sensible mais qui n'est pas véhiculé dans les flux
6	I	Nouvelles exigences hors API LPS - Evolution des indicateurs d'usage MSS côté Opérateur (p 10)	ANS : Une nouvelle possibilité sera présentée de déposer des fichiers d'indicateur volumineux – actuellement 70Mo en taille maximum de fichier. Dans le futur référentiel il y aura une nouvelle méthode pour des fichiers >70Mo.	-

7	A	Nouvelles exigences hors API LPS - Qualité des BAL présentes dans l'annuaire (p11)	Demande d'avis sur la possibilité de réduire le temps de suppression d'une BAL non consultée à 3 mois. Temps actuel de 12 mois ? 3 mois serait une durée trop courte. Des cas particuliers sont à prendre en compte : • Congés maternité • Congés maladie long • Année sabbatique Besoin d'avoir un usage pour le PS avant de commencer à utiliser sa MSSanté (ex : création de lien avec les autres PS du territoire) Si le choix est de fermer les boites inactives, il y aurait un impact sur un éventuel redéploiement, d'autant plus que les usages arrivent. U opérateur indique que dans son cas la création d'une boite prend 1 mois en moyenne (à cause notamment de la signature des conditions d'utilisation)	ANS / CNAM : La cible de l'ANS présente 2 paliers : > une dépublication des BAL non consultées au bout de X temps > suivi d'une suppression après atteinte de X temps sans consultation. Une purge serait utile pour respecter les règles du RGPD. Les durées de dépublication et de suppression seront à concerter. Dans les indicateurs envoyés par les opérateurs, il y a déjà la date de dernière connexion pour chaque boite qui est demandée. L'objectif de ces dépublications est de nettoyer l'annuaire et de le fiabiliser pour chaque PS. Dans le passé de nombreuses boites ont été créés uniquement pour toucher des aides liées au déploiement (sans nécessairement d'usage). Une étude est en cours sur la possibilité pour le PS d'avoir une boite de contact préférentiel. Aujourd'hui les usages arrivent et les BAL MSSanté seront utiles pour la communication entre le PS et ses patients notamment.
8	**I**	Nouvelles exigences hors API LPS - Qualité des BAL présentes dans l'annuaire (p11)	Pharmagest / EFS : Les boîtes personnelles / organisationnelles sont-elles nécessaires en pharmacie et dans le médico-social ?	ANS : Selon l'organisation de l'officine, il est possible d'avoir des BAL personnelles et organisationnelles selon les usages. Pour le Medico Social, des BAL organisationnelles seront certainement nécessaire mais des boites nominatives seront surement utiles également

9	**A**	Focus MIE de l'API LPS (p.16)	Dedalus : Que penser de l'utilisation des services antispam externes (ex: mailinblack) générateurs de mails de retour provenant d'un service externe non autorisé sur l'espace de confiance ?	Nous serions intéressés par une description de ce cas. Pourriez-vous nous écrire pour préciser votre question ? De contruction, MSSanté n'est pas exposé aux Spam. Les solutions antispam ne sont pas nécessaires.
10	**I**	Focus MIE de l'API LPS - Authentification PSC : Cinématique LPS client lourd (p.16)	ANS : Pour les domaines en erreur depuis X mois, merci de le signaler à l'ANS pour instruction. Il est aussi souhaité de développer un outil de monitoring des domaines coté ANS.	-
11	**I**	Focus MIE de l'API LPS - Authentification PSC : Cinématique LPS client lourd (p.16)	ANS : Sur cette architecture, dans le cas client lourd, existe-t-il une brique qui peut jouer le rôle de LPS serveur intermédiaire ?	Pharmagest : Il sera possible d'avoir ce type d'architecture mais la cinématique est en train d'être mise en place. Le LPS serveur intermédiaire sert déjà d'*identity provider* avec son système de token, donc il y aurait un doublon de token avec PSC.
12	**I**	Focus MIE de l'API LPS - Authentification PSC : Cinématique LPS client lourd (p.16)	Xelya : Pourquoi CIBA n'est pas mentionné ?	ANS : Etant donné le calendrier de sortie du référentiel MSSanté, CIBA ne peut être inclus pour l'instant et il faudra utiliser le flux de redirection. Mise en production CIBA planifiée en mai 2022 Pas d'impact dans l'utilisation de l'une ou l'autre des méthodes pour l'opérateur cependant il y en a pour les clients.

13	**I**	Focus MIE de l'API LPS - Authentification PSC : Cinématique LPS client lourd (p.16)	Compugroup : Y a-t-il des préconisations pour la mise en place de ces serveurs LPS intermédiaires ? Quelle nécessité par rapport à une architecture centralisée sur les LPS ?	ANS : Il est prévu de donner des pistes d'implémentation et de codes exemples dans le référentiel, le but est d'accélérer la mise en œuvre pour les éditeurs et les opérateurs. Concernant la nécessité, une des contraintes PSC est de déclarer le logiciel qui sollicite l'authentification, donc dans le cas de clients lourds, il y aurait autant d'instances, ce qui n'est pas tenable en termes de charge. Cela ne serait également pas satisfaisant en termes de sécurité car la clé secrète PSC serait présente sur chaque poste de PS.
14	**I**	Focus MIE de l'API LPS - Authentification PSC : Cinématique LPS client lourd (p.16)	Quelle est la durée de validité des tokens PSC ?	ANS : la durée est vie de l'access token est de 2 minutes. La session PSC est de 15 minutes sur inactivité.
15	**I**	Focus MIE de l'API LPS - Authentification PSC : Cinématique LPS client lourd (p.16)	Quelle disponibilité pour PSC ?	Le SLA actuel de PSC est de 99,8%. L'infrastructure s'adaptera à l'arrivée des nouveaux services. Sachant que les services de facturation seront probablement les plus consommateurs en volume.

16	**A**	Focus MIE de l'API LPS - Authentification PSC : Cinématique Opérateur (p.16)	Pharmagest : Est-il possible d'utiliser un access token qui était destiné à un autre service que MSSanté ? Si l'utilisateur est déjà connecté via PSC, pourquoi l'étape 6 (interrogation du *endpoint*) est-elle nécessaire ? L'audience de l'access token est censée être déclarée pour des raisons de vérification et de sécurité, est-ce que c'est donc bien le même qui est utilisé pour tous les services ?	ANS : l'access token PSC a une portée globale mais pas spécifique à un service en particulier, l'habilitation est gérée par le service. Hors réunion : PSC ne positionne pas d'audience. Une audience commune à tous les services esanté sera peut-être prochainement utilisée. Si la mécanique d'authentification a eu lieu à l'ouverture de session par le LPS, il n'est pas nécessaire de refaire cette mécanique tant que l'access token est valide.
17	**I**	Focus MIE de l'API LPS - Authentification PSC : Cinématique Opérateur (p.16)	Pharmagest : Est ce que PSC sera nécessaire pour tous les services de la vague 2 ?	ANS : Pour la vague 1 tous les éditeurs se mettent en capacité de gérer un flux de redirection. Il y aura sûrement besoin de PSC pour accéder aux différents services esanté à terme.
18	**I**	MIE - Authentification PSC : Cinématique opérateur (p.18)	Architecte Capgemini : Les opérateurs ont-ils un avis sur la durée de session : • Session courte pour IMAP/SMTP • Session longue pour le web	Pas de position partagée en séance.
19	**I**	Rappels : spécification ENS disponibles pour les éditeurs	Dedalus : L'utilisation du HTML pour les envois de mails par MES est délicat car beaucoup de professionnel envoie en texte brut pour réimport automatique dans les LGC.	ANS : c'est une anomalie car ce n'est pas conforme au référentiel MSSanté mais une modification est prévue par la CNAM.