AGENCE
DU NUMÉRIQUE
EN SANTÉ

COMPTE-RENDU

Task Force MSSanté

Atelier industriel #2

Réunion du 21/01/2022

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 #2
Date	21 janvier 2022
Organisateur[1]	Mathieu SLOSAR
Type de réunion	Atelier
Rédacteur[2]	Samy Abdiche

Documents de référence
- Support de présentation «MSS_TF_MSS_Atelier_2_20220121_V1 »

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 second atelier étaient les suivants :

1. Retour sur la concertation à propos du REM v0.1
2. Focus sur les moyens d'authentification électronique (MIE)
    a. Authentification PSC via LPS
    b. Présentation de l'authentification OTP par l'opérateur
    c. Maintien d'une authentification CPS locale à l'opérateur ?
    d. Authentification par certificat IGC Santé pour les BAL applicatives
3. Entêtes spécifiques MSSanté côté client de messagerie
4. ~~Evolution des indicateurs d'usage MSS côté opérateur~~ (reporté atelier #3)
5. ~~Rationalisation des BAL publiées dans l'annuaire~~ (reporté atelier #3)

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 :
	Samy ABDICHE / Capgemini Invent	21/01/22

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

#	Nature	Objet	Question / Remarque	Réponse
1	I	La mise en conformité selon le nouveau référentiel (Exigences V0.1 p.4)	ESEA NA : en tant que GRADeS qui s'appuie sur une solution technique d'un autre opérateur, comment réaliser cette mise en conformité ?	DNS : La mise en conformité est à organiser par l'opérateur, qui peut le faire lui-même ou sous-traiter cette action. Il est alors question d'intégration de solution plutôt que de développement.

2	I	Méthodes d'authentification à PSC (p.6)	ESEA NA : la méthode d'authentification par SMS va-t-elle devenir obligatoire ? Lifen : existe-t-il un risque de surcoût avec cette méthode d'authentification ?	ANS (équipe MSS) : estime que c'est nécessaire d'avoir une méthode alternative à PSC et qui permette une certaine souplesse pour enrôler des acteurs habilités à échanger des données de santé mais non encore présentes dans l'annuaire national. La notion de cout des SMS sera prise en compte.
3	I	Méthodes d'authentification à PSC (p.6)	Maincare : Une possibilité pourrait être de prendre comme modèle le ou les moyens d'authentification dit de transition qui seront retenus à la suite de la concertation sur l'identification électronique. Le dernier document en concertation proposait TOTP et OTP par SMS.	ANS (équipe MSS) : Des moyens d'authentification dits "alternatifs" à double facteur sont bien autorisés jusqu'à fin 2025 : TOTP et l'OTP en font partie. Les alternatives sont à trouver parmi ces moyens.
4	I	Authentification PSC via LPS (p.6)	Quel est l'avantage de la nouvelle architecture ?	ANS (équipe MSS) : Il s'agit ici de proposer des moyens d'authentification standards à la fois suffisamment robustes pour répondre aux normes de sécurité et en même temps standards pour faciliter les usages.

5	I	Authentification PSC via LPS (p.6)	Enovacom : Est-ce que cette solution est pérenne dans le temps ou bien s'agit-il d'une solution transitoire ? La solution actuelle semble suffisante pour répondre aux besoins des clients finaux.	La solution est effectivement pensée pour être pérenne puisque ce sera demandé aux éditeurs en vague 2. Des travaux sont en cours sur Ameli Pro avec l'intégration de PSC depuis des LPS. ANS (équipe PSC) : avoir des fournisseurs d'identité « *en cascade* » pour PSC ne pose pas de problème pour le service MSSanté. L'équipe PSC se rend disponible pour répondre aux questions d'adaptation. Le modèle actuel d'authentification et le nouveau modèle pourraient cohabiter. DNS : *Dans le référentiel d'identification électronique acteurs de santé - personnes physiques :* *[EXI 03] A compter du 01/01/2026, les seuls moyens d'identification électronique autorisés sur les services sensibles sont :* *- Les moyens d'identification électronique disponibles sous Pro Santé Connect ;* *- La carte CPx ;* *- Les moyens d'identification électronique homologués pour cet usage ;* *- Les moyens d'identification électronique certifiés de niveau de garantie eIDAS substantiel ou élevé, et associés à un identifiant conforme aux exigences du référentiel.* *Jusqu'au 1er janvier 2026, des moyens d'identification électronique alternatifs sont tolérés à titre transitoire, moyennant l'application d'exigences de sécurité définies par ce référentiel. Les autres moyens qui n'atteindraient pas ce niveau de sécurité minimal doivent être abandonnés au 1er juin 2022 au plus tard.*

6	I	Authentification PSC via LPS (p.7)	Est-ce facile d'implémenter cela pour des logiciels avec d'anciennes technologies client lourd ?	ANS (équipe PSC) : ce qui compte est l'architecture de ces logiciels et non pas l'intégration des anciennes technologies.
7	**I**	Authentification PSC via LPS (p.6)	Pharmagest : A quel LPS le client s'identifie dans la nouvelle architecture ? Est-ce le LPS serveur ou bien le LPS client ? Quel est le niveau de sécurité de cette connexion LPS ?	ANS (équipe PSC) : Il s'agit d'une logique OpenID des fournisseurs de données. Les LPS sont engagés contractuellement avec PSC, ce qui sécurise l'accès à PSC. Grâce à l'utilisation du « *endpoint* » dédié à la vérification l'identité des opérateurs est aussi vérifiée. S'il existe un problème, il ne peut avoir lieu qu'aux étapes 5 et 6 de la slide 7. Cela ne peut avoir lieu qu'en cas d'attaque ce qui compromet à la fois le LPS serveur et le LPS client. Donc il n'y a pas de faille a priori.
8	**I**	Authentification PSC via LPS (p.6)	GCS SARA : questionnement sur le schéma client lourd et sur le flux 3 : pourquoi est-il indiqué « flux de redirection » mais pas CIBA ? La méthode présentée peut-elle marcher en restant seulement sur un client lourd ?	ANS (équipe PSC) : L'authentification directe depuis le client lourd vers PSC n'est pas possible. Elle doit nécessairement se faire depuis un serveur unique maitrisé par l'éditeur de LPS. Ce serveur est déclaré auprès de PSC. ANS (équipe MSS) : le choix a été fait d'indiquer « *flux de redirection* » pour rester cohérent avec les anciens schémas et ne pas entrainer de confusion. De plus, les éditeurs de LPS devront intégrer le flux de redirection, avant que le flux CIBA ne soit disponible coté PSC.
9	**I**	Authentification opérateur via OTP (p.6)	GCS SARA : Quel est l'intérêt de mettre en place un nouveau moyen d'authentification, si l'OTP applicative est déjà couverte par CIBA ?	ANS (équipe MSS) : l'intérêt d'un moyen d'authentification alternatif serait de continuer à rendre le service en cas d'indisponibilité de PSC.
10	**I**	CPS authentifiée par l'opérateur (P.12)	Pourquoi si CIBA est toujours prévu à fin juin, on parle ici de fin 2022 ?	ANS (équipe PSC) : l'authentification par CPS via CIBA est en cours de construction. Seule la e-CPS fonctionnera en CIBA en juin 2022. Le support de la CPS en CIBA n'est pas envisagé avant fin 2022 (impact forte sur le poste de travail et la cryptolib).

11	**I**	CPS authentifiée par l'opérateur (P.12)	Xelya : Est-ce que le mode gestion OTP permettra l'accès à une BAL organisationnelle par un personnel soignant en remplacement ?	ANS (équipe MSS) : le cas des remplacement et délégation de boite est transverse aux différents modes d'authentification.
12	**I**	Authentification par certificat IGC Santé pour les BAL applicatives (P.17)	La procédure d'obtention de certificats IGC Santé est jugée longue et complexe.	ANS (équipe PSC) : l'ANS en est consciente. Elle mène un projet de dématérialisation intitulé "CPS service" dont l'aboutissement est prévu en juin 2022.
13	**I**	Entêtes spécifiques MSSanté côté client de messagerie (P.19)	Xelya : pourquoi l'INS qualifié n'est pas obligatoire au point 1 (en-têtes spécifiques MSSanté côté client de messagerie) ?	ANS (équipe MSS) : il y a la possibilité aujourd'hui d'envoyer un message sans INS qualifiée jusqu'en 2023 (date de fin de la dérogation). L'objectif est de voir le développement de l'INS qualifié. DNS : sans INS qualifié, il est tout de même possible d'effectuer des échanges professionnels, des documents, ou d'envoyer des messages MSSanté.