MSSanté
Système de messageries sécurisées, données protégées.

Comité Opérateurs MSSanté

Nouveau dispositif de régulation : Atelier #2

18/06/2026

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ

LES INTERVENANTS

Edouard BRIS

Responsable de l'équipe Echanges MSSanté/Mailiz

Mike GUEYE

Responsable de l'Espace de Confiance MSSanté

Mehdi ZINE

Responsable Accompagnement & Déploiement MSSanté

- Mettre son micro **en muet** lors des temps d'explication
- Privilégier l'onglet « Q/R » afin de soumettre vos questions
- **L'atelier sera enregistré et partagé sur le site mssante.fr**

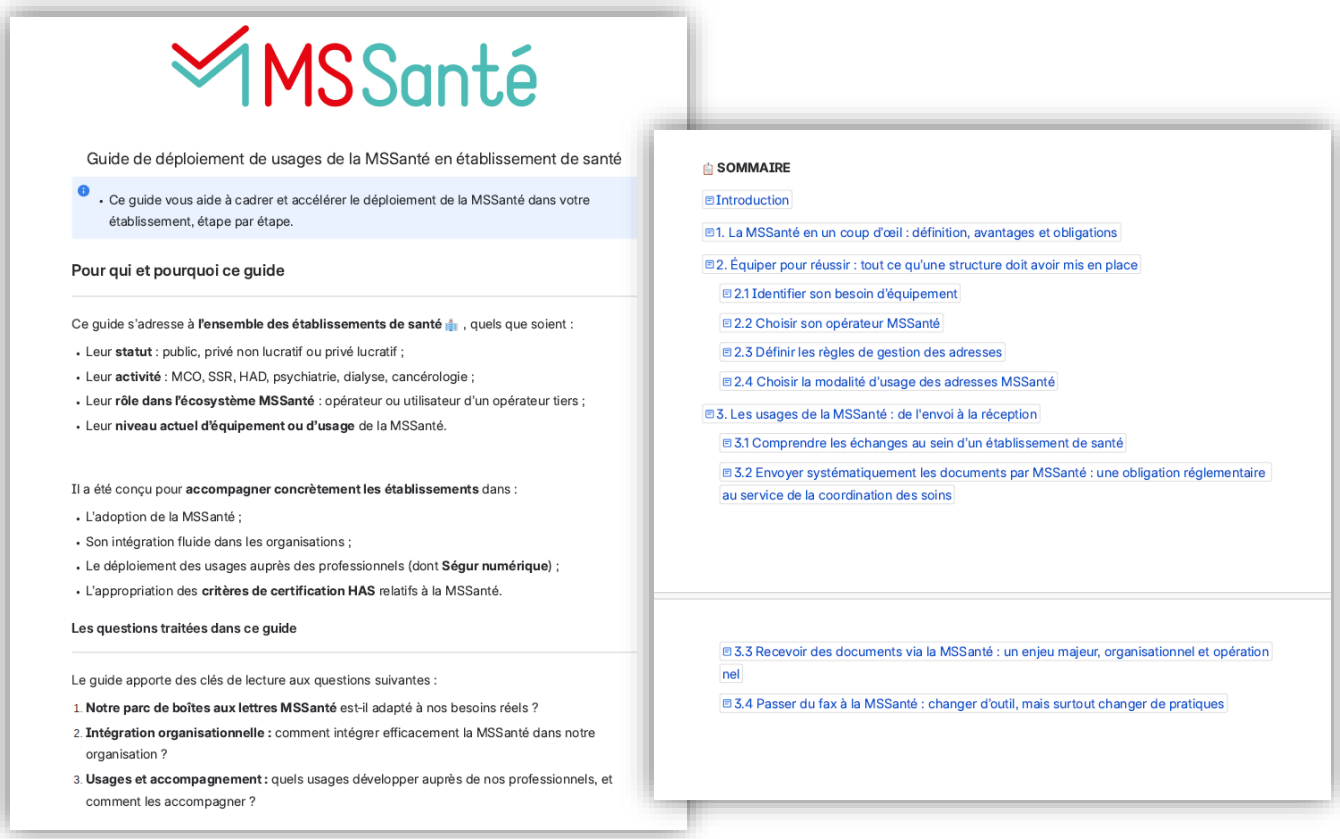
Pour intervenir :

- Utiliser la fonction « lever la main » et attendre l'aval des intervenants
- Ou **utiliser le chat en ligne**, l'onglet « Q/R »

SOMMAIRE

I - GUIDE DE DÉPLOIEMENT DES USAGES MSSANTÉ POUR LES ES

Guide de déploiement des usages à la MSSanté pour les ES



MSSanté

Guide de déploiement de usages de la MSSanté en établissement de santé

- Ce guide vous aide à cadrer et accélérer le déploiement de la MSSanté dans votre établissement, étape par étape.

Pour qui et pourquoi ce guide

Ce guide s'adresse à **l'ensemble des établissements de santé** , quels que soient :

- Leur **statut** : public, privé non lucratif ou privé lucratif ;
- Leur **activité** : MCO, SSR, HAD, psychiatrie, dialyse, cancérologie ;
- Leur **rôle dans l'écosystème MSSanté** : opérateur ou utilisateur d'un opérateur tiers ;
- Leur **niveau actuel d'équipement ou d'usage** de la MSSanté.

Il a été conçu pour **accompagner concrètement les établissements** dans :

- L'adoption de la MSSanté ;
- Son intégration fluide dans les organisations ;
- Le déploiement des usages auprès des professionnels (dont **Ségur numérique**) ;
- L'appropriation des **critères de certification HAS** relatifs à la MSSanté.

Les questions traitées dans ce guide

Le guide apporte des clés de lecture aux questions suivantes :

1. **Notre parc de boîtes aux lettres MSSanté** est-il adapté à nos besoins réels ?
2. **Intégration organisationnelle :** comment intégrer efficacement la MSSanté dans notre organisation ?
3. **Usages et accompagnement :** quels usages développer auprès de nos professionnels, et comment les accompagner ?

SOMMAIRE

Lien vers le guide ES :
ans-esante.atlassian.net/wiki/external/ODY0ZTlkZjIxMzQzNDJmNDk0YjEyMGUzMDJkZDJmYjA

Ce guide a été conçu **pour accompagner concrètement les établissements** dans :

- L'adoption de la MSSanté ;
- Son intégration fluide dans les organisations ;
- Le déploiement des usages auprès des professionnels (dont Ségur numérique) ;
- L'appropriation des critères de certification HAS relatifs à la MSSanté.

Un **guide sous format interactif disponible depuis le site de l'ANS et qui a vocation à s'enrichir au fil du temps** en particulier à partir de retours d'expérience en établissement (interview, fiche capitalisation, etc…)
Actu : Guide de déploiement des usages MSSanté : accompagner les établissements de santé vers une utilisation généralisée de la messagerie sécurisée | Agence du Numérique en Santé

II CONSTRUCTION DU REF #1 V1.7

MODALITES DE CONSTRUCTION DU REFERENTIEL 1.7

Date	Action	Objectif
J	Atelier #N	• Présentation de proposition de modification, ajout ou suppression d'exigences
J+1	Diffusion par l'ANS du tableau des exigences contenant celles présentées lors de l'atelier N	• Permettre aux opérateurs de formuler leurs observations sur chaque exigence présentée • Permettre aux opérateurs de proposer des évolutions du référentiels
J+7	Renvoi à l'ANS du tableau des exigences amandées par chaque opérateur	• Consolidation et anonymisation des remarques opérateurs • Réponse aux remarques opérateurs
J+14	Atelier #N+1	• Partager les remarques anonymisées des opérateurs sur le précédent lot d'exigences • Partager les demandes d'évolution faites pas les opérateurs • Présenter un nouveau lot de proposition de modification, ajout ou suppression d'exigences

Merci aux 9 opérateurs (3 industriels, 1 Grades et 5 CH) qui nous ont transmis leurs remarques, dont 1 avec des demandes d'évolution :

- Intégrer les BAL CAB dans l'extraction globale MSSanté
- S'assurer que le site Annuaire Santé et l'extraction globale MSSanté fournissent des résultats identiques
- Mettre à disposition un annuaire accessible en interrogation directe, permettant des consultations à la fréquence souhaitée *(besoin de précisions).*

RETOURS SUR LES EXIGENCES PRESENTEES LORS DE L'ATELIER 1

Restitution des retours (1/8)

EXIGENCE	FORMULATION	REMARQUES/QUESTIONS	REPONSES
EX_GEN_0300	Tout Opérateur intégré à l'Espace de Confiance, proposant un service MSSanté à des acteurs hors de sa propre structure, doit communiquer à l'ANS les informations nécessaires chaque fois qu'il est sollicité afin de renseigner le "Panorama des offres MSSanté" disponible sur le lien https://esante.gouv.fr/strategie-nationale/mssante/panorama-offres-mssante. ** tout acteur hors Espace de Confiance proposant un service MSSanté (se basant sur un Opérateur présent en Liste Blanche MSSanté) peut également renseigner le "Panorama des offres MSSanté".	**OPERATEUR_1** Déjà fait. **OPERATEUR_3** Quel est le périmètre concerné ? Devons-nous mettre à jour les informations relatives à nos clients (Grades)?	**OPERATEUR_3** : Les Grades qui sont vos clients c'est à eux de renseigner le panorama. En tant qu'opérateur développeur vous pouvez aussi décrire votre offre si elle s'adresse directement à des professionnels
EX_GBM_4312	L'Opérateur doit interdire la création de nouvelle BAL PER de type 10 au profit des BAL de type 8.	**OPERATEUR_1** Pour l'instant on accepte les BALs de type10. **OPERATEUR_2** Plus de détails sur le plan d'assainissement des BALs déjà créées ? **OPERATEUR_3** Comment devons-nous gérer les cas suivants : - Les médecins n'ayant pas obtenu leur diplôme en France ; - Les IDE ayant terminé leurs études mais n'ayant pas encore reçu leur diplôme, et ne pouvant donc pas obtenir de numéro RPPS. Cette situation peut perdurer jusqu'à six mois avant la délivrance effective du diplôme. Existe-t-il un référentiel pour la bascule des BAL PER type 10 vers PER, similaire à celui mis en place pour la migration ADELI vers RPPS ? **OPERATEUR_8 (besoin de précisions)** L'interdiction porte sur la création de BAL PER de type 10 dans l'annuaire ou de manière globale ? Si un opérateur repose l'accès aux BAL cab sur ces BAL PER de type10 sans les publier dans l'annuaire, cela a-t-il un impact ? **OPERATEUR_9** Quid des BAL organisationnelles utilisées aujourd'hui ?	**OPERATEUR_2** : Chaque opérateur doit faire l'inventaire de ses BAL de type 10 afin d'identifier les professionnels : - qui peuvent disposer d'un identifiant RPPS. Modifier le fichier d'alimentation de l'annuaire - qui ne pourraient pas en disposer. Nous transmettre cette liste de profession pour instruction **OPERATEUR_3 :** Nous devons instruire ces 2 cas de figure : médecin avec diplome étranger et IDE nouvellement diplomée **OPERATEUR_8 :** L'objectif est bien de ne plus créer de BAL de type 10 et de migrer les existantes sur un type 8 RPPS. Il ne doit pas y avoir de type 10 qui perdurent non déclarée dans l'annuaire. **OPERATEUR_9 :** pas d'impact a priori sur les BAL ORG.
EX_GBM_4430	A SUPPRIMER L'Opérateur DOIT proposer la fonction de délégation pour toutes les BAL personnelles ou organisationnelles, tel que décrit au §5.4.2 du présent Référentiel #1 Opérateur. Les	**OPERATEUR_6** Effectivement à supprimer : notre DPI par exemple ne sait pas gérer la réception de	

Restitution des retours (2/8)

EXIGENCE	FORMULATION	REMARQUES/QUESTIONS	REPONSES
EX_GBM_4470	Afin de minimiser le risque de non-réception de message, l'Opérateur DOIT informer le ou les l'utilisateurs d'une BAL lorsque celle-ci ~~dépasse 80%, puis 90% du quota~~. Lorsque 100% du quota est atteint le ou les utilisateurs de la BAL doivent être informés qu'il ne pourra plus recevoir ou envoyer de message tant que le quota sera à 100%. Afin de minimiser le risque de non-réception de message, **l'Opérateur dont la BAL dispose d'un quota maximal de stockage** DOIT informer à plusieurs reprises le ou les l'utilisateurs d'une BAL lorsque celle-ci s'approche du quota. Lorsque 100% du quota est atteint le ou les utilisateurs de la BAL doivent être informés qu'il ne pourra plus recevoir ou envoyer de message tant que le quota sera à 100%.	**OPERATEUR_1** Dans notre cas on envoi un mail à l'adresse de notification de la BAL tous les jours une fois que la BAL atteint les 90% du quota. Du coup on n'envoie pas 3 mails (à 80 %, 90 % et 100%) mais un mail par jour à partir de 90 % **OPERATEUR_2** Dans le cas ou le serveur de messagerie (et donc la BAL) n'est pas gérée par l'opérateur industriel, la responsabilité ne peut pas être portée par l'opérateur. **OPERATEUR_3** Non concerné. Nous ne fonctionnons pas avec un système de quota de stockage. Les messages sont conservés pendant une durée définie et sont automatiquement supprimés au terme d'une période de 3 mois. **OPERATEUR_5** Alerte boite mail exchange **OPERATEUR_7** Très utile, il y a de nombreux professionnels avec des BAL pleine **OPERATEUR_9** Aujourd'hui au CH Fougères => Pas de quota messagerie Si gestion quota => limitation Exchange sur le nombre de niveau (1=Avertissement / 2= Interdiction envoi / 3=Interdiction envoi et réception	***QUESTION :*** *A votre avis, quel est le bon canal afin d'adresser l'alerte de quota ? La BAL MSSanté ou la BAL d'enrôlement) ?* **OPERATEUR_1** Reformulation pour accepter plusieurs modalités d'alerte **OPERATEUR_2** Dans le cas ou le serveur de messagerie (et donc la BAL) n'est pas gérée par l'opérateur industriel, la responsabilité porte sur votre client (nécessaire de l'en informer (CGU ?)) **OPERATEUR_3** Précision apportée **OPERATEUR_5** S'il s'agit d'une BAL Exchange des alertes doivent être positionnée **OPERATEUR_9** Si pas de quota maximal, l'exigence ne s'applique pas

Restitution des retours (3/8)

EXIGENCE	FORMULATION	REMARQUES/QUESTIONS	REPONSES
EX_GBM_6021	Lorsqu'un PS dispose d'une BAL personnelle visible au sein de l'Annuaire Santé et n'exerce plus au sein de la structure de rattachement de la BAL, l'Opérateur doit mettre à disposition une procédure de demande de suppression de la BAL à destination du PS.	**OPERATEUR_1** Dans notre cas, notre espace d'administration permet de faire n'importe quelle demande. **OPERATEUR_2** Comment authentifier l'émetteur de la demande ? Est-ce une autre entité peut faire ce type de demande pour un PS (établissement ?) ? Qu'en est-il quand l'opérateur ne gère pas la BAL mais seulement le compte MSSanté ? **OPERATEUR_3** Pourriez-vous nous indiquer sur quel référentiel devons-nous nous appuyer afin de déterminer qu'un professionnel de santé n'exerce plus au sein de la structure ? Par ailleurs, un administrateur a la possibilité de supprimer le compte d'un utilisateur ne faisant plus partie de sa structure. **OPERATEUR_5** Suppression systématique effectuée au départ du professionnel **OPERATEUR_7** Très utile, nous constatons que les professionnels ne savent pas comment mettre à jour leurs coordonnées **OPERATEUR_9** Suppression de la BAL MSSanté lorsque le PS quitte l'établissement (Fait par le service informatique)	**Objectif de l'exigence** : répondre aux PS exerçant en structure pour qui la suppression automatique au départ de la structure n'aurait pas fonctionné. Les PS n'arrivent pas à faire supprimer leurs BAL de l'annuaire ***QUESTION :*** *Quel est votre avis si,* *L'ANS adresse à fréquence régulière, aux Opérateurs concernés, une liste de demandes de suppression de BAL MSSanté. Demande à l'initiative des PS (identité confirmée par les services de l'ANS)*

Restitution des retours (4/8)

EXIGENCE	FORMULATION	REMARQUES/QUESTIONS	REPONSES
EX_GBP_3050	Selon les recommandations de la Cnil, l'opérateur DOIT proposer au gestionnaire de la BAL une solution afin de purger les éléments envoyés d'une BAL afin de ne pas stocker des données de santé à caractère personnel qui n'ont pas d'usage	**OPERATEUR_1** Dans notre cas nous avons un mécanisme de suppression auto des mails plus vieux de x jours (configurable depuis la BAL) Par défaut les mails du répertoire 'envoyés' plus vieux de 30 jours sont supprimés automatiquement **OPERATEUR_2** Dans le cas ou le serveur de messagerie (et donc la BAL) n'est pas gérée par l'opérateur industriel, la responsabilité ne peut pas être portée par l'opérateur. **OPERATEUR_3** Les messages sont supprimés automatiquement au bout de 3 mois. L'utilisateur a également la possibilité de supprimer un message. **OPERATEUR_4** Beaucoup trop ambitieux : Impossible de scanner toutes les BALS à la recherche de celles qui envoient du contenu via MSSANTE et de purger les mails en envoi **OPERATEUR_5 (besoin de précisions)** Suppression systématique effectuée au départ du professionnel. Pas d'action de nettoyage durant la vie de la BAL (demande déplacée, pas d'intervention intrusive)	**OPERATEUR_2** Dans le cas ou le serveur de messagerie (et donc la BAL) n'est pas gérée par l'opérateur industriel, la responsabilité porte sur votre client (nécessaire de l'en informer (CGU ?)) **Objectif** : Eviter que les BAL atteignent leur quota et que les utilisateurs ne sachent pas comment nettoyer leur BAL. Doit-on aller vers une suppression automatique des messages reçus et envoyés après X jours ?

Restitution des retours (5/8)

EXIGENCE	FORMULATION	REMARQUES/QUESTIONS	REPONSES
EX_GBM_4480	Afin de simplifier les usages d'un professionnel disposant de plusieurs BAL PER, le système doit permettre de configurer pour chaque BAL PER une règle permettant de transférer automatiquement les messages recus à une autre BAL PER MSSanté. Le système DOIT informer le professionnel que la BAL de destination doit nécessairement être détenue par le meme professionnel. Rq : Le langage de filtrage d'Email Sieve est défini par la RFC 5228	**OPERATEUR_1** Dans notre cas nous avons un attribut pour chaque BAL PER permettant de mettre une adresse de redirection. Chaque mail reçu sur cette BAL sera donc redirigé vers l'adresse de redirection **OPERATEUR_2** Dans le cas ou le serveur de messagerie (et donc la BAL) n'est pas gérée par l'opérateur industriel, la responsabilité ne peut pas être portée par l'opérateur. **OPERATEUR_5** Actuellement : Transfert possible mais impossibilité de contrôler l'envoi à un tiers. Ce contrôle agirait sur le mode de fonctionnement institutionnel de l'organisation **OPERATEUR_7** Certainement très utile pour permettre aux professionnels multi-structure de centraliser **OPERATEUR_8** S'assurer que cette simplification de l'usage ne créé pas de non-usage sur les BAL redirigées vers une autre. Et plus particulièrement l'absence d'authentification, pouvant amener sa suppression sur le long terme **OPERATEUR_9** Quid du transfert automatique vers BAL organisationnelles (intégration résultats dans DPI par les secrétaires) ?	**OPERATEUR_2** Dans le cas ou le serveur de messagerie (et donc la BAL) n'est pas gérée par l'opérateur industriel, la responsabilité porte sur votre client (nécessaire de l'en informer (CGU ?)) **OPERATEUR_5** L'exigence ne demande pas d'interdire la redirection à un tier, mais demande d'en informer le professionnel **OPERATEUR_8** *Précision sur le cas d'usage :* *Un PS a changé de BAL, pendant une période afin de ne pas perdre de message effectue un transfert de son ancienne BAL vers la nouvelle. À terme l'ancienne BAL devra être décommissionnée.* *Avez vous d'autres cas d'usage ?* En cas de non-connexion de plus de 2 mois la BAL sera dépublié et supprimée au bout d'un an. Cohérent avec le besoin de conserver une BAL avant de la supprimer, afin de s'assurer de ne pas perdre de message dans l'intervalle

Restitution des retours (6/8)

EXIGENCE	FORMULATION	REMARQUES/QUESTIONS	REPONSES
EX_GBM_4460 	Le système DOIT produire un NDR (Non Delivery Report), rédigé en français et indiquant le code retour spécifié, a minima lors des cas suivants : - lorsque le destinataire est non trouvé (code retour 5.1.1) - lorsque le quota de la BAL est dépassé (code retour 5.2.2)	**OPERATEUR_1** Dans notre cas un mail de non-réception est envoyé à l'expéditeur avec les détails de non-réception. **OPERATEUR_2** Dans le cas où le serveur de messagerie (et donc la BAL) n'est pas géré par l'opérateur industriel, la responsabilité ne peut pas être portée par l'opérateur. **OPERATEUR_3** A l'étude. **OPERATEUR_5** Les messages retour sont bien reçus **OPERATEUR_7** Lifen nous signale que le message a été bien remis et améliore les notifications d'erreur **OPERATEUR _X** Quid du risque de backscatter ?	**OPERATEUR_2** Dans le cas ou le serveur de messagerie (et donc la BAL) n'est pas gérée par l'opérateur industriel, la responsabilité porte sur votre client (nécessaire de l'en informer (CGU ?)) **OPERATEUR_X** Sujet restant à instruire

Restitution des retours (7/8)

EXIGENCE	FORMULATION	REMARQUES/QUESTIONS	REPONSES
EX_GBM_4450	Le système DOIT produire un accusé de réception de type DSN, rédigé en française, lors de la réception d'un courrier contenant l'attribut NOTIFY dans la commande SMTP "RCPT TO:". Le mécanisme DSN est décrit dans la RFC 3461.	**OPERATEUR_1** Dans notre cas toutes les BALs peuvent demander un accusé de réception pour tous les mails envoyés. Il s'agit d'un attribut configurable depuis la BAL. **OPERATEUR_2** Dans le cas ou le serveur de messagerie (et donc la BAL) n'est pas gérée par l'opérateur industriel, la responsabilité ne peut pas être portée par l'opérateur. **OPERATEUR_3** A l'étude. **OPERATEUR_5** Le test sera effectué **OPERATEUR_7** Lifen nous signale que le message a été bien remis et améliore les notifications d'erreur	**OPERATEUR_2** Dans le cas ou le serveur de messagerie (et donc la BAL) n'est pas gérée par l'opérateur industriel, la responsabilité porte sur votre client (nécessaire de l'en informer (CGU ?))

Restitution des retours (8/8)

EXIGENCE	FORMULATION	REMARQUES/QUESTIONS	REPONSES
EX_GBM_4471	Le système DOIT permettre de configurer pour chaque BAL PER,ORG, CAB ou APP un message de réponse automatique suivant les préconisations de la RFC 3834.	**OPERATEUR_1** Dans notre cas une réponse automatique est configurable sur chaque type de BAL. **OPERATEUR_2** Dans le cas ou le serveur de messagerie (et donc la BAL) n'est pas gérée par l'opérateur industriel, la responsabilité ne peut pas être portée par l'opérateur. **OPERATEUR_3** Déjà mis en place **OPERATEUR_5** Le test sera effectué **OPERATEUR_7** Certainement utile en cas d'absence prolongée	**OPERATEUR**_2 Dans le cas ou le serveur de messagerie (et donc la BAL) n'est pas gérée par l'opérateur industriel, la responsabilité porte sur votre client (nécessaire de l'en informer (CGU ?))

PRESENTATION DES EXIGENCES MODIFIEES : SSI

Exigences SSI

Pourquoi les faire évoluer ?

- Pas de révision globale depuis plusieurs versions de référentiel
- Elles vont redevenir opposables et être plus « visible » car en PJ de l'arrêté du ministère
- De nouvelles versions de référentiels sécurité ont été publiées : PGSSIS RIE v2, le Référentiel Cyber France (ReCyf ANSSI), ainsi que la directive NIS2

Les exigences en chiffres

- **32** exigences SSI ou relatives aux traces :
  - 12 exigences conservées
  - 13 modifiées / actualisées
  - 2 exigences ajoutées (dont reformulations sans impact)
  - 5 exigences reformulées / précisées : sans impact opérateurs

Thème : Sécurité (MAJ 1/5)

§	# Exigence	Rédaction 1.6	Proposition de rédaction 1.7	Objectif
6.2.1	EX_OPE_5010	Le connecteur MSSanté de l'Opérateur DOIT supporter TLS 1.2 (cf. RFC 5246 - http://tools.ietf.org/html/rfc5246)., avec uniquement les suites de chiffrement TLS1.2 suivantes : · 0xC030: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 · 0xC02F: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 · 0xC028: ~~TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384~~ · ~~0xC027: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256~~ · ~~0x009F:~~ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 · 0x009E: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 Dans le cas contraire, la connexion ne doit pas être établie. Les versions SSLv2, SSLv3 ne doivent pas être activées. La longueur du groupe DH doit être >= 2048 bits ou la longueur du groupe elliptique ECDH doit être >= 256 bits. La confidentialité persistante (PFS - perfect foward secrecy) de DH doit être utilisée (DHE ou ECDHE).	Le connecteur MSSanté de l'Opérateur DOIT **supporter TLS 1.3 et TLS 1.2**. Il DOIT refuser toute connexion utilisant une version inférieure à TLS 1.2. Pour TLS 1.3, seules les suites suivantes sont autorisées : - TLS_AES_256_GCM_SHA384 - TLS_CHACHA20_POLY1305_SHA256 - TLS_AES_128_GCM_SHA256 Pour TLS 1.2, seules les suites suivantes sont autorisées : - 0xC030 : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - 0xC02F : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - 0x009F : TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - 0x009E : TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 Les suites CBC (0xC028, 0xC027) SONT INTERDITES. Les versions SSLv2, SSLv3, TLS 1.0 et **TLS 1.1 NE DOIVENT PAS être activées.** La longueur du groupe DH DOIT être ≥ 2048 bits ou la longueur du groupe elliptique ECDH ≥ 256 bits. La confidentialité persistante (PFS - perfect forward secrecy) DOIT être assurée (DHE ou ECDHE).	Afin de suivre les préconisations des référentiels sécurité : - Supporter dorénavant TLS 1.3 - TLS 1.2 toujours supporté, mais 2 suites considérées comme faibles sont à retirer Guide ANSSI : https://messervices.cyber.gouv.fr/documents-guides/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf

Thème : Sécurité (MAJ 2/5)

§	# Exigence	Rédaction 1.6	Proposition de rédaction 1.7	Objectif
6.9.2	EX_GDT_5050	Pour les traces concernant l'envoi ou la réception d'un message, le champ « type d'action » inclut les informations suivantes : · Identifiant unique interne du message ; · Adresses email de l'émetteur du message et des destinataires du message ; · ~~**Objet du message ;**~~ Le cas échéant, la taille de l'ensemble encodé du message avec les pièces jointes.	Pour les traces relatives à l'envoi ou à la réception d'un message, le champ "type d'action réalisée" DOIT inclure : • un identifiant interne unique du message ; • les adresses email de l'émetteur et des destinataires ; • le cas échéant, la taille totale du message encodé, y compris les pièces jointes. Le contenu du message lui-même n'est jamais journalisé.	Suppression de l'objet du message dans les traces des messages à conserver
6.9.2	EX_GDT_5070	Le service MSSanté proposé par l'Opérateur doit prévoir les mécanismes de paramétrages nécessaires pour permettre au responsable de traitement d'être conforme aux durées de conservation des traces et des données à caractère personnel collectées lors des échanges.	Le service MSSanté proposé par l'Opérateur DOIT offrir des mécanismes permettant au responsable de traitement de configurer les durées de conservation des traces et des données à caractère personnel collectées lors des échanges, dans le respect des obligations légales et réglementaires applicables. **Le service DOIT également garantir la suppression ou l'anonymisation sécurisée des données à l'issue de ces durées.**	Précision sur la suppression ou l'anonymisation des traces à l'issue des durées de conservation
6.9.5.2	EX_SSI_5010	Une analyse de risques SSI doit être réalisée lors de la mise en œuvre d'un service MSSanté. Celle-ci doit être actualisée régulièrement et à chaque évolution majeure du Référentiel #1 pouvant le nécessiter.	Une analyse de risques SSI DOIT être réalisée lors de la mise en œuvre d'un service MSSanté. Elle DOIT être réexaminée **au minimum tous les trois ans**, ainsi qu'à chaque évolution majeure du Référentiel #1 ou de tout changement significatif du service ou de son environnement de sécurité. Un plan d'action DOIT être rédigé en cohérence avec les résultats de cette analyse.	Précision sur la fréquence de la mise à jour de l'analyse de risques
6.9.5.2	EX_SSI_5030	La Politique de Sécurité du Système d'Information (PSSI) doit être rédigée pour prendre en compte ce nouveau service. Celle-ci doit être revue à intervalle régulier. Des audits de la sécurité du système de messageries MSSanté et de son environnement doivent être réalisés à intervalle régulier.	La Politique de Sécurité du Système d'Information (PSSI) DOIT être mise à jour pour intégrer ce nouveau service. Elle DOIT être revue à intervalle régulier et **au minimum tous les 3 ans**. Des audits de sécurité du système de messagerie MSSanté et de son environnement DOIVENT être réalisés à intervalle régulier.	Précision sur la fréquence de la mise à jour de la PSSI

Thème : Sécurité (MAJ 3/5)

§	# Exigence	Rédaction 1.6	Proposition de rédaction 1.7	Objectif
6.9.5.2	EX_SSI_5090	Le système MSSanté doit mettre en œuvre des mécanismes de détection des intrusions. Le système MSSanté doit détecter et bloquer les codes malveillants (virus, vers, chevaux de Troie) contenus au sein de tous les flux d'informations entrants (par exemple, messages et pièces jointes) et sortants. Le système MSSanté doit également alerter les utilisateurs (émetteurs et/ou destinataires) de la mise en quarantaine d'un message et/ou d'une pièce jointe bloqués lors de son envoi ou de sa réception. Pour plus de précisions concernant le traitement à adopter en cas de messages contenant des pièces jointes infectées, le connecteur MSSanté doit être en capacité de filtrer ces pièces jointes, autant en envoi qu'en réception. Ainsi, lors de l'envoi ou de la réception d'un message contenant des pièces jointes infectées, le connecteur MSSanté peut au choix : Transférer au destinataire le message sans la pièce jointe infectée et informer l'émetteur et le destinataire de la non transmission de cette pièce jointe ; Ne pas transférer le message au destinataire et informer l'émetteur que le message ne peut être envoyé pour cause de contenu malveillant détecté dans la pièce jointe.	Le système MSSanté doit mettre en œuvre des mécanismes de détection des intrusions. Le système MSSanté doit détecter et bloquer les codes malveillants (virus, vers, chevaux de Troie) contenus au sein de tous les flux d'informations entrants (par exemple, messages et pièces jointes) et sortants. Le système MSSanté doit également alerter les utilisateurs (émetteurs et/ou destinataires) de la mise en quarantaine d'un message et/ou d'une pièce jointe bloqués lors de son envoi ou de sa réception. Pour plus de précisions concernant le traitement à adopter en cas de messages contenant des pièces jointes infectées, le connecteur MSSanté doit être en capacité de filtrer ces pièces jointes, autant en envoi qu'en réception. Ainsi, lors de l'envoi ou de la réception d'un message contenant des pièces jointes infectées, le connecteur MSSanté peut au choix : Transférer au destinataire le message sans la pièce jointe infectée et informer l'émetteur et le destinataire de la non transmission de cette pièce jointe ; Ne pas transférer le message au destinataire et informer l'émetteur que le message ne peut être envoyé pour cause de contenu malveillant détecté dans la pièce jointe.	Clarification en se focalisant sur la détection des incidents
6.9.5.2	EX_SSI_5160	~~Le système doit bénéficier d'un dispositif de gestion des incidents de sécurité capable de les détecter, les évaluer et les traiter dans les meilleurs délais.~~		Supprimée car redondante avec EX_SSI_5090 qui inclus déjà : détection et traitement

Thème : Sécurité (MAJ 4/5)

§	# Exigence	Rédaction 1.6	Proposition de rédaction 1.7	Objectif
6.9.5.2	EX_SSI_5110	Les sauvegardes doivent être testées à intervalle régulier afin de valider l'ensemble du processus de sauvegarde/restauration. Ces tests doivent inclure au moins une restauration de l'ensemble des composants d'un service.	Les sauvegardes DOIVENT être testées à intervalle régulier afin de vérifier l'efficacité du processus de sauvegarde et restauration. Ces tests DOIVENT inclure, au minimum, une restauration complète de l'ensemble des composants d'un service, ainsi que des restaurations partielles représentatives. **Le processus de sauvegarde et restauration DOIT être documenté, maintenu à jour et mis à disposition des personnes habilitées.**	Ajout la nécessité de documenter le processus de sauvegarde
6.9.5.2	EX_SSI_5120	Le service de messagerie doit bénéficier d'un service de supervision configuré pour générer des alertes automatisées sur des événements spécifiés et jugés critiques pour la sécurité du service (disponibilité, intégrité, confidentialité et auditabilité). Les exigences concernant les traces sont définies dans le § 6.9.2.	Le système DOIT **analyser l'ensemble des flux de messagerie MSSanté**, y compris les messages et leurs pièces jointes, en émission comme en réception, et DOIT filtrer les contenus malveillants détectés. **Lorsqu'un contenu malveillant est identifié, le connecteur MSSanté DOIT** : - soit transmettre le message sans la pièce jointe infectée et informer l'émetteur et le destinataire de la non-transmission de celle-ci ; - soit refuser la transmission du message et en informer l'émetteur en précisant le motif du rejet.	Clarification des analyses demandées en termes de supervision
6.9.5.2	EX_SSI_5140	Les pares-feux protégeant l'infrastructure du SI doivent bénéficier des mécanismes de protection conformes à l'état de l'art.	Les pare-feux DOIVENT être durcis et protégés conformément à l'état de l'art, incluant : **la restriction des accès d'administration, la segmentation des interfaces de gestion, la journalisation et supervision de leur intégrité, la mise à jour régulière de leurs composants logiciels, et la sécurisation de leurs configurations et règles. Toute modification de configuration ou de règles DOIT être tracée et justifiée.**	Précision des modalités de gestion des pare-feux
6.9.5.2	EX_SSI_5150	Les outils déployés pour l'administration et/ou l'exploitation du SI doivent mettre en œuvre une authentification des Opérateurs (exploitants, administrateurs).	Les outils d'administration et d'exploitation du SI DOIVENT mettre en œuvre une **authentification forte** (multifacteur) pour tous les Opérateurs (administrateurs, exploitants).	Ajout de la nécessité de recourir à une authentification forte

Thème : Sécurité (MAJ 5/5)

§	# Exigence	Rédaction 1.6	Proposition de rédaction 1.7	Objectif
6.9.5.3	**EX_SSI_5180**	Comme indiqué dans les documents contractuels les Opérateurs MSSanté intégrés de façon validés ont l'obligation de signaler à l'ANS en tant que gestionnaire de l'Espace de Confiance « […] toute modification, tout dysfonctionnement ou toute anomalie sur leur service de Messageries Sécurisées de Santé qui aurait un impact sur le bon fonctionnement, la disponibilité ou la sécurité du « système MSSanté » […] dans les vingt-quatre (24) heures qui suivent l'identification du dysfonctionnement ou de l'anomalie.». De même, ils doivent informer l'ANS de tout arrêt temporaire supérieur à 8 jours. Les canaux dédiés pour ces déclarations d'incidents sont : l'adresse mail : monserviceclient.mssante@esante.gouv.fr le numéro de téléphone : 0 806 800 213 (appel gratuit).	L'Opérateur DOIT prévenir l'Agence du Numérique en Santé **sous 12h** en cas de détection d'un incident de sécurité et/ou impliquant une violation de données à caractère personnel. Les canaux dédiés pour ces déclarations d'incidents sont : - l'adresse mail : monserviceclient.mssante@esante.gouv.fr - le numéro de téléphone : 0 806 800 213 (appel gratuit). Rq : Cette déclaration doit être faite sans préjudice des obligations de notification à la CNIL prévues par le RGPD.	Fusion avec EX_SSI_5120 + reprise de la rédaction de l'exigence EXI PSC 27 du référentiel de l'espace de confiance PSC
6.9.5.2	**EX_SSI_5020**	~~En cas d'incident de sécurité, et en particulier pour ceux liés à une perte d'intégrité ou de confidentialité, l'Opérateur doit informer l'ANS dans les plus brefs délais.~~		Remplacée par EX_SSI_5180 modifiée

Thème : Sécurité (ajout)

§	# Exigence	Rédaction 1.6	Proposition de rédaction 1.7	Objectif
6.9.5.2	**EX_SSI_5125**	**N/A**	L'Opérateur DOIT mettre en œuvre **un processus de veille sur les vulnérabilités,** les correctifs de sécurité et les mesures d'atténuation préconisées susceptibles de concerner les composants du service MSSanté. Un processus de patch management DOIT être déterminé et mis en oeuvre.	Aucune exigence sur le suivi des vulnérabilités dans Ref#1 1.6
6.9.5.2	**EX_SSI_5155**	N/A	**Les comptes disposant de privilèges d'administration** DOIVENT être nominatifs, distincts des comptes utilisateurs standards, et leurs droits DOIVENT être strictement limités au besoin opérationnel.	Aucune exigence sur les comptes d'administration dans Ref#1 1.6

Thème : Sécurité (reformulation 1/2)

§	# Exigence	Rédaction 1.6	Proposition de rédaction 1.7	Objectif
6.9.2	EX_GDT_5040	Chaque action tracée doit préciser le type d'action, l'identité de son auteur dûment authentifié (ou les informations permettant de la déterminer indirectement), les circonstances attachées à cette action (date et heure précise), les moyens techniques utilisés (nature et version de l'OS, navigateur ou client de messagerie), l'adresse réseau local, le contenu de la demande effectuée au système et la réponse fournie par ce dernier (y compris en cas d'échec) et plus généralement toute information utile à la recherche des causes et des effets d'un incident et à la constitution d'un faisceau de preuve. Le contenu des messages eux-mêmes n'est pas tracé.	Chaque action tracée DOIT inclure : • le type d'action réalisée ; • l'identification de son auteur, de manière directe après authentification ou indirecte via des informations permettant de le déterminer ; • la date et l'heure précises de l'action, issues d'une source de temps synchronisée ; • les caractéristiques techniques du poste ou service ayant initié l'action (par exemple : type et version du système, navigateur ou client de messagerie utilisés, lorsque disponible) ; • l'adresse réseau ou l'identifiant technique de la source ; • le contenu de la requête adressée au système et la réponse obtenue, y compris en cas d'échec ; • et, de manière encadrée, tout élément strictement nécessaire à l'analyse des causes et des conséquences d'un incident ou à l'établissement d'un faisceau de preuve. Le contenu des messages échangés n'est jamais journalisé.	Reformulation pour clarification
6.9.5.2	EX_SSI_5060	Les locaux hébergeant les plateformes de production et de secours du SI doivent bénéficier d'un contrôle des accès physiques.	Les locaux hébergeant les plateformes de production et de secours du SI DOIVENT faire l'objet d'un contrôle strict des accès physiques. Ces locaux DOIVENT être protégés par des dispositifs de sécurité adaptés (ex. contrôle d'accès nominatif, journalisation des entrées, surveillance, détection d'intrusion) et l'accès DOIT être limité aux seules personnes habilitées.	
6.9.5.2	EX_SSI_5070	Les opérations d'exploitation importantes sur le SI (migration, restauration de sauvegarde, dans le cadre d'un plan de continuité, etc…) doivent être formalisées dans des procédures dûment explicitées.	Les opérations d'exploitation critiques du système d'information (telles que les migrations, restaurations de sauvegarde, actions de reprise ou de continuité, ou toute intervention susceptible d'impacter la disponibilité, l'intégrité ou la confidentialité du service) DOIVENT être décrites dans des procédures formalisées, validées, tenues à jour et mises à disposition des personnels autorisés.	

Thème : Sécurité (reformulation 2/2)

§	# Exigence	Rédaction 1.6	Proposition de rédaction 1.7	Objectif
6.9.5.2	EX_SSI_5080	La capacité du système mis en œuvre pour le service MSSanté doit être testée, suivie et anticipée.	La capacité du système mis en œuvre pour le service MSSanté DOIT être testée (tests de charge, stress et montée en capacité), suivie en continu à l'aide d'indicateurs pertinents (CPU, mémoire, I/O, volumétrie, latence, débit, nombre de transactions) et anticipée au moyen d'analyses de tendance permettant d'identifier en amont les besoins d'évolution nécessaires au maintien du niveau de service attendu. Les résultats DOIVENT être documentés et examinés périodiquement.	Reformulation pour clarification
6.9.5.2	EX_SSI_5130	Tout Opérateur doit gérer la liste des utilisateurs autorisés à accéder au service et ses évolutions. Chaque utilisateur doit être identifié puis authentifié avec succès, en s'appuyant sur une base des utilisateurs autorisés, avant de pouvoir accéder au service MSSanté.	L'Opérateur DOIT maintenir une liste à jour des utilisateurs autorisés à accéder au service, en incluant la gestion du cycle de vie des comptes et leur revue périodique. L'accès au service MSSanté ne peut être accordé qu'après identification nominative et authentification forte de l'utilisateur, sur la base de la liste des utilisateurs autorisés, conformément du référentiel d'identification électronique personne physique (RIE PP).	

III SUITE DES TRAVAUX

SUITE DES ATELIERS

UN FICHIER EXCEL VOUS SERA ADRESSÉ APRÈS L'ATELIER *(à retourner avant le 26/06/26)*

> Il contiendra la liste des exigences présentées ce jour

> Il vous permettra de :

** renseigner vos remarques sur les exigences présentées

** préciser tout besoin ou évolution souhaitée concernant le Référentiel #1 ou l'Espace de Confiance

Les réponses seront anonymisées et restituée pendant l'atelier#3.

ATELIER #3

le jeudi 02 juillet, de 14h à 15h30

THEMES

* Restitution des remarques Opérateurs sur les exigences SSI
* Nouvelle interface d'alimentation des BAL MSSanté de l'Annuaire Santé

MS Santé
Système de messageries sécurisées, données protégées.

MERCI DE VOTRE PRESENCE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ