



VERSION
0.1.0

PROJETS / SERVICES

Présentation générale des procédures d'inscription et d'authentification mises en œuvre par l'opérateur ASIP Santé pour l'application MSSanté pour terminaux mobiles

Mars 2015



Sommaire

1	Objet de la note.....	4
2	Présentation générale de l'application MSSanté mobilité	4
3	Présentation fonctionnelle.....	5
3.1	Cinématique d' enrôlement du terminal mobile	5
3.1.1	Ajout d'un appareil mobile via le portail web MSSanté	5
3.1.2	Photographier le QR Code d' enrôlement fourni par le portail Web MSSanté	6
3.1.3	Choix du mot de passe propre à ce terminal mobile	6
3.2	Cinématique d' authentification.....	7
3.2.1	Connexion à l' application mobile MSSanté par mot de passe.....	7
3.2.2	Accès aux services de l' application mobile MSSanté.....	7
4	Mise en œuvre technique	9
4.1	Principe de l' authentification mobile via un OTP push	9
4.2	Listes des écrans de l' application mobile	10
4.3	Démarrage de l' application	10
4.3.1	Cinématique.....	10
4.3.2	Ecran Splashscreen (EC001)	11
4.4	Enrôlement	12
4.4.1	Cinématique.....	12
4.4.2	Workflow de l' enrôlement.....	12
4.4.3	Ecran d' accueil Enrôlement (EC002)	13
4.4.4	Ecran Etape 1 enrôlement (EC003)	14
4.4.5	Ecran Flash du QR code (EC004)	15
4.4.6	Ecran choix du mot de passe mobilité (EC005).....	16
4.4.7	Ecran de fin d' enrôlement (EC006).....	17
4.4.8	Purge des QR Code périmés.....	17
4.5	Authentification.....	18
4.5.1	Cinématique.....	18
4.5.2	Workflow de l' authentification OTP	19
4.5.3	Ecran de connexion (EC007)	20
4.5.4	Ecran de choix de BAL (EC007').....	21
4.5.5	Reconnexion automatique.....	22
4.6	Services appelés	22
4.6.1	Service EnregistrerCanal	22
4.6.2	Service changeNotificationState	23
4.6.3	Service IDP AuthentifierOTP	23
4.6.4	Service IDP ValiderOTP	23
4.6.5	Batch PurgerQRCode	23

1 Objet de la note

Cette note présente les procédures d'enrôlement et d'authentification de l'application MSSanté mobilité mise en œuvre par l'opérateur ASIP Santé pour accéder à son service de messagerie sécurisée de santé via un terminal mobile.

Les terminaux mobiles ciblés sont les :

- smartphones et tablettes sous Android 4.0 et +
- smartphones et tablettes sous iOS 6.0 et +

2 Présentation générale de l'application MSSanté mobilité

L'application MSSanté mobilité de l'opérateur ASIP Santé a été développée en attachant une attention particulière à: **la sécurité** dans le respect des standards d'usage et la **facilité d'utilisation**.

L'authentification se fait dans le **respect du cadre réglementaire**. Une authentification à deux facteurs (le mot de passe saisi par le professionnel de santé et l'envoi d'un OTP Push sur le terminal mobile) a été mise en place.

Un enrôlement préalable du terminal mobile est nécessaire. Il est effectué une seule fois pour un terminal donné.

Les connexions ultérieures à l'application mobile MSSanté **se font par simple saisie du mot de passe** au lancement de l'application, l'OTP Push étant traité automatiquement par l'application.

Les fonctionnalités de l'application mobile MSSanté sont proches des messageries les plus courantes (Gmail, Apple...) :

- Réception / envoi de messages avec ou sans pièces jointes,
- Gestion des messages (répondre, faire suivre, déplacer dans des dossiers, marquer comme lu/non lu...),
- Synchronisation avec le serveur (vue identique des messages entre l'application mobile et le Webmail),
- Notification en cas de réception d'un nouveau message.

Une fonction spécifique permet de rechercher des professionnels de santé dans l'annuaire national MSSanté.

En cas de perte du terminal mobile, il est possible de le bloquer depuis le portail Web MSSanté.

3 Présentation fonctionnelle

3.1 Cinématique d' enrôlement du terminal mobile

Prérequis : le professionnel de santé a préalablement créé son compte MSSanté et téléchargé l'application mobile MSSanté sur son terminal mobile.

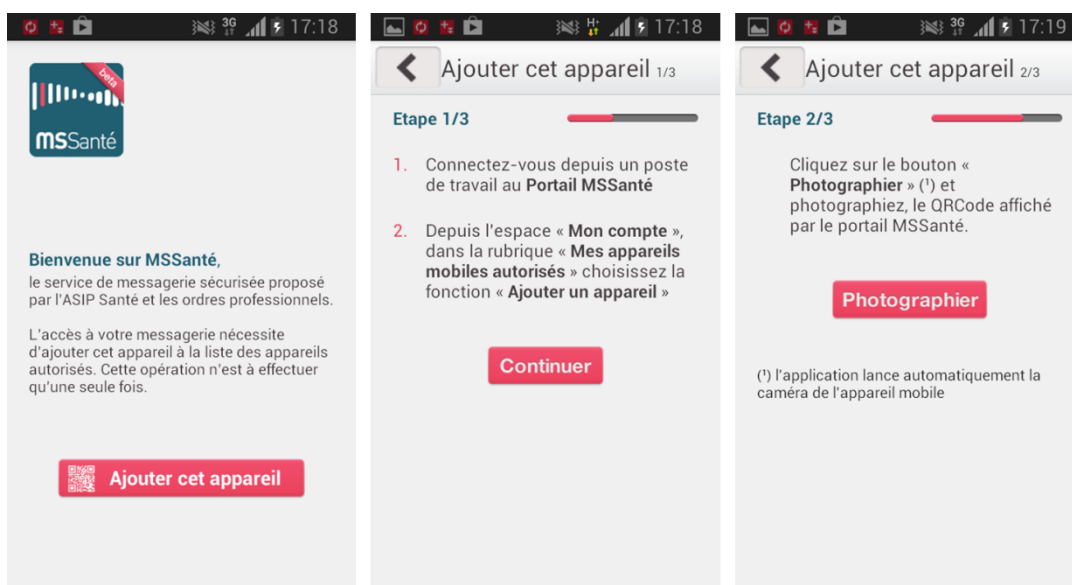
L' enrôlement d' un terminal mobile se déroule en 3 étapes :

1. Sur le portail Web MSSanté, initier l' action d' ajout d' un terminal mobile : un QR code d' enrôlement est alors généré par le portail ;
2. Avec le terminal mobile, photographier le QR Code affiché sur le portail Web MSSanté ;
3. Sur le terminal mobile, saisir le mot de passe propre à ce terminal qui sera utilisé pour la connexion à MSSanté.

3.1.1 Ajout d' un appareil mobile via le portail web MSSanté

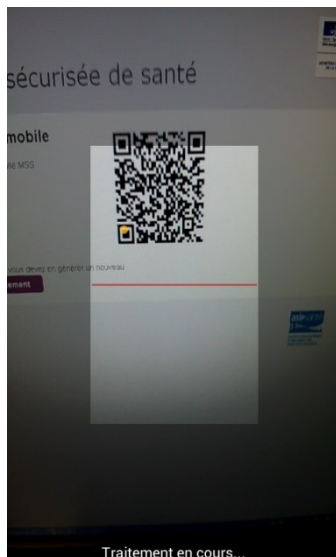
Le professionnel de santé doit se connecter depuis un poste de travail sur le portail Web MSSanté, s' authentifier en utilisant sa carte CPS ou par OTP, puis cliquer sur « Ajouter un appareil mobile ».

Cette étape est décrite lors du premier lancement de l' application mobile sur le terminal mobile (voir les captures d' écrans ci-dessous).



3.1.2 Photographier le QR Code d' enrôlement fourni par le portail Web MSSanté

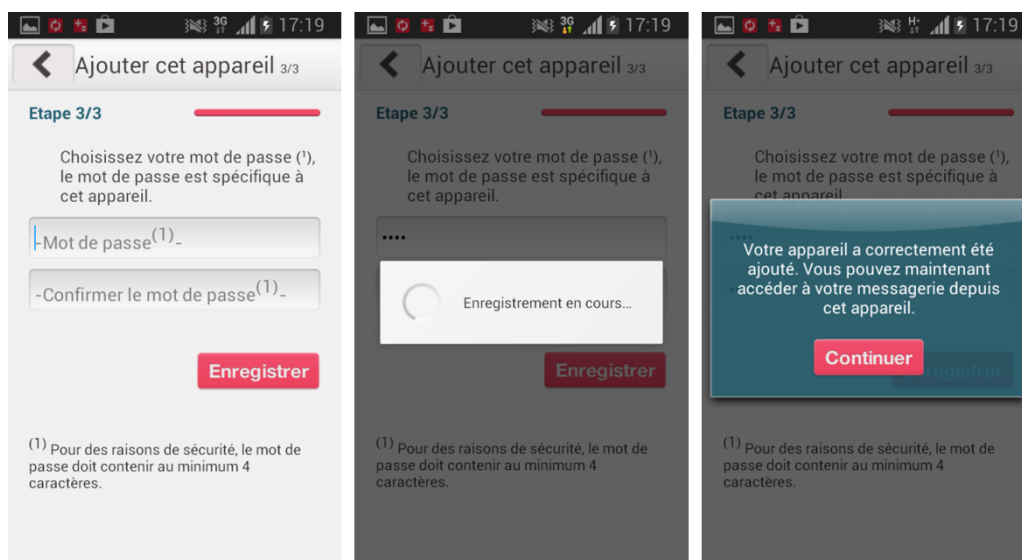
Avec son terminal mobile, à partir de l'application mobile MSSanté, le professionnel de santé doit photographier le QR-Code d' enrôlement affiché sur le portail Web MSSanté.



3.1.3 Choix du mot de passe propre à ce terminal mobile

Sur le terminal mobile, l'utilisateur doit saisir le mot de passe propre à ce terminal qui sera utilisé pour la connexion à MSSanté.

Ce mot de passe sera utilisé lors des futures authentifications à l'application mobile MSSanté.



A la fin de cette étape, le terminal mobile du professionnel de santé est enrôlé.

3.2 Cinématique d'authentification

Prérequis : le professionnel de santé a préalablement réalisé l'enrôlement de son terminal mobile.

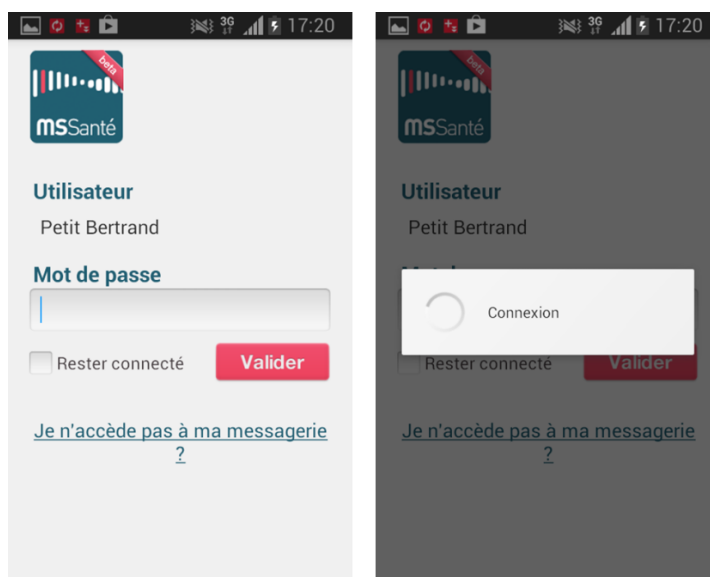
L'authentification du professionnel de santé pour accéder à l'application mobile MSSanté se déroule en 2 étapes :

1. Sur le terminal mobile, lancer l'application mobile MSSanté,
2. Saisir le mot de passe propre à ce terminal.

Un OTP (cf. [Principe de l'authentification mobile via un OTP push](#)) est échangé entre le système MSSanté et le terminal mobile du professionnel de santé pour finaliser l'authentification. Cette opération est transparente pour le professionnel de santé.

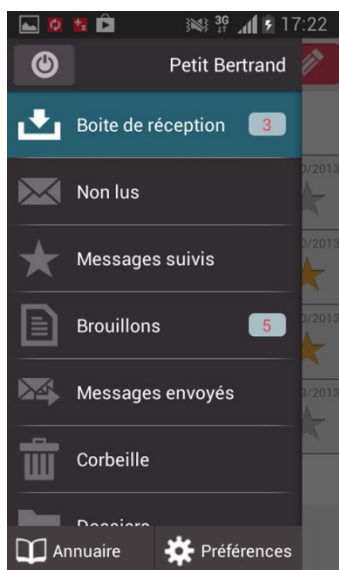
3.2.1 Connexion à l'application mobile MSSanté par mot de passe

Les connexions à l'application mobile se font par simple saisie du mot de passe (préalablement enregistré) au lancement de l'application.



3.2.2 Accès aux services de l'application mobile MSSanté

Une fois le professionnel de santé authentifié, il peut accéder directement à sa messagerie sécurisée avec les fonctionnalités courantes des messageries actuelles.



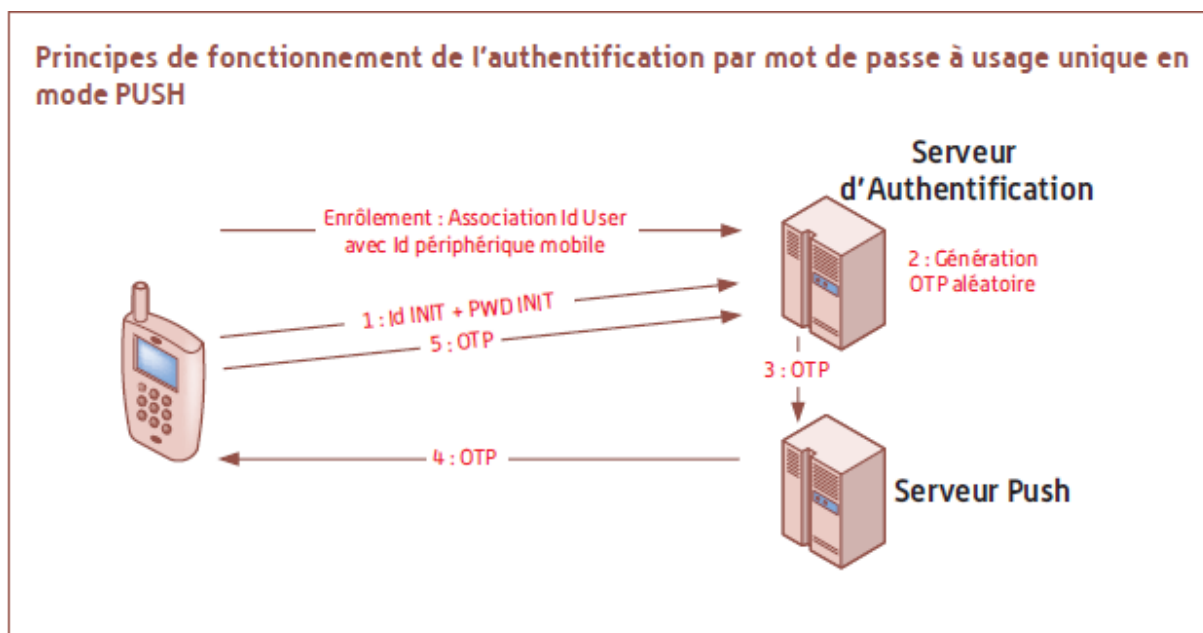
4 Mise en œuvre technique

4.1 Principe de l'authentification mobile via un OTP push

En environnement de mobilité, le mot de passe à usage unique peut être transmis en mode « Push » : après authentification de la personne, l'OTP est envoyé vers le terminal mobile depuis le système d'authentification par un canal dédié et intercepté par l'application mobile, qui renvoie ce mot de passe pour finaliser l'authentification.

Ce système repose sur l'usage des plateformes de Push mises à disposition par les éditeurs des principaux OS mobiles (Google, Apple, Microsoft).

L'enrôlement du terminal mobile de l'utilisateur est possible par scan d'un QR Code avec l'appareil photo du terminal.



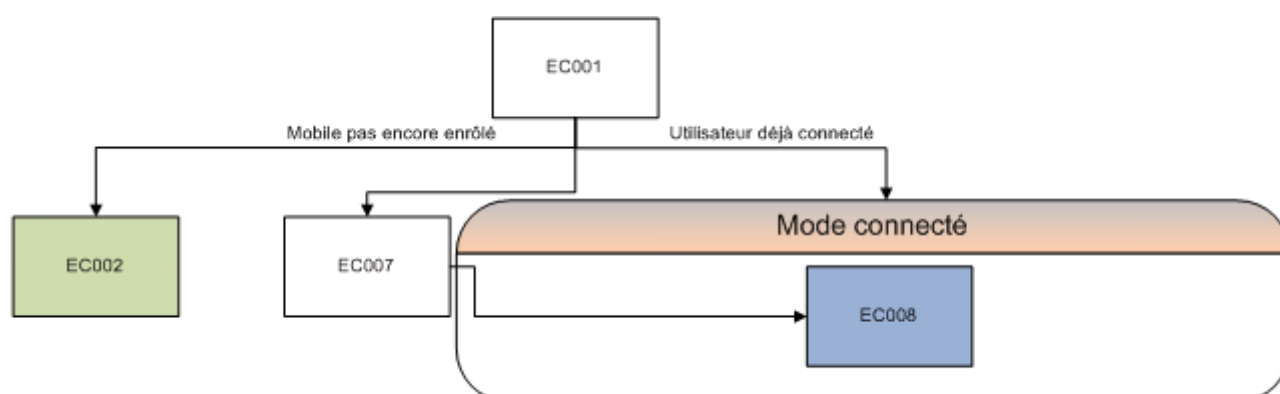
Ce principe est décrit dans le Référentiel d'authentification des acteurs de santé issu de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) publiée par l'ASIP Santé.

4.2 Listes des écrans de l'application mobile

Ecran	Description
EC001	Ecran Splashscreen
EC002	Ecran d'accueil enrôlement
EC003	Ecran étape 1 enrôlement
EC004	Ecran flash du QR Code
EC005	Ecran choix du mot de passe mobilité
EC006	Ecran fin d'enrôlement
EC007	Ecran de connexion
EC007'	Ecran de sélection de BAL
EC008	Ecran de consultation de la boîte de réception

4.3 Démarrage de l'application

4.3.1 Cinématique



4.3.2 Ecran Splashscreen (EC001)

4.3.2.1 Description



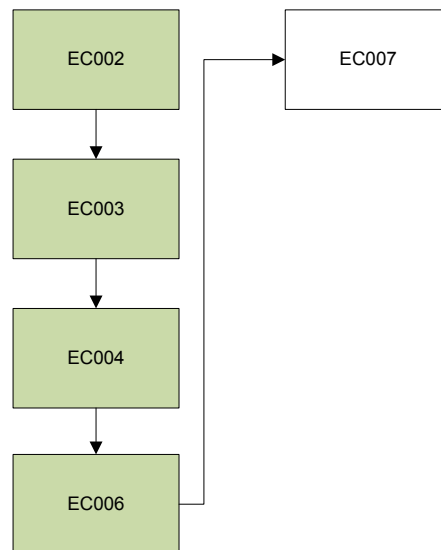
4.3.2.2 Action

Cet écran permet d'effectuer la redirection vers la page d'accueil de l'utilisateur :

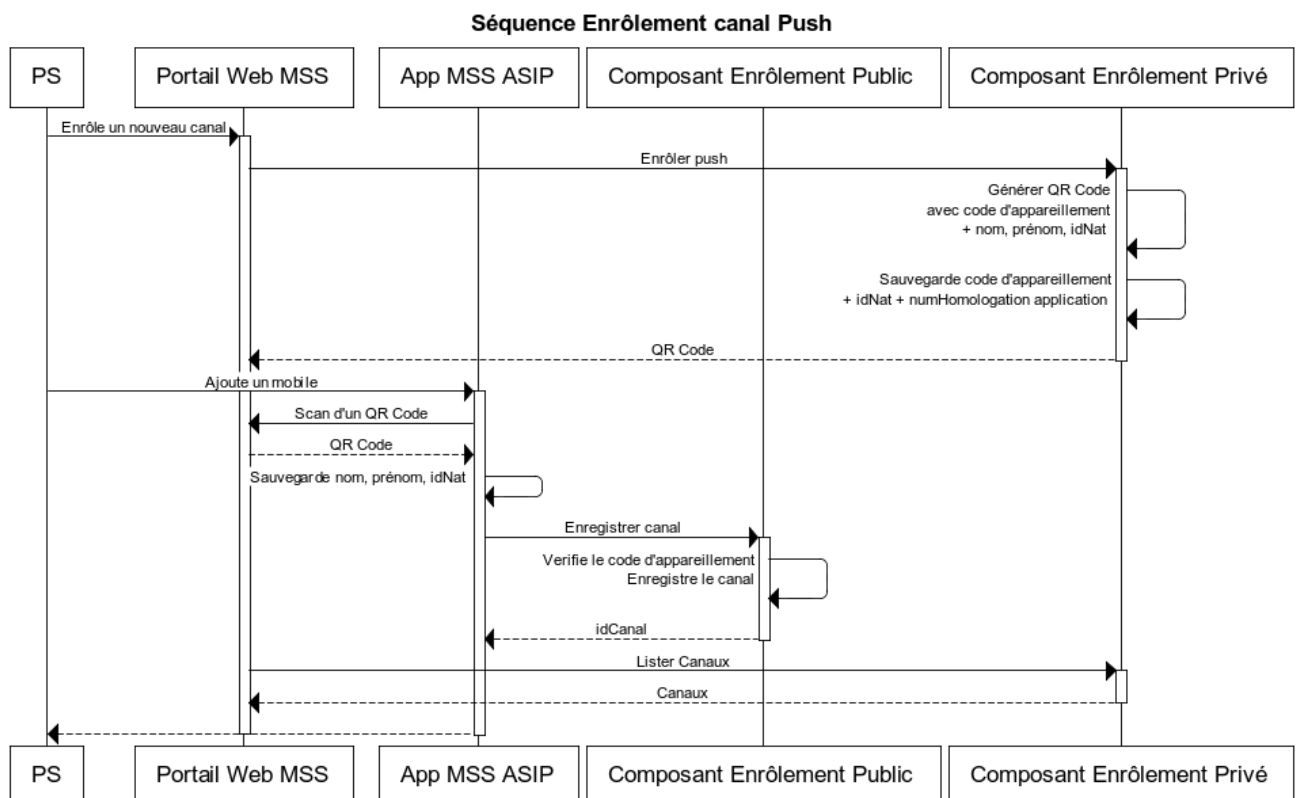
- [Ecran d'accueil Enrôlement \(EC002\)](#) si le mobile n'est pas encore enrôlé,
- [Ecran de connexion \(EC007\)](#) si le mobile est enrôlé et que l'utilisateur n'est pas encore connecté,
 - Ecran de consultation de la boîte de réception (EC008) si l'application est en mode redémarrage (c'est-à-dire que l'application a été killée et qu'on l'a redémarrée).
 - Dernier écran visualisé sinon

4.4 Enrôlement

4.4.1 Cinématique



4.4.2 Workflow de l'enrôlement



4.4.3 Ecran d'accueil Enrôlement (EC002)

4.4.3.1 Description



Cet écran est l'écran d'accueil dans le cas où le mobile n'a jamais été enrôlé depuis la dernière installation de l'application.

4.4.3.2 Action

Le clic sur « Ajouter cet appareil » redirige vers l'[Ecran Etape 1 enrôlement \(EC003\)](#).

4.4.4 Ecran Etape 1 enrôlement (EC003)


4.4.4.1 Description



Cet écran est accessible à partir de :

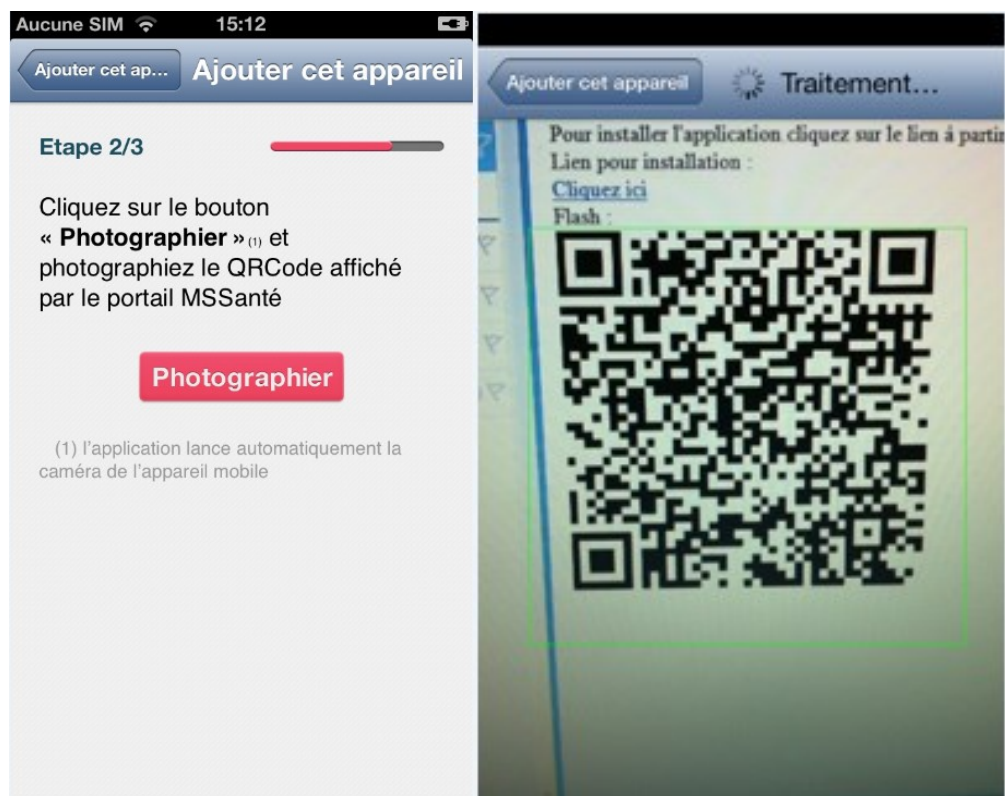
- L'[Ecran d'accueil Enrôlement \(EC002\)](#) en cliquant sur le bouton « Ajouter cet appareil »,
- L'[Ecran de connexion \(EC007\)](#) en cliquant sur le lien « Je n'accède pas à mon compte ? ».

4.4.4.2 Champs

Champ	Description et RG
	Redirection vers : <ul style="list-style-type: none">• Ecran d'accueil Enrôlement (EC002) lors du premier enrôlement• Ecran de connexion (EC007) si on vient de l'écran d'authentification (cas du mot de passe oublié)
Bouton « Continuer »	Redirection vers l' Ecran Flash du QR code (EC004)


4.4.5 Ecran Flash du QR code (EC004)

4.4.5.1 Description



Cet écran est accessible à partir de l'[Ecran Etape 1 enrôlement \(EC003\)](#) suite au clic sur le bouton « Continuer ».

4.4.5.2 Champs

Champ	Description et RG
	Redirection vers l' Ecran Etape 1 enrôlement (EC003)
Bouton « Photographier »	Affichage de l'écran de scan
Bouton « Ajouter cet appareil »	Redirection vers l' Ecran Flash du QR code (EC004)
	Dès que le scan est terminé, la redirection s'effectue automatiquement vers l' Ecran choix du mot de passe mobilité (EC005)

4.4.5.3 Action

4.4.5.3.1 Service scan

- Récupération du code d'appariement, de la date de création du QR code, du nom, du prénom et de l'idNat.
 - Si le QR Code est malformé ou ne contient pas les données nécessaires un message d'erreur est affiché
- Affichage de l'[Ecran choix du mot de passe mobilité \(EC005\)](#).

4.4.6 Ecran choix du mot de passe mobilité (EC005)

4.4.6.1 Description

Retour Ajouter cet appareil

Etape 3/3

Choisissez votre mot de passe ⁽¹⁾, le mot de passe est spécifique à cet appareil.

-Mot de passe(1)-

-Confirmez le mot de passe(1)-

Enregistrer

⁽¹⁾ Le mot de passe doit contenir au minimum 4 caractères.

Cet écran est accessible à partir de l'[Ecran Flash du QR code \(EC004\)](#) suite au scan du QR Code.

4.4.6.2 Champs

Champ	Type	Obligatoire	Description et RG	Message d'erreur
Mot de passe	Alphanumérique	X	4 caractères minimum 255 caractères maximum Au moins une lettre et un chiffre	Mot de passe invalide
Confirmez le mot de passe	Alphanumérique	X	Doit avoir la même valeur que le mot de passe. Au moins une lettre et un chiffre	Mot de passe invalide

4.4.6.3 Action

Le clic sur le bouton « Enregistrer » permet d'envoyer les informations d' enrôlement.

4.4.6.3.1 Service enroler

1. Si le mobile est non connecté, affichage du message : « Connexion impossible »
2. Récupération des informations contenues dans le QR Code (code appairèlement, nom, prénom, idNat et date de création du QR code) et du mot de passe.
3. Appel du [Service EnregistrerCanal](#)
4. Affichage de l'[Ecran de fin d' enrôlement \(EC006\)](#).

4.4.7 Ecran de fin d'enrôlement (EC006)

4.4.7.1 Description



Cet écran est accessible à partir de l'[Ecran choix du mot de passe mobilité \(EC005\)](#) suite à l'enregistrement du mot de passe.

4.4.7.2 Action

Le clic sur le bouton « Continuer » redirige vers l'[Ecran de connexion \(EC007\)](#).

4.4.8 Purge des QR Code périmés

4.4.8.1 Description

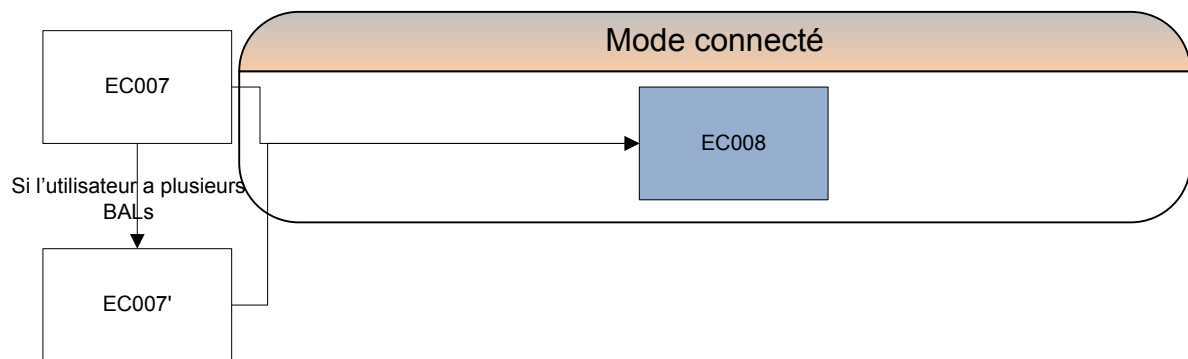
Les QR Code périmés, c'est-à-dire générés sur la passerelle d'authentification à partir du portail Web mais non scannés et utilisés par l'application mobile pendant plus de 2 minutes doivent être purgés.

4.4.8.2 Action

[Batch PurgerQRCode](#) de la passerelle d'authentification.

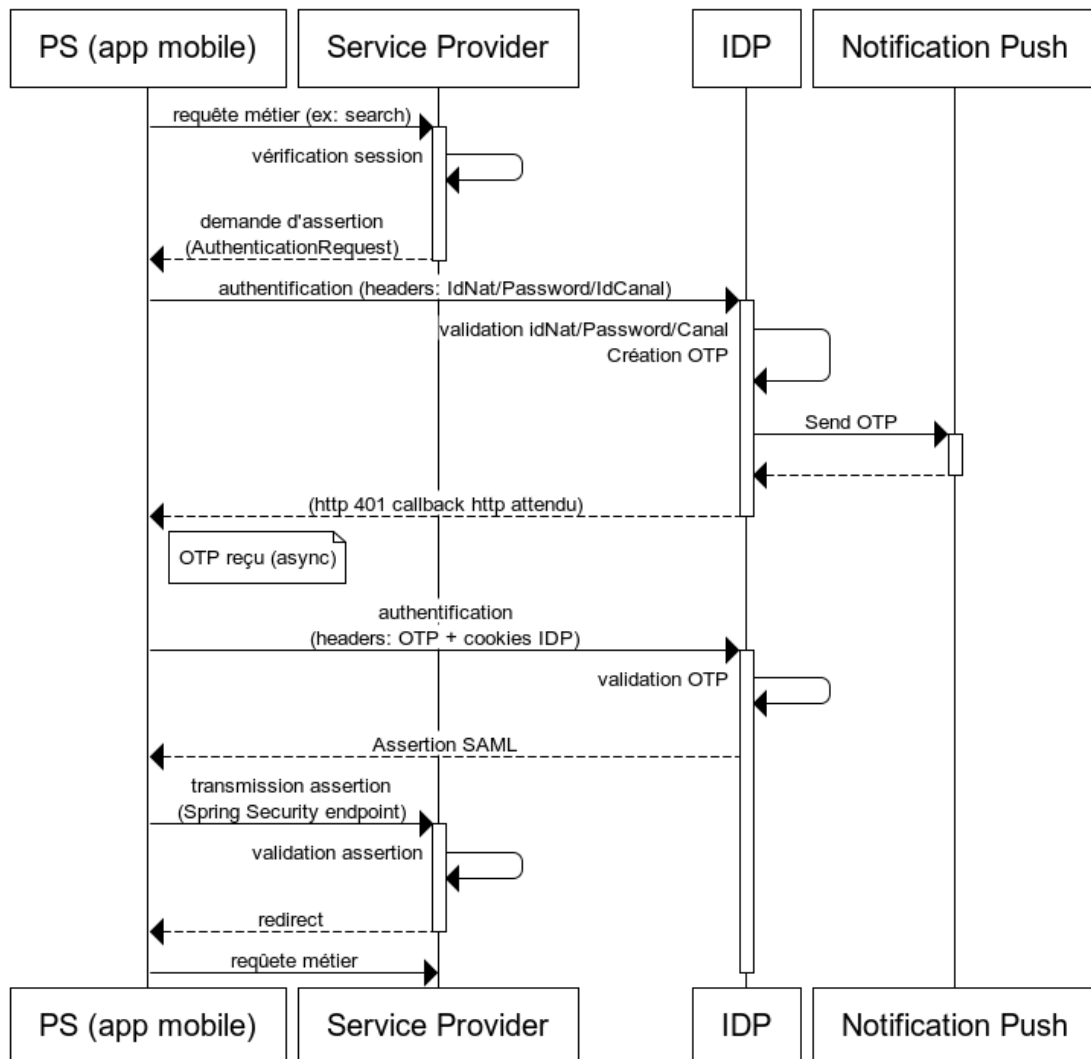
4.5 Authentification

4.5.1 Cinématique



4.5.2 Workflow de l'authentification OTP

Séquence Authentification OTP Push



4.5.3 Ecran de connexion (EC007)


4.5.3.1 Description



Cet écran s'affiche :

- Comme page d'accueil lorsque le mobile est enrôlé et qu'aucun utilisateur n'est connecté,
- A la fin de l'enrôlement.

4.5.3.2 Champs

Champ	Type	Obligatoire	Description et RG
Utilisateur	Label		Nom Prénom de l'utilisateur enrôlé sur cet appareil
Mot de passe	Alphanumérique	X	4 caractères min et 255 caractères max
Valider	Bouton		Si l'utilisateur est en mode connecté : appel au Service d'authentification Sinon, appel au Service d'authentification locale
Je n'accède pas à mon compte ?	Lien		Redirige vers l' Ecran Etape 1 enrôlement (EC003) suite à l'affichage du message de confirmation suivant : 

4.5.3.3 Action

4.5.3.3.1 Service d'authentification

1. Vérification que les champs obligatoires sont renseignés
2. Si l'OTP Push a changé afficher le message « Veuillez-vous enrôler de nouveau »

3. Si le compte est bloqué (date de blocage du compte supérieur à J-X minutes) : affichage du message « Compte bloqué »
4. Appel au service de la passerelle d'authentification-IDP [Service IDP AuthentifierOTP](#)
5. Le mobile intercepte la notification push OTP
 - a. Si pas de notification au bout de X secondes : affichage du message « Authentification impossible, veuillez réessayer »
6. Appel au service de la passerelle d'authentification-IDP [Service IDP ValiderOTP](#)
7. Rapatriement des messages
8. Redirection vers l'Ecran de consultation de la boite de réception (EC008)

Dans les cas d'erreurs lors de l'appel au [Service IDP AuthentifierOTP](#), on incrémente le nombre d'erreur de connexion pour gérer le blocage de compte.

4.5.3.3.2 Service d'authentification locale

1. Vérification que les champs obligatoires sont renseignés
2. Vérification que l'utilisateur s'est au moins connecté une fois et a rapatrié les messages, sinon affichage du message « Connexion impossible »
3. Si le compte est bloqué (date de blocage du compte supérieur à J-X minutes) : affichage du message « Compte bloqué »
4. Vérification de la validité du mot de passe.
 - a. Si le mot de passe est invalide : affichage du message « Les informations de connexion sont invalides » et incrémentation du compteur du nombre d'erreurs de connexion (pour la gestion du blocage de compte)
 - b. Si le mot de passe est correct : redirection vers l'Ecran de consultation de la boite de réception (EC008)

4.5.4 Ecran de choix de BAL (EC007')

4.5.4.1 Description



Cet écran s'affiche suite à la première connexion si l'utilisateur a plusieurs emails.

4.5.4.2 Champs

Champ	Type	Obligatoire	Description et RG
Liste des BAL	Radio bouton	X	Liste des emails de l'utilisateur

Valider	Bouton		Enregistrement de la BAL dans la BDD du mobile, on appelle le service Service changeNotificationState de la passerelle d'authentification pour créer la notification associée puis rapatriement des messages et redirection vers l'Ecran de consultation de la boîte de réception (EC008)
---------	--------	--	---

4.5.5 Reconnexion automatique

4.5.5.1 Description

La session utilisateur a une durée de vie :

- de X minutes d'inactivité,
- de X heures en activité.

L'utilisateur est redirigé vers l'[Ecran de connexion \(EC007\)](#).

4.5.5.2 Action

4.5.5.2.1 Service reconnexion

1. Si l'OTP Push a changé : afficher le message « Veuillez-vous enrôler de nouveau »
2. Si l'utilisateur a accès à une connexion internet
 - a. Appel au service de la passerelle d'authentification-IDP Service IDP AuthentifierOTP
Si une erreur est remontée, redirection vers l'[Ecran de connexion \(EC007\)](#).
 - b. Le mobile intercepte la notification push OTP
 - i. Si pas de notification au bout de 30 secondes : affichage du message « Authentification impossible » et redirection vers l'[Ecran de connexion \(EC007\)](#).
 - c. Appel au service de la passerelle d'authentification-IDP [Service IDP ValiderOTP](#)
 - i. Si erreur redirection vers l'[Ecran de connexion \(EC007\)](#).
3. Si l'utilisateur n'a pas accès à une connexion internet
 - a. Vérification de la validité du mot de passe dans la BDD du mobile (on reste en mode déconnecté)

4.6 Services appelés

4.6.1 Service EnregistrerCanal

4.6.1.1 Objectif

- Valider un code d'appareillement
- Terminer le processus d'enrôlement
- Enregistrer un canal d'authentification Push pour un utilisateur et une application
- Associer un mot de passe spécifique à ce canal Push

4.6.1.2 Algorithme

1. Contrôle du format des champs en entrée du service
2. vérifie le code de service
3. Vérifie le numéro d'homologation
4. Vérifie que le code d'appareillement n'a pas expiré (durée de validité X minutes)
 - a. Si le code d'appareillement n'est plus valide le service renvoie une erreur

5. Confronte le code d'appareillement et l'application qui demande l'enregistrement aux codes d'appareillement émis et aux applications pour lesquelles ils ont été générés
 - a. Si le code d'appareillement n'est pas trouvé dans les codes émis le service répond une erreur
 - b. Si les applications ne correspondent pas le service répond une erreur
6. Vérifie la validité du mot de passe à associer au canal Push
 - a. Si le format du mot de passe est invalide le service répond une erreur
7. Recherche de l'utilisateur en fonction de l'idNat (qui se trouve dans le code d'appareillement) : si celui-ci n'existe pas, on le crée en base
8. Recherche le canal en base :
 - a. Si le canal existe, on le met à jour avec le bon mot de passe et on supprime les notifications associées
 - b. Si le canal n'existe pas, on le crée en base

4.6.2 Service changeNotificationState

4.6.2.1 Objectif

- Permet d'activer/désactiver de façon logicielle l'envoi des push notification vers un mobile lors de l'arrivée d'un nouveau message.

4.6.2.2 Algorithme

- Vérification des champs en entrée du service
- Recherche du canal à partir de l'idPush
- Recherche de la notification à partir de l'adresse de messagerie et de l'idCanal
 - Si pas de notification, on la crée
 - Si la notification existe, on la met à jour

4.6.3 Service IDP AuthentifierOTP

4.6.3.1 Objectif

- Initialisation de la phase de connexion avec OpenAM, qui déclenche l'envoi de l'OTP push.

4.6.4 Service IDP ValiderOTP

4.6.4.1 Objectif

- Clos la phase de dialogue avec OpenAM et valide l'OTP envoyé.

4.6.5 Batch PurgerQRCode

4.6.5.1 Objectif

- Purger la passerelle d'authentification des codes d'appareillement émis dont la date de validité a été dépassée

4.6.5.2 Algorithme

1. Supprime tous les codes émis dont la date de validité est dépassée



Pour en savoir plus :

Le site internet : <https://www.mssante.fr>

Le service clients de l'ASIP Santé :

0 825 852 000 Service 0,06 € / min
+ prix appel

24/24 Heures - 7/7 Jours