Référentiel d'authentification des acteurs de santé

Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) - Décembre 2014 – V2.0

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES
D'INFORMATION
PARTAGÉS DE SANTÉ

Le présent document a été élaboré dans le cadre d'un processus collaboratif avec les principaux acteurs du secteur (institutionnels, utilisateurs et industriels) et le grand public.

La Délégation à la Stratégie des Systèmes d'Information de Santé (DSSIS) et l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) remercient l'ensemble des personnes et organisations qui ont apporté leur contribution à son élaboration et à sa relecture.

SOMMAIRE

SOMMAIRE 3

1. OBJET DU DOCUMENT 5

2. PÉRIMÈTRE D'APPLICATION DU RÉFÉRENTIEL 7

3. ENJEUX DE L'AUTHENTIFICATION DES ACTEURS DE SANTÉ 8

4. DÉFINITION DE L'AUTHENTIFICATION DES ACTEURS 9

4.1. Authentification

4.2. Acteur de santé

4.3. Portée d'un identifiant

4.4. Facteur d'authentification

4.5. Niveau d'authentification

4.6. Authentification directe

4.7. Architectures d'authentification (indirecte ou par délégation)

5. PALIERS DE L'AUTHENTIFICATION DES ACTEURS DE SANTÉ 12

5.1. Paliers de l'authentification « publique » des acteurs de santé

5.1.1. Palier 2 de l'authentification publique

5.1.2. Palier 3 de l'authentification publique

5.2. Paliers de l'authentification « privée » des acteurs de santé

5.2.1. Palier 1 de l'authentification privée

5.2.2. Palier 2 de l'authentification privée

5.2.3. Palier 3 de l'authentification privée

5.2.4. Socle commun de règles à respecter pour la mise en place de l'authentification « privée »

6. SYNTHÈSE DES DISPOSITIFS D'AUTHENTIFICATION 18

7. OFFRE INDUSTRIELLE 19

8. IMPACT SUR LES PRATIQUES PROFESSIONNELLES 20

ANNEXES 21

ANNEXE 1 - Présentation et conditions d'emploi des dispositifs d'authentification

A.1. Dispositifs d'authentification par carte CPS

A.2. Dispositifs d'authentification par certificat logiciel de personne morale

A.3. Dispositifs d'authentification par certificat logiciel de personne physique

A.4. Dispositifs d'authentification par OTP

ANNEXE 2 - Glossaire

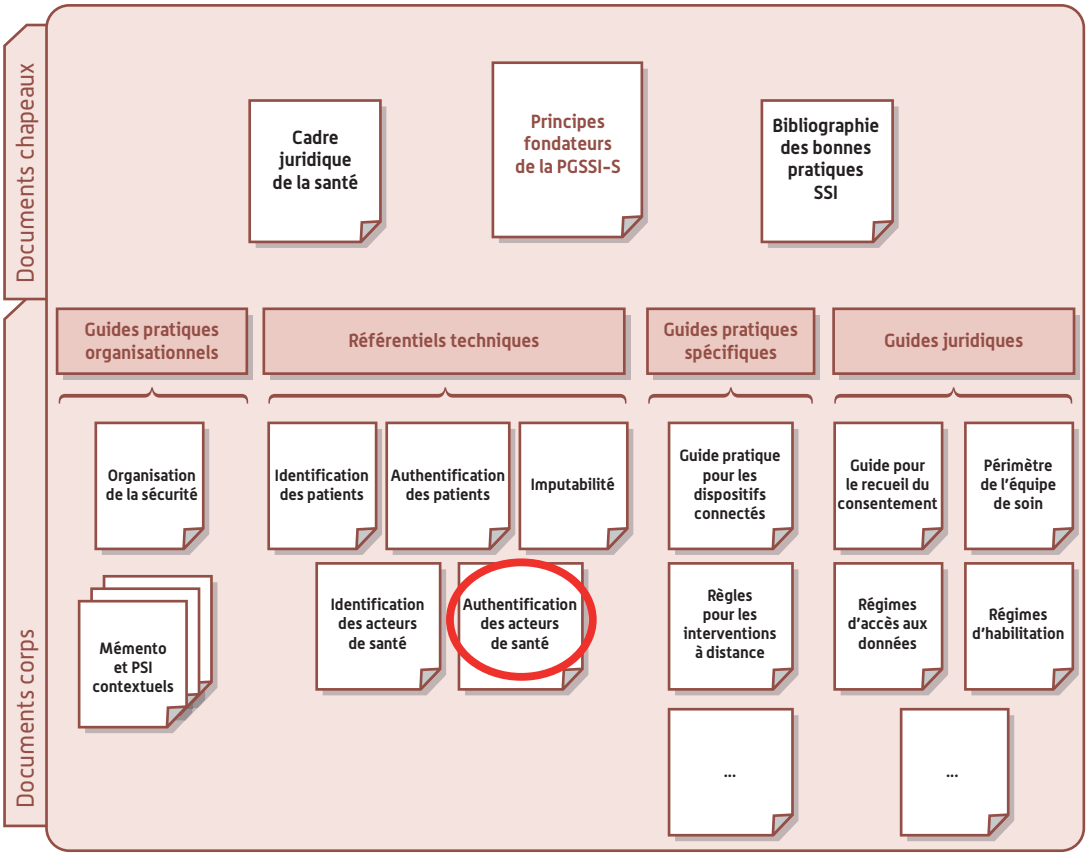
ANNEXE 3 – Documents de référence

1. OBJET DU DOCUMENT

Le présent document constitue le référentiel d'authentification des acteurs de santé de la Politique Générale de Sécurité des Systèmes d'Information de Santé.

Il fait partie des référentiels thématiques techniques de la PGSSI-S (cf. schéma ci-après).

FIGURE 1 : ORGANISATION DU CORPUS DOCUMENTAIRE DE LA PGSSI-S



Le présent référentiel définit l'ensemble des dispositifs utilisables pour authentifier un acteur de santé, personne physique ou morale, vis-à-vis d'un Système d'Information de Santé (SIS).
Les enjeux de l'authentification sont détaillés dans les documents de référence nº 2 et 4.

Cette fonction de sécurité concerne les acteurs de santé, personnes physiques ou personnes morales définis dans le référentiel d'identification des acteurs sanitaires et médico-sociaux (document de référence nº 1).

Deux périmètres sont distingués pour la mise en place de la fonction d'authentification d'un acteur :

- **Authentification « publique »** : l'authentification est dite publique lorsque les dispositifs d'authentification utilisés sont associés à des identifiants de portée nationale (ou identifiants publics)[1] et que leur utilisation n'est pas limitée à des systèmes d'information spécifiquement identifiés. Ces dispositifs sont définis dans le présent référentiel.
- **Authentification « privée »** : l'authentification est dite privée lorsque les dispositifs d'authentification utilisés sont diffusés pour une utilisation limitée à des systèmes d'information spécifiquement identifiés. Ils sont choisis par le responsable de traitement sur la base d'une analyse de risques. Ils peuvent être associés à des identifiants de portée nationale ou locale.

Ce document s'adresse aux responsables de traitement qui doivent définir ou choisir les dispositifs d'authentification acceptables et leurs conditions d'emploi ainsi qu'aux personnes agissant sous

1. Tels que définis dans le référentiel d'identification des acteurs sanitaires et médico-sociaux (Référence nº 1).

leur responsabilité et impliquées dans la mise en œuvre de la politique de sécurité de systèmes d'information de santé.

Il s'adresse aussi aux fournisseurs de produits ou de services utilisés dans le cadre de systèmes de santé. En effet, ces fournisseurs doivent offrir des solutions qui mettent en œuvre les dispositifs identifiés dans le présent référentiel et respectent leurs conditions d'emploi définies.

2. PÉRIMÈTRE D'APPLICATION DU RÉFÉRENTIEL

Le cartouche ci-après présente de manière synthétique le périmètre d'application du référentiel d'authentification des acteurs.

Santé						Médico Social
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Veille sanitaire	Etudes et recherche	Dépistage et prévention	
✓	✓	✓				
Commentaire						
La présente version du référentiel est applicable dans le cadre des usages santé ci-dessus. Le périmètre d'application sera élargi dans une version ultérieure du référentiel. Le mode d'exercice des acteurs ou encore le cycle de vie de la donnée n'ont pas d'incidence sur l'applicabilité des moyens définis.						

3. ENJEUX DE L'AUTHENTIFICATION DES ACTEURS DE SANTÉ

Le développement des services d'e-santé et la dématérialisation des services médico-sociaux ne pourront devenir effectifs que dans la mesure où les conditions requises pour créer et maintenir la confiance des acteurs sont atteintes.

La qualité de l'authentification des acteurs de santé constitue l'un des piliers de cette confiance.

L'authentification d'un acteur est la propriété sur laquelle s'appuient les fonctions de sécurité permettant :

- d'accorder un accès au système aux seules personnes autorisées ;
- de différencier les possibilités d'accès aux services et aux données de santé en fonction des droits attachés à l'identité de ces utilisateurs ;
- de pouvoir imputer les actions à leur auteur ;
- la qualité de l'authentification d'un acteur de santé conditionne donc la maitrise des accès au SIS (SI de Santé).

4. DÉFINITION DE L'AUTHENTIFICATION DES ACTEURS

4.1. Authentification

Le Référentiel Général de Sécurité (RGS) définit l'authentification dans les termes suivants : *« L'authentification a pour but de vérifier l'identité dont se réclame une personne ou une machine (S'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifier consiste à apporter la preuve de cette identité. L'authentification est généralement précédée d'une identification)*[2] *».*

Le niveau de sécurité d'une fonction d'authentification est lié :
- au niveau de l'identifiant utilisé et de son processus d'attribution (assurance que l'identité préalablement enregistrée correspond à l'entité enregistrée et à elle seule) ;
- au niveau du dispositif d'authentification, de ses conditions d'attribution ainsi que de ses conditions d'emploi (assurance que le moyen d'authentification est utilisé par l'entité enregistrée).

Dans le cadre du présent référentiel, l'authentification porte sur des personnes physiques ou des personnes morales ; le terme « personne » est donc utilisé pour désigner une entité objet d'une opération d'authentification.

4.2. Acteur de santé

Dans le cadre de la PGSSI-S, un acteur de santé est une personne physique ou morale participant directement ou indirectement à la prise en charge médicale d'un patient.

4.3. Portée d'un identifiant

L'identifiant utilisé dans le cadre d'une authentification peut avoir une portée locale ou nationale[3]. Pour mémoire, les identifiants de portée nationale (ou identifiants publics), sont attribués lors de l'enregistrement dans un référentiel d'identité national (RPPS, ADELI, FINESS, SIRET/SIREN, …).

4.4. Facteur d'authentification

En pratique, la preuve de l'identité présentée lors d'une opération d'authentification peut être basée sur un ou plusieurs des facteurs d'authentification suivants :
- ce que la personne sait (ex. mot de passe) ;
- ce que la personne possède (ex. carte à puce, certificat électronique, token OTP, carte OTP, téléphone, tablette, boite aux lettres de messagerie, etc.) ;
- ce que la personne est (ex. caractéristique physique de type biométrie) ;
- ce que la personne sait faire (ex. biométrie comportementale telle que la signature manuscrite ou la manière de taper sur un clavier d'ordinateur aussi appelée « frappologie »)[4].

Plus le nombre de facteurs utilisés lors d'une opération d'authentification est grand, plus l'authentification est considérée comme fiable (cf. section 4.5 « Niveau d'authentification »).

2. (§3.2.a.1 du document « Référentiel Général de Sécurité » version 2.00).
3. Tel que défini dans le référentiel d'identification des acteurs sanitaires et médico-sociaux (Référence n° 1).
4. Ce facteur est généralement encore au stade expérimental et il existe pour l'instant peu de solutions d'authentification robustes qui s'appuient fortement sur ce facteur.

4.5. Niveau d'authentification

On distingue deux niveaux d'authentification :

- **l'authentification simple** lorsque celle-ci ne repose que sur un seul facteur (exemple : l'utilisateur indique son mot de passe) ;
- **l'authentification forte** lorsque plusieurs facteurs différents sont combinés (par exemple, ce que je sais et ce que je possède : mot de passe saisi sur un terminal lui-même authentifié et enregistré comme appartenant à la personne authentifiée).

Les facteurs d'authentification sont associés à une personne physique ou morale. En cas d'authentification forte, les différents facteurs utilisés doivent être associés à la même personne (physique ou morale).

4.6. Authentification directe

Une authentification de personnes physique est dite directe lorsque la personne physique accède au système d'information intuitu personae, sous sa propre responsabilité, en utilisant directement son dispositif d'authentification sur le système d'information (ex. utilisation d'un couple identifiant/mot de passe pour accéder à un récapitulatif de commande sur un site internet).

4.7. Architectures d'authentification (indirecte ou par délégation)

Lorsque l'authentification directe n'est pas envisageable, il est possible de mettre en œuvre des architectures d'authentification alternatives dans lesquelles la fonction d'authentification de la personne physique est confiée à une personne morale tierce.

Deux architectures d'authentification sont définies :

- l'**authentification indirecte**, quand une personne physique accède au système d'information de santé cible[5] au travers d'un autre système d'information opéré par une personne morale qui définit elle-même les modalités d'authentification de la personne physique.

  C'est, par exemple, le cas d'un établissement de soin qui authentifie localement ses utilisateurs en prenant la responsabilité de cette authentification et s'authentifie lui-même auprès du SI cible via son certificat de Personne Morale.

  La personne morale est alors responsable de s'assurer de l'identité de cet accédant et propage au système de santé cette identification/authentification après s'être elle-même authentifiée de manière appropriée auprès du système cible.

  L'authentification indirecte correspond donc à la combinaison d'une authentification « publique » de la personne morale (certificat logiciel[6] de personne morale suivant les conditions d'emploi présentées en annexe) et d'une authentification « privée » d'une personne physique acteur de santé (par exemple par identifiant / mot de passe, par biométrie ou par dispositif d'authentification de portée nationale comme les cartes CPS).

  La personne morale est également responsable de gérer l'identification de cet acteur authentifié localement, ainsi que les éventuelles évolutions dans le temps de l'identifiant (aussi appelée gestion diachronique). La durée de conservation des éléments sur lesquels repose cette gestion

5. Système d'information auquel la personne physique veut obtenir accès après authentification.
6. Certificat électronique stocké dans un système logiciel (navigateur, application, système d'exploitation…), par opposition à un certificat électronique confiné dans un dispositif matériel (microcircuit de carte à puce ou de clé USB, …).

est à déterminer par le responsable du traitement en fonction de la finalité et de l'analyse de risques du traitement.

L'authentification indirecte ne peut pas être utilisée pour confier l'authentification d'une personne morale à une autre personne morale.

- **l'authentification par délégation**, quand une personne physique accède au système d'information de santé cible[7] au travers d'un autre système d'information opéré par une personne morale qui met en œuvre les dispositifs d'authentification « publique » que le système d'information cible met en œuvre dans le cadre de l'authentification directe.

  C'est, par exemple, le cas d'un fournisseur offrant un service à valeur ajoutée dont l'une des composantes est l'authentification directe du client sur ses propres machines et la prise en charge de l'authentification sur le système cible, permettant ainsi d'éviter l'installation de composants lourds sur le poste de travail de ses clients.

  L'authentification par délégation correspond donc à la combinaison d'une authentification « publique » de la personne morale (certificat logiciel de personne morale suivant les conditions d'emploi présentées en annexe) et d'une authentification « publique » d'un acteur de santé (personne physique).

  L'authentification de l'acteur de santé auprès de la personne morale mettant en œuvre l'authentification par délégation doit être directe ; il n'est par exemple pas possible de combiner une authentification indirecte et une authentification par délégation.

7. Système d'information auquel la personne physique veut obtenir accès après authentification.

5. PALIERS DE L'AUTHENTIFICATION DES ACTEURS DE SANTÉ

Les différents paliers définis pour la mise en œuvre de l'authentification des acteurs de santé sont présentés par ordre croissant de niveaux de confiance des différents dispositifs d'authentification susceptibles d'être mis en œuvre.

Les paliers définissent des niveaux d'authentification combinant la force du dispositif d'authentification et la portée de l'identification sur laquelle repose l'authentification (Identifiant local, Identifiant national).

Les paliers sont numérotés par ordre croissant. Le palier correspondant au niveau le plus élevé définit les mesures permettant l'authentification d'acteurs de santé avec le niveau de force le plus élevé et la portée la plus étendue de l'identification.

Le choix du palier à atteindre découle de l'analyse de risque du SIS et des contraintes règlementaires. Le cas échéant, l'atteinte de ce palier peut suivre une trajectoire fondée sur les paliers de niveau moins élevé.

Une vue synthétique de l'ensemble des paliers pour les authentifications publique et privée est présentée en chapitre 6.

5.1. Paliers de l'authentification « publique » des acteurs de santé

Par convention et pour des raisons de parallélisme avec les niveaux d'authentification privée, les deux paliers présentés pour l'authentification « publique » sont numérotés 2 et 3.

5.1.1. Palier 2 de l'authentification publique

5.1.1.1. Authentification de personne physique

5.1.1.1.1. Authentification directe

En **palier 2** de l'authentification « publique », l'authentification directe d'une personne physique acteur de santé est réalisée avec un **« Certificat logiciel[8] de personne physique »** (c'est-à-dire bi-clé d'authentification, associée à son certificat de clé publique), diffusé par une IGC identifiée dans le *Référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé*.

Ce type de produit de certification est susceptible d'être utilisé pour la mise en œuvre de SIS en mode SAAS (Software As A Service – abonnement à un service internet qui offre les fonctions d'un SIS)[9].

Les conditions d'emploi de ces certificats dans le cadre de l'authentification directe sont détaillées en annexe.

5.1.1.1.2. Architecture d'authentification – Authentification indirecte

En palier 2 de l'authentification « publique », les architectures d'authentification de type authentification indirecte, sur la base d'une authentification « publique » de la personne morale et d'une authentification « privée » de l'acteur de santé, sont acceptées.

En authentification dite indirecte, seule la personne morale est authentifiée vis-à-vis du SIS cible. Elle est responsable de l'authentification des personnes physiques intervenant sous sa responsabilité.

8. Certificat électronique stocké dans un système logiciel (navigateur, application, système d'exploitation…), par opposition à un certificat électronique confiné dans un dispositif matériel (microcircuit de carte à puce ou de clé USB, …).
9. Dans ce cas, la personne physique est amenée à confier le certificat logiciel de personne physique à l'opérateur de solution SAAS.

Elle doit en particulier :
- déterminer les dispositifs d'authentification « publique » ou « privée » utilisables ;
- déterminer les exigences de sécurité pour la fonction d'authentification des personnes physiques et mettre en œuvre les dispositions de sécurité adéquates en découlant ;
- permettre l'identification de la personne physique en cas de litige (gestion des identifiants de portée locale et de leurs éventuelles évolutions dans le temps).

L'identifiant d'acteur de santé utilisé est de portée nationale ou locale[10].

5.1.1.2. Authentification de personne morale

En **palier 2**, l'authentification de la personne morale vis-à-vis d'un système d'information de santé doit s'effectuer à l'aide du dispositif suivant :

Type d'acteur de santé	Dispositifs autorisés
Tout type de personne morale	**« Certificat serveur »** c'est-à-dire une bi-clé d'authentification dont la clé publique est signée par une Autorité de Certification identifiée dans le *Référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé.*

Bien que le dispositif « Certificat serveur » soit initialement destiné à l'authentification de serveur, pour des raisons opérationnelles, son utilisation est acceptée pour l'authentification de la personne morale responsable du serveur et identifiée dans le certificat.

5.1.2. Palier 3 de l'authentification publique

5.1.2.1. Authentification de personne physique

5.1.2.1.1. Authentification directe

En **palier 3** de l'authentification « publique », l'authentification directe d'une personne physique acteur de santé est réalisée avec un des dispositifs listés dans le *Référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé* et présentés dans les sections suivantes.

5.1.2.1.1.1. Dispositifs d'authentification pour l'authentification directe - cartes de la famille CPx

Les dispositifs nominaux d'authentification des acteurs de santé agissant en tant que personnes physiques pour le palier 3 sont présentés dans le tableau ci-après :

Type d'acteur de santé	Dispositifs autorisés (voir conditions d'emploi en annexes)
Personnes physiques : Professionnel de santé enregistré dans le Répertoire Partagé des Professionnels de Santé (RPPS) Autres PS non enregistrés au RPPS (inscription ADELI ou autres référentiels nationaux)	• **Carte de Professionnel de Santé** (CPS) Contenant en particulier un certificat[11] d'authentification en provenance d'une IGC agréée par le groupement identifié dans l'Art. R 161-54 du code de la sécurité sociale et confiné dans une carte à puce désignée par le terme carte CPS
Personnes physiques : Personnel non professionnel de santé employé par un professionnel de santé ou une personne morale du domaine de la santé[12]	• **Carte de Personnel d'Etablissement** (CPE) Contenant en particulier un certificat d'authentification en provenance d'une IGC agréée par le groupement identifié dans l'Art. R 161-54 du code de la sécurité sociale et confiné dans une carte à puce désignée par le terme carte CPE

10. L'usage d'un identifiant local et non national affaiblit d'autant le niveau d'authentification.
11. Certificat : carte d'identité électronique attestant du lien entre les moyens cryptographiques fournis à un acteur pour mettre en œuvre les fonctions d'authentification ou de signature, et une identité réelle.
12. Cf. Référentiel d'identification des acteurs sanitaires et médico-sociaux de la PGSSI-S (Référence n° 1), pour les personnes morales considéré comme dans le domaine de la santé et en habilitées en tant que telle à gérer des CPE.

5.1.2.1.1.2. Dispositifs d'authentification - dispositifs alternatifs

Par « dispositif alternatif » il faut entendre un ensemble de dispositifs mis en œuvre par le même organisme et adossés à la carte CPS, c'est-à-dire que l'authentification de l'utilisateur lors de l'enrôlement doit s'effectuer avec une carte CPS. Sont également considérées comme « dispositifs alternatifs » toutes les combinatoires de ces dispositifs.

Les dispositifs alternatifs répondent à un besoin d'authentification publique lorsque l'authentification par carte CPS ne peut pas être utilisée. Le choix du dispositif dépend des possibilités de mise en œuvre. Si plusieurs dispositifs d'authentification peuvent être mis en œuvre, le choix du dispositif à mettre en œuvre doit respecter la hiérarchie suivante :

- dans le cas général : carte CPS, à défaut OTP SMS, à défaut OTP mail ;
- dans un environnement de mobilité : carte CPS, à défaut OTP SMS, à défaut OTP push, à défaut OTP mail.

Ces dispositifs sont détaillés dans les sections suivantes.

A. Mot de passe à usage unique – OTP SMS ou OTP mail

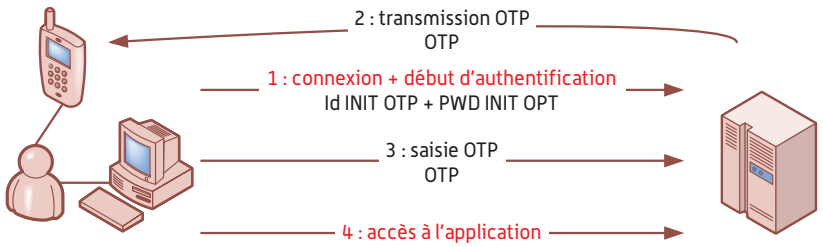
L'authentification par mot de passe à usage unique (aussi appelé OTP pour One Time Password) consiste à transmettre, par courriel[13] ou SMS, un mot de passe à l'utilisateur au moment où il effectue sa demande d'accès à un service en ligne.

Ce mot de passe est généré automatiquement par le service en ligne, après authentification de la personne. Il doit être saisi par l'utilisateur après réception dans un délai maximum défini[14] et n'est valable que pour une et une seule session.

Principes de fonctionnement de l'authentification par mot de passe à usage unique

L'obtention d'un OTP requiert la saisie préalable par l'utilisateur d'un identifiant (login) et d'un mot de passe.
Le login permettant de solliciter l'envoi d'un OTP est appelé **« ID INIT OTP »** dans la suite du document.
Le mot de passe permettant de solliciter l'envoi d'un OTP est appelé **« PWD INIT OTP »** dans la suite du document.
On parle ainsi d'une authentification forte en 2 temps.

Cinématique de connexion par OTP



Le mécanisme d'authentification par mot de passe à usage unique requiert, pour tout utilisateur, une phase « d'enrôlement » préalable adossée à la CPS.
Cette phase permet d'associer les paramètres d'accès (**ID INIT OTP** et **PWD INIT OTP**) à un utilisateur connu du système et d'enregistrer les canaux (adresse mail et/ou numéro de téléphone pour l'envoi de SMS) susceptibles d'être utilisés pour la transmission des futurs mots de passe à usage unique (**OTP**).

13. aussi appelé mail par référence au terme anglais e-mail d'où le terme OTP mail.
14. Généralement dans un délai inférieur à 10mn.

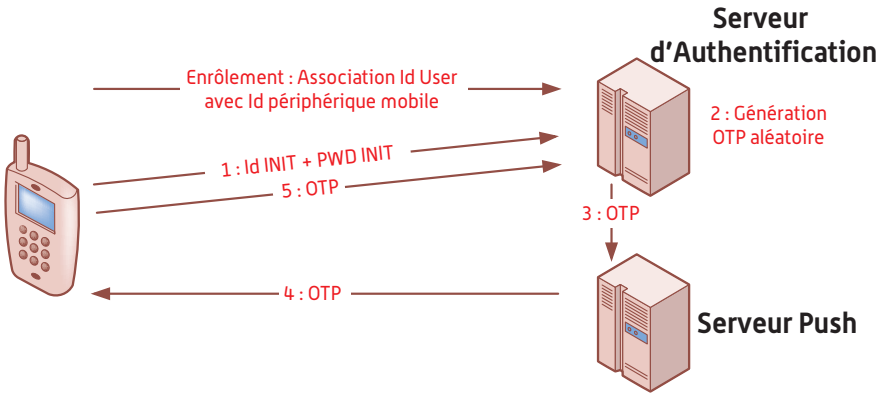
B. Mot de passe à usage unique en contexte de terminaux mobiles – OTP Push

En environnement de mobilité, le mot de passe à usage unique peut être transmis en mode « Push » : après authentification de la personne et de son terminal, l'OTP est envoyé 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.

Principes de fonctionnement de l'authentification par mot de passe à usage unique en mode PUSH



5.1.2.1.2. Architecture d'authentification – Authentification par délégation

En palier 3 de l'authentification « publique », les architectures d'authentification de type authentification par délégation, sur la base d'une authentification « publique » de la personne morale et d'une authentification « publique » de l'acteur de santé, sont acceptées.

En authentification dite authentification par délégation, seule la personne morale est authentifiée vis-à-vis du système d'information cible, l'acteur de santé n'étant qu'identifiée. La personne morale est responsable de mettre en œuvre l'authentification des acteurs de santé intervenant dans le cadre de l'authentification par délégation selon les mêmes modalités que le système d'information cible.

Elle doit en particulier :

- baser l'authentification des acteurs de santé sur les dispositifs d'authentification « publique » acceptés par le système d'information cible pour une authentification directe ;
- mettre en œuvre au minimum le palier 3 du référentiel d'imputabilité pour la fonction d'authentification ;
- mettre en œuvre les dispositions de sécurité correspondant aux exigences de sécurité du système d'information cible pour la fonction d'authentification des personnes physiques.

Une architecture d'authentification de type authentification par délégation nécessite un lien de type contrat ou convention entre le responsable de traitement du système d'information cible et la personne morale mettant en œuvre la fonction d'authentification par délégation. Ce lien doit au minimum identifier les dispositifs d'authentification « publique » acceptés ainsi que les exigences de sécurité à prendre en compte dans le cadre de l'architecture d'authentification par délégation et la procédure de validation de cette prise en compte.

5.1.2.2. Authentification de personne morale

L'authentification de la personne morale vis-à-vis d'un système d'information de santé doit s'effectuer à l'aide du dispositif suivant :

Type d'acteur de santé	Dispositifs autorisés
Tout type de personne morale	**« Certificat logiciel de personne morale »** c'est-à-dire une bi-clé d'authentification dont la clé publique est signée par une Autorité de Certification identifiée dans le *Référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé.*

Le processus de délivrance d'un certificat de personne morale s'appuiera sur une habilitation spécifique permettant de garantir la bonne accréditation du demandeur.
L'identifiant de la personne morale utilisé est national (FINESS, SIRET / SIREN, …).

5.2. Paliers de l'authentification « privée » des acteurs de santé

L'authentification privée des acteurs de santé ne porte que sur les personnes physiques, l'authentification des personnes morales doit toujours être de type authentification publique.

5.2.1. Palier 1 de l'authentification privée

En **palier 1**, une authentification basée sur un couple [identifiant individuel / mot de passe] peut être mise en œuvre, avec des contraintes sur les mots de passe, notamment en termes de construction, de conservation et de renouvellement.

On se référera ainsi à la note de l'ANSSI sur les mots de passes (cf. référence n° 3).

L'identifiant d'acteur de santé utilisé est national ou local[15].

5.2.2. Palier 2 de l'authentification privée

En **palier 2**, l'authentification « privée » d'un acteur de santé peut être réalisée par tout dispositif d'authentification forte (cf. définition du chapitre 4), au choix et sous la responsabilité du responsable de traitement.

Par exemple :
- Combinaison d'un couple identifiant/mot de passe avec :
  - un dispositif du type calculette physique ou virtuelle,
  - ou l'usage des capacités sans contact de la CPS3 ;
- Carte à puce d'établissement (contenant une bi-clé d'authentification en provenance de l'IGC de l'établissement) ou autre support confiné de certificat d'établissement (ex. clé USB), avec protection de l'accès à la bi-clé (ex. code PIN, biométrie…).

Le responsable de la personne morale s'appuie pour étayer son choix sur une analyse de risques spécifique.
Les règles d'identification sont les mêmes que celles présentées au palier 1.

Le responsable de traitement est responsable des accès réalisés sur le Système d'Information et il doit être capable d'identifier tous les acteurs qui se connectent. Il assure donc une gestion de l'identification de ces acteurs ainsi que des éventuelles évolutions dans le temps de l'identifiant: sur la base d'une identification nationale, ou locale mais en rendant possible l'identification certaine de l'acteur.

15. L'usage d'un identifiant local et non national affaiblit d'autant le niveau d'authentification.

En pratique, le responsable de traitement devra :

- Associer une identité à un identifiant, et intégrer cet identifiant à un dispositif d'authentification.
- Mettre en place un moyen de diffusion permettant de s'assurer de la délivrance du dispositif d'authentification au porteur de l'identifiant et à lui seul (enrôlement comprenant un face à face avec présentation de la carte d'identité par exemple).

5.2.3. Palier 3 de l'authentification privée

En **palier 3**, l'authentification « privée » d'un acteur de santé doit être réalisée selon les mêmes modalités que le palier 3 de l'authentification « publique » (cf. chapitre 5.1.2).
L'identifiant d'acteur de santé utilisé est alors national[16] et lié au dispositif d'authentification utilisé.

5.2.4. Socle commun de règles à respecter pour la mise en place de l'authentification « privée »

La mise en place de dispositifs d'authentification pour l'accès au SI doit s'appuyer sur des comptes individuels. Toute exception à cette règle doit être dûment autorisée et motivée par des impossibilités techniques ou matérielles et faire l'objet d'une analyse de risques spécifique.

Des modes d'accès particuliers au SI doivent être prévus pour gérer les cas d'exception : accès transitoire, solution de contournement avec même niveau de robustesse (CPE de service gérée localement), processus d'attribution en mode dégradé [login / mot de passe].

Ces modes doivent permettre les usages de type « bris de glace » permettant l'attribution temporaire et exceptionnelle de droits étendus en situation de crise (exemple : prise en charge de patient en urgence ou déclenchement du plan blanc en cas de crise sanitaire).

Ces accès particuliers doivent faire l'objet d'une journalisation, telle que définie dans le référentiel d'imputabilité.

Les outils informatiques doivent au minimum :

- gérer l'authentification sur une base d'utilisateurs[17] faisant référence à des identifiants nationaux ou locaux ;
- permettre la gestion du changement d'utilisateur, avec une ergonomie/rapidité adaptée au contexte (exemple : application d'urgence ou de prise en charge pluri disciplinaire) ;
- prendre en compte un délai d'inactivité (time out) différencié ;
- implémenter une durée maximum de session configurable/adaptable en fonction des contraintes métier ;
- rendre la gestion des sessions multiples paramétrable sous la responsabilité du chef d'établissement (exemple : pour la continuité de la prise en charge du patient).

16. Cf. Référentiel d'identification des acteurs sanitaires et médico-sociaux (Référence n° 1)
17. Ces utilisateurs pouvant être des personnes qui agissent dans le cadre des missions qui leur ont été confiées par la personne morale ou des tiers.

6. SYNTHÈSE DES DISPOSITIFS D'AUTHENTIFICATION

		Palier 1	Palier 2	Palier 3
Authentification « publique » des personnes physiques	Directe		Certificat logiciel de personne physique	• Carte de la famille CPx • Dispositifs alternatifs : Mot de passe à usage unique (OTP Push, à défaut OTP SMS, à défaut OTP Mail)
	Architecture d'authentification (indirecte ou par délégation)		Authentification indirecte : • Authentification « publique » de la personne morale • Identification de portée nationale ou locale de la personne physique • Authentification « privée » de la personne physique	Authentification par délégation : • Authentification « publique » de la personne morale • Identification de l'acteur de santé de portée nationale • Authentification « publique » de la personne physique • Exigences de sécurité imposées par le système d'information cible
Authentification « privée » des personnes physiques	Directe	Authentification basée sur un couple [identifiant individuel / mot de passe] Identification de l'acteur de santé de portée nationale ou locale. Contraintes pour la construction des mots de passe (cf. Recommandations de sécurité relatives aux mots de passe – Réf 3).	Tout dispositif d'authentification forte, au choix et sous la responsabilité du directeur d'Etablissement. Identification de l'acteur de santé de portée nationale ou locale.	Authentification selon les mêmes modalités que pour le palier 3 de l'authentification « publique » en mode direct des personnes physiques.
Authentification « publique » des personnes morales			Certificat serveur Référence à la personne morale responsable du serveur et identifiée dans le certificat. L'identifiant de la personne morale utilisé est national (FINESS, SIRET / SIREN).	Certificat logiciel de personne morale L'identifiant de la personne morale utilisé est national (FINESS, SIRET / SIREN).

Rappel : L'authentification des personnes morales doit toujours être de type authentification publique.

7. OFFRE INDUSTRIELLE

Le présent référentiel décrit une trajectoire d'exigences portant sur l'authentification des acteurs de santé ayant des impacts sur les solutions techniques (produits commerciaux, produits développés par les acteurs eux-mêmes…) qui les mettent en œuvre. À ce titre, il permet aux industriels de bâtir leur propre feuille de route de développement de leurs produits et d'afficher de façon formelle la conformité de leurs produits aux paliers d'authentification exprimés dans le présent référentiel. Selon les paliers, cette conformité pourrait par ailleurs faire l'objet d'une démarche d'homologation telle que préconisée par le RGS.

Ainsi, les responsables de traitement pourront choisir de manière éclairée des produits et des solutions offrant un niveau de compatibilité clair avec les exigences de la PGSSI-S.

8. IMPACT SUR LES PRATIQUES PROFESSIONNELLES

La connaissance des paliers possibles, permet aux acteurs de santé d'intégrer l'authentification dans l'évolution des pratiques professionnelles prérequis obligatoire à la généralisation de la dématérialisation des données de santé.

Parallèlement, la capacité qu'ont les industriels à définir les feuilles de route de développement de leurs produits par rapport aux paliers du référentiel d'authentification des acteurs de santé leur permet d'intégrer dès la conception de leurs produits les impacts sur l'utilisation et donc sur les pratiques professionnelles.

ANNEXE 1 – Présentation et conditions d'emploi des dispositifs d'authentification

A.1. Dispositifs d'authentification par carte CPS

Pour ces dispositifs, la personne physique voulant accéder au système utilise une carte à microcircuit qui contient une bi-clé d'authentification c'est-à-dire un couple (clé privée, clé publique) dédié à cet usage, en provenance d'une IGC agréée par le groupement identifié dans l'Art. R. 161-54 du code de la sécurité sociale.
La carte est accessible au travers d'un lecteur intégré dans le système. Ce lecteur doit être visible depuis le poste de travail de l'utilisateur.
Le principe de l'authentification repose sur un dialogue entre le système et la carte, via le lecteur. Ce dialogue permet au système de vérifier que l'accédant détient la clé privée.
Le mécanisme cryptographique d'authentification est implémenté dans la carte. Il ne peut être activé que lorsque la carte a vérifié le code porteur (code PIN) de son détenteur.
L'authentification de la personne physique est réputée forte car elle est dite « à deux facteurs » dans la mesure où elle repose sur ce que la personne connaît (son code porteur) et sur ce qu'elle possède (sa carte).

Carte CPS	
Caractéristiques particulières	La carte et le certificat d'authentification sont nominatifs et portent l'identité du PS. La carte CPS contient d'autres données de sécurité, en particulier les données d'assurance maladie qui permettent au professionnel de santé de produire des feuilles de soin électroniques ou des demandes de remboursement électroniques.
Modalités de gestion	La procédure de demande et de délivrance de la carte à un professionnel de santé, la procédure de demande et de délivrance de la bi-clé d'authentification, la procédure à suivre en cas de vol, de dégradation, de perte ou de retrait de service de la carte sont définies par le groupement identifié dans l'Art. R 161-54 du code de la sécurité sociale.
Conditions d'emploi	Une fois délivrée à son titulaire, la carte CPS est incessible. Son emploi et les conséquences de celui-ci sur l'accès au système d'information de santé sont mis sous la responsabilité du PS titulaire de cette carte.

A.2. Dispositifs d'authentification par certificat logiciel de personne morale

Pour ce dispositif, la personne physique voulant accéder au système, pour le compte de la personne morale, utilise, dans les conditions définies par la personne morale, une bi-clé d'authentification c'est-à-dire un couple (clé privée, clé publique) dédié à cet usage, en provenance d'une IGC identifiée dans le *Référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé*.
Le stockage et l'utilisation de cette bi-clé, ainsi que l'implémentation du mécanisme cryptographique d'authentification dans le système d'information de santé sont du ressort du responsable du traitement. Les clés ne doivent bien sûr pas être dupliquées – il doit y avoir une bijection entre la clé et le système qui l'héberge.
Le principe de l'authentification repose sur un dialogue entre le système et le moyen ou module réalisant le mécanisme cryptographique. Ce dialogue permet au système de vérifier que l'accédant détient la clé privée.
L'usage du certificat de personne morale est fait sous la responsabilité de la personne morale qui garantit que seuls les acteurs légitimes mettent en œuvre le mode d'authentification indirect ou par délégation.

L'usage du certificat de personne morale est sous la responsabilité de la personne morale qui garantit que seuls les acteurs légitimes mettent en œuvre le mode d'authentification indirect.

« Certificat logiciel de personne morale »	
Caractéristiques particulières	La bi-clé est délivrée au représentant de la personne morale, qui se charge de la placer dans l'environnement d'utilisation souhaité. Le certificat d'authentification est nominatif et porte l'identité de la personne morale.
Modalités de gestion	La procédure de demande et de délivrance de la bi-clé d'authentification, la procédure à suivre en cas de vol, de compromission, d'altération ou de retrait de service de la bi-clé sont définies par l'entité responsable de l'IGC qui délivre la bi-clé.
Conditions d'emploi	Une fois délivrée au représentant de la personne morale, l'emploi de la bi-clé et les conséquences de celui-ci sur l'accès au système d'information de santé sont mis sous la responsabilité de ce dépositaire. Ce dernier doit veiller à ce que le moyen permettant aux utilisateurs de la bi-clé de stocker et mettre en œuvre la clé privée, et le cas échéant de générer la bi-clé, réponde aux exigences de sécurité suivantes : • si la bi-clé d'authentification de la personne morale est générée par ses propres moyens, garantir que cette génération est réalisée exclusivement par des personnes autorisées et garantir la robustesse cryptographique de la bi-clé générée ; • assurer l'absence de duplication de la clé ; • détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ; • garantir la confidentialité et l'intégrité de la clé privée (par exemple en conditionnant son déverrouillage à la fourniture d'un mot de passe) ; • assurer la correspondance entre la clé privée et la clé publique ; • générer une authentification qui ne peut être falsifiée sans la connaissance de la clé privée ; • assurer la fonction d'authentification pour les utilisateurs légitimes uniquement et protéger la clé privée contre toute utilisation par des tiers ; • permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du moyen de stockage. L'identifiant de la personne morale titulaire de la bi-clé peut être pris en compte dans l'imputabilité des actions effectuées sur le système d'information de santé. En conséquence, le représentant de la personne morale doit pouvoir à chaque instant déterminer les utilisateurs de la bi-clé.

A.3. Dispositifs d'authentification par certificat logiciel de personne physique

Pour ce dispositif, la personne physique voulant s'authentifier utilise une bi-clé d'authentification, c'est-à-dire un couple (clé privée, clé publique) dédié à cet usage, en provenance d'une IGC identifiée dans le Référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé.
Le stockage et l'utilisation de cette bi-clé, ainsi que l'implémentation du mécanisme cryptographique d'authentification dans le système d'information de santé sont du ressort du porteur du certificat. Ils peuvent être confiés à un tiers du moment où celui-ci s'assure que seul le porteur peut utiliser la bi-clé pour mettre en œuvre une authentification.
Les clés ne doivent bien sûr pas être dupliquées – il doit y avoir une bijection entre la clé et le système qui l'héberge.
Le principe de l'authentification repose sur un dialogue entre le système et le moyen ou module réalisant le mécanisme cryptographique. Ce dialogue permet au système de vérifier que l'accédant détient la clé privée.

« Certificat logiciel de personne physique »	
Caractéristiques particulières	La bi-clé est délivrée au porteur du certificat, qui se charge de la placer dans l'environnement d'utilisation souhaité ou confie cette tâche à un tiers. Le certificat d'authentification est nominatif et porte l'identité de la personne physique.
Modalités de gestion	La procédure de demande et de délivrance de la bi-clé d'authentification, la procédure à suivre en cas de vol, de compromission, d'altération ou de retrait de service de la bi-clé sont définies par l'entité responsable de l'IGC qui délivre la bi-clé.
Conditions d'emploi	Une fois délivrée au porteur, l'emploi de la bi-clé et les conséquences de celui-ci pour l'accès à un système d'information de santé sont mis sous la responsabilité de ce dépositaire. Ce dernier doit veiller à ce que le moyen permettant de stocker et mettre en œuvre la clé privée, et le cas échéant de générer la bi-clé, réponde aux exigences de sécurité suivantes : • si la bi-clé d'authentification de la personne physique est générée par ses propres moyens, garantir que cette génération est réalisée exclusivement par le porteur ou un tiers qu'il a autorisé et garantir la robustesse cryptographique de la bi-clé générée ; • assurer l'absence de duplication de la clé ; • détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ; • garantir la confidentialité et l'intégrité de la clé privée - pour l'utilisation en palier 2 par tout moyen de protection limitant l'accès au système ou logiciel sur lequel est stocké le certificat, et en conditionnant son déverrouillage à la fourniture d'un mot de passe qui respect les contraintes sur la construction du mot de passe présentées dans la note de l'ANSSI sur les mots de passes (cf. référence n° 3) ; • assurer la correspondance entre la clé privée et la clé publique ; • générer une authentification qui ne peut être falsifiée sans la connaissance de la clé privée ; • assurer la fonction d'authentification pour le porteur uniquement et protéger la clé privée contre toute utilisation par des tiers ; • permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du moyen de stockage.

A.4. Dispositifs d'authentification par OTP

Structure de l'identifiant « ID INIT OTP »

L'identifiant « ID INIT OTP » utilisé peut être :

- l'identifiant national de l'acteur (Id RPPS, id ADELI, …) ;
- ou un identifiant ad hoc éventuellement calculé par le système sur la base de l'identifiant national de l'acteur.

Dans ce deuxième cas, l'identifiant devra être unique.
De façon à éviter des erreurs de saisie, les lettres utilisées ne contiennent ni de O, ni de i, ni de l. Elles peuvent être en majuscule et/ou en minuscule. L'identifiant est composé d'un code alphanumérique [A-Z] + [0-9] sans caractères accentués ni de caractères spéciaux.

Structure du mot de passe initial « PWD INIT OTP »

Le mot de passe initial généré par le Service doit être codé sur 8 caractères minimum dont la composition est la suivante :

- au moins une majuscule, une minuscule, un chiffre et un caractère spécial.
- pas de caractères accentués.
- Les caractères spéciaux peuvent être : _-+=<>@&'!?$*,;:

Un contrôle sur l'absence de caractères consécutifs identiques doit être effectué.

Création et structure du mot de passe en usage courant « PWD INIT OTP »

Le mot de passe initial doit être modifié par l'utilisateur lors de la première connexion ; le nouveau mot de passe doit alors être codé sur 8 caractères minimum avec au moins une majuscule, une minuscule, un chiffre.

Structure du code d'accès à usage unique « PWD OTP »
Le code d'accès à usage unique sera composé d'un ensemble de 6 caractères numériques (appartenant à l'intervalle [1..9]) choisis aléatoirement.

ANNEXE 2 – Glossaire

Sigle / Acronyme	Signification
ADELI	Automatisation DEs LIstes Système d'information national sur les professionnels de santé du social et les psychologues
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
COPIL	Comité de Pilotage
CPE	Carte de Personnel d'Etablissement
CPM	Carte de Personnel Mandaté
CPS	Carte de Professionnel de Santé
DMP	Dossier Médical Personnel
FINESS	Fichier National des Etablissements Sanitaires et Sociaux
GT	Groupe de Travail
IGC	Infrastructure de Gestion de Clé
OS	Operating System
OTP	One Time Password
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PIN	Personal Identification Number
PS	Professionnel de Santé
PTS	Pôle Technique et Sécurité
QR Code	Quick Response Code
RGS	Référentiel Général de Sécurité
RPPS	Répertoire Partagé des Professionnels de Santé
SAAS	Software As A Service
SIM	Subscriber Identity Module (carte SIM)
SIREN	Système d'Identification du Répertoire des ENtreprises
SIRET	Système d'Identification du Répertoire des ETablissements
SIS	Système d'Information de Santé
SMS	Short Message Service
USB	Universal Serial Bus

ANNEXE 3 – Documents de référence

Référence n° 1 : PGSSI-S – Référentiel d'identification des acteurs sanitaires et médico-sociaux
Référence n° 2 : Référentiel général de sécurité (RGS) et ses annexes
Référence n° 3 : Note ANSSI - Recommandations de sécurité relatives aux mots de passe
Référence n° 4 : PGSSI-S – Principes fondateurs
Référence n° 5 : PGSSI-S – Référentiel d'imputabilité
Référence n° 6 : PGSSI-S – Référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr