Usages et besoins d'identification et d'authentification des professionnels en établissement de santé

Rapport d'étude

Version 1.0 - Juin 2017

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTÉ

asipsanté
L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Documents de référence

1. Corpus documentaire de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) : http://esante.gouv.fr/pgssi-s/espace-publication
2. Décret de confidentialité de 2007, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000466727&dateTexte=20170201
3. Loi HPST de 2009, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020879475&dateTexte=20170201
4. Loi de santé de 2016, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031912641&dateTexte=20170201
5. Atlas SIH 2014, 2015, 2016, et 2017 http://social-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/article/atlas-des-systemes-d-information-hospitaliers
6. Référentiel Général de Sécurité : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
7. Décret n° 2016-524 du 27 avril 2016 relatif aux groupements hospitaliers de territoire
8. PSSI MCAS : http://www.legifrance.gouv.fr/eli/arrete/2015/10/1/AFSZ1523362A/jo
9. Annuaire Santé : http://esante.gouv.fr/services/referentiels/identification/annuairesantefr
10. Programme Hôpital Numérique : http://social-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/hopital-numerique/Hopital-Numerique
11. Certification HAS des établissements de santé, http://www.has-sante.fr/portail/jcms/c_411173/fr/mieux-connaitre-la-certification-des-etablissements-de-sante

Sommaire

PREMIERE PARTIE : OBJECTIFS DE L'ETUDE ET SYNTHESE

1.1 Objectifs de l'étude

Le développement **des systèmes d'information de santé (SIS) et de leurs usages** est un **levier essentiel pour la transformation du système de santé** et, en particulier, **pour l'amélioration de** la **coordination des soins et la mise en œuvre de véritables parcours de santé au bénéfice des patients**.

Dans cette perspective, les professionnels de santé sont de plus en plus amenés à utiliser des **télé-services nationaux et régionaux**, non seulement pour partager et échanger des données de santé (DMP, DP, PACS régionaux pour l'imagerie médicale, etc.), mais également pour de nombreux autres usages en voie de généralisation (déclarations en ligne de décès ou de maladies à déclaration obligatoire, signalements sanitaires, orientation des patients, etc.).

La création **des groupements hospitaliers de territoire (GHT) en 2016**, et **la mise en convergence du système d'information hospitalier (SIH) à l'échelle des territoires va accentuer davantage encore** le besoin de partage des informations de santé entre les établissements et services des secteurs sanitaire et médico-social.

Les systèmes d'information de santé étant ainsi de plus en plus ouverts et communicants, la **protection des données de santé** à caractère personnel qu'ils contiennent constitue plus que jamais un **enjeu majeur de la politique publique de santé numérique**. Cette protection nécessite la mise en œuvre d'une authentification forte des professionnels de santé, dans le respect du référentiel d'authentification des acteurs de santé de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S).

Toutes ces évolutions font de **l'identification et de l'authentification des acteurs de santé** un élément crucial de maîtrise de la protection des données de santé.

Afin de favoriser la mise en œuvre de l'authentification au plus près des usages et des besoins, **l'ASIP Santé a mené une étude sur les conditions requises** dans les **établissements de santé (ES),** en centrant plus particulièrement l'analyse, dans un premier temps, sur les établissements publics dans le cadre de la mise en place des GHT. Cette étude a été menée entre juillet 2016 et février 2017.

Après avoir rappelé le **contexte**, ce document présente une **synthèse des constats de l'étude** et énonce une série de **recommandations.**

1.2 Synthèse

La transformation numérique du système de santé est caractérisée par deux évolutions concomitantes qui font de la **protection des données de santé un enjeu central**. Le développement des usages du numérique au service des pratiques professionnelles (informatisation des processus de soins, mise à disposition de dispositifs adaptés à la mobilité des professionnels, etc.) d'une part, et l'utilisation de systèmes d'information de plus en plus communicants pour favoriser la prise en charge coordonnée du patient dans le cadre de son parcours de santé, d'autre part. Afin d'anticiper et d'accompagner ces évolutions en garantissant la protection des données médicales à caractère personnel, un cadre règlementaire national a été construit progressivement autour d'un espace de confiance numérique. Il repose sur plusieurs composantes de référence, notamment, la PGSSI-S[1] et **ses référentiels** qui deviendront opposables en 2018.

L'étude a permis de constater, dans les établissements de santé, une **prise de conscience des enjeux liés à la sécurité des SI** et un effort pour améliorer les dispositifs de protection de l'accès au SIH avec notamment la généralisation des comptes nominatifs. Néanmoins, l'accès aux applications qui manipulent les données de santé des patients s'effectue, dans la grande majorité des établissements de santé, exclusivement par identifiants/mots de passe, c'est-à-dire **dans des conditions non conformes au référentiel d'authentification de la PGSSI-S,** qui recommande une authentification renforcée (forte) dans les zones ouvertes au public[2], et le respect des règles de l'ANSSI[3] sur la robustesse et la confidentialité des mots de passe dans les contextes d'usage permettant une authentification simple.

Le manque de maitrise des concepts et du contenu des référentiels de la PGSSI-S[4] et le manque de compréhension de son positionnement au regard de l'ensemble des recommandations ministérielles de sécurité (PSSI-E et PSSI-MCAS, circulaire ministérielle dédiée au plan d'action sécurité…), tant par les établissements de santé que par leurs éditeurs, n'est pas l'unique raison qui explique la faible conformité aux exigences de sécurité de la PGSSI-S.

L'acquisition et le déploiement d'une solution d'authentification unique (SSO) s'avère nécessaire dans de nombreux cas : pour permettre au professionnel de n'avoir à mémoriser qu'un seul mot de passe robuste[5], pour pouvoir utiliser des dispositifs d'authentification renforcée que les applications ne savent actuellement pas gérer nativement. D'une manière plus générale, **la mise en place de l'authentification forte au sein d'un établissement de santé constitue l'ultime étape d'un projet complexe et pluridimensionnel,** à la fois organisationnel et technique, de gestion des identités et des accès, qui nécessite des moyens humains et financiers, de l'expertise et l'appui de la direction de l'établissement. Lorsqu'un établissement met en place l'authentification forte de ses personnels, il s'oriente généralement vers un support de type « carte » couplé à un identifiant, ce support ayant l'avantage de pouvoir être personnalisé pour favoriser l'identification physique du professionnel, être utilisé comme moyen d'accès multi-services (accès au parking, aux locaux, au système d'information,…), et d'être bien accepté par les professionnels dans leurs pratiques.

[1] Politique générale de sécurité des systèmes d'information de santé (PGSSI-S), corpus documentaire accessible sur le site esante.gouv.fr/pgssi-s

[2] Zones sans contrôle des entrées et sorties, par exemple lorsque l'accès s'effectue via un poste sur chariot laissé dans le couloir des unités de soin ou dans le service d'urgence.

[3] Agence nationale de sécurité des systèmes d'information

[4] Dont la publication est toutefois récente, puisqu'elle date de 2014

[5] En lieu et place des différents mots de passe demandés par les applications, limitant ainsi les risques de mots de passe conservés à portée du poste.

L'utilisation des téléservices régionaux et nationaux demeure relativement faible et concerne un nombre limité de professionnels de l'établissement. Les téléservices ne sont, dans la grande majorité des cas, pas intégrés au SIH et se présentent principalement sous la forme de portails web avec authentification directe de l'utilisateur ; les directions des SI des établissements ne les prennent pas en compte dans leur réflexion d'urbanisation du SI. Peu de téléservices proposent une authentification indirecte du professionnel, sous la responsabilité du directeur d'établissement (ce qui implique une certaine maturité du SI de l'établissement, par exemple pouvoir conserver la traçabilité de l'authentification individuelle dans le temps, et la mise en place par l'établissement d'une passerelle[6] ou l'adaptation de fonctionnalités de son SIH).

Enfin, **l'identification des professionnels de santé gérée en établissement gagnerait à être renforcée en s'appuyant sur les données d'identification des référentiels nationaux RPPS/ADELI** ; les identifiants nationaux des professionnels de santé mériteraient d'être systématiquement récupérés en prévision du développement des usages de partage et d'échange de données de santé avec les correspondants de l'établissement. Peu d'établissements savent qu'il existe un service de publication permettant de récupérer ces informations. La mise en place de projets de raccordement aux référentiels nationaux et d'exploitation de ces données concerne peu d'établissements à ce jour.

Au regard des constats formulés dans le cadre de cette étude, il apparait nécessaire que les pouvoirs publics définissent une **cible de convergence en matière d'authentification forte**, permettant à la fois d'orienter les établissements vers un nombre limité de solutions communes pour maîtriser les risques de recours à des solutions non conformes et de maîtriser les coûts liés à la multiplicité des choix réalisés par les établissements. Les **dispositifs d'authentification forte** retenus pour la protection des données de santé **doivent ensuite être promus** (en cohérence avec l'ensemble des actions menées par les pouvoirs publics autour de la sécurité du SI). Un **plan d'accompagnement** systémique doit être défini et mis en place pour s'assurer de la **conformité de l'offre industrielle** à ces exigences, ainsi que pour **appuyer et encadrer leur mise en œuvre par les établissements de santé** et par les **promoteurs de téléservices**.

[6] Via un EAI ou via une solution de proxy

DEUXIEME PARTIE : ELEMENTS DE CONTEXTE

La stratégie nationale e-santé 2020 fait du **développement des SI de santé et de leurs usages** une voie essentielle pour **«** [...] *dépasser les difficultés de coordination entre professionnels, faire face à une part croissante de patients atteints de maladies chroniques, permettre aux citoyens et patients d'être plus impliqués dans leur prise en charge* », et pour améliorer :

- la coordination et le suivi des soins tout au long du parcours du patient[7] ;
- l'accès aux soins (orientation des patients, télémédecine, télésurveillance, etc.) ;
- la connaissance agrégée sur l'état de santé à l'échelle nationale.

Ce développement repose à la fois sur **l'informatisation des offreurs de soins** tout au long du parcours du patient et sur la **capacité à créer des interactions entre des systèmes d'information des acteurs de santé**.

2.1 La nécessité de développer l'échange et le partage dématérialisés des données de santé rend les SI de santé de plus en plus communicants

2.1.1 L'informatisation des offreurs de soins, aujourd'hui largement répandue

Le processus de soins est aujourd'hui largement informatisé aussi bien en ville (cabinets médicaux, laboratoires de biologie, etc.) qu'à l'hôpital, ce qui rend de fait **possible le partage et l'échange de données de santé dans une logique de parcours de santé**, voire de parcours de vie. En effet :

- En 2015, 88% des médecins (81% en 2013) déclarent disposer de dossiers médicaux informatisés et utiliser les téléservices de l'Assurance maladie[8]. Les laboratoires de biologie médicale et les cabinets de radiologie en ville gèrent également les dossiers des patients de manière informatisée.

- En 2016, 94% des établissements déclarent l'informatisation de leur dossier patient achevée ou en cours - le pourcentage de projets achevés atteignant 63% et montrant une forte progression (55% en 2015 et 44% en 2014).[9]

Cette informatisation a été fortement portée par les pouvoirs publics, avec un soutien opérationnel et financier continu dans le cadre de divers programmes de modernisation et promotion**,** tels que:

- les plans hôpital 2007 et 2012, puis le programme hôpital numérique (PHN) pour les établissements de santé ;
- le projet de système électronique de saisie de l'assurance maladie (SESAM) pour l'informatisation du cabinet médical, dispositif de rémunération sur objectif de santé publique (ROSP) dans le secteur ambulatoire ;
- l'accréditation des laboratoires de biologie médicale, qui repose sur des exigences relatives à la mise en place d'un SI.

[7] Le raccourcissement des durées d'hospitalisation (chirurgie ambulatoire,…) accroit le besoin de coordination hôpital/ville ; la coordination des parcours de santé complexes nécessite le partage d'information entre les professionnels de santé et les intervenants du domaine social…

[8] Bilan de la Rémunération sur objectifs de santé publique 2015

[9] Atlas SIH 2014, 2015, 2016 et 2017

L'informatisation des offreurs de soins est donc bien amorcée et se voit également soutenue par le développement progressif de technologies numériques permettant l'échange et le partage entre les systèmes déployés à l'échelle nationale ou régionale.

2.1.2 Le développement des services dématérialisés d'échange et de partage

On a vu apparaître ces dernières années de nombreux projets visant à développer des services pour favoriser la coordination des soins. De ces initiatives résultent une variété de **téléservices[10] qui se caractérisent par une échelle de déploiement** (nationale, régionale) **et des objectifs de nature différente :**

- les téléservices visant au partage et à l'échange de données de santé : dossier médical partagé (DMP)[11], dossier pharmaceutique (DP)[12], PACS régional favorisant le partage d'images, système des messageries sécurisées de santé (MSSanté)[13], etc. ;
- les téléservices nationaux de déclaration règlementaire dématérialisée, tels que la déclaration en ligne des décès (Cert-DC)[14], le portail de signalement des événements sanitaires indésirables (PSIG)[15], le service dématérialisé de déclaration des maladies à déclaration obligatoire (E-DO)[16], ou permettant la transmission des fiches d'incident transfusionnel (E-FIT)[17] ;
- les téléservices régionaux visant à fluidifier le parcours de santé, tels que les projets lancés dans le cadre du programme Territoire de soins numérique (TSN), les services de télémédecine, les services d'orientation et d'aide au placement des patients, etc.

Le **cadre commun des projets d'e-santé[18]**, aussi appelé cadre d'urbanisation des projets de e-santé, précise le socle commun minimum de services à utiliser dans l'ensemble des territoires pour garantir la cohérence et l'efficience des actions régionales de promotion et d'usage de services numériques.

Afin de faciliter la coopération professionnelle et d'optimiser ainsi la coordination des soins, la loi de modernisation de notre système de santé de 2016 a par ailleurs élargi la notion **d'équipe de soins** au-delà de la stricte équipe intra-hospitalière (art. L1110-4[19]). Cet élargissement renforce le besoin d'identification et d'authentification forte des acteurs lors de leur accès aux données de santé partagées ou échangées afin d'assurer la traçabilité des accès.

[10] Le terme de « téléservice » est utilisé dans tout le document pour tout système d'information permettant aux professionnels de santé d'échanger, de partager, de déclarer par voie électronique des informations relatives à l'usager du système de santé, qu'il s'agisse d'un portail web ou d'une application plus intégrée dans l'application métier du professionnel.

[11] Le DMP permet le partage de documents utiles à la coordination des soins. Il est géré par l'Assurance maladie (CNAMTS)

[12] Le DP recense les médicaments délivrés au patient au cours des 4 derniers mois, il permet de repérer les risques d'interactions médicamenteuses. Le DP est proposé par l'ordre des pharmaciens.

[13] Le système MSSanté est géré par l'ASIP Santé

[14] Cert-DC est proposé par la DGS avec l'appui de l'INSERM

[15] Ce portail permet aux professionnels et au public de déclarer des évènements sanitaires indésirables. Il est proposé par la DGS avec l'appui de l'ASIP Santé

[16] E-DO est géré par Santé Publique France.

[17] E-FIT est géré par l'Agence Nationale de Sécurité des Médicaments et produits de santé

[18] http://esante.gouv.fr/actus/politique-publique/publication-de-l-instruction-relative-au-cadre-commun-des-projets-de-e

[19] Décret n° 2016-994 du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel et Décret n° 2016-1349 du 10 octobre 2016 relatif au consentement préalable au partage d'informations entre des professionnels ne faisant pas partie de la même équipe de soins

2.1.3 La tendance au regroupement des établissements de santé

2.1.3.1 Les GHT et leur schéma directeur des systèmes d'information (SDSI)

Les **Groupements Hospitaliers de Territoire (GHT)** ont pour objectif **de mettre en œuvre une gradation des soins hospitaliers et de développer des stratégies médicales et soignantes de territoire.**

Depuis le 1er juillet 2016 les signatures des conventions ont marqué la constitution officielle des GHT dont les membres sont unis par un projet médical partagé organisant une offre de soins de proximité et de recours. Les membres des groupements doivent également travailler sur un schéma directeur des systèmes d'information (SDSI) commun.

Le code de la santé publique[20] stipule que l'établissement support du GHT assure, pour le compte des établissements du groupement :

- la stratégie, l'optimisation et la gestion commune d'un SIH « convergent », en particulier la mise en place d'un dossier patient pour la prise en charge coordonnée au sein du groupement ;
- la mise en œuvre des mesures techniques de nature à assurer le respect des obligations prévues par la loi informatique et libertés.

Échéances

- 1er juillet 2016 : Convention constitutive du GHT
- 1er juillet 2017 : Projet médical partagé
- 1er janvier 2018 : SDSI du GHT
- 1er janvier 2021 : atteinte de la cible du SIH convergent et homogène

A cet effet, et afin d'atteindre la cible au 1er janvier 2021, un SDSI du GHT, conforme aux objectifs du projet médical partagé, doit être élaboré par le directeur de l'établissement support du groupement d'ici le 1er janvier 2018[21].

Ainsi, deux enjeux majeurs d'urbanisation sont au cœur de la mise en œuvre du SDSI du GHT :

- d'une part la construction d'une trajectoire de convergence du SI au sein du GHT (composante « intra-GHT ») ;
- d'autre part l'articulation du SI du GHT avec l'écosystème e-santé territorial, régional et national (composante « extra-GHT »).

2.1.3.2 Les mouvements de concentration des cliniques privées

Un mouvement de concentration s'observe également sur le secteur privé depuis de nombreuses années, et le nombre d'établissements et de structures indépendants diminue de façon continue.

Les évolutions de la tarification représentent un des facteurs ayant amené les établissements à se rapprocher pour rationaliser leurs coûts et mutualiser certaines activités. Ainsi plusieurs opérations de rachat et fusion se sont succédées[22]. A fin 2015, les 10 premiers groupes d'hospitalisation privée concentraient environ 45% des établissements de santé de court séjour et près de 60% des capacités d'accueil MCO du secteur privé.

La mise en place des GHT a renforcé la tendance, les cliniques étant amenées à se regrouper pour former un maillage local d'acteurs en mesure d'adopter une stratégie territoriale et de proposer une continuité de soins qui suggère également une trajectoire de convergence entre les SI des établissements regroupés.

[20] Premier alinéa de l'article L6132-3 du CSP
[21] Art. R. 6132-15.-I du CSP
[22] Rachat de Générale de Santé par Ramsay, Fusion de Korian et Medica en 2014, Rachat de Médi-Partenaires par Médipôle Sud Santé, Rachat de Vitalia par Vedici, etc.)

2.1.4 Des enjeux de mobilité croissants

A cela s'ajoute également la **plus forte mobilité des professionnels de santé** et les **évolutions des modes de travail** qui **augurent** une place croissante à l'usage des smartphones et tablettes comme outils de consultation des données de santé.

2.2 Le cadre juridique mis en place pour réguler ces évolutions

2.2.1 Un cadre juridique progressivement enrichi pour garantir la protection des données de santé

Du fait de la conservation sous un format électronique, la multiplication des usages des systèmes d'information dans le domaine de la santé s'accompagne d'un accroissement des risques d'atteinte au respect des droits de la personne en matière de protection des données la concernant.

C'est pourquoi le traitement des données de santé est encadré juridiquement par la loi informatique et libertés[23] et par une série de dispositions législatives et réglementaires **spécifiques au secteur de la santé,** ayant pour objet de garantir la confidentialité des données de santé et le respect des droits des patients :

- la **loi du 4 mars 2002[24] relative aux droits des malades a apporté des changements importants au code de la santé publique en matière de gestion des données de santé ;**
- le **décret de confidentialité du 15 mai 2007[25]** impose la carte CPS pour sécuriser l'accès aux systèmes d'information contenant de la donnée médicale à caractère personnel, à l'intérieur des structures de santé et pour l'accès à des systèmes d'information externes ;
- la **loi du 21 juillet 2009[26]**, portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires (loi HPST), élargit les modalités d'authentification aux dispositifs équivalents à la CPS, le tout étant décrit dans les référentiels de la PGSSI-S ;
- la **loi du 26 janvier 2016 de modernisation de notre système de santé[27]** supprime toute référence à la carte CPS, renvoie directement aux référentiels de sécurité (référentiels de la PGSSI-S détaillés infra), et prévoit leur opposabilité.

En réponse à l'accroissement du risque d'atteinte au respect des droits de la personne en matière de protection des données la concernant, la DSSIS[28] (maitrise d'ouvrage stratégique) et l'ASIP Santé (maitrise d'ouvrage opérationnelle) pilotent l'élaboration de la **politique générale de sécurité des systèmes d'information de santé (PGSSI-S),** en concertation avec les directions ministérielles concernées, l'ensemble des acteurs des secteurs sanitaire et médico-social, l'ANSSI et la CNIL.

[23] La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de loi informatique et libertés, est une loi française qui règlemente la liberté de traitement des données personnelles.
[24] Articles L1110-1 est suivants du Code de la Santé Publique
[25] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000466727&categorieLien=id
[26] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020879475&categorieLien=id
[27] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031912641&categorieLien=id
[28] Délégation à la stratégie des systèmes d'information de santé, rattachée au Ministère des Affaires Sociales et de la Santé.

2.2.2 La définition d'une doctrine publique de sécurité

2.2.2.1 Présentation générale de la PGSSI-S

Constituant **la principale référence pratique pour la protection des données de santé à caractère personnel**, elle s'applique à l'ensemble des acteurs publics ou privés intervenant dans les secteurs sanitaire, médico-social et social[29], et a également vocation à structurer l'offre logicielle des industriels.

La PGSSI-S se décline en plusieurs documents s'adressant aux différents professionnels exerçant au sein des structures de santé et aux acteurs qui les accompagnent :

- des guides d'accompagnement portant sur les bonnes pratiques de mise en œuvre et sur certains sujets spécifiques (par exemple pour les dispositifs connectés, la mise en place d'un accès WIFI, les règles de sauvegarde…) ;
- **des référentiels portant sur les concepts essentiels : identification, authentification et imputabilité** (dont les référentiels d'identification et d'authentification des acteurs de santé auxquels se réfère cette étude), qui vont devenir opposables.

2.2.2.2 Les référentiels d'identification et d'authentification

L'identification a pour but de déterminer l'identité d'un acteur via un identifiant qui lui a été attribué préalablement lors de la vérification et de l'enregistrement de ses traits d'identité. **L'identification est un préalable à l'authentification**, comme le définit le Référentiel Général de Sécurité (RGS) : «*L'authentification est toujours précédée ou combinée avec une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté : un identifiant. En résumé, s'identifier c'est communiquer un identifiant présumé, s'authentifier c'est apporter la preuve que l'entité s'est vue attribuer cet identifiant.*»[30]

L'objet des référentiels d'identification et d'authentification est de définir des niveaux d'exigences, appelés palier, et les dispositifs qui y sont associés.

Pour exemple, le référentiel d'authentification, publié en 2014, fixe des paliers minimums en fonction des contextes d'usages et des risques identifiés par le responsable de traitement[31] :

- dans la **sphère de responsabilité d'un établissement de santé** (exercice collectif avec mutualisation d'un SI entre plusieurs utilisateurs), le référentiel préconise la mise en place de **l'authentification forte pour l'accès au SIH** (palier 2), **avec une possibilité d'authentification simple (palier 1) dès lors que l'accès physique au terminal est physiquement contrôlé ou régulé ;**
- pour **l'accès aux téléservices utilisant de la donnée de santé à caractère personnel**, le référentiel :
  - préconise une **authentification publique par carte CPx ou dispositif alternatif associé à la carte CPS (palier 3) ;**
  - ouvre également la possibilité d'utiliser un **dispositif d'authentification indirecte** du professionnel sous la responsabilité du responsable de la structure qui l'emploie.

[29] Le « référentiel de gouvernance et de mise en œuvre de la PGSSI-S » actuellement en concertation précise son champ d'application (esante.gouv.fr/sites/default/files/asset/document/pgssi-s_referentiel_gouvernance_v0.1.pdf)

[30] Page 4/29 §A.1.b de l'annexe B3 du « Référentiel Général de Sécurité » version 2.0 de juin 2014.

[31] La réalisation d'une analyse des risques en matière de sécurité du SI est obligatoire avant toute mise en œuvre d'un système d'information de santé, puis revue périodiquement.

- Dans ce cas le **responsable d'établissement est garant du bon usage de l'authentification dans sa sphère privée** et de la **traçabilité de l'authentification dans le temps ;**
- Il est donc responsable des actions induites au travers du téléservice via la mise en place d'un flux sécurisé, et l'établissement s'authentifie avec un **certificat de personne morale**.

Ces documents s'adressent également aux fournisseurs de produits ou de services utilisés dans le cadre de systèmes de santé.

2.2.2.3 Des référentiels rendus opposables en 2018

La loi de modernisation de notre système de santé de 2016 a énoncé le principe du caractère opposable des référentiels de la PGSSI-S. Les référentiels en vigueur datant de 2014, un travail se poursuit actuellement avec le groupe de travail PGSSI-S afin d'évaluer la nécessité de les faire évoluer. Une nouvelle version de ces référentiels sera mise en concertation publique à la fin du premier semestre pour une publication de la version finale dans le courant du deuxième semestre 2017. **L'opposabilité des référentiels sera effective en 2018.**

Le mécanisme d'opposabilité, encore non précisé, pourrait être mis en œuvre dans le cadre d'un dispositif similaire à ceux déjà mis en place actuellement (Certification Hôpital Numérique, Labellisation e-santé des logiciels des maisons et centres de santé).

2.2.3 Construction et maintien d'un espace de confiance numérique

L'ASIP Santé est garante de la construction et du maintien d'un espace de confiance numérique reposant sur plusieurs composantes de référence :

- la **politique générale de sécurité des systèmes d'Information de santé (PGSSI-S),** citée dans le paragraphe *supra* ;
- **l'annuaire santé** permettant l'identification nationale des professionnels de santé inscrits dans les répertoires RPPS et ADELI, accessible par web service et via le portail annuaire.sante.fr ;
- **des produits de certification : les cartes de la famille CPS et certificats logiciels** (de personnes morale et physique) délivrés par l'ASIP Santé en tant qu'autorité de certification du monde de la santé, grâce à son infrastructure de gestion de clés (IGC Santé)[32],

En application de l'article 110 de la loi du 26 janvier 2016 de modernisation de notre système de santé, l'ASIP Santé est en outre chargée d'animer le dispositif opérationnel de déclaration et de traitement des incidents de sécurité des SI de santé, apportant à partir d'octobre 2017[33] son expertise pour analyser les incidents graves et significatifs de sécurité, et amener un appui aux acteurs.

[32] L'Infrastructure de Gestion de Clés (IGC) est un ensemble de personnes, procédures, matériels et logiciels visant à créer, délivrer, révoquer et publier des certificats électroniques au profit d'une communauté d'utilisateurs

[33] La date d'applicabilité du décret relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité remontés par les établissements de santé, laboratoires de biologie médicale et centres de radiothérapie est octobre 2017. www.legifrance.gouv.fr/affichTexte.do;jsessionid=142F4DFED42CD0D4E296A75A73BFC2BA.tpdila21v_3?cidTexte=JORFTEXT000033117678&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033117518

TROISIEME PARTIE : ETAT DES LIEUX ET CONSTATS

La qualité des processus d'identification et d'authentification des professionnels, de gestion de leurs droits d'accès et habilitations dans les applications, est un prérequis essentiel à la protection des données de santé des patients que ces professionnels prennent en charge.

La mise en place de l'authentification des professionnels auprès des systèmes d'information de santé intra et extra hospitaliers amène les établissements à devoir réunir les conditions suivantes :

- **identifier tous les professionnels de l'établissement**, salariés ou non, qui accèdent au SIH de l'établissement et aux téléservices, en tenant compte de leurs données d'identification nationale lorsqu'elles sont disponibles ;
- mettre en œuvre des **mécanismes d'authentification adaptés**, simple d'utilisation pour les professionnels et respectant le niveau de sécurité recommandé par la PGSSI-S ;
- **maîtriser les droits d'accès au SIH**, de même que les accès physiques[34] ;
- se mettre en situation de **garantir un accès sécurisé aux téléservices extrahospitaliers** dans un contexte grandissant de partage et d'échange dématérialisés de données de santé.

3.1 Identifier tous les professionnels dans l'établissement et s'adosser aux référentiels nationaux

3.1.1 Disposer d'une vue exhaustive et centralisée des professionnels

L'identification de l'ensemble des professionnels qui travaillent au sein de l'établissement constitue le **socle indispensable pour la mise en œuvre effective de la sécurisation des accès**, qu'il s'agisse de contrôles d'accès physiques ou logiques[35].

Si le sujet est **identifié comme important par les établissements**, le niveau de **mise en œuvre observé est variable.** De façon générale, l'enregistrement des salariés dans le SI RH par la direction des affaires médicales (DAM) et la direction des ressources humaines (DRH) est un processus maitrisé[36] ; l'identification des professionnels non-salariés est en revanche plus complexe.

En pratique, l'organisation de l'identification des professionnels repose sur **plusieurs voies d'entrée** (DAM/DRH, direction de soins, direction des systèmes d'information ou délégation dans les services), chacune responsable d'identifier certaines catégories de professionnels. Ce mode d'organisation nécessite la formalisation d'un circuit d'information entre les différentes entités **pour anticiper les mouvements de personnel** (arrivées/départs, absences, renouvellements, changements d'affectation, etc.) et pour **assurer une vérification optimale de l'identité et de la capacité d'exercer des professionnels**.

Compte-tenu de la forte corrélation entre la gestion des identités des professionnels et la gestion des habilitations et du contrôle d'accès aux applications, la **direction des systèmes d'information (DSI) est perçue comme l'entité la plus à même de porter un discours promoteur sur le sujet** et se voit ainsi attribuer, de fait, la responsabilité de piloter ce projet d'identification exhaustive des

[34] Si l'étude porte avant tout sur la mise en place de dispositifs d'authentification adaptés à la protection des données de santé, elle ouvre également des pistes sur la protection des accès physiques

[35] Des professionnels qui en fonction de leur métier (médecins, soignants, éducatifs et sociaux, administratifs, médicotechniques et techniques) et de leur statut (salariés, libéraux, prestataires, intérimaires, etc.) seront ensuite potentiellement concernés par le contrôle d'accès.

[36] L'enjeu porte sur l'anticipation de la communication de ces données d'identification pour que les dispositifs de contrôle d'accès soient disponibles dès l'arrivée du salarié.

professionnels. **Les DSI sont demandeurs d'un appui institutionnel pour que ce type de projet soit porté par la direction générale,** en lien avec les directions concernées (DRH/DAM,…).

En matière d'outils, la mise en place d'un annuaire d'établissement, centralisant les identités de l'ensemble des professionnels, se développe, sans être pour autant généralisée dans l'ensemble des établissements.

3.1.2 Un adossement encore limité aux référentiels nationaux

La gestion de l'identification des professionnels **gagne à être renforcée par l'usage des référentiels nationaux.** L'annuaire santé géré par l'ASIP Santé contient et publie[37] les données d'identification des professionnels de santé inscrits dans les répertoires nationaux RPPS et ADELI[38].

Son utilisation par les établissements de santé leur permet de disposer de données enregistrées et certifiées par les autorités concernées (ordres professionnels et ARS) pour la vérification des compétences des professionnels de santé.

L'adossement aux référentiels nationaux leur permet ainsi de compléter leurs données d'annuaire, et d'associer à l'identifiant local du professionnel **son identifiant national qui est indispensable pour le partage et l'échange de données de santé[39]** entre acteurs de santé.

L'utilisation des identifiants nationaux reste aujourd'hui encore limitée à certains usages :

- pour les prescriptions hospitalières exécutées en ville (identifiant RPPS du prescripteur), le dispositif est dans ce cas bien maîtrisé ;
- avec la mise en place des boîtes à lettre nominatives de messagerie sécurisée MSSanté, pour lesquelles les identifiants RPPS ou ADELI sont nécessaires ;
- lorsque l'établissement a généralisé l'usage de la carte CPS dans sa structure, les cartes CPS portant nativement les données d'identification nationales ;
- pour l'usage de téléservices régionaux et nationaux.

Deux raisons principales expliquent cette faible utilisation :

- mis en place depuis 2014, **le service d'annuaire proposé par l'ASIP Santé est récent et dans l'ensemble méconnu** ;
- une **large majorité d'établissements ne dispose pas d'annuaire fédérateur** (ou méta-annuaire) ; l'accès à l'annuaire santé nécessite alors la mise au point d'interfaces entre les annuaires intégrés aux applications du SIH auxquelles accèdent les professionnels de santé et l'annuaire santé national. Ces interfaces, basées sur l'usage du protocole LDAP[40], ne sont pas toujours proposées nativement dans les applications du SIH et représentent des coûts supplémentaires.

[37] Les données sont publiées via un portail (consultation, extraction publique sous forme de fichier) et par web services pour faciliter l'interrogation automatisée des données de l'annuaire par les établissements, à partir de leur SIH.

[38] Le répertoire partagé des professionnels de santé (RPPS) contient les données d'identification des médecins, sages-femmes, pharmaciens, chirurgiens-dentistes et masseurs-kinésithérapeutes. Il a vocation à regrouper les données d'identification de l'ensemble des professionnels de santé (qui, dans cette attente, restent identifiés avec leur n° ADELI).

[39] Référentiel d'identification des acteurs sanitaires et médico-sociaux dans la PGSSI-S

[40] LDAP (Lightweight Directory Access Protocol) est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau. Il simplifie la gestion des profils de ces utilisateurs, favorise l'interopérabilité des systèmes d'informations à travers le partage de ces profils, et améliore la sécurité d'accès aux applications.

3.1.3 Un besoin d'identification qui s'intensifie dans le cadre des GHT

La mise en place des GHT ne fera qu'accroître la nécessité d'identifier l'ensemble des professionnels exerçant au sein des établissements du GHT, déjà mis en avant aujourd'hui au titre d'établissement individuel.

La mise en place d'un annuaire fédérateur (ou méta-annuaire), contenant les identifiants nationaux des professionnels de santé, semble indispensable pour faciliter la maitrise des processus de gestion des identités, des habilitations, et des échanges avec les autres acteurs de santé. Au sein du GHT, la responsabilité du traitement de l'identification, de l'authentification et des habilitations reste à définir et des politiques communes devront être mises en place (politiques d'identification, d'authentification, d'habilitation, plan d'urbanisation du SI, etc.).

3.2 Sécuriser les accès au SIH : des progrès mais une gestion des droits rarement automatisée

3.2.1 Un changement de culture favorisé par les incitations publiques

3.2.1.1 Une prise de conscience autour des problématiques de sécurité

Soutenue depuis de nombreuses années par les pouvoirs publics[41] dans un contexte d'informatisation croissante des processus de soins et d'ouverture des SIH vers les SIS, **la sécurité du système d'information hospitalier est de mieux en mieux appréhendée dans les établissements de santé** : élaboration et mise en application d'une politique de sécurité des systèmes d'information (PSSI)[42], désignation de RSSI dans chaque établissement, etc.

Selon l'Atlas SIH 2017, *90% des établissements répondants sont conformes au prérequis P.3.1 imposant l'existence d'une politique de sécurité interne (contre 63% en 2014), et plus de 95% des établissements répondants dispose d'un référent sécurité (affecté le plus souvent à temps partiel, voire mutualisé pour plus d'un quart des répondants).*

La déclinaison de la **PSSI** en **plan d'action SSI** permet la mise en œuvre d'un certain nombre de règles et mesures de sécurité, dont celles associées à la **gestion des accès** (règles sur l'utilisation des dispositifs d'authentification ; comptes nominatifs, verrouillage des comptes sur connexion infructueuse,…).

3.2.1.2 Suppression des comptes génériques

De grands progrès ont eu lieu depuis plusieurs années pour **généraliser les comptes nominatifs** et faire disparaitre les comptes génériques (parfois encore utilisés pour gérer les professionnels intervenant de façon temporaire dans l'établissement par exemple).

[41] Au travers, par exemple, des travaux de sensibilisation à la sécurité des SI portés par le GMSIH jusqu'en 2009, de la publication DGOS en novembre 2013 d'une introduction à la SSI à destination des directeurs d'établissement, de l'intégration d'exigences de sécurité dans les prérequis du programme Hôpital Numérique, des travaux menés dans le cadre de la PGSSI-S etc.

[42] Pour aider les établissements de santé, la PGSSI-S contient un « Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Structure sans approche SSI formalisée » (esante.gouv.fr/pgssi-s/espace-publication)

Atlas SIH 2017 : *Score atteignant 97% pour le critère P.3.4. Hôpital Numérique, imposant un taux de 90% d'applications contenant des données de santé avec authentification personnelle*[43].

En effet, l'adossement de la **certification HAS** aux **indicateurs Hôpital Numérique** ainsi que la **certification des comptes** (comprenant l'auditabilité des SI) ont accéléré ces changements au sein des établissements.

3.2.2 Une gestion des droits peu automatisée

Malgré la progression du nombre d'établissements de santé équipés d'un AD (Active Directory)**, la gestion des droits reste encore majoritairement manuelle** :

- à partir de la saisie réalisée dans le SIRH de l'établissement par le service des ressources humaines, la DSI crée les comptes nominatifs des personnes accédant au SIH. Les modalités de communication entre les DRH et les DSI sont complexes et cette transmission d'information, si elle n'est pas automatisée, pose souvent problème ;
- la DSI crée ensuite les droits d'accès techniques aux différents composants du SIH (espaces réseaux, accès internet, applications connectées à l'AD) en fonction du profil métier et des affectations du personnel ; pour la majorité des applications, une création manuelle des comptes dans chacune d'elles est souvent requise ;
- enfin, la création des rôles (ou droits fins) dans chacune des applications est souvent déléguée à un référent métier localisé dans le ou les service(s).

Les freins à la progression vers un dispositif centralisé et automatisé sont de différentes natures.

Le premier frein est « technique » et concerne la synchronisation entre le SIRH, l'Active Directory (AD) et les différents annuaires intégrés des applications du SIH, qui nécessite la mise en œuvre d'un méta-annuaire et d'un composant de synchronisation intermédiaire central. De plus, le bon fonctionnement repose sur la capacité des applications du SIH, de l'AD, du méta-annuaire et des composants de synchronisation à communiquer nativement entre eux.

Le second frein réside dans la difficulté pour les entités « métier » à définir une matrice d'habilitation (droits fins au sein de chacune des applications) par profil de professionnel. Le **responsable de traitement,** souvent commanditaire de l'achat de l'application et principal usager avec ses équipes, **n'est que rarement au fait de ses responsabilités**, en particulier celle de **définir précisément les rôles des utilisateurs au sein de l'application.**

Selon l'Atlas SIH 2017, *près de deux tiers des établissements (60%) procède à une revue des comptes au moins une fois par an et un peu plus de la moitié (53%) procède à une revue des droits d'accès avec la même fréquence.*

Les DSI/RSSI souhaitent une **plus forte implication des représentants des professionnels de santé** dans l'élaboration et la mise en place des dispositifs de protection des données de santé informatisées.

[43] Taux d'applications gérant des données de santé à caractère personnel intégrant un dispositif d'authentification personnelle, via la CPS ou dispositif équivalent ou un identifiant/mot de passe individuel avec système de renouvellement de mot de passe. Le système doit comprendre une déconnexion de l'utilisateur sur temporisation d'inactivité.

3.3 L'authentification forte pour l'accès aux données de santé : indispensable et pourtant peu diffusée

3.3.1 Une authentification basée sur l'identifiant/mot de passe

La grande majorité des établissements (probablement de l'ordre de 90% des établissements) propose à leurs utilisateurs d'accéder depuis leur poste de travail aux applications du SIH **exclusivement avec des identifiants/mots de passe.**

3.3.1.1 Un niveau de sécurité insuffisant

L'authentification par identifiant/mot de passe suppose que les recommandations de l'agence nationale de sécurité des systèmes d'information (ANSSI) relatives à la **construction, la conservation et le renouvellement des mots de passe** soient respectées.

L'instruction[44] relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information dans les établissements et services concernés (octobre 2016) rappelle d'ailleurs l'importance d'une sécurisation des comptes par mots de passe robustes et renouvelés périodiquement (l'une des mesures de priorité 1 à mettre en place dans les six mois). La CNIL a récemment publié de nouvelles recommandations sur les mesures de sécurité élémentaires relatives à l'authentification par mot de passe[45].

Par ailleurs, le SIH reste composé de multiples applications « métier » (dont le nombre peut fluctuer largement, en fonction de la taille de l'établissement, d'une dizaine à plus d'une centaine) pour lesquelles les contraintes de construction des identifiants et mots de passe ne sont pas complètement harmonisées. Ainsi, bien que certains établissements parviennent à l'unicité des identifiants, la majorité estime qu'il existe entre 3 et 5 couples identifiant /mot de passe par utilisateur en fonction des profils, ce qui amène souvent les utilisateurs à conserver leur mot de passe sur un papier à portée de main (ex : sous le clavier) pour ne pas l'oublier, pratique qui ne peut que se renforcer dans un contexte où les mots de passe doivent être robustes (mots suffisamment longs et composés de caractères de types différents) et renouvelés périodiquement.

Au sein de l'établissement, si **l'authentification simple** par identifiant/mot de passe peut suffire pour accéder aux applications administratives ou aux applications métier dans certains contextes d'usage (accès au terminal physiquement contrôlé ou régulé), **elle n'apporte en revanche pas un niveau de sécurité suffisant pour protéger les données de santé contenues dans des applications accessibles dans des zones en libre accès** (lorsque l'accès s'effectue dans une zone ouverte au public par exemple). **Dans ce contexte, la PGSSI-S[46] requiert une authentification forte.**

L'authentification est dite forte lorsqu'au moins deux des facteurs suivants sont combinés :
- ce que la personne sait (ex. mot de passe) ;
- ce que la personne possède (ex. carte à puce) ;
- ce que la personne est (ex. biométrie) ;
- ce que la personne sait faire (ex. signature manuscrite).

[44] INSTRUCTION N°SG/DSSIS/2016/309 du 14 octobre 2016 ; Cette instruction adresse la sécurité sous l'angle de l'organisation et des infrastructures générales, et permet ainsi d'imposer le minimum de sécurité aux infrastructures avec lesquelles sont ensuite implémentées les processus métier manipulant les données de santé.

[45] www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

[46] Exigences fixées dans le référentiel d'authentification des acteurs de santé (décembre 2014). La révision, en cours, de ce référentiel ouvre la possibilité de mise en place d'une authentification renforcée (en lieu et place d'une authentification forte) dans certains contextes, tout en confirmant que l'authentification simple par identifiant /mot de passe est insuffisante dans les zones en libre accès.

Si un seul facteur est vérifié, l'authentification est considérée comme **simple**.
Parmi les solutions d'authentification forte (à double facteur) :
- usage d'un certificat de personne physique (sur carte à puce, sur clé cryptographique, ou sur un poste de travail fixe ou mobile *après enrôlement du poste*), couplé avec code PIN ;
- usage d'un dispositif de reconnaissance vocale, faciale ou digitale, couplé avec code PIN.

Dans ces conditions, les établissements de santé qui ont mis en place des accès au SIH exclusivement avec des identifiants/mots passe ne respectent pas le référentiel d'authentification de la PGSSI-S et se trouvent donc dans une situation de non-conformité par rapport aux règles en vigueur.

3.3.1.2 Concilier la facilité d'usage et la sécurité des mots de passe

Tel que décrit dans le chapitre précédent, le SIH est composé de multiples applications « métier » pour lesquelles les contraintes de construction des identifiants et mots de passe ne sont pas complètement harmonisées, ce qui oblige l'utilisateur à retenir plusieurs mots de passe robustes.

A cette multiplicité des mots de passe, pesante pour les professionnels, s'ajoute, en l'absence de solution d'authentification unique (SSO[47]), la saisie plusieurs fois par jour de ces identifiants et mots de passe requis.

La mise en place d'une solution de SSO facilite le renouvellement automatique et régulier des mots de passe dans les applications, et **permet à l'utilisateur de n'avoir à mémoriser qu'un seul mot de passe robuste.** Elle représente toutefois un coût d'achat, de déploiement et de maintenance ; sans oublier la charge humaine récurrente nécessaire pour tester les jeux SSO lors de la mise en place de toute nouvelle version d'application.

Selon l'atlas SIH 2014 : *23% des établissements disposent d'une solution de SSO.*

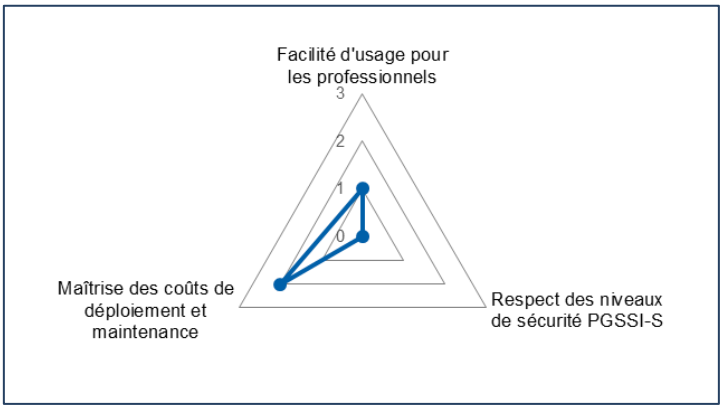


Figure 1 : évaluation du modèle identifiant /MDP avec SSO au regard du triptyque usage / coût / sécurité

Des initiatives se développent également pour faciliter l'authentification des professionnels qui ont besoin d'accéder aux données de santé en utilisant des postes partagés, telle que l'utilisation du badge d'établissement, en mode sans contact, dans le cadre d'une session ouverte après authentification par mot de passe.

[47] SSO = Single Sign On

Exemple du Centre Hospitalier Métropole Savoie à Chambéry **:**

La création du nouvel hôpital à Chambéry a fait émerger l'opportunité de sécuriser les accès physiques au sein de l'établissement. C'est dans ce contexte que le CH Métropole Savoie s'est engagé dans un projet de gestion des identités et des accès (IAM) s'appuyant sur un méta-annuaire, des badges d'authentification et une solution SSO. Porté par la direction générale, ce qui a permis l'implication forte de l'ensemble des directions concernées, le projet a connu un rythme de déploiement soutenu en 2015 sous la contrainte d'ouverture du nouvel hôpital à fin 2015. Plus de 5000 badges ont été déployés, dont 1500 pour des professionnels non-salariés de l'établissement (médecins, ambulanciers, prestataires externes). Hormis les prestataires externes sans contrat, tous les autres professionnels disposent de badges nominatifs personnalisés (identité et code couleur correspondant à la profession), permettant l'identification visuelle, gérant les accès physiques aux locaux et parkings, la récupération des tenues professionnelles (distributeur automatique), l'utilisation du système pneumatique, le paiement du self ou l'authentification sur le système d'information.

Concernant la fonctionnalité SSO, les connexions se font via une identification sans contact (technologie MIFARE). Deux modes d'utilisation coexistent :

1) **les postes «mono-utilisateur»** : connexion nominative au postes de travail et aux applications

2) **les postes «kiosque»** (partagés par plusieurs utilisateurs) : La connexion est générique sur le poste de travail, mais le passage du badge nominatif permet d'ouvrir les applications avec ses identifiants personnels.

Les sessions restent actives pendant 12h avec nécessité de s'authentifier de nouveau au-delà de l'échéance des 12h par saisie des identifiants réseau. Des lecteurs sans contact sont largement déployés sur les postes de travail fixes ou mobiles.

3.3.2 Un usage encore très limité des dispositifs d'authentification à double facteur

Moins de 10% des établissements semblent avoir mis en œuvre un dispositif d'authentification à double facteur. Ces établissements se sont généralement orientés vers des supports de type carte à puce couplée à un code PIN.

L'étude n'a pas permis d'observer d'établissement utilisant des *tokens* (clés USB cryptographique), d'autres supports physiques, ou d'autres dispositifs d'authentification forte.

3.3.2.1 Une authentification à double facteur utilisant la carte à puce

Le recours à la carte, pour les établissements qui en ont fait le choix, semble tenir aux avantages identifiés de ce support :

- Il peut inclure des **fonctionnalités sans contact** qui facilitent **l'accès au SIH en situation de mobilité** (accès via un poste sur chariot dans les unités de soins par exemple) et **l'usage domotique** (accès physique aux locaux ou au parking par exemple), cette diversification des usages de la carte favorisant l'appropriation par l'utilisateur et la mutualisation des coûts de gestion des supports ;
- Il peut **contenir des données visuelles** (nom de l'établissement, nom du professionnel, photo..) et donc servir d'identification visuelle ;

- Il supprime la gestion des mots de passe complexes (le code PIN est composé de 4 chiffres faciles à mémoriser et qui n'ont pas besoin d'être renouvelés fréquemment) et permet une **meilleure maîtrise des risques** ;
- Il constitue pour l'établissement un support **peu couteux et éprouvé**[48].

Ce choix permet donc de mieux concilier la facilité d'usage pour le professionnel et le respect des exigences de sécurité à un coût qui demeure raisonnable.

3.3.2.2 Différents types de cartes, dont le niveau de conformité à la PGSSI-S n'est pas égal

L'étude a permis d'observer plusieurs modèles de fonctionnement :

- **L'usage de cartes à puce intégrant un certificat de l'IGC de l'établissement**

Exemple du CHRU de Lille **:**
En 2007, le CHRU de Lille constatait la **nécessité de moderniser la gestion des accès physiques** (parking, accès aux bâtiments) et des **paiements à la cantine**, d'une part, et le besoin urgent de **sécurisation globale du SIH**, d'autre part. Partant de ce constat, l'établissement s'est engagé dans un projet **visant à sécuriser le contrôle d'accès informatique**, dans le respect du décret de confidentialité et de la loi informatique et libertés, au travers d'une **carte d'établissement unique multi-usage**.

Le **CHRU souhaitait garder la maitrise de son parc de cartes** et de la **personnalisation des cartes** (visuel, fonctionnalité sans contact) et comptait embarquer à terme les certificats logiciels émis par le GIP-CPS dans ses propres cartes à puce d'établissement (conformité aux textes envisagés à la suite du décret de confidentialité) en sus du **haut niveau de sécurité déjà garanti par la mise en place d'une IGC interne à l'établissement** pour la production des certificats intégrés dans les cartes.

Partant sur un déploiement massif de 12 000 cartes (dont 6 500 utilisateurs informatiques) sur la période 2009 – 2010, le projet s'est articulé autour de quatre grands axes :

- une **organisation transversale** d'identification et de délivrance des cartes impliquant la DRH, la DSI et le équipes d'encadrement des services ;
- un **méta-annuaire d'établissement** (de personnes, des droits et des affectations) ;
- des **cartes à puce** multi-usages (parking, self, bâtiments sécurisés), ergonomiques et sécurisées ;
- un **environnement sécurisé** par un serveur de sécurité et une solution SSO.

Cette expérience acquise par le CHRU de Lille de mise en place d'un projet de gestion des identités et des accès (IAM) avec une carte à puce d'établissement a servi ensuite à plusieurs établissements.

- **L'usage des cartes de la famille CPS**

Les cartes CPx (CPS, CPE,...) sont utilisées de manière généralisée dans une soixantaine d'établissements de santé[49], dont huit CHU.

[48] La carte à puce (à microprocesseurs) est utilisée depuis plus de 30 ans et est considérée comme un support ayant un très bon niveau de sécurité (usage dans le domaine bancaire, etc).

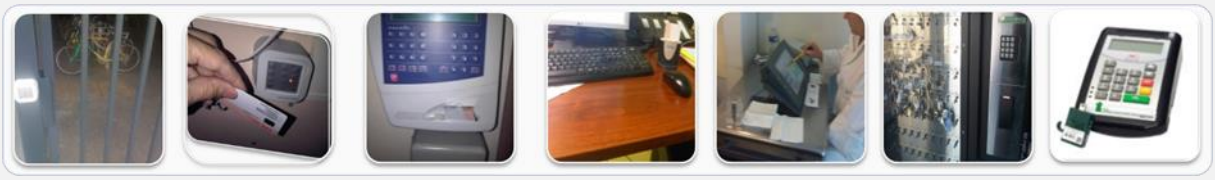
[49] Dans les autres établissements, les cartes CPx sont utilisées via un sous-ensemble de postes ciblés pour permettre à quelques professionnels d'accéder à certains téléservices,

***Exemple du CHU d'Angers* :**

Le CHU d'Angers a opté pour les cartes CPx pour le contrôle d'accès au SIH depuis 2003, après avoir déjà déployé les cartes pour le badgeage (gestion des temps) en 1998 et pour le paiement des repas du personnel en 2001. La stratégie a reposé sur deux principes : équiper l'ensemble des intervenants du CHU de carte CPx et multiplier les services rendus par la carte. Le contrôle d'accès physique aux zones protégées en 2011, aux parkings en 2013 puis aux nouveaux vestiaires et garages à vélos en 2016. En 2014, plusieurs fonctionnalités ont été déployées : paiement élargi à la cantine de l'internat, accès à l'armoire à clefs des services et des véhicules du CHU, et lecture et mise à jour des cartes vitales. Enfin en 2016, la gestion des FSE.

En 2016, l'ensemble des bâtiments restés ouverts la nuit ont été sécurisés avec la carte CPS.

L'objectif fixé en 2017-2018 est que l'ensemble des bâtiments du CHU soit accessible de nuit par carte CPS et remplacer progressivement les digicodes, en fonction de la criticité d'accès, par un lecteur de carte CPS.



L'accès au SIH repose sur une solution de gestion des identités et des accès (IAM). Son interface avec la gestion des ressources humaines permet de gérer en temps réel les accès aux applications métiers autorisées à travers un SSO installé sur l'ensemble des postes. De plus, l'ensemble des personnes ayant accès au SIH y sont enregistrées, rémunérées ou non par le CHU. L'atout majeur étant que les droits d'accès au SIH sont automatiquement verrouillés lorsque la personne quitte l'établissement.

Trois modes d'utilisation ont été définis, qui permettent de prendre en compte les différents cas d'usages dans les services:

1) Les **postes « dédiés » (bureaux, points d'accueil, salles de consultations et salles de réunions)** équipés d'un lecteur de carte à puce avec contact. La **session de travail Windows ouverte est la session personnelle** de l'utilisateur et le temps de changement d'utilisateur est inférieur à deux minutes.
2) **Les postes partagés « classiques » ou postes « kiosques » (unité de soins, salle de réveil, bloc opératoire)** avec des changements d'utilisateur qui peuvent être très fréquents. Ils sont équipés d'un lecteur de carte à puce avec contact et la **session de travail Windows ouverte est « générique »** ; ce qui permet de réduire le temps de changement utilisateur **en dessous de 6 secondes.**
3) Les postes partagés avec lecteur sans contact et itinérance de session (urgences, réanimation chirurgicale, réanimation médicale, néonatalogie, stérilisation centrale, et tous les PC des secteurs d'urgences situés au chevet du patient ou dans la zone géographique proche). Les changements d'utilisateur peuvent être très fréquents sur un même poste. Ils sont équipés d'un lecteur de carte à puce BI-MODE à la fois contact et sans contact. Tous les moyens envisageables sont mis en œuvre de manière à limiter au maximum la manipulation de la carte par les utilisateurs et ne pas les gêner dans leur travail. En particulier l'itinérance de session : l'utilisateur ne saisit son code PIN qu'une seule fois par vacation pour ouvrir une session ; par la suite, il lui suffit de présenter sa carte (en mode contact ou sans contact) et la session est déverrouillée. Il n'a pas besoin d'entrer à nouveau son code PIN. Le temps de changement d'utilisateur **est inférieur à 6 secondes.**

Le **CHU d'Angers gère un parc de plus de 10 000 cartes de la famille CPS**.

La solution carte à puce avec une IGC propre à l'établissement offre un bon niveau de sécurité et est conforme à la PGSSI-S (palier 2) pour l'authentification dans un contexte privé. Mais **elle ne permet pas l'authentification publique (palier 3) pour l'accès direct aux téléservices nationaux, au même titre que les cartes CPx.**

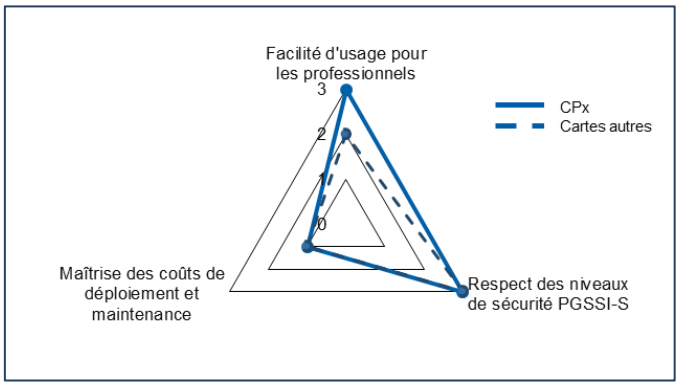


Figure 2 : évaluation des modèles « carte à puce » avec SSO au regard du triptyque usage / coût / sécurité

Le coût lié à l'acquisition des cartes[50] est relativement faible comparativement au coût des lecteurs[51], lui-même relativement minime par rapport à l'investissement lié à l'intelligence qui entoure le dispositif, en particulier le méta-annuaire et la solution SSO.

Quoi qu'il en soit, **le dispositif d'authentification s'inscrit dans un contexte organisationnel et technique global qui concourt à la bonne gestion de la sécurité du SI**.

Deux points de vigilance : remettre le dispositif d'authentification au bon professionnel, et responsabiliser celui-ci lors de la délivrance de son moyen d'authentification.

3.3.2.3 Les freins à l'usage généralisé des cartes CPS en établissement vus par la DSI…

Les raisons majoritairement invoquées comme freins à l'usage de la CPS sont les suivantes :

1. La dépendance à un tiers dans le processus de délivrance et de personnalisation des cartes

Les cartes achetées par l'établissement auprès d'un industriel apportent à l'établissement une plus grande maîtrise et réactivité dans le processus de délivrance et de gestion des cartes.

Elles peuvent être personnalisées comme l'établissement le souhaite pour tenir compte des dispositifs existants (ex : lecteurs utilisés pour le parking, le self…) et de la charte graphique voulue par l'établissement (logo de l'établissement, choix des fonctions et des couleurs…).

Par ailleurs, la délivrance des cartes CPS pour les professionnels de santé encore enregistrés avec un identifiant ADELI, tels les infirmiers, pâtit d'un circuit non optimisé mais nécessaire au contrôle des données d'enregistrement réalisé par les ARS (cette situation étant considérée comme provisoire, puisque ces professions ont vocation à rejoindre le RPPS).

Enfin, si le téléservice TOM amène un premier niveau de services en facilitant les demandes en ligne de cartes CPx et la gestion du parc de cartes de l'établissement, il lui manque certaines fonctionnalités permettant de couvrir l'ensemble des besoins, notamment une interface de type web services pour faciliter les commandes et résiliations automatiques de cartes en volume, depuis le SIH.

[50] Pour des volumes conséquents : compter environ 1€/ badge et 5 €/ carte à puce du commerce

[51] Pour des volumes conséquents : compter moins de 10€/ lecteur monofente et environ 50€/lecteur bi-mode (avec et sans contact)

2. La méconnaissance de l'ensemble des bénéfices apportés par la carte CPx :

Ces bénéfices d'usage, il convient de le rappeler, sont de trois types :
La carte CPS : « 3 cartes en une »

- une carte **« d'identité visuelle »** qui comprend le nom du professionnel, l'identité de la structure, le logo de l'ordre professionnel, et qui peut être personnalisée par l'établissement avec la photo du porteur ;
- une carte **« d'identité professionnelle électronique »** embarquant les données d'identification nationale RPPS/ADELI des professionnels de santé ;
- une carte **« d'authentification et de signature »**, **dispositif hautement sécurisé** par une composante cryptographique comprenant les certificats électroniques d'authentification ou signature.

Fonctionnalités *avec* ou *sans* contact :

- les cartes CPx permettent de mettre en œuvre **l'authentification forte** du professionnel et la signature numérique, **en mode contact** pour réaliser pleinement les opérations cryptographiques permettant de sécuriser le partage et l'échange d'informations médicales à caractère personnel, et ainsi être **référencées dans le palier cible (palier 3) de la PGSSI-S** ;
- elles permettent également l'authentification de la carte **en mode *sans-contact*** (lecture de la carte à moins de 5 cm du lecteur) pour faciliter **l'usage de la carte en situation de mobilité** du professionnel au sein d'une organisation de santé, avec des terminaux partagés, dans le cadre d'une session de quelques heures et initialement ouverte dans le cadre d'une authentification forte. Le mode *sans contact* facilite également les usages de la carte CPS pour sécuriser les accès physiques (parking, locaux) et la généraliser en tant que **carte multi-services**.

La CPS sert également de titre fondateur pour enrôler des terminaux (tablette, téléphone portable, etc.) et faciliter ensuite l'authentification directe via ces terminaux sans avoir à utiliser la carte CPS**.**

Fin 2017, la carte évolue avec l'intégration de la technologie *Mifare* au niveau de la puce et l'ajout d'un code barre correspondant à la valeur de l'identifiant national du porteur.

Plus de soixante établissements de santé (dont huit CHU) ont généralisé l'usage de la carte CPS/CPE dans leur établissement, pour sécuriser l'accès au système d'information hospitalier et aux SI externes, et parfois sécuriser également les accès physiques (locaux, parking…) utilisant la CPx comme une carte multi-services. **Leur expérience reste insuffisamment connue et partagée**.

3. Un coût important lié au manque d'intégration native par les applications du SIH et à la nécessité d'équiper les postes de lecteur de cartes

Très peu d'applications métier (ex : DPI) sur le marché intègrent nativement les cartes CPx, ce qui oblige l'établissement à **s'équiper d'une solution de SSO** et représente donc un coût d'investissement et un coût récurrent (maintenance du SSO, nécessité de tester à nouveau les jeux SSO lors de la mise en place de toute nouvelle version d'application).

La carte CPS s'utilise avec un lecteur de cartes. Lorsque les postes n'en sont pas nativement équipés, l'établissement doit investir dans l'achat de lecteurs mono-fente permettant l'authentification avec *contact*, et bi-mode si l'utilisateur a besoin d'accéder à la fois en mode *contact* et *sans contact*. Cela peut représenter un coût humain[52] et financier[53] important pour les établissements de taille importante, équipés de plusieurs centaines de postes.

[52] Installation des postes

4. La perception d'une véritable « marche à franchir » non prioritaire

Passer d'une authentification par identifiant/mot de passe (le plus souvent non conforme à la PGSSIS) **à la mise en place d'une authentification forte par carte CPS est un projet d'envergure**.

Il amène à reposer les règles de la gestion des identités, des habilitations et des accès, oblige l'établissement à s'équiper d'une solution de SSO et de lecteurs de cartes, à potentiellement mettre en place des dispositifs pour faciliter la persistance de session utilisateurs dans les contextes de mobilité, le verrouillage de session…, à optimiser son réseau (WIFI) et enfin à gérer un parc de cartes CPS, le tout dans un délai contraint pour faciliter l'adhérence et l'usage (déploiement « monolithique »).

Le déploiement généralisé de cartes d'établissement (quelles qu'elles soient) représente donc un investissement humain et financier conséquent hors de portée d'une grande majorité d'établissements qui maintiennent un dispositif d'authentification en identifiant/mot de passe.

Selon l'atlas SIH 2017 : *en moyenne 0,73% des ETP sont dédiés au SIH/Total en 2015 et 1,70% des charges d'exploitation SIH/ Total sur la même année.*

5. Absence de constance de la politique publique

Jusqu'en 2009, les pouvoirs publics ont favorisé l'usage des cartes CPx pour sécuriser l'accès aux systèmes d'information de santé, qu'ils soient internes en établissement de santé ou externes, et pour accompagner la mise en application du décret de confidentialité du 15 mai 2007. Cette volonté s'est concrétisée par :

- la publication du *guide méthodologique de mise en œuvre de la carte CPS dans les établissements public de santé* (Ministère de la santé, septembre 1998) ;
- l'étude menée par le GIP-CPS[54] en 2006 avec des établissements de santé et des éditeurs de SIH pour préciser les modalités d'utilisation de la carte CPx dans le contexte d'un établissement. Cette étude a servi à spécifier les évolutions de la carte CPx, notamment pour l'ajout de la fonctionnalité « sans contact » ;
- le programme d'accompagnement 2007-2009 à la mise en œuvre du décret de confidentialité, piloté par la DHOS[55], avec l'appui du GMSIH[56] et du GIP-CPS, et qui a impliqué une vingtaine d'établissements pilotes et favorisé la diffusion de bonnes pratiques en matière de sécurité en région ;
- le financement de quelques projets de gestion des identités et des accès SIH par carte CPx dans le cadre du programme Hôpital 2012.

Ces priorités n'ont pas été maintenues ensuite compte-tenu du faible usage des téléservices, de la nécessité d'amener les établissements à un premier palier de maturité vis-à-vis de la sécurisation de leur système d'information[57], de la volonté de prioriser les investissements sur l'information de leurs processus métier[58], puis de la prise en considération de l'émergence de dispositifs d'authentification complémentaires à la carte CPx.

---

[53] Pour des volumes conséquents : compter moins de 10€/ lecteur mono-fente et environ 50€/lecteur bi-mode (avec et sans contact)

[54] Les activités du groupement d'intérêt public carte de professionnels de santé (GIP-CPS) ont été reprises par l'ASIP Santé

[55] La DHOS était la direction de l'hospitalisation et de l'offre de soins, son périmètre s'est élargi pour devenir la direction générale de l'offre de soins (DGOS).

[56] Les activités du groupement pour la modernisation des systèmes d'information hospitalier (GMSIH) ont principalement été reprises l'ANAP, mais aussi pour partie par l'ASIP Santé sur les sujets d'interopérabilité et sécurisation du SI notamment.

[57] Voir les prérequis Hôpital numérique (P1. Identités et mouvements ; P2 – fiabilité et disponibilité – P3- confidentialité)

[58] Voir les 5 domaines prioritaires retenus dans le cadre du programme Hôpital numérique.

6. Autres raisons évoquées

Même si depuis plusieurs années l'ASIP Santé a simplifié l'usage des composants logiciels[59] nécessaires à l'utilisation des cartes CPS, **certains établissements gardent le souvenir de difficultés de fonctionnement** (configuration des postes, fonctionnement des lecteurs, utilisation difficile avec des postes Mac...) souvent associés à l'utilisation conjointe de la carte CPS et de la carte Vitale.

Le **non référencement RGS**** des technologies d'authentification et de signature proposées par l'ASIP Santé représente également un frein à leur déploiement au sein des établissements de santé (par exemple pour la dématérialisation des titres de recette, des mandats de dépense et des bordereaux récapitulatifs, dans le cadre du projet PES V2), qui doivent opter pour d'autres solutions, éventuellement plus coûteuses, pour diversifier les usages.

L'utilisation de certains types de terminaux (tablette, téléphone) est aussi évoquée comme un frein puisqu'il n'est pas possible ni ergonomique d'installer un lecteur de carte sur ce type de terminal. Toutefois, ces terminaux restent peu déployés ; des solutions alternatives existent (enrôlement du terminal avec la carte CPS) bien que peu connues par les établissements de santé.

L'ensemble de ces freins reflète le point de vue de la DSI, à l'opposé du point de vue du professionnel utilisateur d'une CPS.

3.3.2.4 …. et les avantages vus par le professionnel.

La carte CPS est considérée comme **simple d'utilisation par les professionnels utilisateurs**.

Le **code PIN à 4 chiffres est apprécié** (au regard d'identifiants/mots de passe compliqués à mémoriser et à renouveler), tout comme la **fonctionnalité sans contact** de la carte qui facilite les accès en situation de mobilité au sein de l'établissement. Les professionnels sont généralement déjà habitués à l'utilisation d'un badge pour les accès domotiques et adhèrent facilement à ce nouveau support carte.

La CPS est reconnue comme un outil très sécurisé, délivré par un « organisme national » et qui permet de favoriser la bonne traçabilité de l'accès aux données de santé dans le SIH. Elle **permet également de conserver le même dispositif d'authentification lors de l'accès aux téléservices** régionaux et nationaux qui proposent ce type d'authentification.

L'usage de la carte CPS en tant que carte multi-services (pour les accès au SIH et les accès domotiques) facilite l'appropriation du support et évite les oublis. Toutefois, certains utilisateurs craignent que l'usage domotique ne dénature la perception de la carte CPS par le professionnel de santé : **sa carte CPS est avant tout un titre sécurisé pour la protection des données de santé**.

3.3.3 Une demande croissante d'accès au SIH en dehors de l'établissement

On observe un **besoin croissant** pour les professionnels de pouvoir accéder au SIH en dehors de l'établissement. Les professionnels concernés et les cas d'usage restent cependant encore limités. Il s'agit principalement de professionnels ayant une activité dans l'établissement, tels les agents ayant une fonction technique ou professionnels de santé (imagerie par exemple) d'astreinte ;

[59] L'utilisation des cartes de la famille CPS nécessite d'installer les composants logiciels Cryptolib CPS (version 5) mis à disposition gratuitement par l'ASIP Santé. L'ASIP Santé délivre un « pack établissement » facilitant la mise en œuvre de la carte CPx sur des postes administrés. Plusieurs guides techniques aident à la mise en œuvre des composants logiciels et l'utilisation des cartes CPS dans des environnements variés : manuel d'installation et d'utilisation de la Cryptolib CPS, guide de mise en œuvre d'un smartcard logon Windows avec une carte CPS, guide de mise en œuvre de la Cryptolib CPS en environnement TSE/Citrix, guide de mise en œuvre d'une authentification forte par carte CPS sur une application Web, guide de mise en œuvre de la partie sans-contact de la Carte CPS.

L'accès se fait majoritairement sur demande du professionnel, avec attribution d'un PC portable d'établissement équipé d'un Virtual Private Network (VPN) et éventuellement d'un lecteur de carte, avec un accès limité uniquement aux applicatifs nécessaires.

Les usages observés étant encore récents et limités, le mode d'authentification est le même que celui utilisé en interne. Mais devant la demande croissante, des établissements entament des réflexions pour faciliter les usages en ouvrant davantage l'accès depuis l'extérieur :

- solutions d'authentification forte spécifiques (type OTP), pour permettre l'usage sur des postes personnels non gérés par l'établissement ;
- extension de DMZ[60] afin pour permettre plus de connexions en simultané.

3.3.4 Un besoin avéré d'accompagnement pour la mise en œuvre

3.3.4.1 Un projet qui se doit d'être soutenu par la direction de l'établissement

Compte tenu des enjeux de sécurité[61] et de la multiplicité des directions et services impliqués dans la gestion des identités et des habilitations, **ce type de projet doit être fortement soutenu par la direction de l'établissement (directeur et président de CME). Le corps médical et soignant est particulièrement concerné par la protection des données de santé des patients** qu'il prend en charge.

De plus, la notion de sécurisation des accès s'applique, en théorie, aux lieux physiques (locaux), aux équipements et machines et au système d'information hospitalier. La réflexion liée à la mise en œuvre doit porter, dans tous les cas, sur :

- le caractère a priori ou a posteriori du contrôle ;
- le dispositif de contrôle (visuel badge d'identité, caméra de surveillance), physique (serrure, etc.) ou logique (Identifiant/mot de passe, etc.) ;
- les processus et l'organisation permettant d'en assurer la réalisation.

En pratique, la stratégie et les décisions ont très souvent été conduites de manière indépendantes (entre lieux physique, équipements et SI) et les processus de contrôle qui en résultent font intervenir des acteurs différents :

- direction des services généraux et/ou services techniques et/ou sécurité des sites pour les accès aux locaux et aux équipements ;
- direction des systèmes d'information pour les accès aux SI.

A l'inverse, **les projets importants de déménagement, travaux et restructuration des locaux (incluant un volet sécurisation) représentent un élément déclencheur d'une réflexion visant à mutualiser les stratégies d'accès aux locaux et au SIH.** Mutualisation qui se traduit également par un portage de projet, au niveau supérieur, par la direction d'établissement. Ce point est important car il est garant d'une impulsion diffusée auprès de l'ensemble des professionnels et d'une meilleure adhésion au projet ; la direction des systèmes d'information n'étant plus seule à porter le projet.

Enfin, la réflexion commune « physique / logique » s'avère incontournable au regard de la corrélation faite entre les paliers de sécurité de la PGSSI-S et la protection des accès physique. (Le palier 1 n'étant acceptable que lorsque l'accès aux postes de travail est contrôlé ou régulé physiquement).

[60] Zone démilitarisée : zone isolée du réseau local, hébergeant des applications mises à disposition à l'extérieur.
[61] Gestion des risques numériques relatifs à la confidentialité des données de santé du patient

Les exigences de protection[62] de l'accès aux bâtiments sensibles dans le cadre de la lutte contre le terrorisme s'ajoutent à ces réflexions.

Exemple de l'AP-HP **:**

En 2015, l'AP-HP choisit la carte CPS comme dispositif d'authentification dans le cadre de son projet de gestion des identités et des accès (IAM) et dans la perspective d'en faire un **support multi-usages.**
La mise en œuvre du **Plan Vigipirate** en 2014 et le renforcement de la vigilance en région Ile-de-France suite aux attentats de 2015 **accélère le déploiement de cartes CPS/CPE**, avec décision de renforcer l'identification physique du personnel en ajoutant sur la carte la photo d'identité du porteur (sécurisation du processus avec un dispositif anti-falsification). Le **projet est suivi de près par la Direction Générale de l'AP-HP**.

En moins d'un an (2016), l'AP-HP a **sensibilisé son personnel** et **l'a équipé d'une carte CPS/CPE personnalisée avec photo** : 70 000 personnes, réparties dans 43 établissements et pôles d'intérêt commun.
Ce déploiement a été permis par la forte mobilisation coordonnée de l'AP-HP, de l'ASIP Santé, de l'ARS Île-de-France, et du conseil national de l'ordre des médecins (CNOM), ces deux dernières entités étant impliquées respectivement dans la validation et la mise à jour de données d'identification nationale des professionnels de santé (ADELI et RPPS) intégrées dans les cartes CPS.

Au bilan, les cartes CPx permettent à l'AP-HP de concilier :
- le **renforcement de l'identification physique** de son personnel
- **l'accès sécurisé aux télé-services de la sphère santé et au système d'information interne**, dans le cadre d'un projet global de gestion des identités et des accès via une solution d'authentification unique SSO (dans ce cadre, l'annuaire d'entreprise AP-HP est adossé à l'annuaire santé national) ;
- **l'homogénéisation des badges et cartes d'accès** pour ses personnels (accès aux hôpitaux, parking, locaux sensibles, paiement des repas).

3.3.4.2 Un retour d'expérience instructif sur le niveau d'accompagnement nécessaire à la mise en œuvre

Soucieuse de la protection des données de santé, l'agence régionale de l'hospitalisation (ARH) du Limousin a soutenu[63] un projet visant à déployer dans l'ensemble des établissements publics et privés de la région, réunis au sein d'un groupement d'achat :

- un annuaire d'établissement centralisant les acteurs (identité, activité, rôle), synchronisé avec le SI RH et le fichier de structure de l'établissement (pour la récupération des données RH et d'activité) et interfacé avec l'annuaire régional existant ;
- une gestion centralisée des droits d'accès et habilitations et une synchronisation avec les référentiels applicatifs métiers ;
- une solution de sécurisation des accès par carte CPx et SSO et une gestion coordonnée des cartes CPx et des comptes.

[62] Voir annexe 1 de l'instruction N° SG/HFDS/2016/340 du 4 novembre 2016 relative aux mesures de sécurisation dans les établissements de santé
[63] Cet ambitieux projet a été partiellement financé dans le cadre du Plan Hôpital 2012.

L'ARH s'est appuyée sur le GIP SILPC[64] et le GCS eSanté Limousin pour la coordination du projet (31 établissements) - étude préalable, acquisition, etc.-. Le GIP SILPC a réalisé l'accompagnement spécifique des dix-neuf établissements publics dans la mise en œuvre du projet. **L'accompagnement, à partir du socle d'outils commun (annuaire et SSO), s'est construit autour d'un vrai projet personnalisé de gestion centralisée des identités et des accès s'appuyant sur des méthodes mutualisées :**

- état des lieux initial pour cartographier les référentiels, les applications et leurs contextes d'utilisation, les identifiants et connaître l'organisation interne ;
- définition d'une politique d'habilitation commune validée institutionnellement et mise en place de processus d'information adaptés ;
- « nettoyage » et mise à niveau des référentiels d'authentification existants ;
- mutualisation des travaux avec les éditeurs et prestataires impliqués pour la synchronisation.

Un accompagnement personnalisé qui a pu s'étendre entre six mois et jusqu'à plus de dix-huit mois par établissement selon la taille et le parc applicatif existant[65], et impliquant nécessairement l'ensemble des acteurs de l'établissement. Ce projet de gestion centralisée des identités et des accès **a permis également le déploiement des cartes CPx et d'un dispositif d'authentification forte et de SSO dans tous ces établissements accompagnés et pour toutes les applications.** La mise en place du SSO étant spécifiquement adaptée aux cas d'usage des postes et applications dépendant du contexte d'utilisation (kiosques, urgences, admissions, etc.)

La réussite du déploiement est ainsi conditionnée par le soutien de la direction générale (qui facilite les arbitrages et porte la communication), **l'implication d'une équipe projet pluridisciplinaire** (ressources humaines, encadrement soignant, SI, etc.) et par **un accompagnement professionnalisé, à la fois en matière d'assistance à maîtrise d'ouvrage (AMOA)**[66] (pour les chantiers organisationnels et de conduite de changement) et de maîtrise d'œuvre (**MOE)** (dans les étapes d'intégration, pour l'adaptation aux cas d'usage par type de poste, etc.).

La réussite d'un tel projet porte surtout dans sa capacité à simplifier les processus et les usages et à limiter l'obsolescence des référentiels métiers. En effet, *« du fait d'un turnover important et des difficultés de communication des mouvements de personnels internes et externes, on observe souvent qu'entre 1/3 et la moitié des comptes actifs sont « périmés » et la perte en qualité est de 5 et 10% chaque année ».*

3.3.4.3 Un besoin d'accompagnement des éditeurs

Les entretiens menés avec les éditeurs de dossier patient informatisé (DPI) et de solutions de gestion des identités et des accès (Identity Access Management – IAM) font apparaitre que **les référentiels de la PGSSI-S ne sont pas toujours connus ou lus**, et parfois pas bien compris.

L'établissement pilote seul sa stratégie d'authentification. Les éditeurs s'adaptent en général aux contextes des établissements, selon leur niveau de maturité, mais ils ne sont pas « promoteurs » de solution d'authentification.

Les éditeurs souhaitent être **mieux informés et accompagnés** sur cette thématique de l'authentification forte et sur les évolutions prévues autour des services de confiance liés à la dématérialisation des données de santé. **La mise à disposition de composants « clés en main »** permettant la mise en œuvre des dispositifs d'authentification conformes à la réglementation est souhaitée.

[64] Le GIP SILPC est un groupement d'intérêt Public intégrateur des SI Santé agissant sur tout le territoire depuis plus de 30 ans

[65] Entre 15 et 18 mois dès lors qu'on atteint une vingtaine d'applications et au-delà pour les gros établissements.

[66] AMOA disposant d'une connaissance approfondie de l'environnement des ES et de compétences méthodologiques et d'animation permettant de favoriser la prise de décision par les équipes.

En ce qui concerne l'évolution des supports envisagés pour embarquer les technologies d'authentification, les idées suivantes sont exprimées :

- le Smartphone professionnel[67] avec l'embarquement de certificats conformes et de systèmes de communication avec le poste de travail (Bluetooth, QR code lu par le smartphone) ;
- le développement des technologies RFID (en minimisant l'action de l'utilisateur) ;
- les reconnaissances biométrique et faciale.

3.3.5 Authentification auprès du SI convergent du GHT : amorce d'une réflexion

L'élaboration du schéma directeur du SI du GHT amène le GHT à se réinterroger sur les dispositifs à prévoir pour la protection des données de santé contenues dans le SI convergent. Dans un contexte où le GHT ne dispose pas d'une personnalité morale, la question du responsable du traitement se pose.

Les établissements de santé rencontrés (au deuxième semestre 2016) démarraient leur réflexion sur ce sujet.

3.4 L'authentification publique et l'accès aux téléservices extrahospitaliers : des enjeux peu pris en compte

3.4.1 L'accès aux téléservices : un déploiement récent et un usage encore naissant

Les téléservices contenant des données de santé à caractère personnel sont apparus progressivement et le **niveau de déploiement actuel est encore relativement limité,** que ce soit au regard du périmètre géographique adressé[68], du nombre de professionnels concernés[69] (CERT-DC, service de déclaration en ligne des décès ; e-DO, service de déclaration des maladies à déclaration obligatoire, qui ne concerne pour l'instant que le VIH et le Sida ; Syrenad et Cristal, services de déclaration des dons et donneurs d'organes), ou de la fréquence d'usage (E-FIT dans le domaine des incidents transfusionnels et prochainement E-Saturne, dans celui des demandes d'ATU nominatives[70]).

Les téléservices nationaux les plus déployés sont aujourd'hui les téléservices de la CNAM-TS à destination des professionnels de santé, au sens large, en exercice libéral ou salarié, et le dossier pharmaceutique (DP) qui s'est largement déployé auprès des pharmaciens. Plus de 34 millions de dossiers ont été créés et plus de 99% des officines sont équipées[71]. Le déploiement est en cours dans le secteur hospitalier. Le dossier médical partagé (DMP), dont la maitrise d'ouvrage a été transférée à la CNAMTS mi-2016, reprend sa phase de déploiement en 2017, après une première période de déploiement (2011-2012) qui avait permis la création de plus de 600 000 DMP[72], avec un raccordement de 730 structures de santé et 6 800 professionnels de santé libéraux. Le déploiement des messageries sécurisées de santé, initié en 2014 continue de progresser : 150 établissements[73] et

[67] L'usage de smartphone personnel (BYOD) n'est pas autorisé par l'ANSSI.

[68] Déploiement des téléservices nationaux dans des territoires pilotes, téléservices régionaux utilisables à l'échelle de quelques territoires,…

[69] Principalement des médecins (ou des professionnels habilités par les médecins : secrétaires médicales, externes, internes, infirmiers) et pharmaciens

[70] Téléservice de l'ANSM dont le déploiement démarre en 2017

[71] www.cnil.fr/fr/le-dossier-pharmaceutique-dp

[72] Chiffres de l'été 2016, lorsque le DMP est passé de l'ASIP santé à la CNAMTS

[73] Un chiffre qui va croitre fortement dans les prochains mois puisque plus de 500 établissements sont raccordés et donc en capacité d'envoyer des mails dans l'espace de confiance.

plus de 3 000 professionnels de santé libéraux utilisent quotidiennement l'espace de confiance MSSanté.

Au niveau régional, un certain nombre de téléservices[74] sont portés par les groupements régionaux de maîtrise d'ouvrage e-santé, sous le pilotage de l'ARS. Leur déploiement est variable d'une région à l'autre. La réforme territoriale les amène à faire converger les services proposés en région.

3.4.2 En majorité : authentification forte et directe du professionnel auprès du téléservice (portail web)

L'essentiel des téléservices sont des portails (navigateurs web), exposés sur un réseau public, sans connaissance préalable de leurs utilisateurs. Ces téléservices doivent en conséquence être conformes au **palier 3 (le plus élevé)** du référentiel d'authentification de la PGSSI-S : authentification publique, généralement sous la forme d'une authentification directe du professionnel avec sa carte CPS.

La PGSSI-S ouvre également la possibilité d'une authentification par délégation (palier 3) ou authentification indirecte (palier 2). Les modalités d'authentification sont déterminées par le responsable de traitement de chaque téléservices (après analyse de risque SSI[75], en fonction de la réglementation,…).

Les scénarios d'usage pour l'accès aux téléservices, au sein d'un établissement de santé, résultent de la combinaison des choix réalisés :

- par le **responsable de traitement** s'agissant du dispositif d'identification et d'authentification défini pour l'accès au téléservice qu'il propose ;
- et par **l'établissement,** s'agissant de sa politique SI interne (gestion des identités et des accès au SIH, architecture du SIH, accès internet, parc informatique, mise à disposition de device, communication sur les possibilités offertes).

Politique de l'établissement		
Différents choix	Accès **indirect** : architecture permettant un accès au téléservice via le SIH ou une passerelle (via un EAI[76], une solution de proxy,…)	L'architecture permet une authentification indirecte de la personne physique : **l'établissement** définit les modalités d'authentification privée du professionnel en tant que personne physique et est **responsable de garantir l'identité de la personne physique et de propager au système cette identification / authentification après qu'elle se soit authentifiée de manière publique auprès du système cible**. Il est **garant de la traçabilité de l'authentification dans le temps**.
	Accès **direct**	**Le professionnel accède directement au téléservice intuitu personae** via le web ou un web service, sous réserve de connexion internet. Il s'agit d'une authentification directe de personne physique.

[74] Services support aux actes de télémédecine, outils collaboratifs pour les réseaux de santé, ROR (Répertoire Opérationnel des Ressources), service d'orientation et d'aide au placement des patients et usagers (ex : ViaTrajectoire), …

[75] sécurité des système d'information

[76] EAI est le sigle international pour désigner l'intégration d'applications d'entreprise (IAE) ; il s'agit d'une architecture permettant à des applications informatiques hétérogènes de gérer leurs échanges.

3.4.3 Simplifier l'accès des professionnels aux systèmes d'information de santé

Compte tenu du fait que les téléservices ne sont pas intégrés à leur SIH et qu'ils se présentent principalement sous la forme de portail web avec authentification directe de l'utilisateur, les DSI des établissements ne les prennent **pas en compte dans leur réflexion d'urbanisation du SI.**

Ils ne les recensent pas, et équipent *sur demande* le professionnel qui souhaite accéder à un téléservice défini avec le dispositif d'authentification requis par l'application. C'est dans ce cadre qu'un certain nombre d'établissements disposent de quelques postes équipés de lecteurs, utilisés par les seuls professionnels de santé qui ont besoin d'accéder à un téléservice donné par carte CPS.

Dans ce contexte (faible nombre de professionnels concernés, peu d'usages), les établissements n'envisagent pas de moyen unique d'authentification adapté à l'ouverture vers l'extérieur de l'établissement.

3.4.4 Deux cas d'usage à échelle régionale et nationale

3.4.4.1 L'accès aux téléservices régionaux : exemple du portail web du GCS SISRA pour la région Auvergne - Rhône Alpes

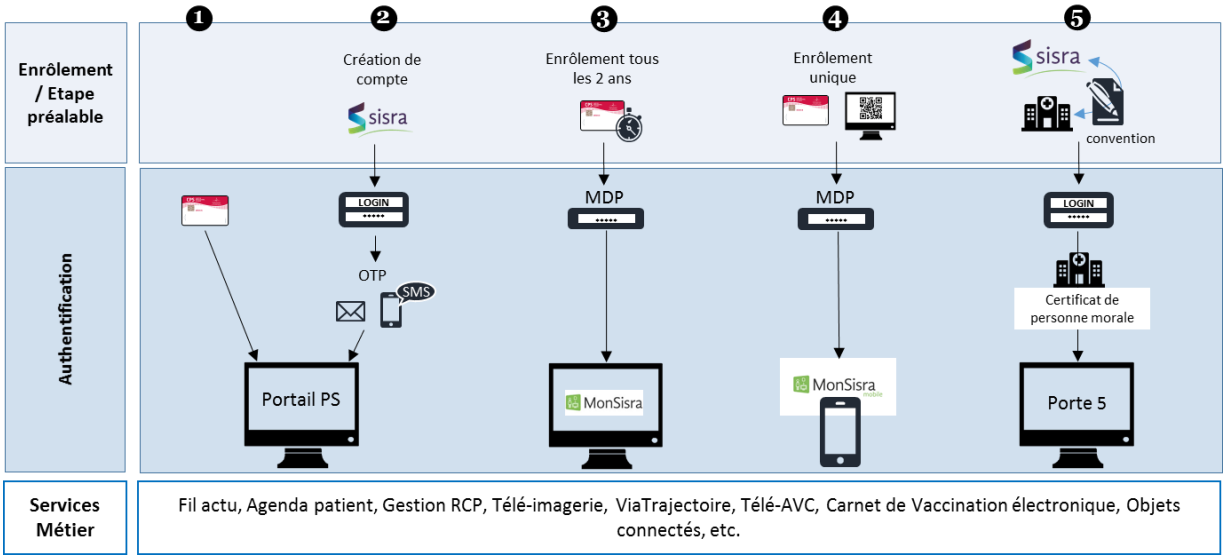
3.4.4.1.1 Fonctionnement général

Afin de faciliter l'usage des services promus dans la région Rhône-Alpes, le GCS SISRA a mis en place un portail web, porte d'entrée unique vers différents services dédiés à la pratique des professionnels de santé, quel que soit leur mode d'exercice:

- Messagerie régionale sécurisée (ZEPRA, membre de l'espace de confiance MSSanté)
- ViaTrajectoire, outil d'aide à l'orientation de patients/usagers ;
- Outil de gestion des réunions de concertation pluridisciplinaire ;
- Ainsi qu'une quinzaine d'applications métier (cf. schéma *infra*).

Le portail des professionnels de santé (qui couvre les secteurs sanitaire et médico-social) a un rôle double :

- Agrégation de contenu métier en provenance de tous les services et applications métier.
- Dispositif d'authentification unique (SSO) construit autour de différents modes de d'authentification forte :
  - ❶ Carte de la famille CPx ;
  - ❷ OTP (One Time Password, reçu par mail ou SMS), après création d'un compte;
  - ❸ Via MonSISRA, logiciel installé sur poste fixe, avec enrôlement préalable par CPx ;
  - ❹ Via MonSISRA, logiciel installé sur mobile, avec enrôlement préalable par CPx ;
  - ❺ Par l'intermédiaire d'une authentification de l'établissement employeur, en tant que personne morale, via un dispositif nommé Porte 5 ;



Modes d'authentification proposés par le GCS SISRA

3.4.4.1.2 Focus sur le dispositif « Porte 5 » d'authentification indirecte, basé sur un domaine de confiance

Les cartes CPx étant déployées dans peu d'établissements de la région, et l'utilisation d'OTP étant peu adaptée à un usage quotidien en continu, le GCS a déployé un **dispositif d'authentification indirecte** pour se connecter à la plateforme SISRA sans carte CPx, fondé sur la signature préalable d'une **convention** avec l'établissement qui s'appuie sur les critères de sécurité du programme Hôpital Numérique et une sélection de **bonnes pratiques et règles de sécurité extraites de la PGSSI-S** et nécessaires pour ce dispositif.

L'authentification indirecte amène un transfert de responsabilité entre SISRA et l'établissement de santé signataire. Lorsque le professionnel se trouve physiquement dans l'établissement de santé qui l'emploie, le dispositif permet d'accéder aux services régionaux à partir :

- **d'une authentification du professionnel de santé**. Celle-ci s'appuie sur les mécanismes internes d'authentification propres à l'établissement et permettant l'accès au système d'information local (synchronisation avec l'active directory);
- **d'une authentification de l'établissement de santé**, en tant que personne morale via un certificat de personne morale.

3.4.4.2 L'accès aux Téléservices nationaux : exemple du DMP

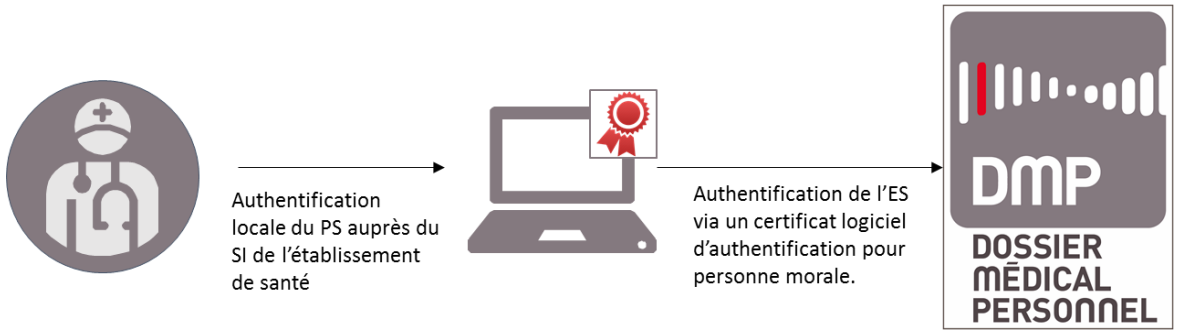
L'analyse de risque SSI faite à l'époque par l'ASIP Santé avait conduit à la mise en place d'une **authentification directe par carte CPS, ou indirecte via une solution « DMP compatible »[77], pour la *création* et *l'alimentation* du DMP,** et **d'une authentification exclusivement par carte CPS pour la *consultation* du DMP**.

En établissement de santé, l'accès au DMP peut s'effectuer, en fonction du profil d'utilisateur et de la fonction adressée (création/alimentation/consultation), en authentification directe ou indirecte de la manière suivante :

[77] Encadré dans le cadre d'un dossier fonctionnel et technique (DSFT) et d'une homologation à la « DMP compatibilité »

Fonction	Professionnels autorisés	Authentification directe	Authentification indirecte
Création	PS, Personnel d'accueil, Agent de préadmissions et admissions, Secrétaire médicale.	*Carte CPS ou CPE*	*Sous la responsabilité du chef d'établissement avec un certificat de ''personne morale''*
Alimentation	PS	*Carte CPS*	*Sous la responsabilité du chef d'établissement avec un certificat de ''personne morale''*
	Personnel habilité par l'établissement		
Consultation	PS autorisés par le patient	*Carte CPS, dans la limite d'habilitations qui dépendent de la profession et des types de document.*	

Pour l'authentification indirecte, le professionnel s'authentifie localement auprès du SIH sous la responsabilité de l'établissement, qui s'authentifie ensuite en tant que personne morale auprès du DMP en utilisant un certificat logiciel d'authentification pour personne morale émis par l'ASIP Santé.



Création et alimentation du DMP en authentification indirecte

Les responsables de traitement des téléservices nationaux et régionaux proposent généralement un nombre limité (voire unique) de modes d'authentification. Ils **privilégient l'authentification directe du professionnel aux modalités d'authentification indirecte.**

QUATRIEME PARTIE : PISTES DE REFLEXION ET RECOMMANDATIONS

4.1 Faciliter l'identification et la gestion des identités des professionnels accédant au SIH

L'identification des professionnels accédant au SIH d'un établissement de santé est un prérequis indispensable à la mise en place d'un projet de gestion des identités et des accès. Pour des raisons organisationnelles et pratiques, cette première marche vers la sécurisation des accès au SIH constitue un premier enjeu pour les établissements de santé.

4.1.1 *Guider les directions d'établissement et accompagner la mise en œuvre*

L'étude a permis de mettre en exergue le besoin des établissements d'être appuyés dans les projets d'identification et authentification des professionnels. Cela passe dans un **premier temps par la sensibilisation des directions à ces enjeux, et la mise à disposition d'orientations et de guides méthodologiques pour la gestion des identités et accès** ; orientations qui devront couvrir :

- les processus et modes d'organisation pour impulser une adhésion au changement en interne à l'établissement ;
- le référencement pédagogique des outils disponibles : accès à l'annuaire santé contenant les données d'identification nationale des professionnels de santé, accès à un annuaire métier amélioré, etc. ;
- des illustrations par des cas existants, sous forme de retours d'expérience d'établissements pilotes.

Dans ce cadre, l'ASIP Santé aide les établissements de santé (et leurs éditeurs) à adosser leurs annuaires aux référentiels d'identification nationaux des professionnels de santé RPPS/ADELI.

En 2017, l'ASIP Santé accompagnera des GHT volontaires à la mise en œuvre d'un annuaire commun du GHT synchronisé avec les référentiels nationaux, ce qui permettra, outre l'aboutissement de leur projet et la capitalisation sur l'expérience acquise, d'affiner la méthode d'accompagnement et le « kit projet », et de dessiner le plan de généralisation pour l'ensemble des établissements et l'estimation des ressources nécessaires. En parallèle de cette phase expérimentale, l'ASIP Santé prépare un programme d'appui à plus large échelle[78].

4.1.2 *Donner des orientations pour construire l'identifiant unique des professionnels du GHT*

Dans un contexte où les GHT ne disposent pas d'une personnalité juridique, en l'absence de directives clarifiées sur les modalités opérationnelles de mise en œuvre de l'identification des professionnels dans le cadre des GHT, les établissements risqueraient de s'orienter vers des solutions divergentes.

Selon la version en vigueur de la PGSSI-S, l'identifiant devrait être construit à partir du FINESS de l'établissement et de l'identifiant local. Et les réflexions actuelles, au cours des échanges avec les établissements, ont permis d'identifier plusieurs scénarios envisageables pour construire l'identifiant du professionnel, non professionnel de santé, du GHT en l'absence de FINESS juridique.

[78] Tel que fait par le passé, par exemple pour le programme MSSanté.

Aussi, pour répondre aux questionnements des établissements de santé sur les modalités d'identification des professionnels du GHT, et tout particulièrement les professionnels qui ne sont pas enregistrés dans les répertoires nationaux (RPPS / ADELI), l'ASIP Santé a publié un **modèle d'identification des professionnels du secteur santé**[79].

4.2 Converger vers des moyens communs d'authentification forte

4.2.1 *Clarifier les différentes sources réglementaires et assurer leur cohérence*

Le référentiel d'authentification de la PGSSI-S est un **document relativement récent** (version en vigueur datant de décembre 2014) dont le périmètre est restreint à la protection des données de santé, et qui constitue un document de portée règlementaire à deux titres:

- d'une part, la PGSSI-S **décline les principes** de la politique de sécurité du système d'information du ministère chargé des Affaires sociales (PSSI-MCAS) approuvée par décret en 2015 et s'appliquant[80] aux directions, services centraux, services déconcentrés et aux établissements placés sous la tutelle du ministère ;
- d'autre part, les référentiels qui composent la PGSSI-S sont cités en référence par la **loi de modernisation de notre système de santé de 2016 et ont vocation à devenir opposables en 2018**.

En revanche, aucun dispositif n'incite au respect des principes préconisés ; et aucun non plus ne permet de réguler, contrôler ou sanctionner les écarts par rapport à ces principes. Or, les pouvoirs publics ont pu constater à plusieurs reprises que l'incitation matérielle et/ou le contrôle règlementaire sont les seuls leviers qui permettent d'obtenir des résultats. L'adossement de la certification HAS aux indicateurs Hôpital Numérique en est un exemple probant.

Dans les faits, les observations de l'étude démontrent d'une part une **difficulté à faire le tri dans les différents dispositifs et injonctions qui s'appliquent aux établissements de santé**[81] ; et donc une méconnaissance du caractère injonctif du contenu de la PGSSI-S. D'autre part, on constate une méconnaissance générale des concepts définis dans la PGSSI-S avec une tendance à amalgamer son contenu avec les règles de l'ANSSI (qui ne sont qu'une composante sur laquelle s'appuie la PGSSI-S). Et lorsqu'ils sont connus et assimilés, on note également une difficulté à appliquer les concepts.

Ainsi, il apparaît important de clarifier les obligations règlementaires et le lien entre les différents dispositifs existants. De plus, l'opposabilité prochaine des référentiels de la PGSSI-S représente une contrainte règlementaire qui vient s'ajouter aux multiples règlementations existantes, obligatoires ou non (certification des comptes, certification HAS, certification ISO 15189, etc.), auxquelles les établissements de santé sont soumis. **Ainsi les pouvoirs publics devront s'assurer de la non-contradiction entre le contenu des référentiels de la PGSSI-S qui sera rendu opposable et celui des autres référentiels s'appliquant aux établissements de santé.**

[79] Le modèle d'identification des professionnels du secteur santé permet de poser des principes homogènes de gestion des identités et de partager un socle commun de bonnes pratiques permettant, à partir de concepts homogènes pour l'ensemble des acteurs, de répondre aux besoins d'attributions de droits et aux besoins potentiels de partage ou échanges d'information entre périmètres de responsabilité.

[80] https://www.legifrance.gouv.fr/eli/arrete/2015/10/1/AFSZ1523362A/jo

[81] A titre d'exemple, l'instruction d'octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information dans les établissements évoque la sécurisation des comptes par identifiant/mot de passe sans pour autant rappeler les exigences relatives à la protection de l'accès aux applications métier qui contiennent de la données de santé et qui relèvent de la PGSSI-S

4.2.2 Définir une cible commune pour l'authentification forte en établissement de santé et la promouvoir

La PGSSI-S définit aujourd'hui [82] trois paliers d'authentification :

- **le palier minimum (palier 1),** correspondant à l'authentification simple d'une personne intuitu personae au sein de la sphère privée d'un établissement ; ce palier ne s'appliquant que dans certaines conditions de contrôle d'accès physique aux postes de travail ;
- **le palier cible (palier 3)**, correspondant au niveau d'authentification forte maximal et requis pour l'authentification publique ; on distingue le palier 3 pour l'authentification *intuitu personae* (via CPx ou OTP adossé à la CPx) et celui – en palier 2 - pour l'authentification indirecte de la personne physique (sous la responsabilité du directeur d'établissement, l'authentification de la structure s'effectuant avec un certificat logiciel de personne morale de l'IGC Santé) ;
- **le palier 2,** qui correspond à l'authentification forte sous réserve de respect de règles de sécurité et d'un haut niveau de technicité par le responsable de traitement.

Sans compréhension suffisante de la politique publique et se sentant livrés à eux-mêmes dans le choix et la mise en œuvre du dispositif d'authentification des professionnels, les établissements de santé ont tendance à maintenir les pratiques existantes en proposant un accès aux applications de santé par identifiant / mot de passe quel que soit le contexte d'usage. Correspondant au palier 1, ce dispositif n'est toutefois pas conforme aux seuils de sécurité de la PGSSI-S dans plusieurs contextes d'utilisation. **Des orientations claires doivent être données aux établissements sur la cible à atteindre et les moyens matériels permettant d'y parvenir.**

Le palier 2 englobe finalement l'ensemble des dispositifs répondant aux critères de l'authentification forte au sens large (authentification à double facteur). Mais la garantie du niveau de sécurité réel nécessiterait une vérification unitaire des dispositifs d'authentification choisis par chaque établissement de santé. Ce qui exigerait des moyens importants et donc un coût pour l'ensemble de la communauté.

Ainsi, l'état se doit, dans un premier temps, de s'accorder sur un nombre limité de cibles (palier 2 et 3), en tenant compte de l'existant dans les établissements et des moyens déjà investis pour le développement et le déploiement des produits de certification de l'ASIP Santé. Il convient de rappeler que la carte CPS est aujourd'hui le seul dispositif d'authentification directe qui respecte les exigences de l'ensemble des paliers du référentiel d'authentification de la PGSSI-S, et donc permet la protection de l'accès aux données de santé quel que soit le contexte d'usage.

De plus, il apparait nécessaire de clarifier les **modalités de mise en œuvre de l'authentification indirecte du professionnel de santé**, pour les structures intéressées à s'engager dans cette voie : quels sont les engagements du directeur d'établissement ? Quelles sont les exigences à respecter dans l'établissement ? Ce mode d'authentification correspond en effet à une prise de responsabilité par l'établissement vis-à-vis de la protection des données de santé gérées dans des applications tiers, et cette prise de responsabilité se doit d'être encadrée. **Cet encadrement devrait s'appuyer sur :**

- **la matérialisation concrète des engagements dans un document de référence (par exemple dans les référentiels PGSSI-S) s'appliquant aux établissements de santé ;**

[82] Une nouvelle version du référentiel d'authentification est prévue courant 2017. Elle fait mieux faire ressortir les paliers d'authentification minimum requis selon le niveau d'exposition des données de l'application (caractéristique du réseau sur lequel est déployée l'application, caractéristique de la zone physique dans laquelle se situe le terminal d'accès, caractéristique du terminal dédié ou mutualisé entre plusieurs utilisateurs). Le référentiel conserve la distinction entre l'authentification *privée* et l'authentification *publique* du professionnel, ainsi que la dissociation entre l'authentification *directe* du professionnel à une application et l'authentification (indirecte ou déléguée) *via une personne morale*.

- **l'adossement à un dispositif de contrôle (par exemple la certification HAS) pour assurer la bonne mise en œuvre des principes en interne.**

Enfin, un programme de **promotion des dispositifs d'authentification forte, d'information et de formation s'appuyant sur un ensemble d'outils et de méthodes de conduite du changement** est également indispensable pour faciliter la compréhension et l'appropriation par les acteurs de santé.

4.2.3 Clarifier les principes d'authentification s'appliquant aux GHT, sans personne morale unique

A plusieurs reprises, la notion de « domaine de confiance » a été évoquée dans le rapport pour traduire la responsabilité de l'établissement concernant le bon usage de l'authentification dans sa sphère privée et la traçabilité de l'authentification dans le temps. **C'est le principe même retenu dans le cadre de l'authentification indirecte du professionnel** : seule la personne morale est authentifiée auprès du système d'information de santé cible, elle est responsable de l'authentification du professionnel intervenant sous sa responsabilité.

Le GHT n'étant pas une structure juridique (personne morale), la mise en place des principes d'authentification pour l'accès aux données de santé dans le cadre des GHT mérite d'être approfondie.

- Est-ce qu'une authentification publique (directe ou indirecte du professionnel) est requise lorsqu'un professionnel d'un établissement *partie* accède au système d'information du GHT (dont la responsabilité de traitement est assurée par l'établissement *support*) ?
- Comment mettre en œuvre l'authentification indirecte du professionnel de l'établissement *partie*, via le SI convergent géré par l'établissement *support*, auprès des téléservices ?

4.3 Généraliser l'authentification forte en s'appuyant sur trois leviers interdépendants

Les constats mettent en avant l'interdépendance entre les efforts réalisés par les éditeurs, les établissements de santé et les promoteurs de téléservices. Ainsi, l'assurance du respect des principes définis dans les référentiels de la PGSSI-S, qui seront rendus opposables en 2018, nécessite d'agir de façon concomitante auprès des trois catégories d'acteurs.

4.3.1 *Editeurs : assurer l'existence d'une offre industrielle répondant aux exigences*

Pour les éditeurs de progiciels de santé, l'authentification forte (rendue obligatoire par la PGSSI-S dans une majorité des contextes d'usage) représente aujourd'hui un coût financier et une contrainte fonctionnelle. Le manque d'intégration native des cartes CPx dans les offres logicielles représente un frein majeur à leur déploiement, et rend les établissements dépendants d'une solution SSO coûteuse dans le cas d'un choix de déploiement.

Il apparaît ainsi essentiel d'assurer la disponibilité, sur le marché, d'offres compatibles avec les exigences règlementaires et les moyens d'authentification forte promus par les pouvoirs publics.

Il pourrait s'agir d'un mécanisme de type label ou certification. **La labellisation des solutions d'authentification privées sur la base d'un CSPN**[83] pourrait aussi être envisagée.

[83] CSPN : Certification de sécurité de premier niveau. Un CSPN attribué par un CESTI (Centre d'évaluation de sécurité des technologies de l'information-procédure ANSSI) vérifie que le dispositif satisfait au profil de protection préalablement défini.

L'ASIP Santé doit également travailler sur le renforcement du niveau technique des API de ses modules (type Cryptolib) en favorisant la conformité aux référentiels européens et ainsi limiter le coût de mise à niveau du secteur industriel.

4.3.2 *Etablissements de santé : accompagner et encadrer la mise en œuvre*

Sous réserve de la disponibilité d'une offre industrielle répondant aux exigences, il s'agit dans un deuxième temps d'appuyer les établissements de santé dans la mise en œuvre des préconisations.

L'étude met en exergue le besoin des établissements d'être appuyés dans les projets de déploiement des moyens d'authentification forte, ce qui passe entre autres **par la mise à disposition de guides méthodologiques** visant à rappeler les enjeux liés à la protection des données de santé et relativiser la complexité réputée des modes d'authentification forte, cartes ou certificats**. Les cibles sont tout autant les DSI/RSSI que les DG et représentants du corps médical et soignant.**

Le manque de ressources internes reste le frein majeur à la progression des établissements. Et l'impact extrêmement positif de l'accompagnement des établissements réalisé par des acteurs locaux compétents, sur l'exemple de l'accompagnement des établissements par le SILPC**,** a démontré l'intérêt que des démarche similaires et autres actions d'accompagnement soient promues et soutenues par les pouvoirs publics. Un accompagnement qui se veut de proximité pour être efficace.

Il pourrait donc s'agir de renforcer les acteurs locaux en présence, qui accompagnent aujourd'hui les établissements de santé, à travers la mise à disposition de ressources et moyens supplémentaires pour se déployer sur l'ensemble du territoire. Une autre option pourrait consister à mettre en place une démarche de qualification / labellisation pour des acteurs en mesure d'accompagner les établissements de santé.

4.3.3 *Accompagner les promoteurs de téléservices dans la déclinaison des référentiels de la PGSSI-S*

Nous avons constaté que le critère « accès aux téléservices régionaux ou nationaux » représente aujourd'hui un critère mineur dans le choix réalisé par les établissements de santé. Néanmoins, leur développement et l'appétence grandissante des professionnels de santé laissent présager une pondération croissante de ce critère.

Ainsi, il est essentiel de s'assurer que de leur côté, les promoteurs de téléservices appliquent les principes, au même titre que les éditeurs et les établissements de santé, **et puissent proposer des modalités d'identification et d'authentification conformes aux référentiels de la PGGSI-S.**

Afin d'appuyer les promoteurs de téléservices dans leurs développements, l'ASIP pourrait proposer une offre de composants facilitant la déclinaison opérationnelle du référentiel PGSSI-S, et notamment l'authentification forte. Dans un premier temps, il s'agirait de promouvoir et accompagner la mise en œuvre de composants d'authentification déjà disponibles dans la «banque de composants » gérés par l'ASIP Santé, que l'agence utilise pour ses propres systèmes d'information.

4.4 Favoriser le retour d'expérience tout en améliorant la qualité des services proposés aux établissements

La carte CPS a fortement pâti de son image de complexité pour les établissements de santé.

Ainsi l'ASIP Santé doit éclairer les établissements sur les possibilités multi-usages de la carte CPx, et ainsi que sur les usages naissant des certificats logiciels de personne physique de l'IGC Santé, à travers des retours d'expérience d'établissements utilisateurs. Il s'agirait également d'introduire de façon plus systématique des démarches pilotes, sous forme de PoC, afin de disposer de ces retours d'expérience utilisateurs. Mettre en place un club utilisateurs serait également bénéfique, notamment pour mieux prendre en compte les évolutions induites par la mise en place des GHT.

De plus, l'ASIP Santé doit poursuivre ses efforts pour fluidifier la délivrance des cartes, faciliter la commande et la gestion d'un parc important de cartes, et améliorer la qualité du processus de suivi des commandes. Dans ce cadre, l'ASIP Santé a engagé des travaux visant à mettre à disposition un web service permettant de faciliter la demande et la gestion automatisée des cartes, et étudie la possibilité de simplifier le circuit de commande de cartes pour les professionnels de santé ADELI.

Par ailleurs, l'ASIP se doit de favoriser le partage d'expérience entre établissements qui utilisent ou utiliseront à terme, des solutions d'authentification autres que la carte CPS, dans le respect du référentiel d'authentification des acteurs de santé de la PGSSI-S.

ANNEXES

5.1 Annexe 1 : Glossaire

Sigle	Terminologie
A	
AD	Active Directory
ADELI	Automatisation DEs Listes
ANSSI	Agence Nationale de Sécurité des Systèmes d'Information
ANSM	Agence Nationale de Sécurité des Médicaments et des produits de Santé
C	
Cert-DC	Service dématérialisé de déclaration des Certificats de Décès
CLCC	Centre de Lutte Contre le Cancer
D	
DMP	Dossier Médical Partagé
DP	Dossier Pharmaceutique
E	
ES	Etablissement de Santé
ESPIC	Etablissement de Santé Privé d'Intérêt Collectif
E-DO	Service dématérialisé de déclaration des maladies à Déclaration Obligatoire
E-FIT	Service dématérialisé de déclaration des incidents transfusionnels
G	
GCS	Groupement de Coopération Sanitaire
GHT	Groupement Hospitalier de Territoire
H	
HAS	Haute Autorité de Santé
HPST	Hôpital Patient Santé Territoire
I	
IGC	Infrastructure de Gestion de Clé
MSSanté	Messagerie Sécurisée de Santé
P	
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PSSI-MCAS	Politique de Sécurité des Systèmes d'Information des Ministères en Charge des Affaires Sociales
R	
RPPS	Répertoire partagé des professionnels intervenant dans le système de santé
ROSP	Rémunération sur Objectifs de Santé Publique
RSSI	Responsable de la Sécurité des Systèmes d'Information
S	
SIH	Système d'Information hospitalier
SIRH	Système d'Information de gestion des Ressources Humaines
SSI	Sécurité des systèmes d'Information
SIS	Système d'Information de santé
SSO	Single Sign On
O	
OTP	One Time Password

5.2 Annexe 2 : Contributeurs de l'étude

5.2.1 Etablissements de santé et représentants

Club RSSI Santé :

- Béatrice BERARD : HCL
- Pr. Patrice BEUTTER : CHU Tours
- Frédéric CABON : CHU Brest
- Guillaume DERAEDT : CHU Lille
- Fabrice D'HOLLANDER : CHU Limoges
- Nicolas DE SAINTE AGATHE : CHU Besançon
- William GROLLIER : CHU Nice
- Astrid LANG : APHP
- Laurent LEPAGE : CH Annecy Genevois
- Patrick MERCIER : CHU Tours
- Stéphane PASQUIER, FFSI Adjoint
- Michel RAUX : Chargé de mission systèmes d'information, DGOS
- Philippe ROUAS : CH Le Havre
- Pascal SABATIER : CH Intercommunal Aix Pertuis
- Pierre TAVEAU : CHU Poitiers
- Véronique VALLEE : CHU Angers et CH Chollet
- Thierry VEAUVY : CHU Toulouse
- Marc WALDMANN : CHU Clermont-Ferrand et CHU Rennes

FEHAP

- Jean-François GOGLIN, Conseiller Systèmes d'Information de la FEHAP

Région Centre

- M. Julien BERTHEL : DSI du CHRU de Tours (support du GHT 37)
- Pr. Patrice BEUTTER : Médecin médiateur et co-RSSI du CHRU de Tours
- M. Patrick MERCIER : DSI Adjoint du CHRU de Tours
- René PAPON : Cadre supérieur de santé, coordonne le déploiement des outils SI coté médical, CHRU Tours
- Corinne THEURIER : Centre de service (responsable des commandes de cartes), CHRU de Tours

- Jean Luc PEAN : RSI CH du Chinonais
- Bruno REBOUILLEAU : RSI CH Paul-Martinais de Loches

- Didier DATY, DSI du Groupe de Clinique St Gatien

Région Auvergne Rhône Alpes

- Jean-Christophe BERNADAC : DSI du CHU de St Etienne (support GHT Loire)
- Catherine BRIAUT : Cadre de santé et référent Informatique, CHU de St Etienne
- Dr Damien THIBAUDIN : Médecin Néphrologue / dialyse et transplantation rénale, CHU de St Etienne

- William ELMIDORO: Chef de projet (IAM, SSO, badges), CH Métropole Savoie
- Norbert GRATALOUP : DSI, CH Métropole Savoie
- Philippe KOCH : Chef de projet (SIS), CH Métropole Savoie
- Guy-Pierre MARTIN: Directeur du CH Métropole Savoie

Région Nouvelle Aquitaine

- Alexandre ANDRE : RSI, CHU de Limoges
- Christophe BERTIN : Chef de projet, CHU de Limoges
- Fabrice D'HOLLANDER : RSSI, CHU de Limoges

5.2.2 GT SSI Agences sanitaires (animé par la DGS)

- Agnès RAMZI : Chargée de mission SI des opérateurs nationaux, DGS
- Pascal FERARD : EFS
- David GIORGIS : ANSM
- Nin KHIEU : ANSES
- Arnaud PARALIEU : ANSES
- Dominique SOULIER : Agence de Biomédecine
- Laurent VIGNALOU : INCA

5.2.3 Accompagnateurs et MOA régionaux

- Christophe BAUDOT, RSSI, SILPC
- Patrice BOISSEUIL, Directeur Technique - Pôle Sécurité & Urbanisation, SILPC
- David ROBINE, Chef de projet - Pôle Sécurité-Urbanisation-Hébergement, SILPC

- Thierry DURAND : DSI Centre Léon Bérard et Administrateur, GCS SISRA
- Jean Baptiste FREYMANN : en charge Portail des PS, équipe exploitation et assistance utilisateur sur les projets pilotés par le réseau, GCS SISRA
- Bertrand PELLET : Secrétaire Général, GCS SISRA
- Hervé SPACAGNA : Directeur de projet et responsable cohérence SI régional (déclinaison en région du cadre commun des SI de Santé), GCS SISRA

5.2.4 Editeurs

AGFA

- Laurette ABOU RJEILY : Country Solution Manager France | HE/HCIS Business Management
- Lan GUICHOT : Directeur Innovation et Business Développement

Bluelinea
- Laurent LEVASSEUR, Président du directoire

Corwin - Evolucare
- Manuel CORREIA : Responsable technique de la partie DPI
- Romain LE GUILCHER, Directeur de la production

Enovacom
- Jean-Yves HAGUET : Avant-vente sur les technologies de sécurité
- Sébastien WETTER : Chef produit sécurité
- Sophie WHITE : Directrice marketing

Evidian
- Michel AMIEL, Business Development Manager
- Gérard CREMIER, Responsable commercial Evidian pour le Secteur Santé France

GIP Symaris
- Sophie NOEL : Responsable du département Développement

Ilex
- Guillaume GUERRIN : Consultant avant-vente
- Luc TARI : Responsable secteur public, santé, social. Pays francophone et Europe

Maincare
- Philippe LAGOUARDE : Directeur de programmes

Medasys
- Nicolas JOBERT : Responsable des Services Opérations Techniques et ASP

MIPIH
- Olivier CAZALS : Direction Commerciale - Responsable de l'Avant-Vente Service & Solution
- Guillaume MAQUAIRE : Chef de service adjoint sécurité

SIB
- Karine HERNIOTE : Chargée de l'offre d'accompagnement des établissements sur les sujets d'identification / authentification

Softway
- Shirley BROTHIER : Directeur technique en charge du développement logiciel et de l'exploitation
- Jean-Marc LESAVRE : RSSI

Wallix
- Edwige BROSSARD : CMO
- Marc BALASKO : Product Manager
- Rachida MAJERI : Territory Sales Manager

L'ASIP Santé, remercie chaleureusement tous les contributeurs sus-cités, qui ont bien voulu accorder de leur temps pour participer à des réunions, à des entretiens ou accueillir ses représentants en région.

L'ASIP Santé a été accompagnée pour la réalisation de cette étude par Madame Lorie PANTANI et Monsieur Arnaud BORIE du cabinet PWC ainsi que Monsieur Vincent TRELY du cabinet Proxima Conseil (sous-traitant du cabinet PWC), qu'elle remercie pour la qualité de leurs contributions.

asipsanté
L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE
Agence des Systèmes d'Information Partagés de Santé
9, rue Georges Pitard - 75015 Paris
Standard : 01 58 45 32 50
Du lundi au vendredi de 8h30 à 18h30 (hors jours fériés)
esante.gouv.fr