Note introductive sur la nouvelle IGC-Santé

Destinataires : éditeurs et gestionnaires d'application

Thématique : produits de certification

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

v1.0.0 du 07/01/2016

Note introductive sur la nouvelle IGC-Santé

« ASIP Santé »

Version 1.0.0 du 07/01/2016

Historique du document			
Version	Date	Auteur	Commentaires
V 1.0.0	07/01/2016	ASIP Santé	Première version publiée

Table des matières

1 Objet du document

Le présent document est destiné aux **éditeurs[1] et aux gestionnaires[2] d'applications** qui utilisent ou souhaitent utiliser les certificats[3] émis par l'ASIP Santé pour sécuriser l'accès, l'échange et le partage de données de santé, dans le respect de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S).

Il a pour objectif de **présenter globalement la nouvelle infrastructure de gestion de clés mise en place par l'ASIP Santé***,* en se concentrant sur les produits et services disponibles à l'ouverture de l'IGC-Santé[4], et **engager le lecteur à organiser sa migration** lorsque son application utilise des certificats des anciennes IGC.

Ce **document introductif est complété d'un ensemble de documents techniques** disponibles sur le site *integrateurs-cps.asipsante.fr*.

[1] Editeur de logiciels de système d'information de santé utilisés par les PS et par les structures de santé, éditeur de proxy…

[2] Gestionnaire d'applications nationales (DMP, DP, MSSanté, RPPS, DP, E-Fit, Cert-DC, E-Do, Téléservices de l'assurance maladie…), régionales, territoriales favorisant l'échange et le partage de données de santé

[3] Certificats logiciels ou certificats confinés dans les cartes de la famille CPS

[4] Ouverture prévue au 1er trimestre 2016

2 Présentation de l'IGC-Santé

2.1 Contexte : sécuriser l'accès, l'échange et le partage des données de santé

Le développement rapide de l'usage des technologies de l'information et de la communication dans le domaine de la santé et du médico-social, et son corollaire, la dématérialisation des données de santé, constitue un levier majeur de la modernisation du système de santé et contribue à l'amélioration de la qualité des soins. Il est aussi facteur de progrès dans les domaines de la recherche, de la santé publique et de la gestion des données médico-économiques.

Toutefois, il s'accompagne d'un accroissement significatif des menaces et des risques d'atteinte à la sécurité des informations transmises et conservées sous forme électronique et plus généralement des processus de santé s'appuyant sur les systèmes d'information de santé.

Pour favoriser le développement de la e-santé au service des professionnels de santé et pour le bénéfice des patients, l'agence des systèmes d'information partagés de santé (ASIP Santé) construit et fait évoluer un **espace de confiance numérique** qui repose sur les piliers suivants :

- la **politique générale de sécurité des systèmes d'Information de santé (PGSSI-S).** Elle contient des guides et des référentiels, notamment le référentiel d'authentification des acteurs de santé qui définit entre autres l'ensemble des dispositifs utilisables pour authentifier un acteur de santé, personne physique ou morale, vis-à-vis d'un système d'information de santé, et le référentiel des autorités de certification éligibles pour l'authentification « publique » dans le secteur de la santé;
- le **répertoire partagé des professionnels de santé (RPPS),** répertoire de référence permettant d'identifier les professionnels de santé avec un numéro unique valable tout au long de leur carrière. Dans ce cadre, l'ASIP Santé organise en amont l'enregistrement des professionnels avec les autorités d'enregistrement (ordres professionnels, service de santé des armées, agences régionales de santé), et assure en aval un service de publication de ces données dans le respect de l'arrêté du 6 février 2009 modifié. Les données d'identité certifiées du RPPS sont intégrées dans la chaine de production des certificats contenus dans les cartes CPS.
- les **infrastructures de gestion de clés (IGC)** dédiées au secteur santé[5] qui :
  - respectent des procédures rigoureuses de recueil des données d'identification professionnelle avec les autorités compétentes (autorités d'enregistrement du RPPS,…) ;
  - émettent des certificats électroniques logiciels [6] ou des certificats électroniques confinés dans les cartes de la famille CPS ;
  - assurent la publication de ces certificats, et la prise en compte de leur révocation, signalée aux applications utilisatrices par des listes de révocation de certificats.

[5] sous la maitrise d'ouvrage de l'ASIP Santé dans le cadre de sa mission d'autorité de certification du domaine de la santé ; la gratuité des produits et services des IGC santé a pour objectif de favoriser les usages de la e-santé en toute confiance, ils sont financés par les pouvoirs publics (budget de l'ASIP Santé).

[6] certificat électronique stocké dans un système logiciel (navigateur, application, système d'exploitation…).

Les conditions d'applicabilité d'un certificat pour la communauté de la santé ainsi que les modalités de gestion et d'usage de ce certificat sont précisées dans les « Politiques de Certification ».

2.2 Une nouvelle IGC-santé qui remplace les deux IGC existantes

L'ASIP Santé met en place une nouvelle infrastructure de gestion de clés, appelée **IGC-Santé**, qui a vocation à devenir **l'unique infrastructure de gestion de clés** gérée par l'ASIP Santé, et à remplacer progressivement les deux IGC-CPS qui expirent fin 2020 et qui sont devenues obsolescentes (vieillissement cryptographique…) :

- D'une part, l'IGC-CPS2bis qui émet des certificats logiciels ;

  L'IGC-CPS2bis délivre 3 types de certificats logiciels :
  - des certificats SSL Classe-4 pour des serveurs, *utilisés pour permettre l'authentification mutuelle (SSL/TLS), par exemple entre une structure de santé et le répertoire partagé des professionnels de santé (RPPS), ou entre deux opérateurs de messagerie sécurisée de santé (MSSanté). ;*
  - des certificats S/MIME Classe-4 pour des applications, *utilisés par exemple pour la signature d'un VIHF et d'un lot de soumission lors de la création et de l'alimentation du DMP* ;
  - certificats S/MIME Classe-5 (certificats de confidentialité) pour des personnes physiques, *utilisés par exemple pour le (dé)chiffrement de données lors des échanges par messagerie sécurisée.*

- D'autre part, l'IGC-CPS2ter qui émet les certificats d'authentification et de signature embarqués dans les cartes de la famille CPS.

Par ailleurs, il existe à ce jour une « IGC-technique » indépendante qui émet des certificats d'authentification embarqués dans les cartes de la famille CPS. Leur l'usage est limité à l'authentification du support ; ces certificats ne contiennent aucune information concernant leurs porteurs.

L'IGC-Santé est conçue pour délivrer trois gammes en fonction du niveau de confiance[7] attendu ; leur mise en œuvre s'effectue par étapes.

- Etape 1 (à l'ouverture du service) : **l'IGC-Santé fournit les certificats logiciels** de la gamme « Elémentaire » [8], et à ce titre prend le **relais l'IGC-CPS2bis**.
- Etape 2 (avec la mise en place des autres gammes) : l'IGC-Santé prend le **relais de l'IGC-CPS2ter et de l'IGC-technique** pour délivrer des certificats confinés dans les cartes de la famille CPS.

La suite de ce document porte plus particulièrement sur l'étape 1.

[7] le niveau de confiance dépend notamment de la qualité de l'enregistrement des porteurs de certificats et de la qualité de protection de la clé privée associée au certificat ;

[8] la gamme « Elémentaire » permet d'offrir des services avec une infrastructure technique conforme aux exigences du référentiel général de sécurité (RGS) sans être qualifiée formellement

2.3 Les atouts de l'IGC-Santé dès son ouverture

L'IGC-Santé apporte trois principales évolutions au regard de l'ancienne IGC-CPS2bis :

1. Des **mécanismes cryptographiques à l'état de l'art**
   Les certificats délivrés par l'IGC-Santé sont conformes au référentiel général de sécurité (RGS) et aux standards internationaux de gestion des identités et des signatures/cachets électroniques[9]. Dans ce cadre, une mise à niveau des caractéristiques techniques de l'IGC a été effectuée (taille de clés, algorithmes utilisés, …).

2. Une **offre diversifiée de certificats logiciels**
   L'IGC-Santé est en capacité de délivrer une variété de certificats logiciels destinés aux personnes morales (établissement de santé, structure médico-sociale, structure d'exercice coordonnée, GCS e-santé, ...) et aux personnes physiques (professionnels de santé, employées de structures de santé, …), à la fois pour les besoins de production et de test/recette.

   Cette nouvelle offre permet de mieux répondre aux spécificités des usages cryptographiques (authentification, signature, chiffrement) et à l'évolution des conditions d'utilisation (dispositifs mobiles, mode SaaS, …), dans le respect des référentiels de la PGSSI-S.

   Par exemple, le *référentiel d'authentification des acteurs de santé* de la PGSSI-S prévoit, au palier 2 de l'authentification « publique », qu'une authentification d'un professionnel de santé puisse être réalisée avec un certificat logiciel de personne physique [10] diffusé par l'ASIP Santé. L'IGC-Santé fournit désormais ce type de certificat (produit *PS-AUTH* ou *PRO-AUTH*). Ce type de produit de certification est particulièrement utile pour la mise en œuvre de système de santé en mode SaaS [11], le professionnel de santé confiant alors son certificat d'authentification à l'opérateur de solution Saas.

   L'offre de certificats logiciels est présentée en annexe 1.

3. **Une amélioration des services associés**
   L'IGC-Santé met en œuvre **deux nouvelles interfaces** pour faciliter la demande, le retrait, la révocation et le suivi des certificats :
   - Un **portail internet** permettant aux porteurs de cartes CPx ainsi qu'aux administrateurs dûment authentifiés d'effectuer les différentes opérations ;
   - Une interface de type **web-services** facilitant la prise en compte des opérations dans les applications métiers.

   La demande de certificats (hors renouvellement) reste sujette à une étape administrative amont. *Les modalités de commande de certificats logiciels sont décrites en annexe 2.*

   Par ailleurs, l'IGC-Santé met en place un **répondeur OSCP** permettant un contrôle en ligne du statut du certificat « validé/révoqué/inconnu », ce service complétant les services actuels de publications des listes de révocation (CRLs) et des listes de delta-révocation (delta-CRLs).

[9] une certification ETSI des certificats confinés dans la CPS et ainsi une reconnaissance européenne (eIDAS, Trusted List) de la carte CPS est envisagée.

[10] c'est-à-dire avec sa bi-clé d'authentification, associée à son certificat de clé publique

[11] SaaS = Software As A Service - abonnement à un service internet qui offre les fonctions d'un système d'information

2.4 Les enjeux de déploiement

Les principaux enjeux de déploiement associés à la mise en œuvre de l'IGC-Santé sont :

- **les précautions habituelles liées à l'utilisation de certificats logiciels :**
  Les mesures de protection techniques et organisationnelles doivent être mises en œuvre pour assurer la sécurité des clés privées associées aux certificats émis par l'ASIP Santé. Il faut notamment veiller à limiter l'accès à ces clés privées à des personnes dûment autorisées et qu'elles ne puissent pas être dupliquées ni installées dans de multiples équipements.

  Les opportunités de diversification des usages apportées par la variété des certificats émis par l'IGC-Santé doivent s'effectuer dans le respect des règles habituelles de sécurité (analyse de risque, politique de sécurité, …), des conditions définies dans les « Politiques de Certification », et en conformité avec les référentiels de la PGSSI-S.

  L'annexe 1 du *référentiel d'authentification des acteurs de santé* de la PGSSI-S précise les conditions d'emploi des dispositifs d'authentification par certificat logiciel de personne morale, et certificat logiciel de personne physique.

- **assurer la continuité de service :**
  De nombreuses applications de santé utilisent les certificats émis par les deux IGC-CPS. Elles doivent évoluer dans des délais contraints pour prendre en compte les certificats émis par l'IGC-Santé et gérer une phase transitoire de cohabitation des différentes IGC (certains utilisateurs [12] utilisant des certificats de l'IGC-CPS2bis, d'autres des certificats de l'IGC-Santé[13]).

  Le paragraphe suivant permet de mieux comprendre les impacts « terrain » liés au changement d'IGC pour anticiper la migration.

[12] des clients qui n'ont pas encore renouvelé leur ancien certificat

[13] des clients qui commandent pour la première fois un certificat (l'ASIP Santé ne permettant plus de commander des certificats logiciels avec l'IGC-CPS2bis mais uniquement avec l'IGC Santé)

3 Organiser la migration liée au changement d'IGC

3.1 Impacts généraux associés au changement d'IGC

La mise en œuvre de l'IGC-Santé implique l'utilisation progressive de nouveaux types de certificats, cohabitant durant quelques années avec des certificats émis par les anciennes IGC. Elle nécessite des adaptations dans les applications et leur déploiement sur un volume conséquent de postes de travail et de serveurs.

Chaque éditeur/gestionnaire d'application organise l'adaptation de son application et la migration de ses clients.

De manière générale, les adaptations concernent :

- l'ajout des chaînes de confiance de l'IGC-Santé dans le « coffre-fort » des applications (serveurs et postes de travail) et / ou des systèmes d'exploitation utilisant des certificats de l'IGC ;
- la prise en compte de la nouvelle cryptographie de l'IGC-Santé, et l'adaptation des algorithmes permettant aux applications d'interpréter les certificats ;
- le renouvellement des certificats dans la nouvelle IGC. Le renouvellement des certificats ne s'effectue pas forcément à « iso-périmètre » compte-tenu de la richesse de l'offre de certificats proposés par l'IGC-Santé (versus celle contenue dans les précédentes IGC) [14].

☞ Le document technique *Migration des IGC-CPS vers l'IGC-Santé ; analyse des impacts sur les applications terrain et consignes de migration :*

- analyse les impacts sur les applications et leurs infrastructures ;
- décrit les consignes pour gérer la migration des certificats des IGC-CPS vers l'IGC-Santé et pour assurer la continuité des services.

L'éditeur/promoteur d'application :

- **prend connaissance de la documentation technique** fournie par l'ASIP santé, en particulier le document *Migration des IGC-CPS vers l'IGC-Santé ; analyse des impacts sur les applications terrain et consignes de migration ;*
- réalise une **étude d'impact** de la prise en compte de l'IGC-Santé (avec cohabitation des différentes IGC) et détermine sa **stratégie de déploiement** vis-à-vis de ses clients ;
- **effectue les développements** nécessaires sur son application pour la prise en compte des différents IGC ;
- *peut mettre en œuvre l'interface web-services pour faciliter les demandes et révocation des certificats de l'IGC-Santé pour ses clients ;*
- commande ses certificats de test en utilisant le portail internet mis à disposition par l'ASIP Santé, authentifié avec une carte CPx de test, et **effectue les tests** pour valider ses développements ;
- **informe l'ASIP Santé** (editeurs@asipsante.fr) lorsqu'il est prêt à migrer ses clients ;

[14] plus de détail en annexe 1.

- **assiste ses clients dans les opérations de migration** (mise à jour des applications et postes clients, information donnée au client du(des) nom(s) du(des) certificat(s) de l'IGC-Santé à commander, procédure de demande et d'installation du certificat, …).

L'ASIP Santé est impactée à double titre :
- en tant que *gestionnaire de l'IGC-Santé* : elle met en œuvre l'IGC-Santé et l'offre de services associée (information, support,…) à destination du secteur santé et médico-social ;
- en tant que *responsable d'applications* (MSSanté, Annuaire Santé/RPPS) *qui utilisent les certificats émis par les IGC (serveur/client)* : elle organise la stratégie de migration pour ses bénéficiaires.

3.2 Les principaux jalons calendaires

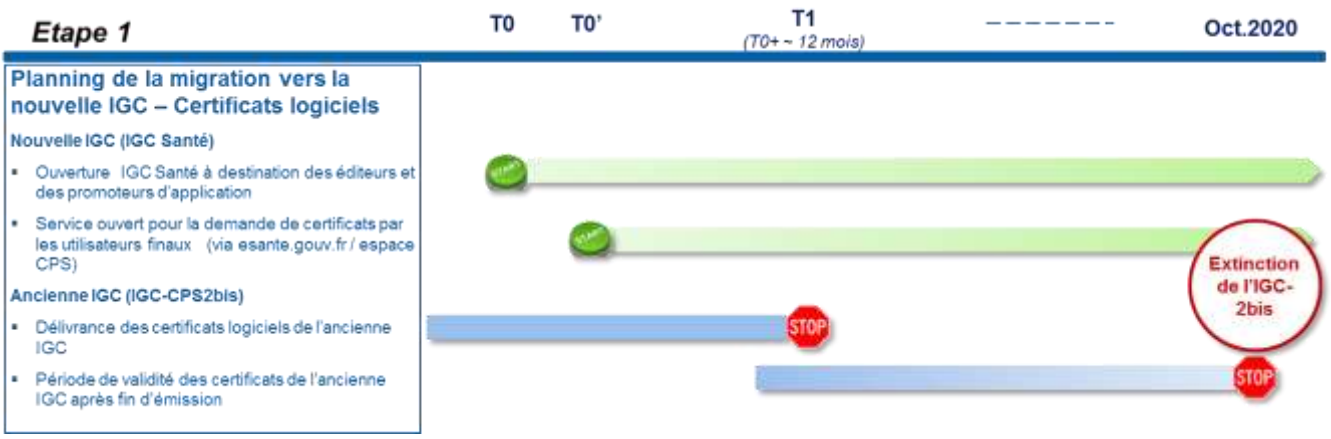
L'ouverture de l'IGC-Santé est matérialisée par la date T0 [15].
La migration vers la nouvelle IGC est un projet divisé en deux étapes :
- Etape 1 : émission et prise en compte des nouveaux certificats logiciels (possible dès T0) ;
- Etape 2 : émission et prise en compte des nouvelles cartes de la famille CPS (possible courant 2017).

Etape 1 : émission et prise en compte des nouveaux certificats logiciels

La migration vers la nouvelle IGC est organisée de manière à permettre un déploiement des nouveaux certificats dans les meilleures conditions :

- *A partir de T0*, l'ASIP Santé informe les éditeurs et gestionnaires d'application que l'IGC-Santé est en service et qu'ils peuvent commander les certificats de test dont ils ont besoin pour tester l'évolution de leurs applications. Dès T0, l'IGC-Santé permet techniquement de délivrer des certificats logiciels de production, toutefois l'ASIP Santé anticipe avant tout des besoins de produits de test au démarrage ;
- *A partir de T0' (T0 + 3 mois - à valider)*, l'ASIP Santé ouvre le service de demande de certificats logiciels destiné aux utilisateurs finaux, permettant d'effectuer les démarches administratives et techniques pour obtenir des certificats émis par l'IGC-Santé. T0' tient compte de l'état d'avancement des éditeurs dans la prise en compte par leurs applications des certificats de la nouvelle IGC. La demande de certificats logiciels de l'ancienne IGC (IGC-CPS2bis) reste possible encore quelques mois, mais s'effectue alors dans le cadre d'une procédure *annexe* qui sera décrite dans un document dédiée ;
- *A partir de T1* (T0 + 12 mois), l'IGC-CPS2bis n'émettra plus de certificats ; les certificats utilisés sur le terrain restent néanmoins valides et utilisables jusqu'à leur expiration [16] et les CRLs continuent à être fournies (jusqu'à l'extinction de l'IGC-CPS2bis fin 2020).

[15] à la date de rédaction de ce document, l'ouverture de l'IGC-Santé est prévue au 1er trimestre 2016. La date précise d'ouverture est précisée sur le site *integrateurs-cps.asipsante.fr* à l'ouverture du service.



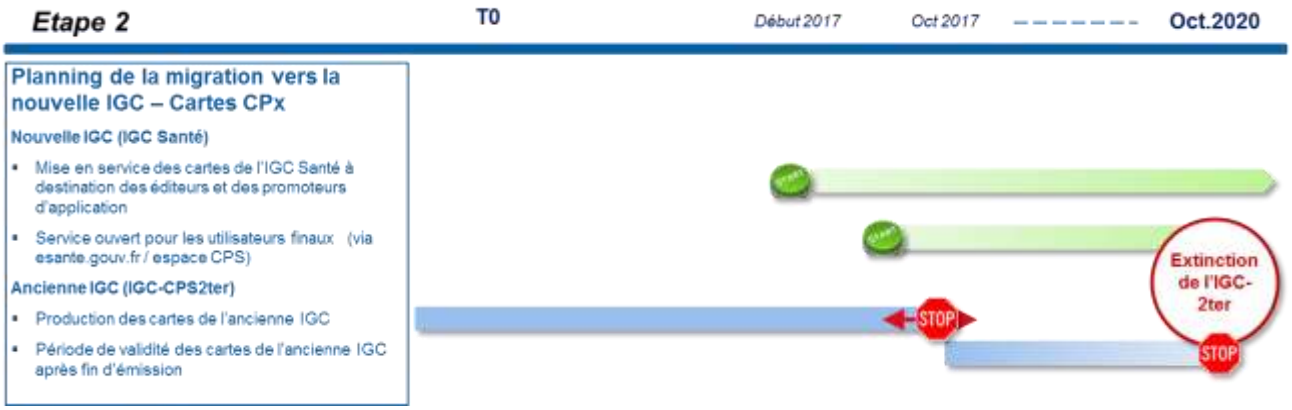
Les éditeurs / gestionnaires d'application doivent s'organiser pour :

- faire évoluer leurs applications afin de prendre en compte les certificats de la nouvelle IGC en amont de la fin de l'émission des certificats de l'ancienne IGC (soit avant T1) ;
- gérer une période de cohabitation terrain pendant laquelle les certificats de l'ancienne IGC (IGC-CPS2bis) restent valides tandis que les certificats de la nouvelle IGC (IGC-Santé) sont mis en production.

Etape 2 : émission et prise en compte des nouvelles cartes de la famille CPS

L'intégration des certificats émis par l'IGC-Santé et embarqués dans les cartes CPS commencera début 2017 [17], et suivra un processus similaire à celui de la délivrance des certificats logiciels :

- *A l'ouverture de l'étape 2 :* communication auprès des éditeurs et gestionnaires d'application, et délivrance de cartes CPS de test produites par l'IGC-Santé.
- *Quelques mois plus tard (la date de bascule tenant compte également des projections de renouvellement de cartes CPx*) : ouverture du service de commande et de délivrance de carte CPS pour les utilisateurs finaux. L'ensemble des applications client et serveur utilisant des certificats L'IGC-Santé devront alors être compatibles avec la nouvelle IGC.



[16] Les certificats logiciels ont une durée de vie de trois ans

[17] Date prévisionnelle

4 Ressources mises à disposition par l'ASIP Santé pour accompagner la migration

L'ASIP Santé met à disposition des éditeurs / gestionnaires d'application :

Dès à présent :

- Des **documents techniques d'information, en ligne sur *integrateurs-cps.asipsante.fr***

  en particulier le document *Migration des IGC-CPS vers l'IGC-Santé ; analyse des impacts sur les applications terrain et consignes de migration.*

- Du **support technique : editeurs@asipsante.fr**

  Pensez à vérifier que vous disposez bien d'ores et déjà d'une carte CPx de test valide (le cas échéant, commandez là). Elle permettra à vos administrateurs de s'authentifier sur le service de commande (portail internet) pour demander vos certificats logiciels de test dès l'ouverture de l'IGC-Santé, et ainsi tester vos développements.

A l'ouverture de l'IGC-Santé (T0) :

- Les chaînes de confiance des différentes gammes et leurs domaines de l'IGC-Santé,
- L'IHM et le web services permettant de commander les certificats,
- Un dispositif d'accompagnement (guides, utilitaires et kits d'installation) pour la migration d'IGC.

5 Annexes

5.1 Annexe 1 : les certificats logiciels délivrés par l'IGC-Santé

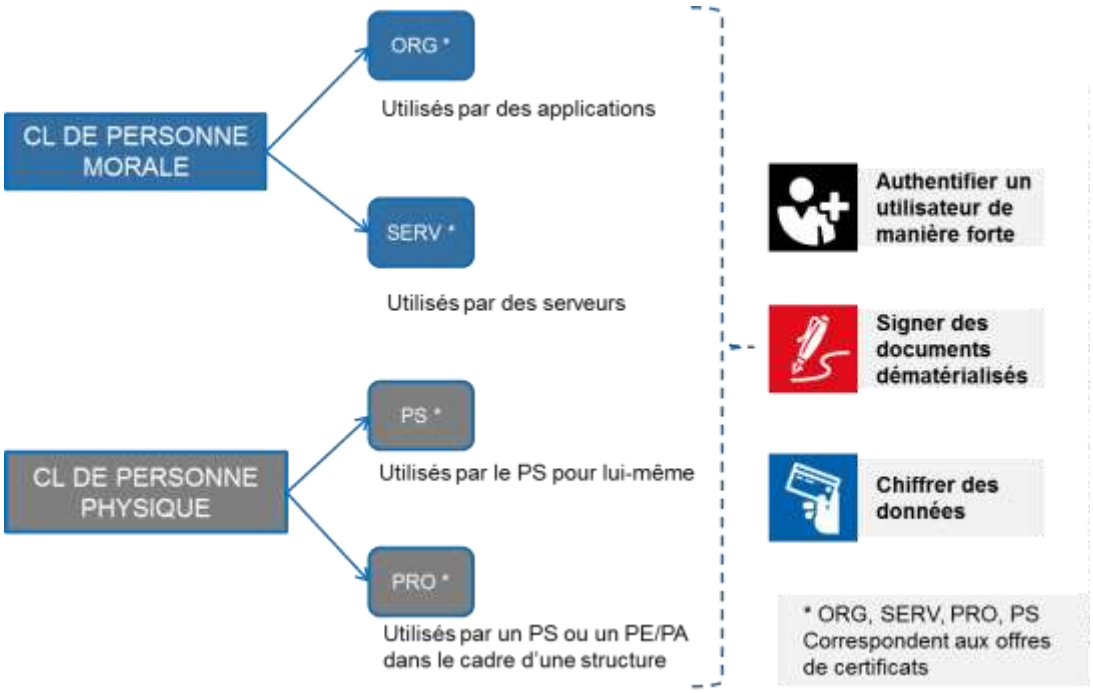
L'IGC-Santé permet de répondre plus finement aux usages cryptographiques des applications actuelles et aux bonnes pratiques en limitant l'usage au strict nécessaire.

Les certificats logiciels de l'IGC-Santé permettent les usages cryptographiques suivants :

- **authentification forte** vis-à-vis de tiers (serveur distant, application, personne physiques, application) ;
- **signature** électronique d'objets ;
- (dé)**chiffrement** de données.

Ils sont associés à différents domaines :

- **des certificats rattachés à une « personne morale » (structure)** garantissant l'identité des applications associées à la structure (appelés ORG), ou d'un serveur (appelés SERV) appartenant à la structure ;
- **des certificats rattachés à une « personne physique »** garantissant l'identité d'un professionnel de santé sous sa propre responsabilité (appelés PS), ou de professionnel de santé (PS), personnel d'établissement (PE) ou personnel autorisé (PA) sous la responsabilité d'un directeur de structure (appelés PRO).



Au total, l'IGC-Santé propose 13 certificats logiciels de production, et de test [18] :

Certificats logiciel de l'IGC-Santé	Usage cryptographique	Type de certificat
ORG_AUTH_CLI	Il permet aux applications associées à une structure de s'authentifier vis-à-vis d'un tiers, un serveur ou une application	Certificat de personne morale – ORGANISATION
ORG_SIGN (cachet)	Il permet la signature électronique d'objets (de documents, courriers électroniques..) par une application sous la responsabilité d'une structure	Certificat de personne morale – ORGANISATION
ORG_CONF	Il permet à un utilisateur de chiffrer des données à destination de cette structure, qui est la seule à pouvoir déchiffrer les données qui lui sont destinées	Certificat de personne morale – ORGANISATION
SERV_SSL_SERV	Il permet à un serveur web appartenant à une structure de s'authentifier vis-à-vis d'un tiers, un module client ou une personne physique, voire en tant que client à un autre serveur distant	Certificat de personne morale – SERVEUR
SERV_SIGN (cachet)	Il permet la signature électronique d'objets par un serveur associé à une structure	Certificat de personne morale – SERVEUR
SERV_S/MIME	Il permet à un serveur de signer des objets et de déchiffrer les données qui lui sont destinées, sous la responsabilité de la structure concernée	Certificat de personne morale – SERVEUR
SERV_CONF	Il permet à un utilisateur de chiffrer des données à destination d'un serveur (sous la responsabilité de la structure concernée) qui est le seul à pouvoir déchiffrer les données qui lui sont destinées	Certificat de personne morale – SERVEUR
PS_AUTH	Il permet à un professionnel de santé de s'authentifier vis-à-vis d'un tiers (serveur, application ou autre personne physique).	Certificat de personne physique – PROFESSIONNEL DE SANTE (demande directe du PS)
PS_SIGN	Il permet à un professionnel de santé de signer des objets (documents électroniques,..)	Certificat de personne physique – PROFESSIONNEL DE SANTE (demande directe du PS)
PS_CONF	Il permet à un utilisateur de chiffrer des données à destination du professionnel de santé porteur de ce certificat de confidentialité, qui est le seul à pouvoir déchiffrer les données qui lui sont destinées.	Certificat de personne physique – PROFESSIONNEL DE SANTE (demande directe du PS)
PRO_AUTH	Il permet à un professionnel de santé (PS), à un personnel d'établissement (PE) ou à un personnel autorisé (PA) dans le cadre d'une structure identifiée, de s'authentifier vis-à-vis d'un tiers (serveur, application ou autre personne physique).	Certificat de personne physique – PROFESSIONNEL de structure dans le cadre de la structure qui l'emploie (demande faite par un mandataire)
PRO_SIGN	Il permet à professionnel de santé (PS), à un personnel d'établissement (PE) ou à un personnel autorisé (PA) dans le cadre d'une structure identifiée, de signer des objets (documents électroniques,..).	Certificat de personne physique – PROFESSIONNEL de structure dans le cadre de la structure qui l'emploie (demande faite par un mandataire)
PRO_CONF	Il permet à un utilisateur de chiffrer des données à destination du porteur* de ce certificat de confidentialité, qui est le seul à pouvoir déchiffrer les données qui lui sont destinées. *le porteur est un professionnel de santé (PS), un personnel d'établissement (PE) ou un personnel autorisé (PA) dans le cadre d'une structure identifiée	Certificat de personne physique – PROFESSIONNEL de structure dans le cadre de la structure qui l'emploie (demande faite par un mandataire)

[18] une IGC-Santé de test a été créée pour les tests d'intégration dans les applications terrain ; elle a exactement la même architecture que l'IGC-Santé de production.

L'éditeur/promoteur d'application conseille ses clients dans le choix du produit de certification à demander à l'ASIP Santé, au regard des usages cryptographiques et du contexte d'utilisation du service qu'il propose.

Attention : certains certificats émis par l'IGC-CPS2bis cumulent plusieurs usages cryptographiques ce qui n'est pas conforme aux bonnes pratiques qui préconisent de réserver un certificat à un usage unique. Le renouvellement des certificats ne s'effectue donc pas forcément à « iso-périmètre » avec l'IGC-Santé.

Les chapitres 5.1 et 5.2 du *document technique Migration des IGC-CPS vers l'IGC-Santé ; analyse des impacts sur les applications terrain et consignes de migration* donnent des précisions sur les équivalences de certificats selon les IGC.

L'annexe 3 fournit un exemple associé aux usages métier du DMP.

5.2 Annexe 2 : modalités de demande des certificats logiciels

Hormis le cas où le professionnel de santé, authentifié de sa carte CPS, demande un certificat logiciel pour lui-même[19], la demande initiale de certificats logiciels nécessite :

- que **la structure ait signée le contrat de commande de produit de certification**[20] **;**
- que le **représentant légal de la structure ou son mandataire**[21] **remplisse un formulaire administratif** qui permet :
  - d'identifier la structure responsable de l'usage du certificat demandé à l'ASIP Santé ;
  - d'identifier l'(les) administrateur(s) technique(s) qui gèrent la demande, le retrait, et la révocation de certificat ;
  - d'enregistrer des informations qui seront contenues dans le certificat[22]

  NB : cette étape administrative n'est pas nécessaire pour la commande d'un certificat de l'IGC-Santé permettant de remplacer un certificat de l'IGC-CPS2bis arrivant à échéance, lorsque la structure et les administrateurs techniques n'ont pas changé.
- que **l'administrateur technique soit équipé d'une carte CPx** (généralement une CPE ou une CPA) **valide** ;

Une fois la demande administrative traitée par l'ASIP Santé, **l'administrateur technique - prévenus par courriel - peut :**

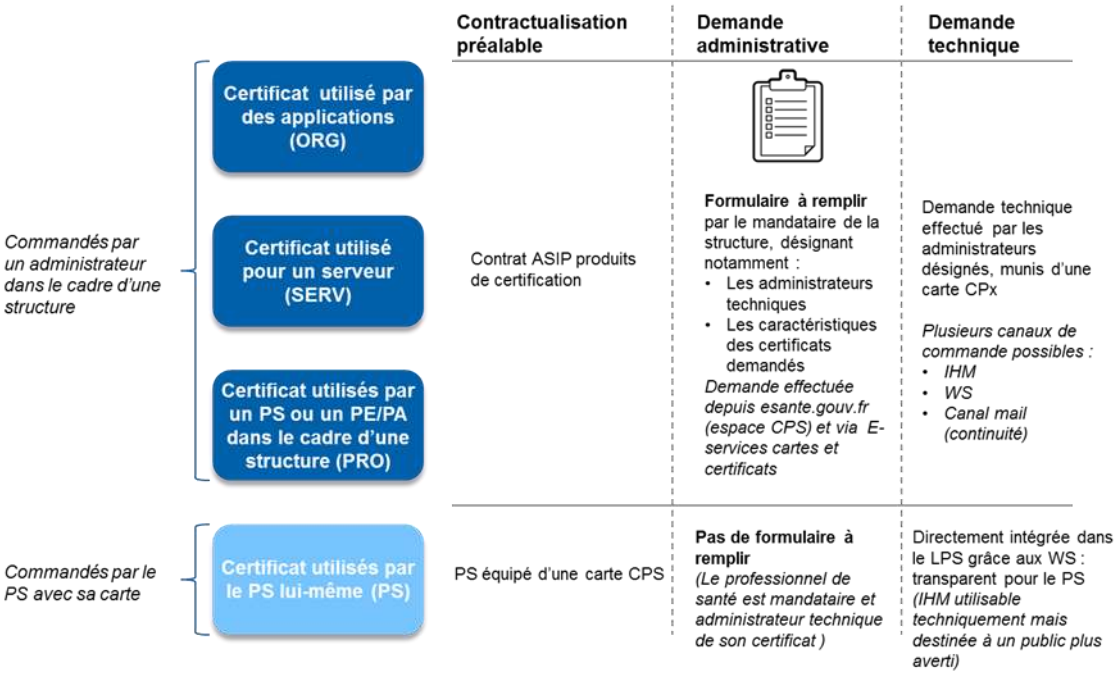
- générer les clés de sécurité,
- **faire certifier la clé publique par l'ASIP Santé en s'authentifiant avec sa carte CPx sur le portail internet ou via l'interface webservice** (ou via l'interface mail qui perdure temporairement pour assurer la continuité du service de demande)
- installer le certificat dans le respect de la politique de sécurité de la structure, et en conformité avec les préconisations du référentiel d'authentification des acteurs de santé de la PGSSI-S sur les conditions d'emploi des dispositifs d'authentification par certificat logiciel de personne morale, et certificat logiciel de personne physique.

[19] par exemple via son logiciel métier utilisant l'interface web service mise à disposition par l'IGC-Santé pour demander, retirer et révoquer un certificat

[20] toute structure exerçant dans le domaine de la santé et du médico-social qui souhaite demander des produits de certification à l'ASIP Santé doit signer un contrat et accepter les conditions générales d'utilisation. Lorsque cette structure n'est pas une structure de santé, elle complète également une demande d'autorisation pour pouvoir utiliser les produits de certification de production émis par l'ASIP Santé

[21] le mandataire est une personne désignée par le représentant légal pour gérer les produits de certification rattachés à la structure

[22] par exemple le nom de serveur et nom de domaine pour la demande d'un certificat SERV_SSL_SERV



La gestion du cycle de vie des certificats est facilitée par l'intégration des fonctions de renouvellement et de révocation accessibles via le portail internet ou le webservice.

Tout prestataire de système d'information de santé peut aider son client à remplir le(s) formulaire(s) administratif(s), et l'assister dans les démarches techniques ou les réaliser pour son compte, en intégrant par exemple la gestion des certificats dans son processus habituel de contractualisation et d'installation logicielle.

Si le prestataire prévoit de réaliser l'étape technique pour le compte de ses clients, il doit informer ses clients des impacts de la délégation (confier à un tiers de confiance la génération des clés de sécurité puis l'installation du certificat), et contractualiser avec l'ASIP Santé afin de pouvoir équiper ses administrateurs techniques en cartes CPA.

Pour tout déploiement à grande échelle, prendre contact auprès de l'ASIP Santé.

5.3 Annexe 3 : exemple d'évolution de l'authentification sur l'application DMP

L'authentification des Professionnels de Santé (PS) pour l'accès au dossier médical partagé (DMP) est réalisée soit par authentification directe soit par authentification indirecte.

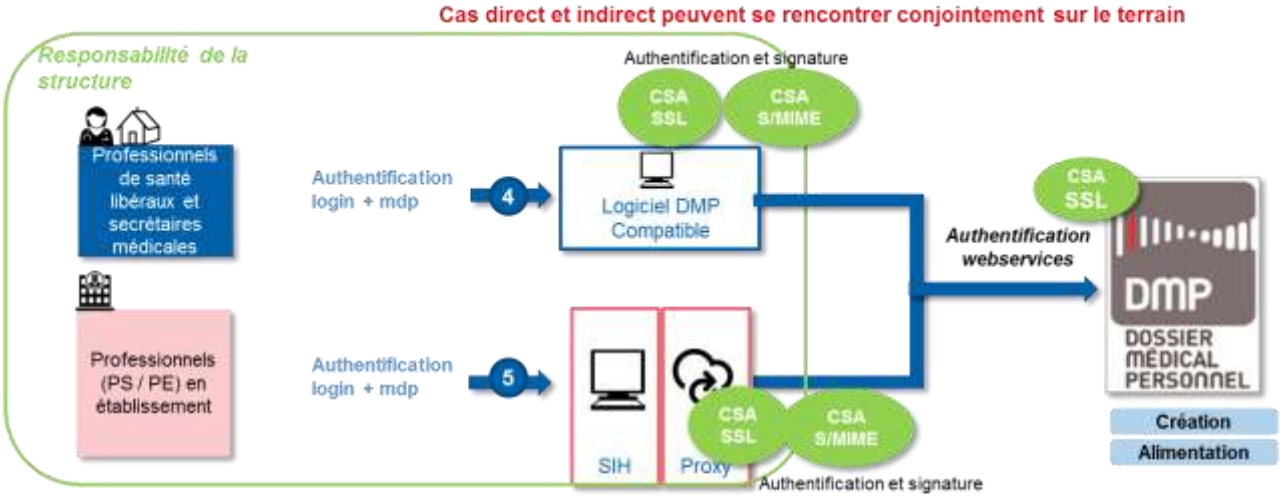
On parle d'authentification *directe* lorsque le professionnel de santé utilise sa carte CPS pour accéder au DMP, via son logiciel de professionnel de santé « DMP compatible », ou via le portail web *www.dmp.gouv.fr*.

Les PS peuvent également créer ou alimenter le DMP en utilisant un logiciel « DMP compatible» homologué en authentification *indirecte*. Dans ce cas, l'authentification des professionnels (qui accèdent généralement au SI en login/mot de passe) et la traçabilité dans le SI est assurée sous la responsabilité du Directeur de la structure de santé ; l'accès au DMP est sécurisé au moyen des certificats serveurs applicatifs (CSA) SSL et SMIME délivrés par l'IGC-CPS2bis.

La migration de l'IGC-CPS2bis vers l'IGC-Santé concerne dans un premier temps les certificats logiciels, et donc l'authentification indirecte.

A) Méthode actuelle d'authentification indirecte au DMP

Le schéma ci-dessous représente les différents modèles d'authentification au DMP et les pastilles vertes représentent les certificats employés actuellement sur chacun des logiciels et serveurs :



4 Le professionnel de santé se connecte à son logiciel DMP compatible à l'aide d'un login + mdp. Son logiciel possède des certificats logiciels CSA SSL et S/MIME qui permettent d'authentifier le cabinet médical auprès du serveur DMP qui, en retour, s'authentifie à l'aide d'un certificat serveur. Le professionnel de santé ne peut que créer ou alimenter le DMP, sous la responsabilité d'une personne morale (cabinet médical).

5 Le professionnel (PE ou PS), dans le cadre d'un établissement de santé, se connecte à son SIH en login + mdp ou autre moyen d'authentification. Le proxy de son établissement possède des certificats CSA SSL et S/MIME qui lui permettent de s'authentifier auprès du serveur DMP qui, en retour, s'authentifie à l'aide d'un certificat serveur. Le professionnel ne peut que créer ou alimenter le DMP, sous la responsabilité de la personne morale (établissement).

Les certificats de type « authentification SSL » (CSA SSL) pour l'authentification de l'établissement.
Les certificats de type « signature S/MIME » (CSA S/MIME) pour la signature des lots de soumission et du VIHF au nom de l'établissement.

Schéma d'authentification indirecte au DMP

B) Méthode d'authentification indirecte au DMP après migration de l'IGC

La première phase de migration de l'IGC concerne uniquement les certificats logiciels, les certificats embarqués dans les cartes CPx ne sont pas concernés.

La migration de l'IGC va entraîner des modifications dans la cinématique d'authentification des utilisateurs au DMP. Les modifications concernent le renouvellement des certificats et introduisent une logique de séparation entre les PS et les PE:

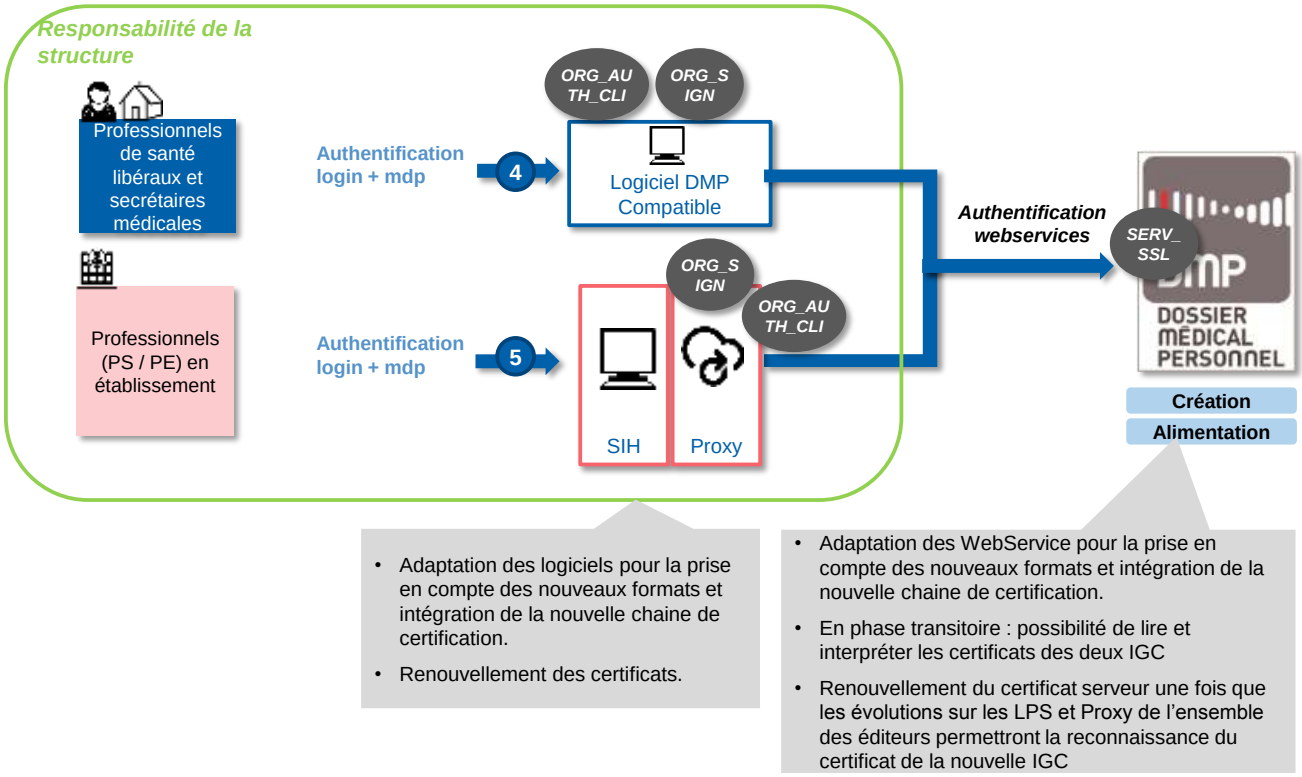
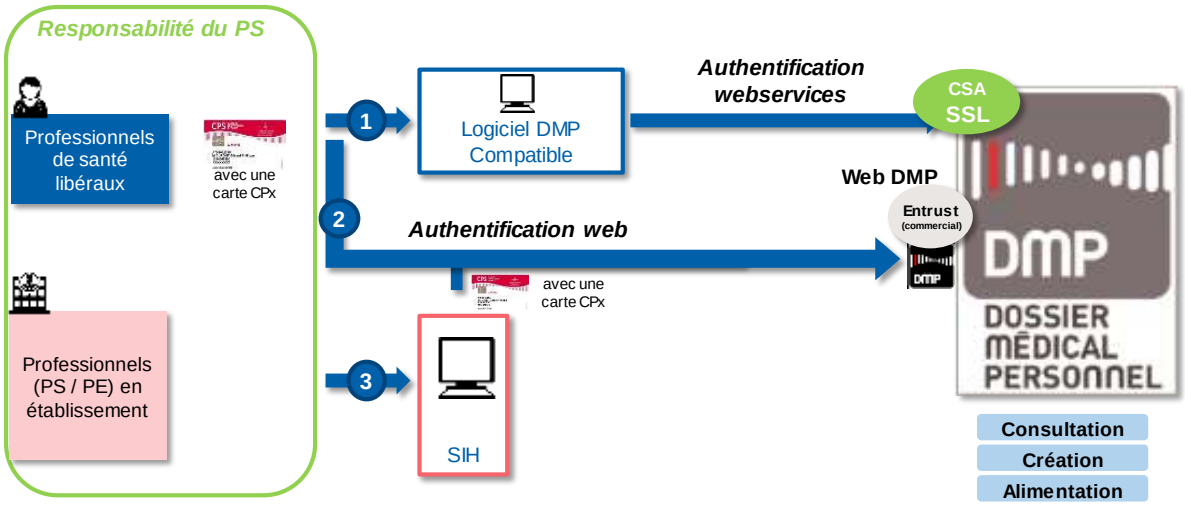


Schéma d'authentification indirecte au DMP après migration avec les impacts associés

C) Méthode actuelle d'authentification directe au DMP

La deuxième étape de la migration d'IGC impliquera de prendre en compte les cartes de la nouvelle IGC (IGC-Santé) tout en continuant à gérer les cartes CPx de l'ancienne IGC (IGC-CPS2ter) jusqu'en 2020.

Le schéma ci-dessous représente le modèle d'authentification direct au DMP et les pastilles vertes représentent les certificats employés actuellement sur chacun des logiciels et serveurs :



1. Le professionnel de santé, muni de sa carte CPS se connecte à son LPS DMP compatible pour créer, alimenter ou consulter. Dans cette situation, aucun certificat logiciel n'est impliqué côté utilisateur . En revanche, le serveur du DMP s'authentifie à l'aide d'un certificat serveur
2. Le professionnel de santé, muni de sa carte CPS, se connecte au portail web du DMP pour créer, alimenter ou consulter. Dans cette situation, aucun certificat logiciel n'est impliqué côté utilisateur. En revanche, le portail web DMP possède des certificats serveurs pour s'identifier
3. Le professionnel de santé, muni de sa carte CPx, se connecte au SIH de son établissement, qui le renvoie directement vers le web DMP pour qu'il s'authentifie avec sa carte et puisse consulter, créer et alimenter le DMP. Pas de certificat logiciel impliqué

Schéma d'authentification directe au DMP

D) Méthode d'authentification directe au DMP après migration de l'IGC

Le schéma ci-dessous représente le modèle d'authentification direct au DMP après migration de l'IGC et les pastilles grises représentent les certificats utilisés en cible sur chacun des logiciels et serveurs :

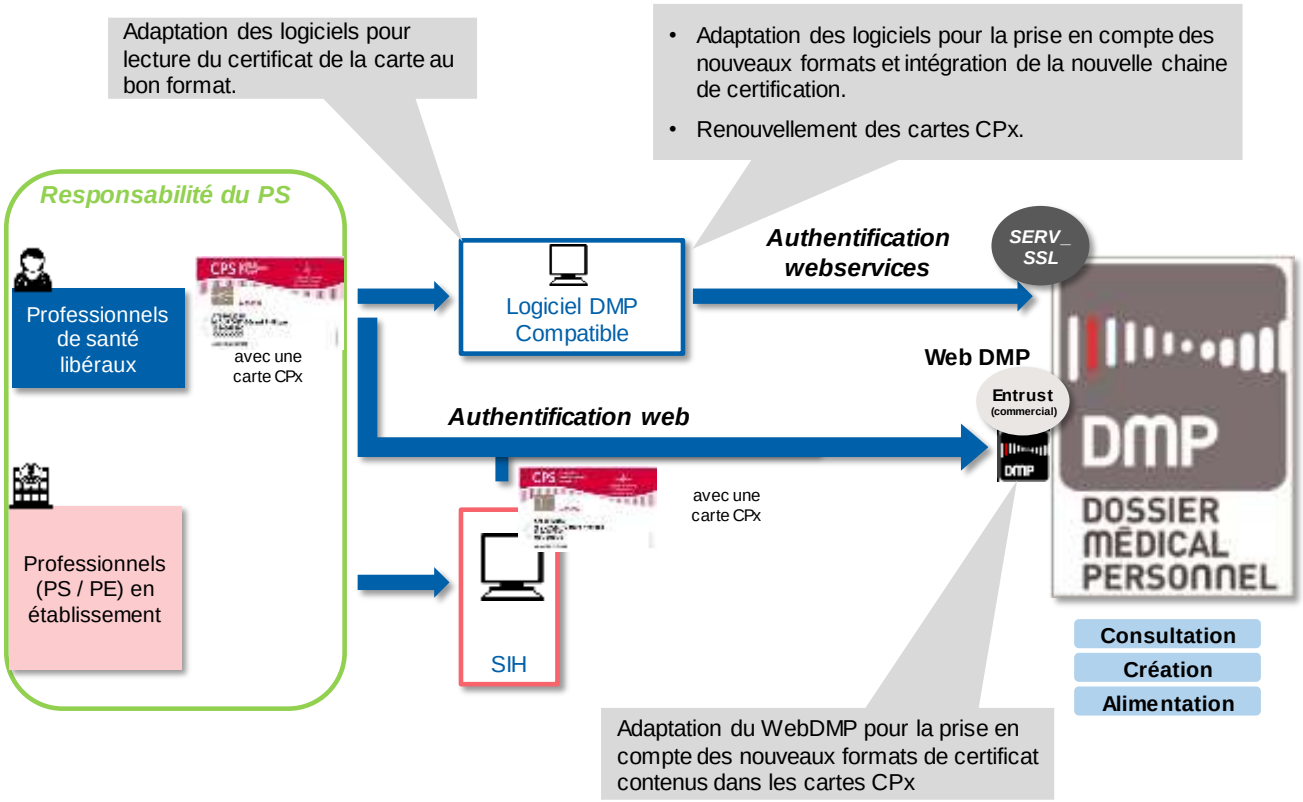


Schéma d'authentification directe au DMP après migration avec les impacts associés

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
Tel : 01 58 45 32 50
esante.gouv.fr