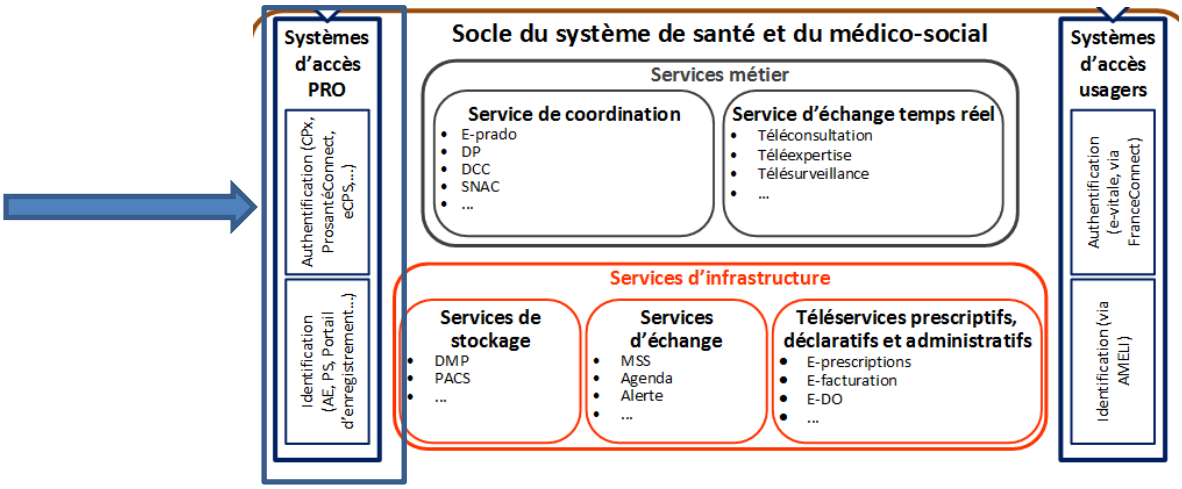
4.4. Identité numérique des acteurs de santé et du médico-social



En fonction du contexte d'utilisation (application accessible depuis Internet, depuis un système d'information privé, depuis un mobile…) et de leurs finalités (nature des données et opération réalisées sur ces données), les services numériques sont amenés à devoir identifier de manière formelle les utilisateurs.

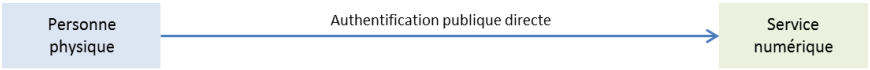
Pour ce faire, ils mettent en œuvre des mécanismes d'authentification qui permettent à l'utilisateur de prouver son identité.

Il peut s'agir d'authentification publique ou privée[1] du professionnel.

DOCTRINE

❶ L'Etat encadre deux types d'authentification publique

a) **L'authentification directe** des professionnels en s'appuyant sur les solutions existantes (carte de professionnel de santé (CPS), OneTime Password (mot de passe à usage unique (OTP), …) et des solutions complémentaires ou alternatives adaptées aux usages en mobilité (e-CPS, Time-Based One-Time Password (TOTP)…) ;



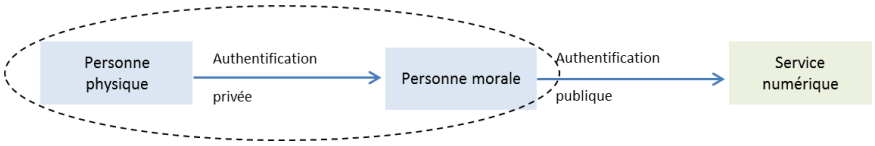
[1] Authentification « publique » : l'authentification est dite publique lorsque le dispositif d'authentification utilisé est associé à un identifiant public (ou identifiant de portée nationale) et que :

- soit son utilisation n'est pas limitée à un ou plusieurs système(s) d'information donné(s) (ex. la carte CPS) ;
- soit il s'appuie, pour l'inscription de la personne concernée, sur un dispositif associé à un identifiant public et dont l'utilisation n'est pas limitée à un ou plusieurs système(s) d'information donné(s).

Authentification « privée » : l'authentification est dite privée quand elle ne répond pas à la définition de l'authentification publique. C'est notamment le cas lorsque les dispositifs d'authentification utilisés sont diffusés pour une utilisation limitée à un ou plusieurs système(s) d'information donné(s) (ex. une authentification par mot de passe pour l'accès à un poste de travail de la structure). Ces dispositifs peuvent être associés à des identifiants publics ou à des identifiants privés.

b) **L'authentification indirecte** des professionnels qui combine :

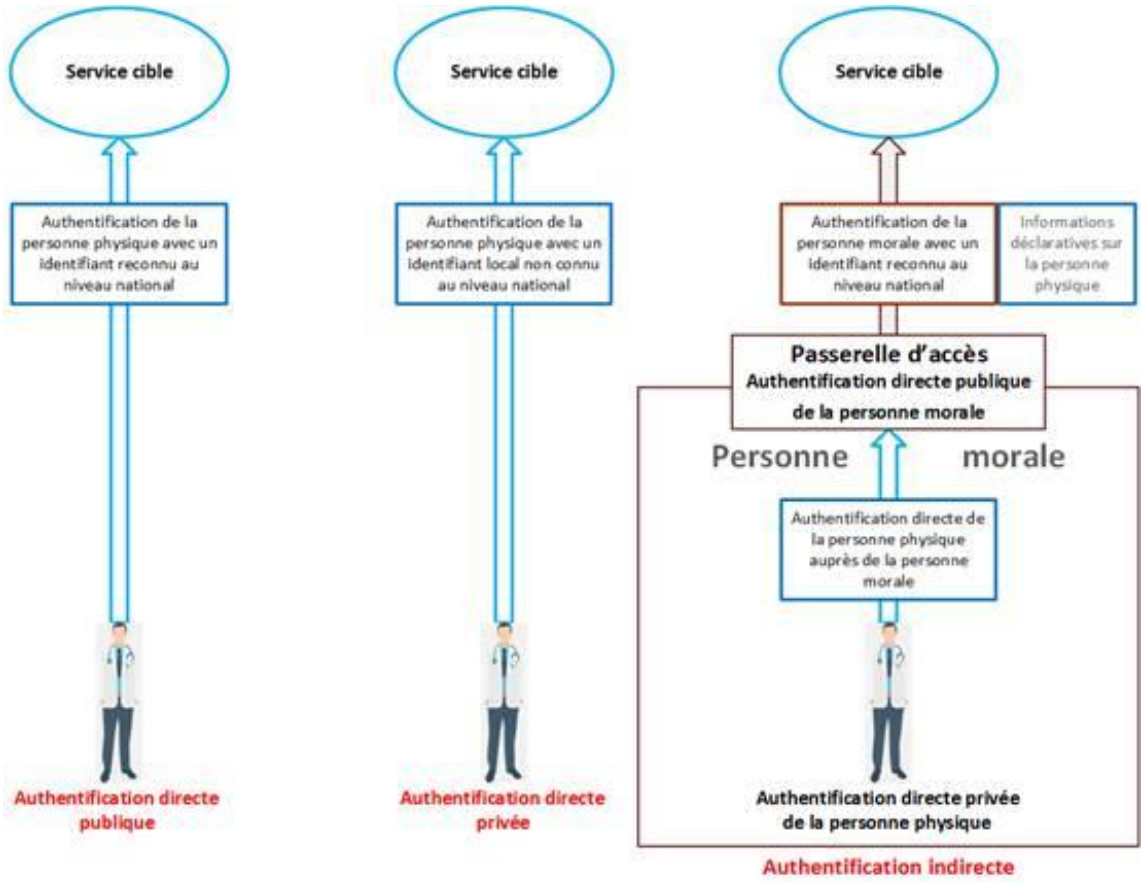
- une authentification directe des structures dans lesquelles ils travaillent,
- et une authentification privée de ces professionnels, sous la responsabilité du responsable de structure.



(Note : pour bénéficier d'une authentification publique, un acteur doit disposer d'un identifiant public de portée nationale enregistré dans le référentiel des acteurs du système de santé).

❷ L'Etat précise les modalités d'authentification privée

Le choix des méthodes d'authentification privée reste de la responsabilité des structures, au regard de la réglementation et de leur propre analyse de risques.



❸ L'Etat propose un fournisseur national d'identité sectoriel : Pro Santé Connect

Pour faciliter la mise en œuvre de l'authentification publique, l'Etat propose[2] un **fournisseur national d'identité sectoriel[3]: Pro Santé Connect.**

Pro Santé Connect réalise l'authentification des professionnels et décharge les services numériques de cette gestion. Il rend donc les services numériques indépendants des moyens d'authentification mis en œuvre.

A date, Pro Santé Connect est capable d'authentifier une identité en utilisant la carte CPS ou la e-CPS. D'autres dispositifs d'authentification seront ajoutés (OTP SMS, TOTP…)

Couplé au référentiel des acteurs du système de santé, Pro Santé Connect fournit également aux services qui le sollicitent, les données d'identification du professionnel utiles au contrôle d'accès par les services. (par exemple, son activité, sa structure…)

❹ L'Etat propose e-CPS, dispositif d'authentification alternatif à la carte CPS

La **e-CPS** permet à un professionnel de s'authentifier auprès de services en ligne en utilisant son smartphone (ou tablette, …). L'authentification permise par e-CPS est d'un niveau de sécurité équivalent à l'authentification par carte CPS.

TRAJECTOIRE

❶ L'Etat définit les niveaux de sécurité requis pour l'authentification des professionnels par les services numériques de santé, harmonisés avec les niveaux inscrits dans le règlement electronic IDentification, Authentication and trust Services (eIDAS)

L'Etat définit pour ces niveaux, les dispositifs acceptables et les conditions de mise en œuvre en fonction des finalités (accès aux données, opération sur les données, nature des données…) et du contexte d'exposition aux risques (application WEB, application mobile,…).

Une matrice de référence permettra d'identifier le niveau d'authentification requis par type de données ou d'usage.

❷ L'Etat met à disposition le Fournisseur national d'identité sectoriel Pro Santé Connect

Actuellement en cours d'expérimentation Pro Santé Connect est en production depuis l'été 2019.

L'expérimentation est réalisée avec la Cnam[4] et quelques industriels pilotes. Il s'agit de vérifier les possibilités d'intégration du service Pro Sante Connect et e-CPS dans les processus d'identification des services en ligne Web et intégrés logiciels existants.

❸ L'Etat met en production le dispositif d'authentification e-CPS

[2] l'utilisation de ce service n'est pas obligatoire

[3] Fournisseur d'identité numérique (au sens de France Connect) que l'on peut aussi appeler fournisseur d'authentification

[4] pour le service Info patient d'Espace pro, et plus tard, pour la consultation du DMP.

a) Pour tous les professionnels inscrits au référentiel d'identité, **en possession d'une carte CPS** : la e-CPS sera alors utilisée comme un dispositif complémentaire à la carte CPS
b) Pour certains professionnels inscrits au du référentiel national **sans obligation de possession de carte CPS** : la e-CPS sera alors utilisée comme un dispositif alternatif à le carte CPS

❹ L'Etat définit les conditions d'une authentification indirecte pour les structures

L'authentification indirecte dépend des capacités d'identification / authentification des acteurs exerçant au sein de structures. Pour proposer des conditions de mises en œuvre organisationnelles et techniques adaptées, une étude est à mener pour :

- proposer une convention entre la structure et les fournisseurs de service (convention pour chaque fournisseur de service ou convention mutualisée) ;
- déterminer les niveaux de sécurité des moyens d'identification et d'authentification acceptables ;
- élaborer une architecture d'authentification qui tienne compte des infrastructures et réseaux des structures.

Pour le mode d'authentification indirecte des professionnels, l'Etat fournit le dispositif permettant l'authentification directe publique de la personne morale (Certificat serveur), le principe étant de pouvoir recourir à une identification à portée nationale. Les modalités diffèrent cependant en fonction du niveau de sécurité requis par les services. Le responsable de traitement pourra choisir s'il y a lieu de recourir en plus à un conventionnement pour la mise en place d'une authentification indirecte dans ce cas dite « renforcée » (AIR).

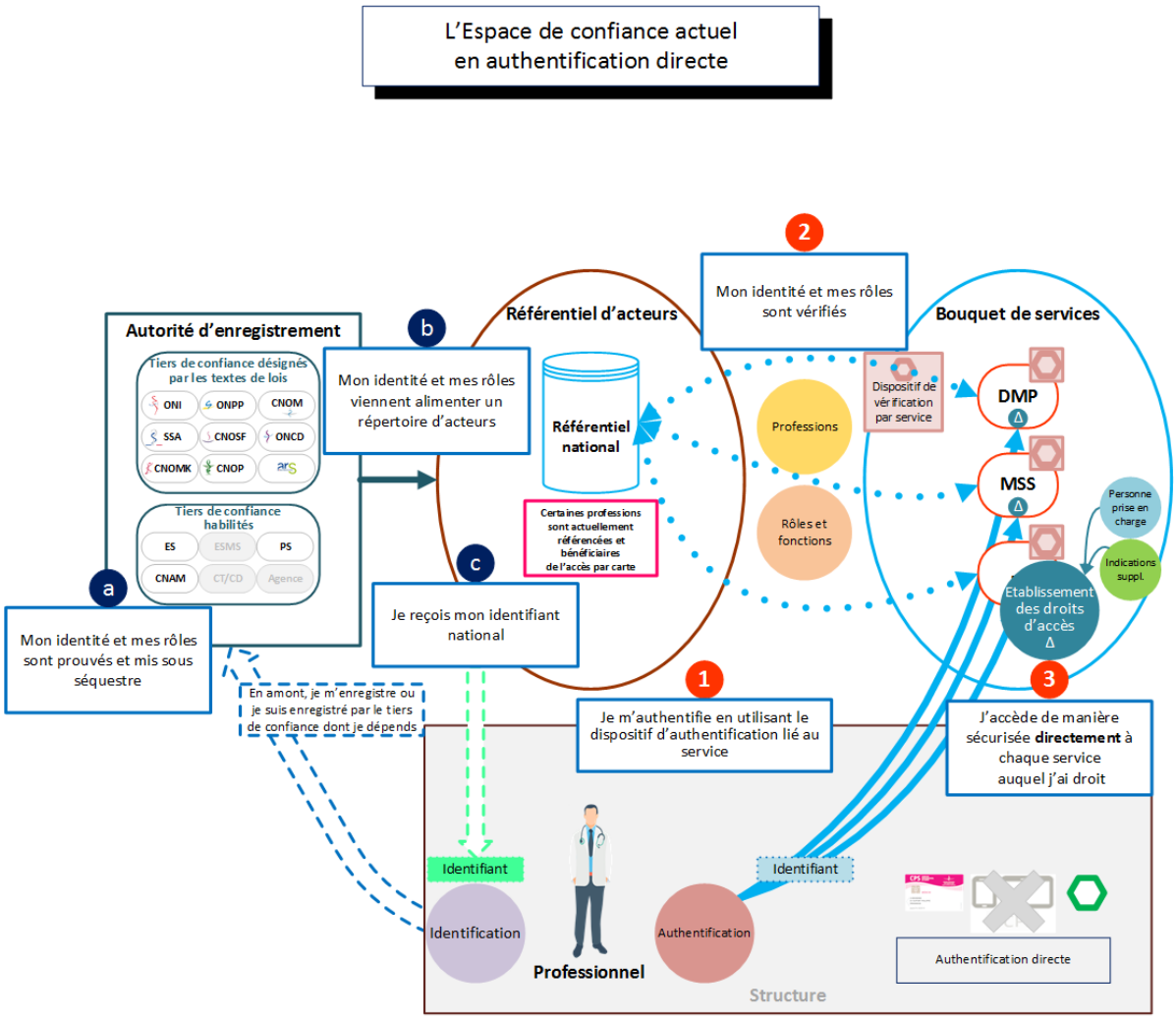
❺ L'Etat fait évoluer la politique générale des systèmes d'information de santé (PGSSI-S)

Le référentiel d'authentification des acteurs de santé de la PGSSI-S doit être revu pour décliner opérationnellement la doctrine technique et expliciter les différents cas d'usage qui seront produits. Ces différents cas d'usage seront en effet déclinés dans un document complémentaire.

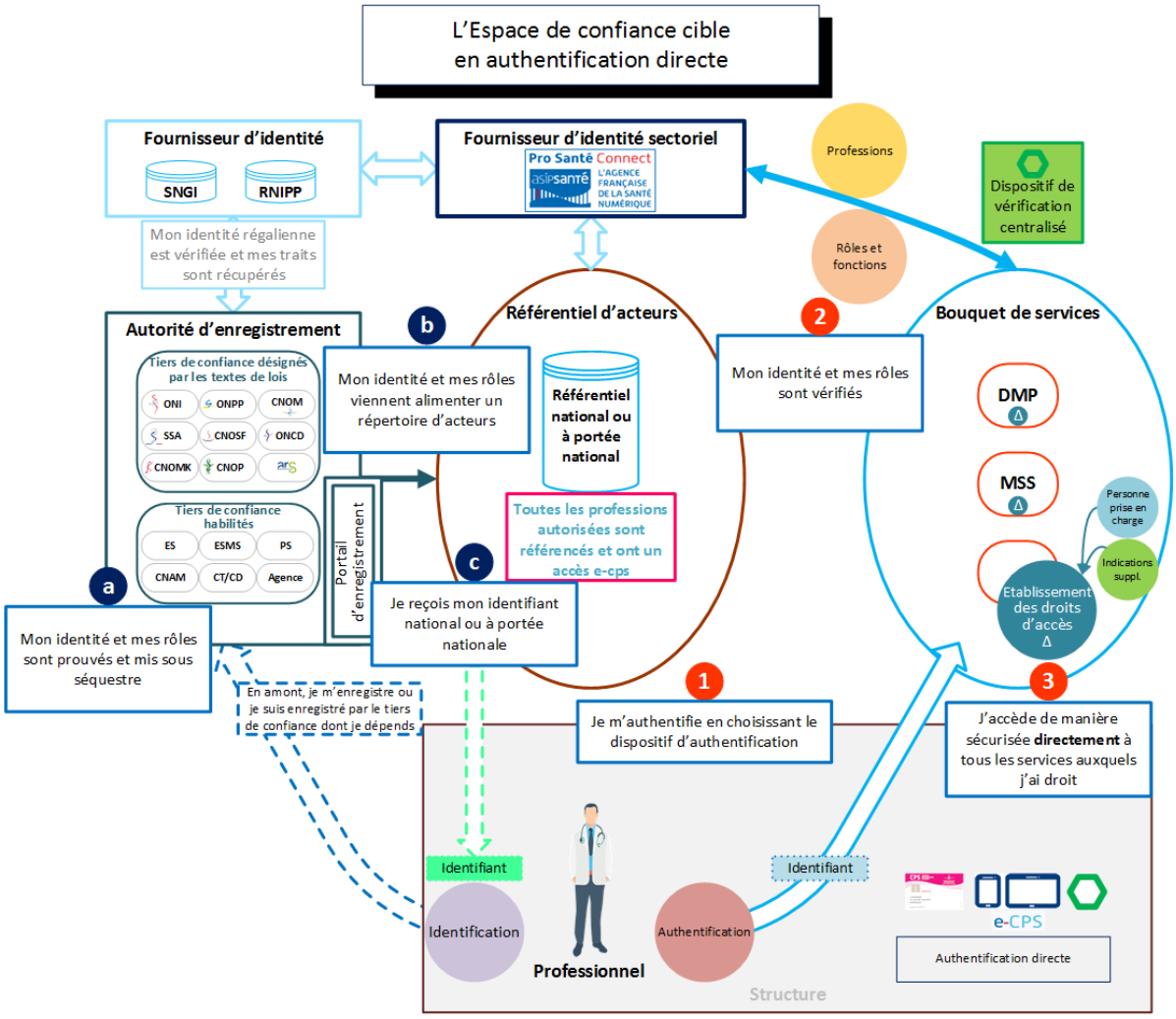
SYNTHESE DES ACTIONS CLES

Action	Date de mise en œuvre
Définition des niveaux de sécurité requis	(A définir)
Mise en œuvre de Pro Santé Connect avec le dispositif e-CPS associé à une carte CPS avec accompagnement des fournisseurs de services et des professionnels	S2 2019
Mise en œuvre de Pro Santé Connect avec le dispositif e-CPS pour tous les professionnels intégrés dans le référentiel national avec accompagnement des fournisseurs de services et des professionnels	S1 2020
Diversification des moyens d'authentification (e-CPS sans avoir besoin d'une carte CPS/OTP/SMS/TOTP…) avec Pro Santé Connect	A partir de 2020
Encadrement juridique du conventionnement pour l'authentification indirecte.	(A définir)
Remise à niveau de la PGSSI-S et des référentiels impactés	(A définir)

Schémas illustratifs

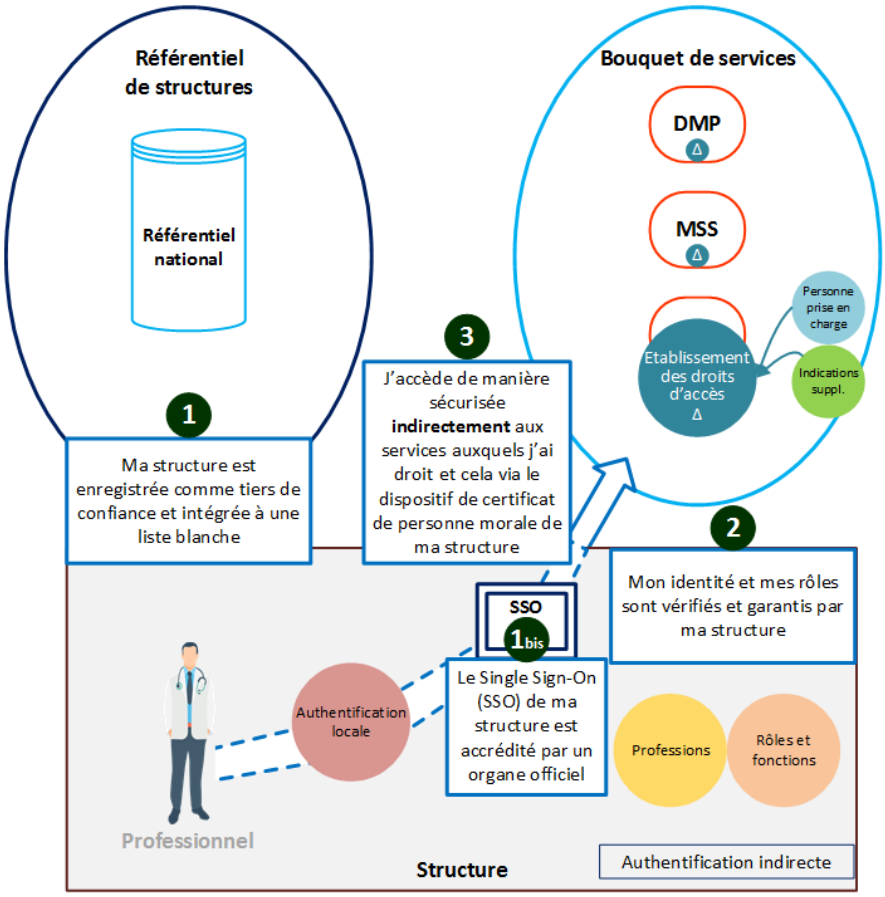


Espace national de confiance ACTUEL avec le référentiel des professionnels du secteur et l'authentification publique directe



Espace national de confiance CIBLE avec le référentiel des professionnels du secteur et l'authentification publique directe

L'Espace de confiance : Accès par sa Structure en authentification indirecte cible



Espace national de confiance CIBLE avec le référentiel des structures du secteur et l'authentification indirecte

Schéma en version de travail