MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Journée régionale CYBER ARA

Programme CaRE - HospiConnect
Atelier HospiConnect

19/11/2024 | Agence du Numérique en Santé

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Sommaire

- Rappel du contexte réglementaire
- Le domaine HospiConnect du programme CaRE : l'Appel à projet alpha
- Témoignage croisé de deux lauréats de l'AAP alpha HospiConnect : ADEF Résidences et Calydial

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

La transformation commence ici

Rappel du contexte réglementaire

Contexte réglementaire - le référentiel relatif à l'identification électronique (RIE) des acteurs des secteurs sanitaire, médico-social et social

- **Le référentiel relatif à l'identification électronique (RIE) des acteurs des secteurs sanitaire, médico-social et social est un pilier de la Politique générale de sécurité des systèmes d'information de santé (PGSSI-S). Rendu opposable par arrêté ministériel le 28 mars 2022, il vise à renforcer la sécurité autour de l'identification électronique, c'est-à-dire le processus utilisé par une personne pour s'identifier et s'authentifier.**

- **Concernant les professionnels, l'identification électronique repose :**
  - D'une part sur le répertoire partagé des professionnels intervenant dans le système de santé (RPPS). C'est le répertoire d'identité sectoriel de référence, permettant d'attribuer à chaque professionnel une identité unique au niveau national (demain au niveau européen).
  - D'autre part, chaque professionnel enregistré doit utiliser un moyen d'identification électronique adapté pour s'authentifier sur les services numériques en santé (apporter la preuve que la personne identifiée est bien celle qui se connecte).

Le RIE détermine la trajectoire de sécurisation progressive de l'identification électronique des professionnels intervenant dans le système de santé.

- ✓ **Qualité du répertoire d'identité local (identités, synchro GRH)**
- ✓ **SSO obligatoire dans les grands établissements**
- ✓ **Engagement de sécurisation de l'IE**

Au 1er janvier 2026, les moyens d'identification électronique (MIE) utilisés devront faire intervenir une authentification renforcée (double facteur), par l'intermédiaire des MIE encadrés par la puissance publique (carte CPS, Pro Santé Connect) ou de MIE homologués ou de MIE certifiés de niveau de garantie eIDAS substantiel ou élevé.

Zoom sur les services numériques dits « sensibles »

- **Les services « sensibles » sont les services numériques en santé au sens du L. 1470-1 du code de la santé publique, qui traitent des données de santé à caractère personnel au sens du RGPD, et qui appartiennent au moins à l'une des catégories suivantes :**
  - Les services partagés, définis comme dépassant le cadre d'une personne morale et/ou mis en œuvre à l'échelle d'un territoire ou au niveau national (ex : dossier médical partagé, plateforme de e-parcours, dossier pharmaceutique, etc.) ;
  - Par transitivité, les services numériques qui intègrent des services partagés (ex : dossier patient informatisé, système de gestion de laboratoire, système d'information de radiologie, boites de messageries sécurisées de santé, etc.) ;
  - Les services proposant un accès web externe aux SI, pour les professionnels d'un établissement (ex : services accessibles en mobilité ou télétravail) ou leurs correspondants de ville ;
  - Les services non partagés mais qui intègrent des traitements de données ou des accès de grande échelle, définis comme les situations où :
    - Soit le nombre de patients dont les données sont nouvellement référencées dépasse 10 000 par an ;
    - Soit le nombre de professionnels distincts s'identifiant électroniquement dépasse 1 000 par an.

Contexte réglementaire - Arrêté du 26 octobre 2023 fixant les règles de gestion des droits d'accès au DMP

Dès à présent, l'accès des professionnels habilités à la consultation du Dossier médical partagé nécessite l'utilisation de MIE à double-facteurs d'authentification (cf. Arrêté du 26 octobre 2023 portant approbation du référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au DMP).

- ✓ **RGPD, information usagers, sensibilisation des professionnels, sécurité (2FA), traçabilité, alimentation/consultation/téléchargement de documents…**
- ✓ **Modalités de mise en œuvre de l'authentification indirecte : AIR Simplifié**

Accès au Web PS DMP	• Cartes CPS • Pro Santé Connect (e-CPS, CPS, futurs MIE compatibles)
Accès au DMP depuis le DPI – lien contextuel vers le Web PS DMP	• Mode AIR simplifié • Pro Santé Connect (e-CPS, CPS, futurs MIE compatibles)
Accès au DMP de manière intégrée depuis le DPI	• Authentification directe via les API PSC • Authentification indirecte renforcée (AIR Simplifié) : modalité de consultation exigée en vague 2 pour les éditeurs

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

La transformation commence ici

Le programme CaRE

Domaine HospiConnect

L’émergence du domaine HospiConnect du programme CaRE

Besoin identifié

Authentification des professionnels pour accéder aux SI de santé

- Utilisation **de moyens d’identification électronique** (MIE)
- Permettre aux professionnels de s’authentifier **facilement** et de **manière sécurisée**

Cadre légal

Référentiel d’identification électronique de la PGSSI-S

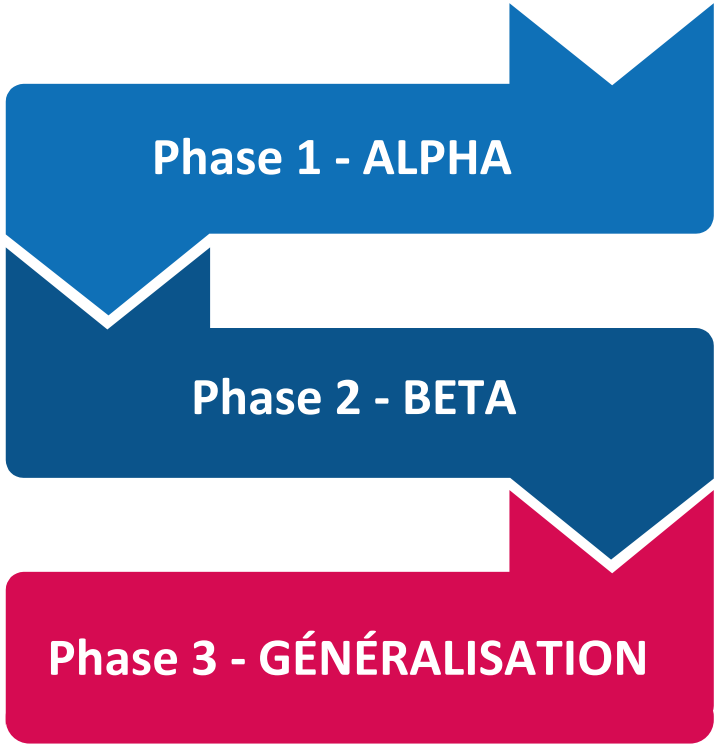
- Présente les **exigences applicables aux MIE**, en cible à partir du 01/01/2026, ou pendant la période de transition jusqu’à cette date

Domaine HospiConnect

Accompagner les établissements sur les plans techniques et financiers afin d’accélérer l’adoption par les établissements de solutions qui soient conformes au référentiel d’identification électronique et permettant de simplifier et sécuriser l’accès des professionnels aux services numériques sensibles.

Domaine HospiConnect - démarche adoptée

- Compte tenu du caractère innovant des organisations et des solutions à mettre en œuvre dans les structures pour l'atteinte de cet objectif, une démarche itérative est proposée pour les expérimenter progressivement sur le terrain



Appel à Projet d'expérimentation destiné à un nombre limité de structures (***15 structures***)

- **Qualifier des solutions** (techniques et organisationnelles) **avec un support renforcé de l'ANS et un soutien financier** tenant compte du caractère innovant, voire expérimental des solutions.
- **Permettre à l'ANS de tester**, avec les candidats proposant **un projet s'appuyant sur les MIE délivrés par l'ANS**, les **organisations et processus cibles** nécessaires à l'atteinte du niveau de garantie **eIDAS substantiel** des MIE fournis par l'ANS

Appel à Projet destiné à un **nombre étendu** de structures

Dispositif destiné à **toutes les structures** dont les modalités seront définies ultérieurement

Domaine HospiConnect – Phase 1 – AAP d'expérimentation

- Les objectifs à atteindre dans le cadre de cet appel à projet sont présentés selon trois niveaux de cibles.
- Le projet proposé par le candidat doit répondre a minima aux objectifs de la cible 1.

Cible 1	Cible 2	Cible 3
Authentification 2FA (réalisée au moyen d'un ou plusieurs moyens d'identification électronique 2FA, conformes au référentiel d'identification électronique de la PGSSI-S) **pour l'accès au DPI/DUI et en consultation au DMP**.	Périmètre cible 1 mais avec une **authentification 2FA sur un composant IAM / webSSO d'authentification interne** à la structure et délégation de l'authentification a minima du DPI/DUI à ce composant interne d'authentification via un connecteur OIDC	Périmètre cible 2 auquel s'ajoute la mise en place et le **déploiement de la fédération d'identités** entre le composant d'authentification interne à la structure et ProSantéConnect.

AAP alpha CaRE HospiConnect – Cible 1

Cible 1 (base)

- **Enregistrement dans un répertoire d'identité local** de l'ensemble des professionnels concerné par le périmètre du projet **selon un principe de dérivation de l'identité nationale** avec :
  - Une vérification d'identité conforme au niveau substantiel eIDAS (contrôle en face à face d'une pièce d'identité ou utilisation d'un MIE conforme lors d'une procédure à distance (ex: France Connect +) ;
  - Une procédure en vigueur de contrôle et de mise à jour des habilitations (profession, catégorie professionnelle, diplôme …) et de gestion des début/fin d'activités au sein de l'établissement.
- **Enregistrement au RPPS** de l'ensemble des professionnels concerné par le périmètre du projet
- **Authentification 2FA pour l'accès au DPI/DUI et en consultation au DMP** sur un sous-ensemble de services/unités de soins.
- L'authentification 2FA doit être réalisée au moyen d'un ou plusieurs **moyens d'identification électronique 2FA**, conformes au **référentiel d'identification électronique de la PGSSI-S** (MIE conforme à la cible, ou MIE de transition valable jusqu'au 01/01/2026). Il n'y pas d'obligation cependant à l'utilisation du même type de MIE par l'ensemble des professionnels d'une même structure.
- L'authentification 2FA au DMP peut être réalisée via ProSantéConnect ou AIR Simplifié.

AAP alpha CaRE HospiConnect – Cible 2

Cible 2

- Le niveau 2 inclut le niveau 1 auquel s'ajoute des **objectifs d'ergonomie et de simplification de l'expérience utilisateur vis-à-vis du SIH**.
- Authentification 2FA sur un **composant IAM/webSSO d'authentification interne à la structure** et **délégation de l'authentification *a minima* du DPI/DUI** à ce composant interne d'authentification **via un connecteur OIDC** :
  - Le connecteur OIDC sera rendu obligatoire sur les LPS référencés dans le couloir hôpital ;
  - La mise en œuvre d'une brique de SSO est rendue obligatoire par le RIE pour certaines structures.
- Cette cible permet aux professionnels de santé de se connecter au minimum à leur DPI en utilisant leur identité provenant du **référentiel d'identités local de l'établissement**.

AAP alpha CaRE HospiConnect – Cible 3

Cible 3

- Le niveau 3 inclut le niveau 1 et le niveau 2 auxquels s'ajoutent des objectifs d'ergonomie et de **simplification de l'expérience utilisateur vis-à-vis de l'écosystème externe à la structure**.
- L'objectif du projet est de mettre en place et déployer la **fédération d'identités entre le composant d'authentification interne à la structure et ProSantéConnect**.
- En tant que FI Tiers PSC, un établissement pourra proposer une expérience utilisateur optimale aux professionnels qui y exercent, tout en restant autonomes dans la gestion des identités au sein de la structure :
  - Navigation sans réauthentification au sein du SIH par l'intermédiaire des MIE choisis et d'une brique d'IAM/SSO (synchronisation des identités avec la base GRH).
  - L'utilisation d'une brique de SSO indépendante de Pro Santé Connect permet notamment de se prémunir d'une indisponibilité du service (hors e-CPS), ou d'une coupure du réseau externe à l'établissement (par exemple en cas de cyberattaque).
  - Navigation « à la demande » sans réauthentification vers tous les services numériques externes raccordés à Pro Santé Connect (éventuellement via API avec les LPS satisfaisant aux exigences de l'EdC).
- L'atteinte de cette cible implique pour l'établissement de satisfaire aux exigences de sécurité de **« Espace de Confiance »** (EdC) en tant que FI Tiers, en utilisant notamment une solution d'IAM reconnue, quels que soient les moyens d'identification électronique utilisés, tant qu'ils sont conformes au Référentiel d'identification électronique (CPS, autres MIE compatibles avec PSC comme les clés de sécurité FIDO, MIE 2FA homologués par l'établissement ou MIE qualifiés par l'ANSSI au niveau substantiel ou élevé eIDAS).

Précisions sur les MIE utilisés

▶ L'authentification 2FA mise en place dans le cadre du projet doit être réalisée au moyen d'un ou plusieurs MIE conforme(s) au référentiel d'identification électronique des personnes physiques

Les grands principes du RIE

- MIE proposés par Pro Santé Connect (PSC)
  ➔ CPx, e-CPS, clés de sécurité FIDO dont la liste sera prochainement communiquée sur le site de l'ANS (la clé de sécurité FIDO compatible devra être activée par l'utilisateur avec sa e-CPS)
- MIE certifiés de niveau eIDAS Substantiel
- MIE destiné à une auto-homologation par la structure

Quelques exemples de solutions expérimentée

Carte à puce (e.g. CPx)
Exploitation du standard sans contact MIFARE DESFIRE
Exploitation du standard FIDO2

Journée régionale CYBER ARA du 19/11/24
Présentation HospiConnect

Adeline Lembré (Cheffe de projet) - *adeline.lembre@algonis.net*

Jean-Pierre Grangier (DSI) - *jean-pierre.grangier@calydial.org*

Agenda

1. Présentation des lauréats
2. Composants fonctionnels IAM
3. Les challenges
4. Projets et retours d'expérience Lauréats
5. Exemple de cycle de vie utilisateurs
6. Planning
7. Annexes : Architecture

Lauréat ESMS : Association Adef Résidences

Caractéristiques

- ✓ **Secteur d'activité :** Hébergement médicalisé pour personnes âgées
- ✓ **Cible choisie :** Cible 3
- ✓ **Secteur de la population pilote :** Médico-social
- ✓ **Nombre de site(s)** : 1 groupement réparti sur 50 sites (3500 utilisateurs)
- ✓ **Nombre de professionnels concernés par le projet** : 300 utilisateurs sur 3 sites (EHPAD)

Editeurs

- ✓ **IAM :** Okta
- ✓ **DUI :** Teranga
- ✓ **Intégrateur** : Lyvoc

Niveau de maturité

Cible d'authentification retenue : Authentification Forte via le AMFA d'Okta pour l'accès aux applications.

MIE retenus (Moyen D'identification Électronique) : Okta Verify et e-CPS (Dématérialisé), CPS et Yubikey (Matériel).

Fédération d'identité et gestion des droits et des accès : Okta gère toutes les identités et les accès, provisionning et déprovisonning de compte pour les applications intégrées. **Fédération permet de déléguer l'authentification PSC à Okta.**

94200 Ivry-sur-Seine

Lauréat ES : Centre Associatif Lyonnais De Dialyse

Caractéristiques

- ✓ **Secteur d'activité :** ESPIC (Établissement de santé privé d'intérêt collectif)
- ✓ **Cible choisie :** Cible 3
- ✓ **Secteur de la population pilote :** Sanitaire
- ✓ **Nombre de site(s)** : 1 établissement réparti sur 4 sites
- ✓ **Nombre de professionnels concernés par le projet** : 165 utilisateurs (Ensemble du personnel Calydial)

Editeurs

- ✓ **IAM :** Okta
- ✓ **DPI :** Médial
- ✓ **Intégrateur** : Lyvoc

Niveau de maturité

69540 - Irigny
38200 - Vienne

Cible d'authentification retenue : Authentification Forte via le MFA d'Okta pour les applications et pour l'ouverture de la session windows.

MIE (Moyen D'identification Électronique) : Okta Verify (Application installée sur le poste et/ou sur les portables).

Fédération d'identité et gestion des droits et des accès : Okta gère toutes les identités et les accès, provisionning et déprovisonning de compte pour les applications intégrées. **Fédération permet de déléguer l'authentification PSC à Okta.**

Composants fonctionnels IAM apportés par Okta

Les Briques Okta essentielles à HospiConnect

Annuaire centralisé UD

Okta à la capacité de se connecter, de communiquer et intégrer en son sein facilement divers annuaires d'identité.

Authentification Unique SSO

Simplifie la connexion en permettant aux utilisateurs de se connecter une seule fois pour accéder à toutes les applications.

Authentification à multiple Facteur MFA

Quand une application est liée à Okta, on peut renforcer la sécurité en demandant une double vérification, comme une empreinte digitale ou un SMS.

Les Briques Okta hors périmètre

Gestion du cycle de vie LCM

Okta peut simplifier et sécuriser les processus d'onboarding et de offboarding des employés depuis le SIRH, depuis Okta ou un autre outil pour les externes.

Automatisation des processus d'identité

Sans écrire de code. Utilisez la bibliothèque de connecteurs préconstruite d'Okta et la possibilité de se connecter à n'importe quelle API publiquement disponible.

Pourquoi Okta répond aux cibles HospiConnect ?

Cibles	Challenges en milieu Santé	Valeur ajoutée d'Okta
Centraliser et gérer l'ensemble de vos comptes au sein d'un référentiel d'identités unique	▪ De multiples sources d'utilisateurs (AD, SIRH, Base de Donnée) ▪ Gestion fine des droits d'accès basés sur des rôles spécifiques ▪ Des exigences fortes de disponibilité et de résilience	▪ Intégration native des sources d'identité via des connecteurs Okta (SIRH, Annuaire AD, LDAP, API, …) ▪ Automatisation des entrée / mouvement / sortie via des formulaires flexibles et des workflows ▪ Une architecture 100% Cloud résiliente et offrant une grande disponibilité
Sécurisation de l'accès au DPI/DUI via un connecteur OIDC et une authentification forte 2FA	▪ Des exigences d'accessibilité et de rapidité ▪ Des profils différents (cadres, infirmières, ...) n'ayant pas les mêmes équipements à dispositions pour le MFA	▪ Intégration SSO simplifiée avec le DPI/DUI via un connecteur custom OIDC ▪ De multiples moyens d'identification électronique 2FA conformes au PGSSI-S (Okta Verify, CPS, clé FIDO…) ▪ Configuration de politiques de sécurité permettant une authentification 2FA adaptée au contexte de connexion
Mettre en place et déployer la fédération d'identités entre le composant d'authentification interne à la structure et Pro Santé Connect	▪ Sécurisation du lien de fédération avec Pro Santé Connect	▪ Fédération possible entre Okta et Pro Santé Connect via les protocoles standards (SAML ou OIDC)

Adef Résidences

CALYDIAL

Etats des lieux du SI

Juin 2024
En cours

Remédiation

- Nettoyage des comptes AD
- Renommage des logins
- Convention de nommage des mails
- Réconciliation des comptes AD/SIRH/Entra

Juillet 2024
En cours

DUI

- Teranga (Netvie)
- Authentification Native avec PSC

Office 365

Novembre 2024
En cours

Intégration SSO/OIDC

Fédération Pro Santé Connect

- Préparation d'un POC avec Okta

Remédiation

- Remédiation des comptes et des groupe AD

Office 365

DPI

- Médial (Echo)
- Développement connecteur assisté par Lyvoc

Octime et Bluekango

Juin 2023

Mars 2024

Août 2024
En cours de finalisation

Juillet 2024
En cours

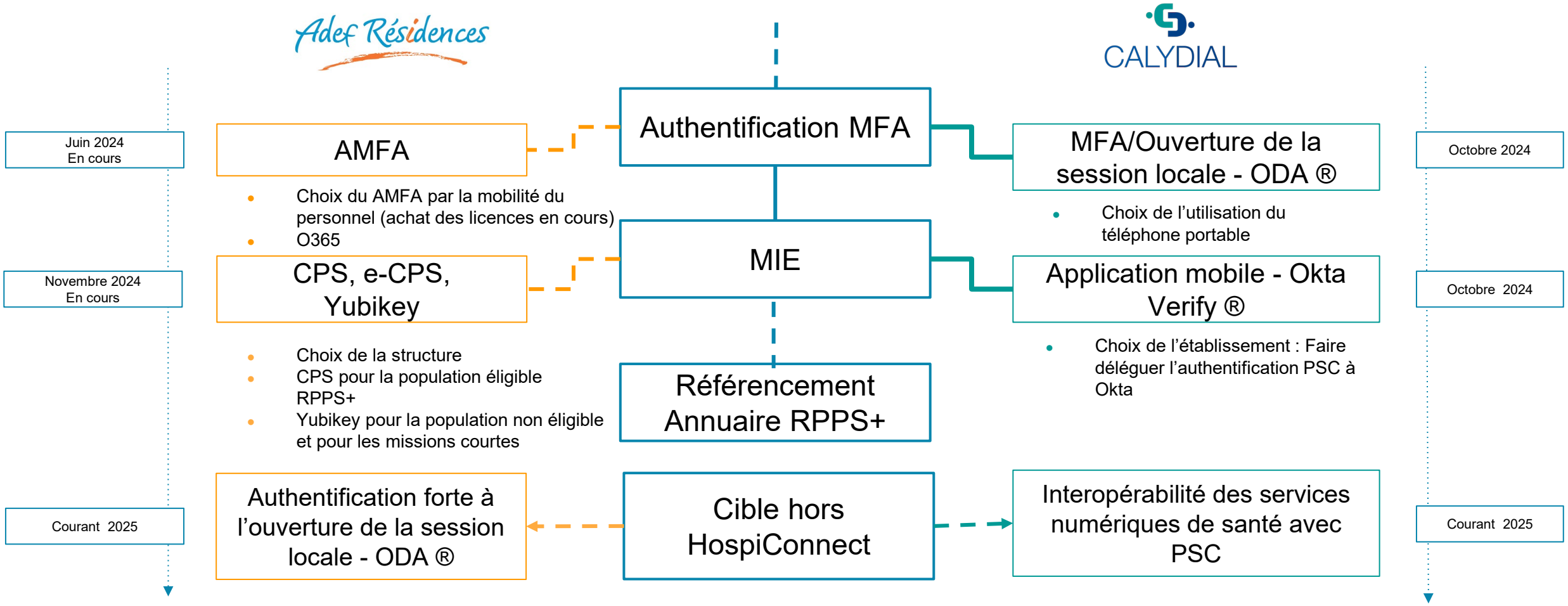
Novembre 2024
En cours

Points d'attention

- Utilisation des comptes génériques dans les ESMS
- Missions courtes absentes du SIRH
- Processus entrée/sortie non définis
- Processus création login, mails… non mis en place
- AD/Entra/SIRH non synchronisés
- La réussite du projet nécessite une bonne coordination entre tous les acteurs des établissements (SIRH, Métiers,IT) et des éditeurs

Points d'attention

- Etats de lieux SI : La gestion du changement, le passage par la validation par le CSE de l'utilisation des terminaux mobiles personnels pour la gestion des MDP
- Avancer en ayant une vision globale des différents protagoniste et de l'état de l'avancement de chaque éditeur



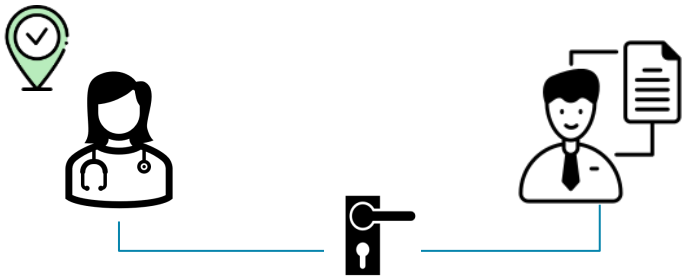
⚠ Points d'attention

- Choix de la Yubikey pour ses capacités multi-usages (contrôle des accès, imprimante, pointage présence)
- Choix du RH de ne pas généraliser l'utilisation des téléphones (coûts)
- Obligation d'un lecteur de badge sur tous les postes
- ODA ® (Okta Device Access) - Limitation des facteurs d'authentification

⚠ Points d'attention

- Définition RPPS+ (personnel sans ordre et ne dépendant pas d'une ARS) et RPPS.
- Bien comprendre les enjeux des annuaires publics/restreints
- Le risque de mise en place de 2 processus en parallèle, l'un ayant comme autorité d'enregistrement l'établissement, l'autre via un ordre ou une ARS.

La gestion du cycle de vie des utilisateurs (RPPS+)



Enregistrement RPPS+

S'identifier avec FranceConnect

Pré-boarding de l'utilisateur

Contrôle de l'identité physique

- Validation dans le e-portail
- Création du compte manuel dans le répertoire d'identité locale via un formulaire

Remise du matériel dont MIE

Ouverture de session locale
Possibilité de 2FA via ODA ®

MFA

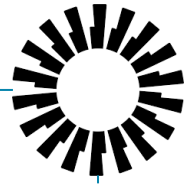
Authentification Okta
Via Okta Verify, Carte CPS, e-CPS, Yubikey.

SSO

PRO SANTÉ CONNECT
Un service du ministère chargé de la Santé

DMP
GCSoara
Doctolib

Création automatique du compte Okta via import/API



Onboarding

Provisioning des Comptes applicatifs

- **Création des comptes**
  Automatisé avec les Workflows et le Lifecycle Management ou Manuel via alerting Okta

Offboarding

Déprovisioning des Comptes applicatifs

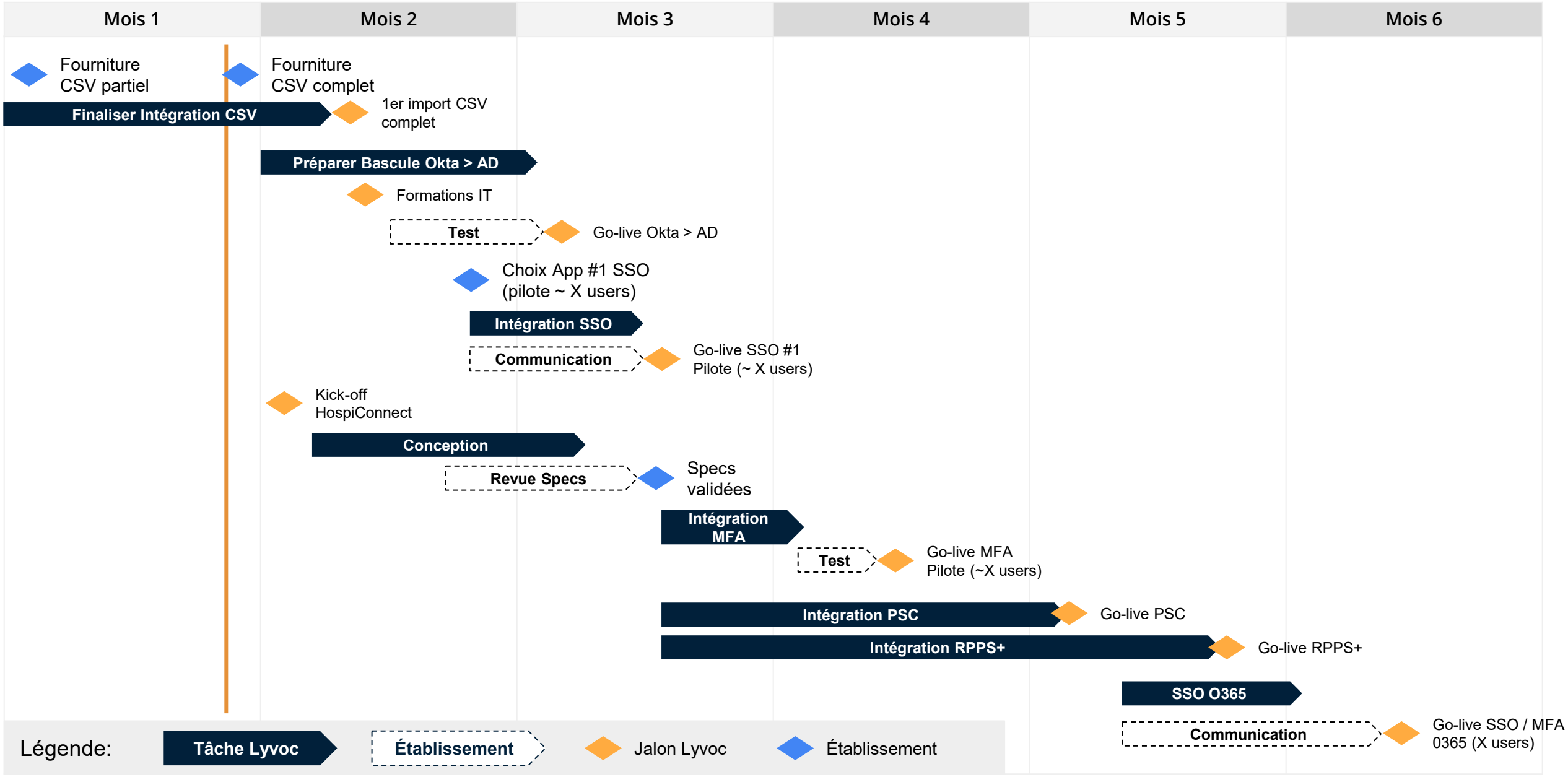
- **Désactivation des comptes**
  Automatisé avec les Workflows et le Lifecycle Management ou Manuel via alerting/routine hebdomadaire d'Okta
- **Consommation de licence** par la mise en place d'un reporting des comptes possible via WF Okta.

SSO

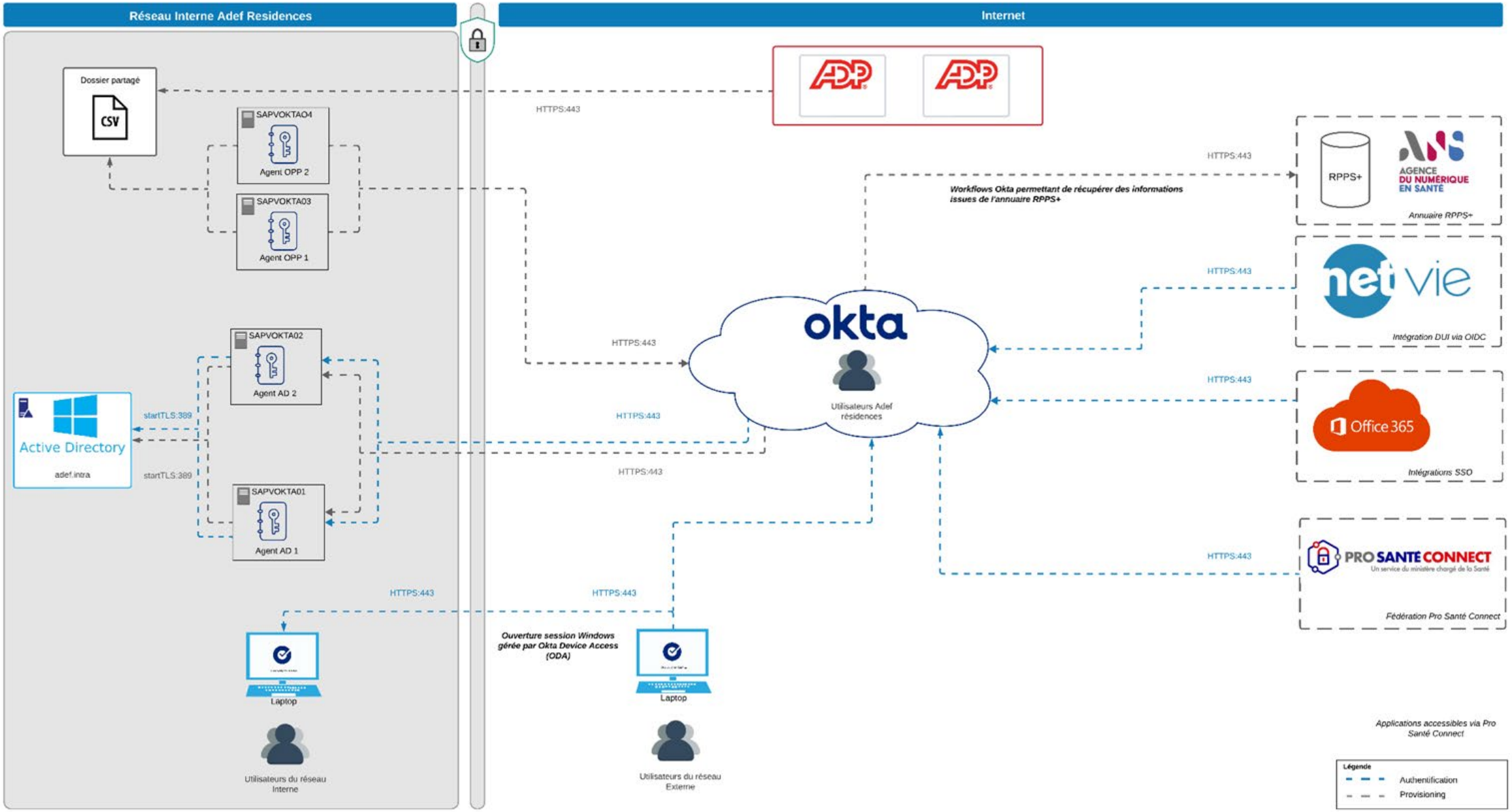
Authentification transparente

netvie
Office 365
CCTIME
GIE MEDIAL MEDECINE - DIALYSE
BlueKanGo

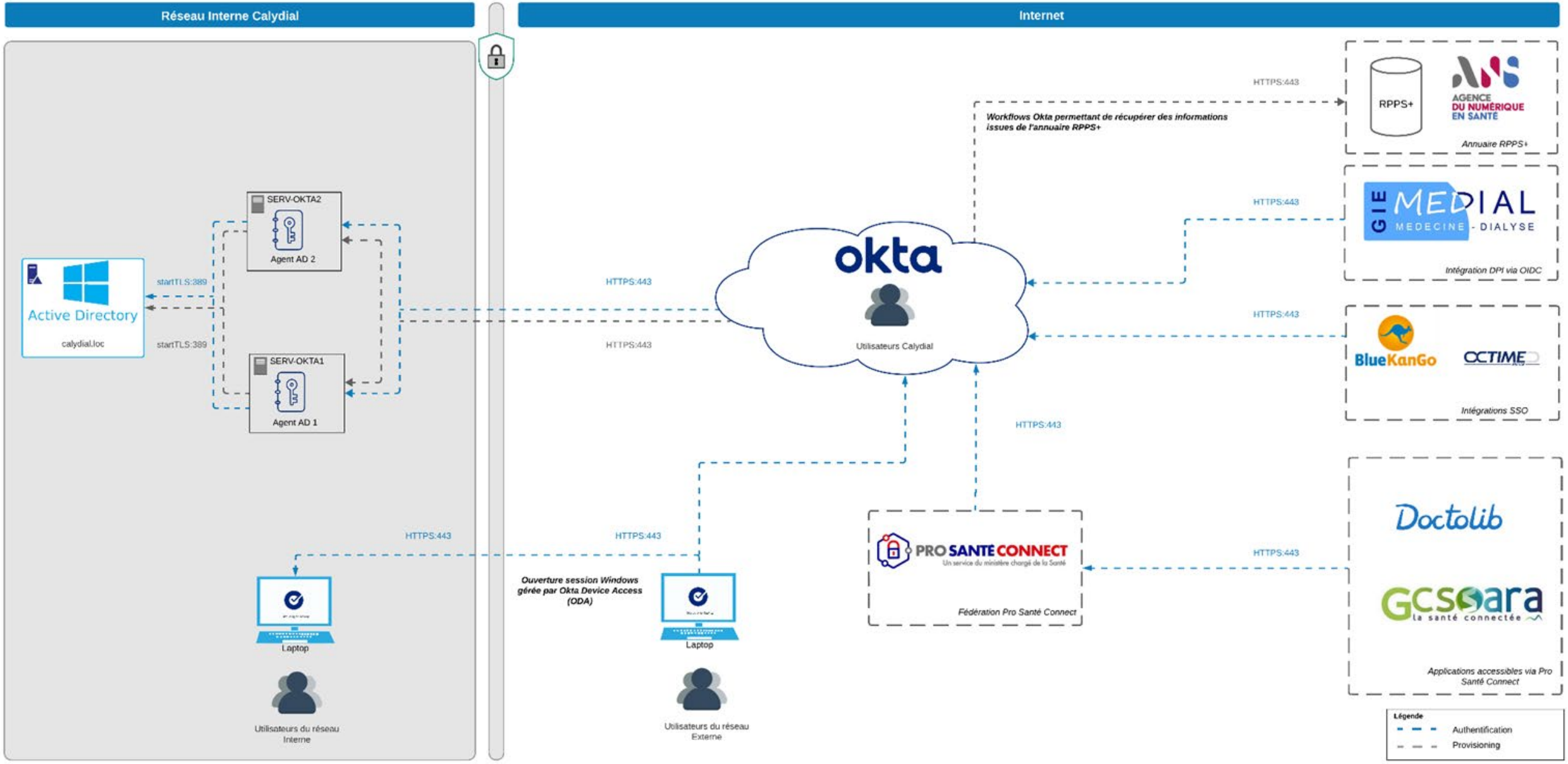
Planning HospiConnect



Architecture Adef Résidences



Architecture Calydial



Points de contacts

Pour toute demande autour du programme, l'adresse mail dédiée : *ans-care-hospiconnect@esante.gouv.fr*

Page web dédiée au Programme CaRE sur le site de l'ANS :
https://esante.gouv.fr/strategie-nationale/CaRE

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

La transformation commence ici

Annexes

Dérivation d'identité

- Le processus de dérivation d'identité est une des deux options de processus pouvant être intégrés au fonctionnement RH des structures.
- En cible, chaque identité éligible au RPPS dans un référentiel local sera dérivée d'une identité nationale de santé présente au RPPS.