AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

# API PSConnectées

## Etude des architectures

22/09/2023

# Bonnes pratiques webinaire

Utilisez l’onglet « questions / réponses » si vous avez une question

Pensez à bien désactiver votre micro lorsque vous ne parlez pas et à lever la main pour intervenir

Ce webinaire est filmé et un replay sera disponible

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

# Sommaire

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

# Rappel du contexte

# Publications & Dates

## Arrêté Pro Santé Connect

Arrêté du 4 avril 2022 relatif à des moyens d'identification électronique immatériels mis à disposition des professionnels, personnes physiques des secteurs sanitaire, social et médico-social pour l'utilisation des services numériques en santé

https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045551195

## Cadre d'Interopérabilité

Publication le 5 juin 2023 du Volet Transport synchrone pour API REST en version 1.1 du Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS).

https://esante.gouv.fr/services/referentiels/ci-sis/espace-publication/couche-transport

# Contexte & objectifs

## Contexte

Afin de **faciliter l'interopérabilité** entre les **SI de santé**, un modèle global s'appuyant sur des échanges via API REST est décrit au travers du CI – SIS API Rest.
Ce modèle propose une approche différente aux architectures actuellement mise en œuvre dans le secteur de santé. Il y a un fort enjeu à **faciliter l'adoption de ce nouveau modèle** auprès des éditeurs de Logiciels de Professionnels de Santé (LPS).

## Objectifs

L'objectif de cette étude est de **présenter les différentes architectures possibles, d'orienter et d'accompagner les éditeurs** au travers de recommandations vers les architectures retenues.
En complément des aspects directement liés à l'architecture (disponibilité, scalabilité, sécurité, etc..), l'aspect organisationnel notamment au travers du modèle de contractualisation cible est pris en compte pour s'assurer de la pérennité du modèle dans son ensemble à l'échelle de l'ensemble des acteurs de la e-santé.

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

# Etude des architectures

# Glossaire

API : « Application Programming Interface »

DMP : Dossier Médical Partagé

ES : Etablissement de Santé

FSE : Feuille de Soin Electronique

IGC : Infrastructure de Gestion des Clés

LPS : Logiciels de Professionnel de Santé

PS : Professionnel de Santé

PSC : Pro Santé Connect

REST : « Representational State Transfer »

SI : Système d'Information

TSE : « Terminal Server Edition »

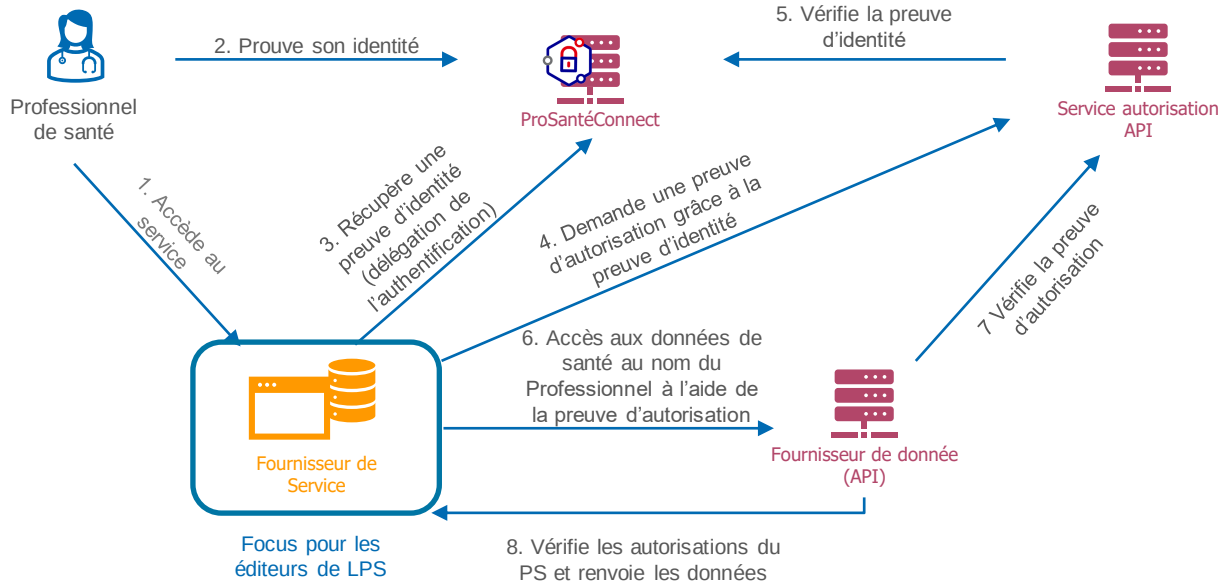
Éditeur * : celui qui fournit la solution logicielle.

Opérateur * : celui qui opère la solution.



** Dans le cas des solutions en SaaS, la plupart du temps les deux notions se confondent, mais dans le cas des solutions déployées au sein d'un ES par exemple, l'opérateur = ES mais l'éditeur en est un autre, et l'éditeur du proxy peut être différent de l'éditeur de l'application.*

# Le modèle API ProSantéConnectée – vue d'ensemble fonctionnelle




Au sein du « Fournisseur de service » décrit dans le CI-SIS, plusieurs composants sont à prendre en compte dans l'architecture cible : l'interface utilisateur, l'applicatif métier et les différents proxy ProSantéConnect & APIs

# Caractéristiques & cas d'usages considérés

## Interface utilisateur

- Client **lourd** (Logiciel installé sur un poste de travail)
- Client **natif** (type mobile).
- Client **léger** (page web).

## Serveur applicatif

- **Local ou sans DSI :** Type logiciel autonome installé sur un poste de travail (utilisé pour les médecins libéraux par exemple).
- **Mutualisé pour plusieurs entités morales :** serveur dédié dans un **centre de données**. Par exemple service SaaS à destination de plusieurs libéraux, ou plusieurs ES type officine.
- **Dédié à un ES ou un groupement d'ES** : serveur dédié dans un **centre de données**, configuré spécifiquement pour un ES (par exemple logiciel installé sur le SI d'un ES)

## Hébergement du serveur applicatif

- **Sur les infrastructures** d'un établissement de santé
- **Par l'éditeur** en tant que service managé
- Sur **un poste de travail**

## Proxy PSC & API

- Proxy **intégré** au serveurs applicatifs
- Proxy **mutualisé** et/ou **externalisé** entre plusieurs applicatifs voire plusieurs éditeurs

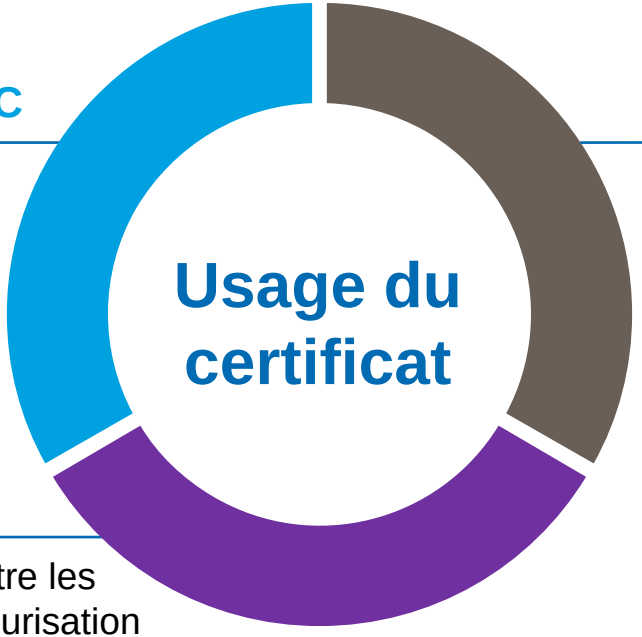
# Certificats et traçabilité (1/2)

## Authentication FS-PSC

Authentifier la solution (FS) souhaitant authentifier le PS auprès de PSC

## Sécurisation des échanges

Sécuriser les échanges entre les composants (mTLS) et sécurisation des jetons d'accès API (si mise en œuvre du token binding)




## Authentification FS-FD

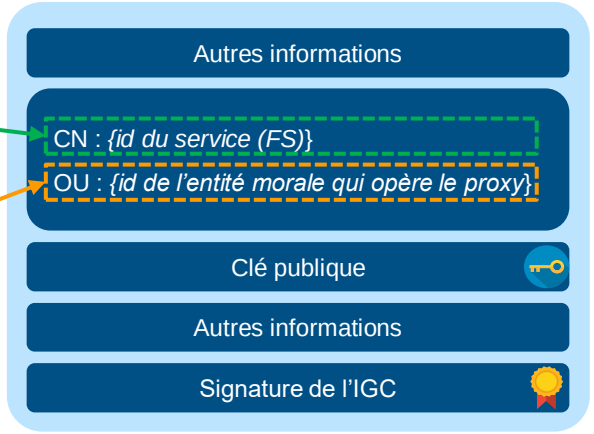
Authentifier la solution souhaitant récupérer des données de santé au nom du PS connecté (échange avec le serveur d'autorisation). Il doit donc permettre de définir des autorisations propres au FS (notions de Scopes par FS)

# Certificats et traçabilité (2/2)

Le certificat d'authentification ORG_CLI sera délivré à **l'entité morale opérant** le proxy PSC/API. Un opérateur pourra se voir délivrer **plusieurs certificats** permettant d'identifier et tracer les différentes solutions (Fournisseurs de services). Le processus d'obtention est en cours de définition (habilitation Datapass)

Identifiant à la main de l'opérateur proxy permettant d'identifier le FS

Identification de l'opérateur proxy (type n° FINESS) vérifié par l'IGC santé




Modèle du certificat

**1** certificat (DN) pour **1** client ID PSC

Client ID ProSantéConnect

Le **certificat** identifie la **solution de LPS (FS) via le CN** et **l'opérateur du proxy via l'OU.** Toute solution FS dispose d'un certificat, d'un numéro d'habilitation et d'un *clientID* uniques.

# Architectures initiales (1/3)

Afin d'accompagner les éditeurs dans la mise en œuvre des API PSC connectées en lien avec le CI-SIS, nous présentons notre vision des différentes architectures actuelles mises en place dans le domaine de la santé en France.

1 **Applications mutualisées (mode SaaS)**

2 **Applications dédiées (sur SI)**

3 **Applications locales (historique)**

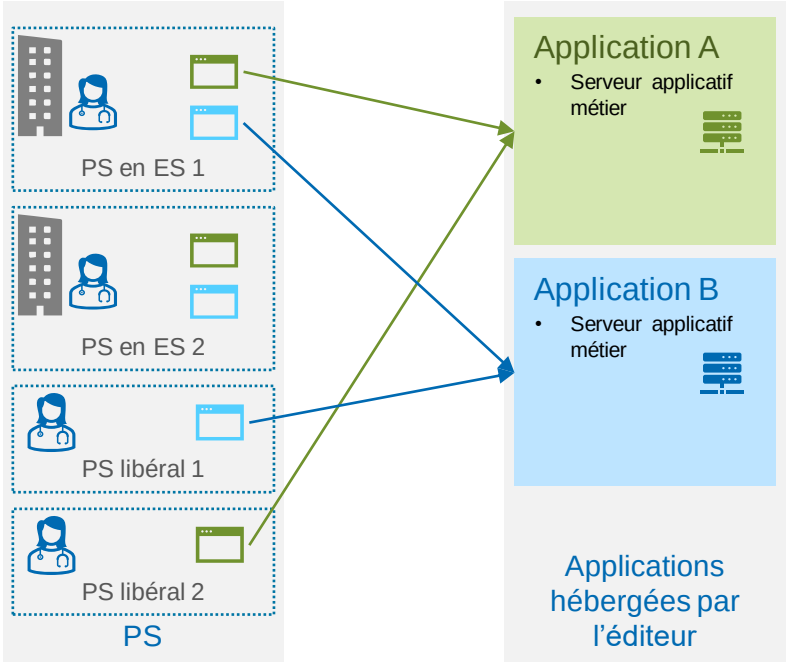
4 **Applications dédiées (hors SI)**

Pour chacun de ces scénarios, une ou plusieurs architectures cibles incluant l'aspect Proxy PSC/API sont présentées & préconisées.

# Architectures initiales (2/3)

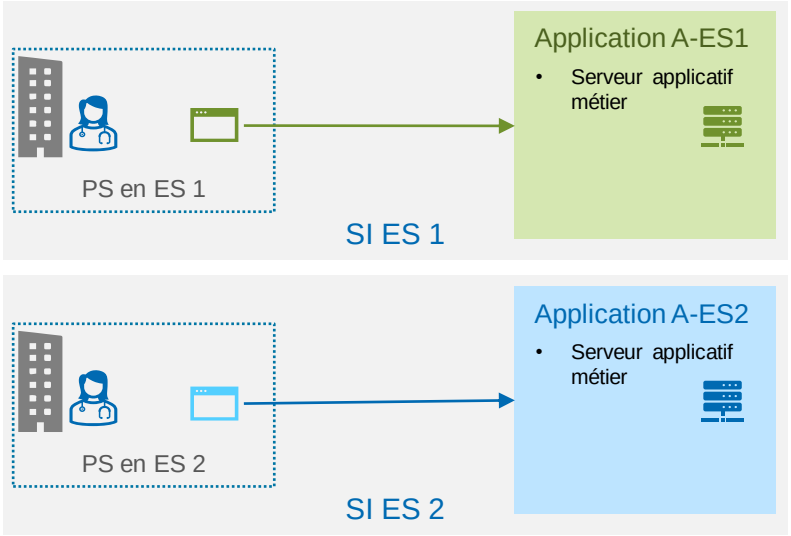
## Cas d'usage #1 : Applications mutualisées (mode SaaS)

Un éditeur qui fournit un **logiciel client/serveur** traditionnel et qui gère déjà des **infrastructures centralisées**.




## Cas d'usage #2 : Applications dédiées (sur SI)

Un éditeur qui fournit un **logiciel client/serveur**, mais la partie **serveur** est **hébergée sur le SI** d'un ES de type centres hospitaliers (CHR, CHI, CHU), grands groupes de cliniques et d'EHPAD.

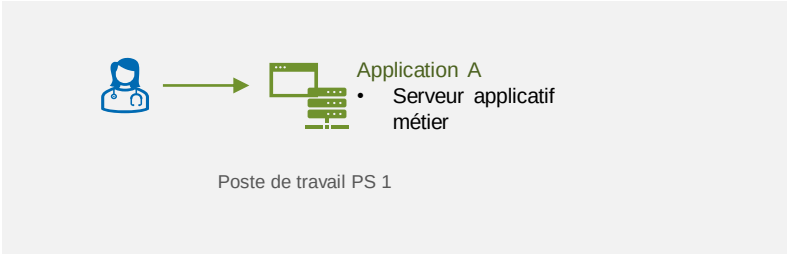



Les instances d'applications sont hébergées sur les SI des ES.

# Architectures initiales (3/3)

## Cas d'usage #3 : Applications locales (historique)

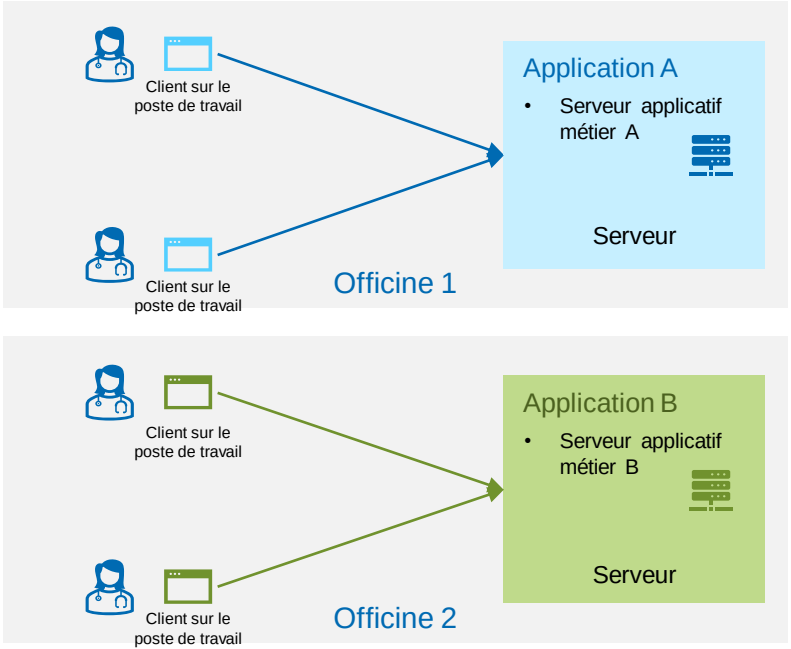
Un éditeur qui fournit un **logiciel « autonome »** installé sur le **poste de travail** d'un PS, mais qui **ne fournit pas de serveur applicatif centralisé**.



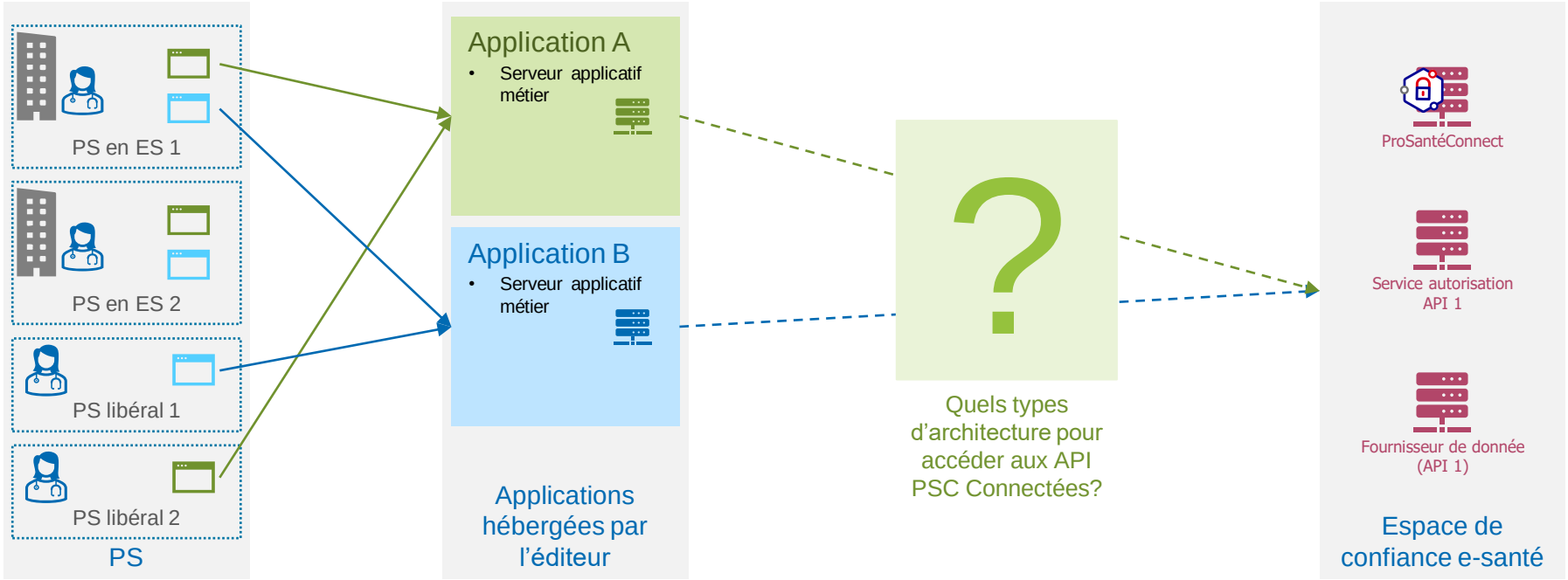

Les serveurs applicatifs métier sont installés sur le poste du PS (type client lourd entièrement local)

## Cas d'usage #4 : Applications dédiées (hors SI)

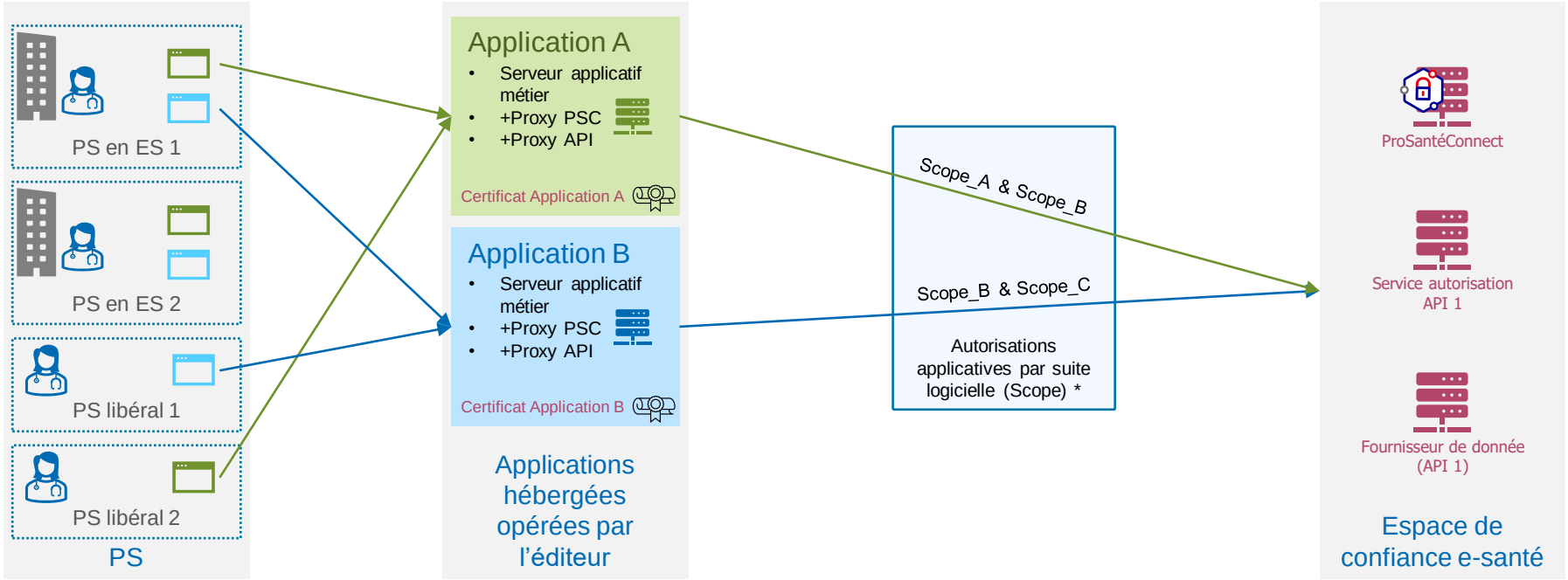
Un éditeur qui fournit un **logiciel client/serveur**, mais la partie **serveur** est **hébergée hors d'un centre de données (cas des officines)**



# Cas d'usage #1 : Application mutualisée



# Cas d'usage #1 : Application mutualisée – Solution 1 : Proxys intégrés




- L'hébergement des applications est réalisé par leur éditeur de manière mutualisée entre les ES.
- Les proxy API et PSC sont intégrés (sous formes de modules) dans chaque application.
- 1 certificat = 1 client id = 1 application (usage « métier »).
- 1 contrat global pour l'éditeur associé à N certificats application.

# Cas d'usage #1 : Application mutualisée – Solution 1 : Proxies intégrés

**Architecture et intégration**

- × Code proxy répliqué pour chaque application
- × Fonctions « métiers » et « proxy PSC » mélangées
- \+ Architecture plus simple (nombre de composants moindre)

**Gestion organisationnelle**

- × Charge de travail supplémentaire pour la mise en place et la maintenance de plusieurs proxys (ex. montée de version)

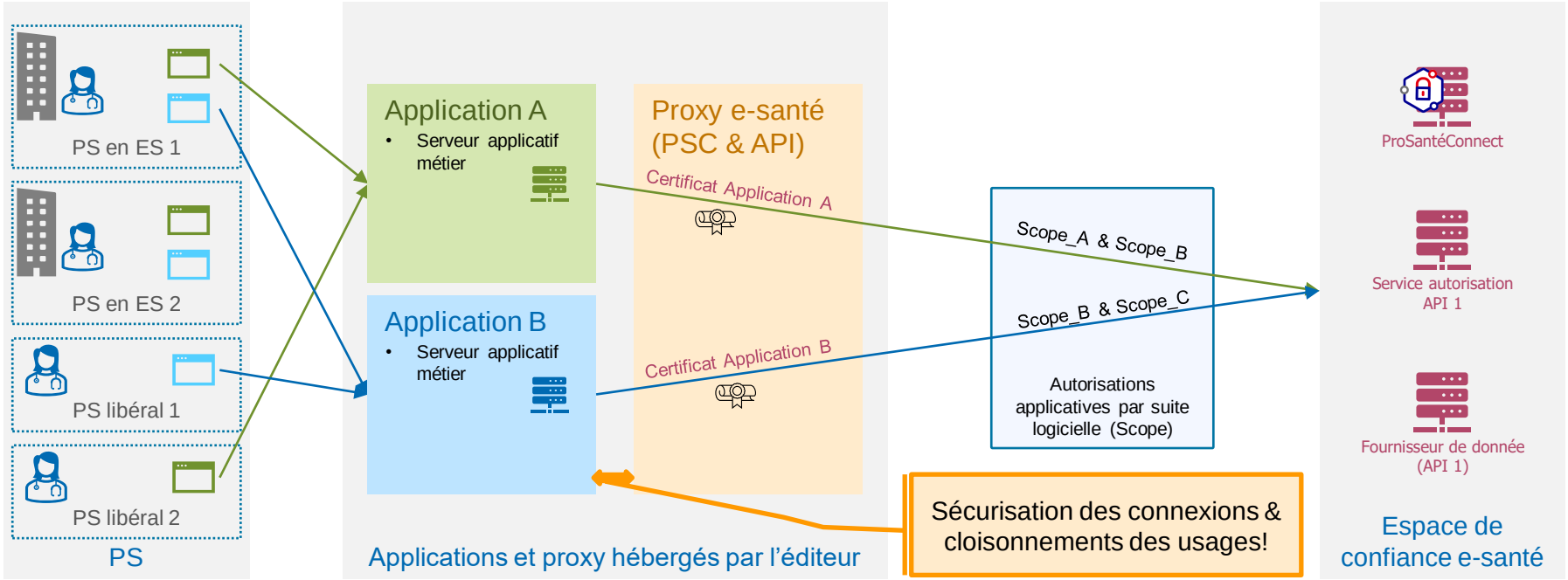
**Gestion de la sécurité**

- × En cas d'audit, chaque application est ciblée dans son intégralité

**Disponibilité et résilience**

- \+ Pas d'effet SPOF

# Cas d'usage #1 : Application mutualisée – Solution 2 : Proxy mutualisé

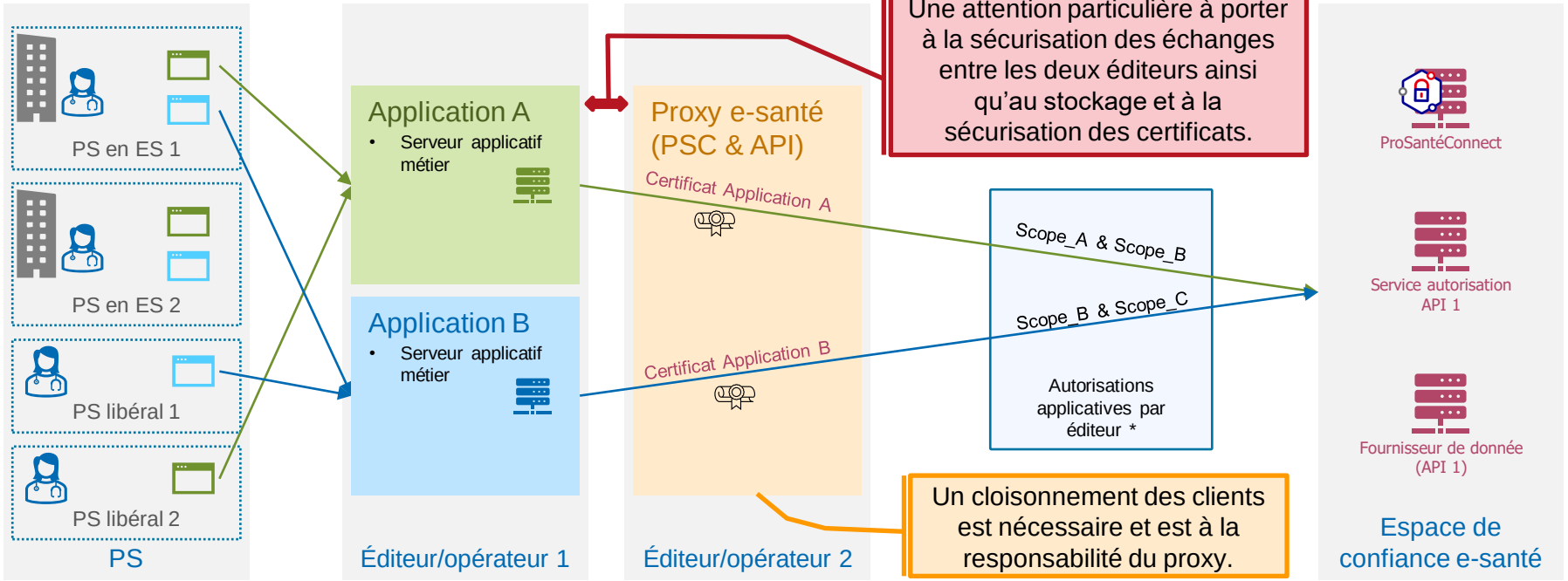



- L'hébergement des applications est réalisé par leur éditeur de manière mutualisée entre les ES.
- Proxy API et PSC mutualisés entre l'ensemble des applications de l'éditeur et opéré par le même éditeur.
- 1 certificat = 1 client id = 1 application.
- 1 contrat global pour l'éditeur associé à N certificats application.

# Cas d'usage #1 : Application mutualisée – Solution 2 : Proxy mutualisé

| | |
|---|---|
| **Architecture et intégration** | + Capacité à mutualiser le développement du proxy<br>+ Logiques métiers & proxy distincts<br>- Architecture plus complexe avec nécessité de gérer la sécurisation serveur LPS <> Proxy |
| **Gestion organisationnelle** | + Maintenance facilitée pour suivre les évolutions des exigences e-santé |
| **Gestion de la sécurité** | + En cas d'audit, seul le proxy est ciblé |
| **Disponibilité et résilience** | - Effet SPOF, nécessitant la mise en place de mesures spécifiques sur le proxy |

# Cas d'usage #1 : Application mutualisée – Solution 3 : Proxy externalisé

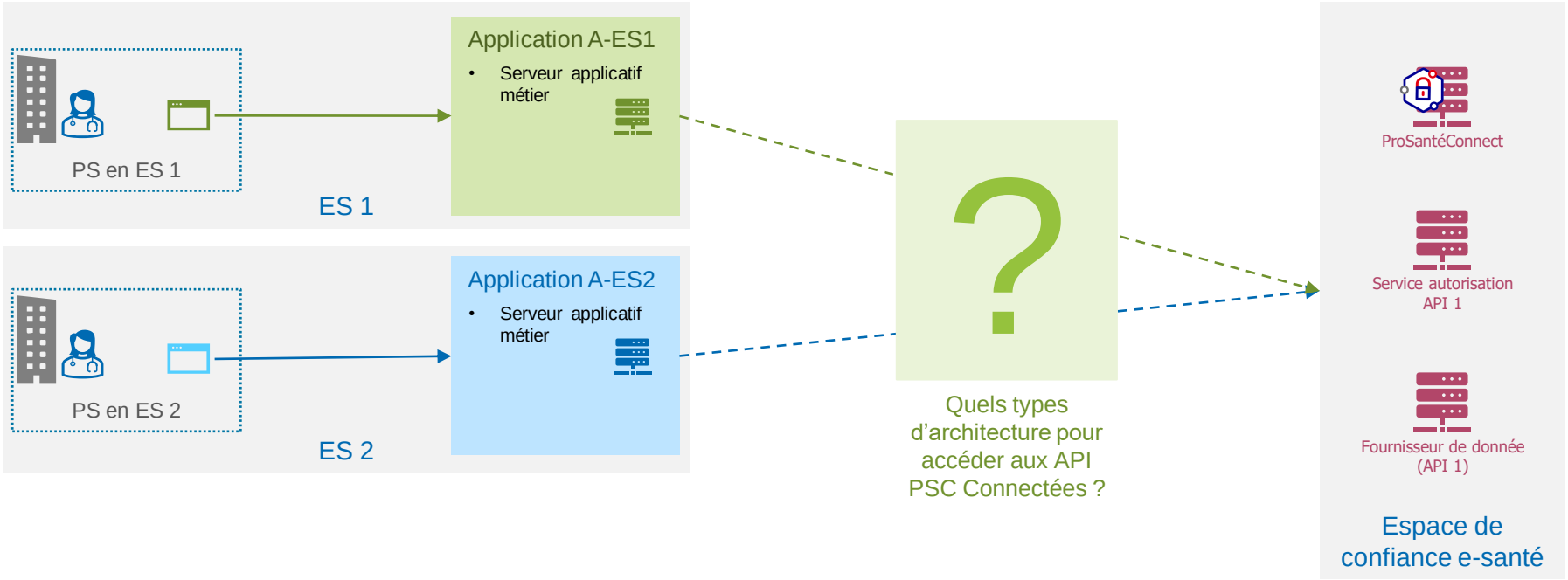



- Application métier opéré par l'éditeur 1
- Proxy mutualisé et proposé en tant que services à d'autres éditeurs (porté et opéré par l'éditeur 2)
- 1 certificat = 1 client id = 1 application
- 1 contrat global pour l'éditeur/opérateur 2 associé à N certificats application

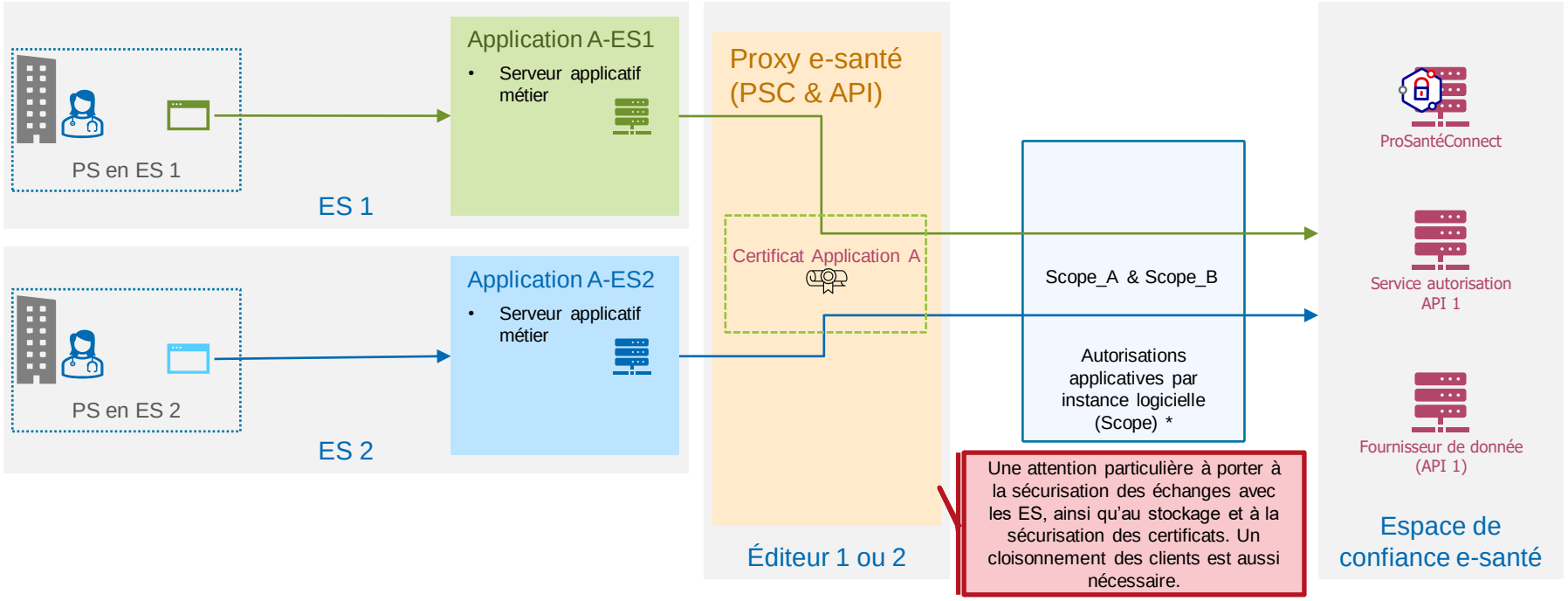
# Cas d'usage #1 : Application mutualisée – Solution 3 : Proxy externalisé

| | |
|---|---|
| **Architecture et intégration** | + Capacité à mutualiser le développement du proxy<br>+ Logiques métiers & proxy distincts<br>- Architecture plus complexe avec nécessité de gérer la sécurisation serveur LPS <> Proxy |
| **Gestion organisationnelle** | + Maintenance facilitée pour suivre les évolutions des exigences e-santé<br>+ Gestion déléguée à un tiers |
| **Gestion de la sécurité** | + En cas d'audit, seul le proxy est ciblé |
| **Disponibilité et résilience** | - Effet SPOF, nécessitant la mise en place de mesures spécifiques sur le proxy et d'accords contractuels entre les parties |

# Cas d'usage #2 : Application dédiée



# Cas d'usage #2 : Application dédiée – Solution 1 : Proxy mutualisé

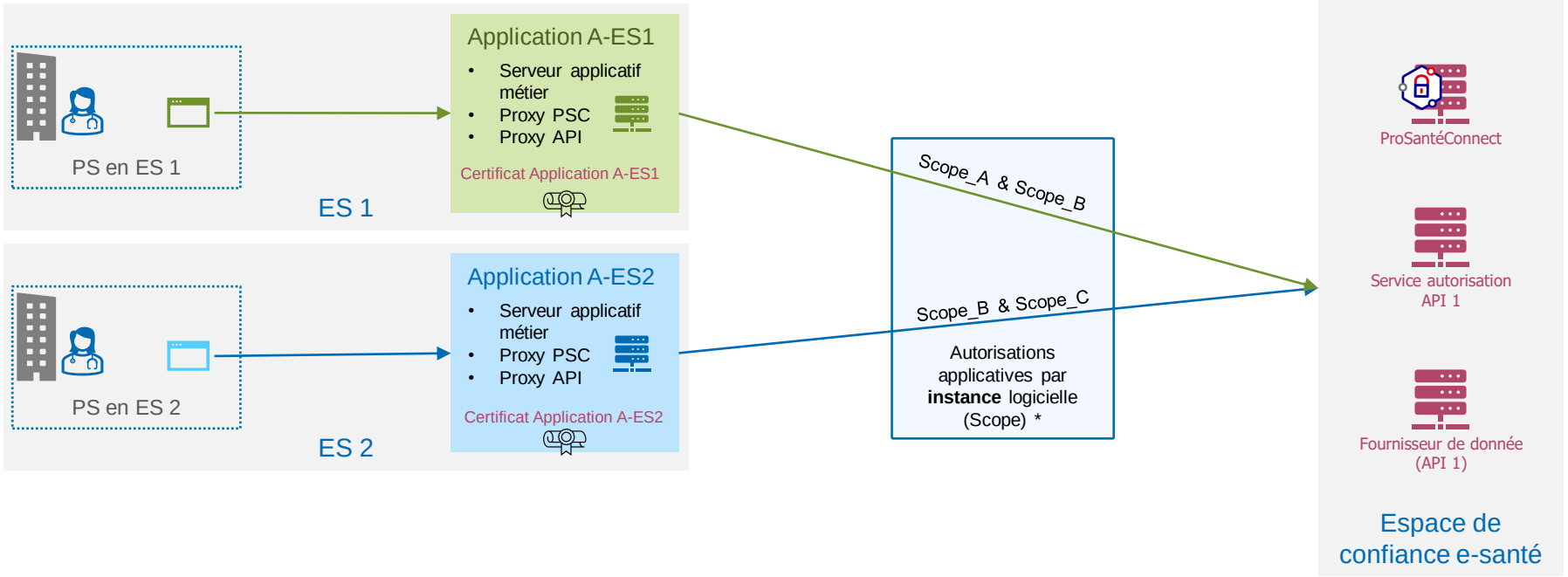



- L'hébergement des instances de l'application est réalisé sur les SI des ES.
- 1 proxy API et PSC est mutualisé entre l'ensemble des instances de l'application de l'éditeur 1 et est hébergé par le même ou un autre éditeur.
- 1 certificat (DN) = 1 client id = 1 application.
- 1 contrat global pour l'opérateur du proxy (éditeur 1 ou 2) avec un seul certificat pour N instances de l'application.

# Cas d'usage #2 : Application dédiée – Solution 1 : Proxy mutualisé

| | |
|---|---|
| **Architecture et intégration** | + Capacité à mutualiser le développement du proxy<br>+ Logiques métiers & proxy distincts<br>- Architecture plus complexe avec nécessité de gérer la sécurisation serveur LPS <> Proxy |
| **Gestion organisationnelle** | + Maintenance facilitée pour suivre les évolutions des exigences e-santé<br>+ Capacité de délégation à un tiers |
| **Gestion de la sécurité** | + En cas d'audit, seul le proxy est ciblé |
| **Disponibilité et résilience** | - Effet SPOF, nécessitant la mise en place de mesures spécifiques sur le proxy et d'accords contractuels entre les parties |

# Cas d'usage #2 : Application dédiée – Solution 2 : Proxies intégrés




- L'hébergement des instances d'applications est réalisé sur les SI des ES. L'ES **porte l'ensemble des exigences de sécurité → Limité aux établissements capables de répondre à un audit de l'ANS (bon niveau de maturité cyber conseillé)**
- Les proxy API et PSC sont intégrés (sous formes de modules) à chaque instance d'application.
- 1 certificat = 1 client id = 1 instance de l'application.
- Une contractualisation est nécessaire avec **chaque ES.**

# Cas d'usage #2 : Application dédiée – Solution 2 : Proxies intégrés

**Architecture et intégration**

- × Code proxy répliqué pour chaque application
- × Fonctions « métiers » et « proxy PSC » mélangées
- \+ Architecture plus simple (nombre de composants moindre)

**Gestion organisationnelle**

- × Charge de travail supplémentaire pour la mise en place et la maintenance de plusieurs proxys (ex. montée de version)

**Gestion de la sécurité**

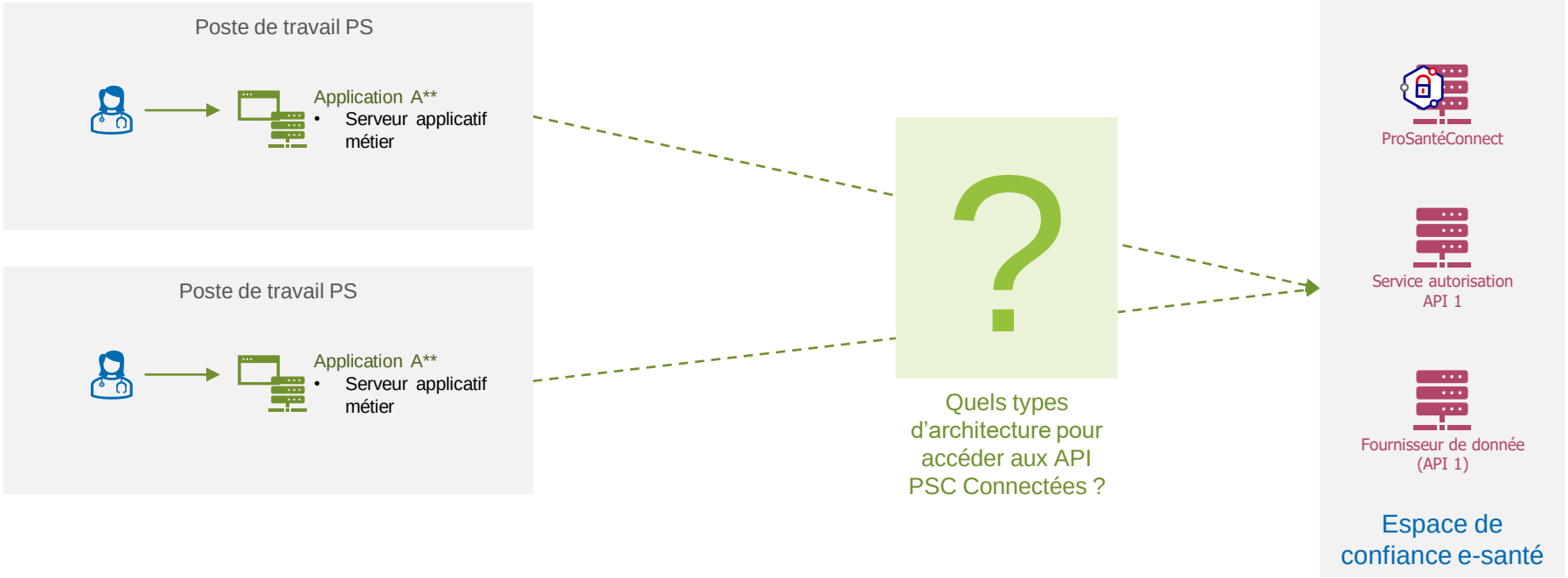
- × En cas d'audit, chaque LPS est ciblé
- × L'ES en tant qu'opérateur doit être en capacité de répondre à un audit
- × Nécessite un bon niveau de maturité cyber

**Disponibilité et résilience**

- \+ Pas d'effet SPOF, aligné avec le LPS

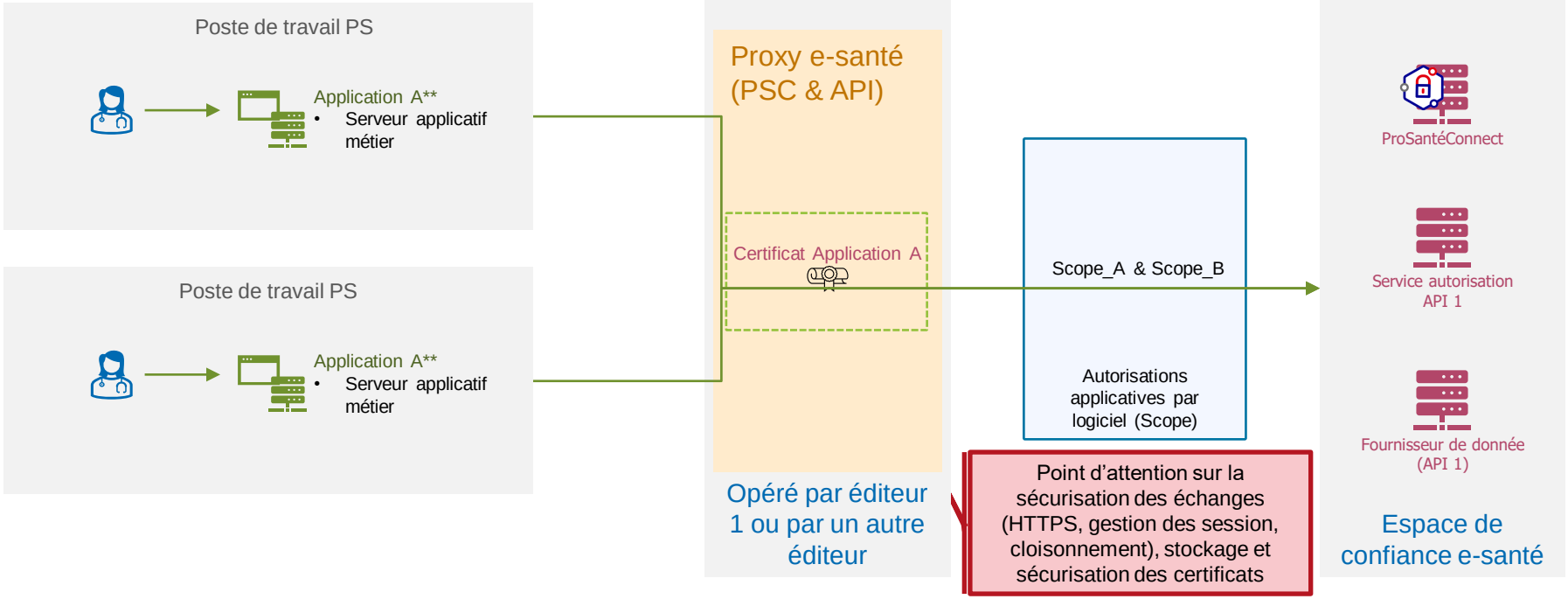
*** Serveur applicatif métier installé sur le poste du PS (type client lourd entièrement local) et développé par l'éditeur 1*

# Cas d'usage #3 : Application locale



*** Serveur applicatif métier installé sur le poste du PS (type client lourd entièrement local) et développé par l'éditeur 1*

# Cas d'usage #3 : Application locale – Solution : Proxy mutualisé

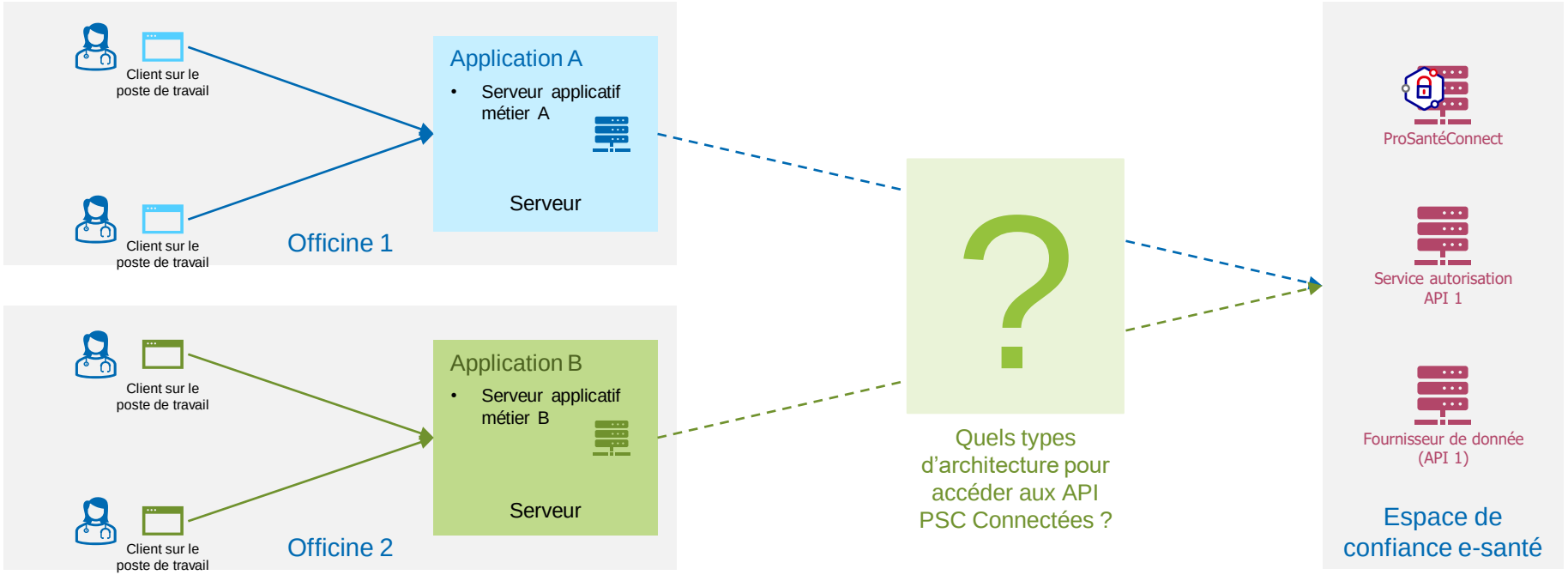



- L'hébergement de l'application est réalisé en local chez le PS.
- 1 proxy API et PSC est mutualisé entre l'ensemble des applications de l'éditeur 1 et est hébergé par le même ou un autre éditeur.
- 1 certificat = 1 client id = 1 application.
- Contractualisation avec **l'opérateur du proxy.**

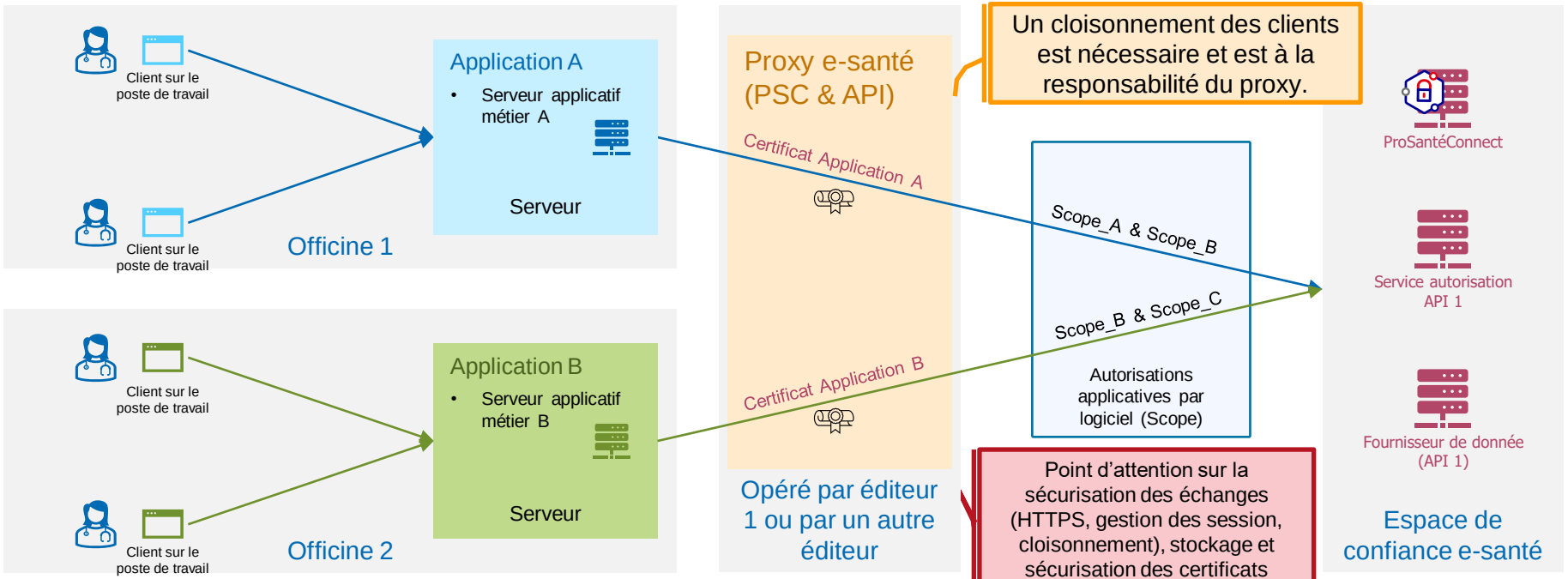
# Cas d'usage #3 : Application locale – Solution : Proxy mutualisé

| | |
|---|---|
| **Architecture et intégration** | + Capacité à mutualiser le développement du proxy<br>+ Logiques métiers & proxy distincts<br>- Architecture plus complexe avec nécessité de gérer la sécurisation serveur LPS <> Proxy |
| **Gestion organisationnelle** | + Maintenance facilitée pour suivre les évolutions des exigences e-santé<br>+ Capacité de délégation à un tiers |
| **Gestion de la sécurité** | + En cas d'audit, seul le proxy est ciblé |
| **Disponibilité et résilience** | - Effet SPOF, nécessitant la mise en place de mesures spécifiques sur le proxy et d'accords contractuels entre les parties |

# Cas d'usage #4 : Application dédiée (hors SI)



# Cas d'usage #4 : Application dédiée (hors SI) – Solution : Proxy mutualisé




- L'hébergement de l'application est réalisé en local sur un poste de travail ou sur un serveur centralisé de l'officine.
- 1 proxy API et PSC est mutualisé entre l'ensemble des applications de l'éditeur 1 et est hébergé par le même ou un autre éditeur.
- 1 certificat = 1 client id = 1 application.
- Contractualisation avec **l'opérateur du proxy.**

# Cas d'usage #4 : Application dédiée (hors SI) – Solution : Proxy mutualisé

| | |
|---|---|
| **Architecture et intégration** | + Capacité à mutualiser le développement du proxy<br>+ Logiques métiers & proxy distincts<br>- Architecture plus complexe avec nécessité de gérer la sécurisation serveur LPS <> Proxy |
| **Gestion organisationnelle** | + Maintenance facilitée pour suivre les évolutions des exigences e-santé<br>+ Capacité de délégation à un tiers |
| **Gestion de la sécurité** | + En cas d'audit, seul le proxy est ciblé |
| **Disponibilité et résilience** | - Effet SPOF, nécessitant la mise en place de mesures spécifiques sur le proxy et d'accords contractuels entre les parties |

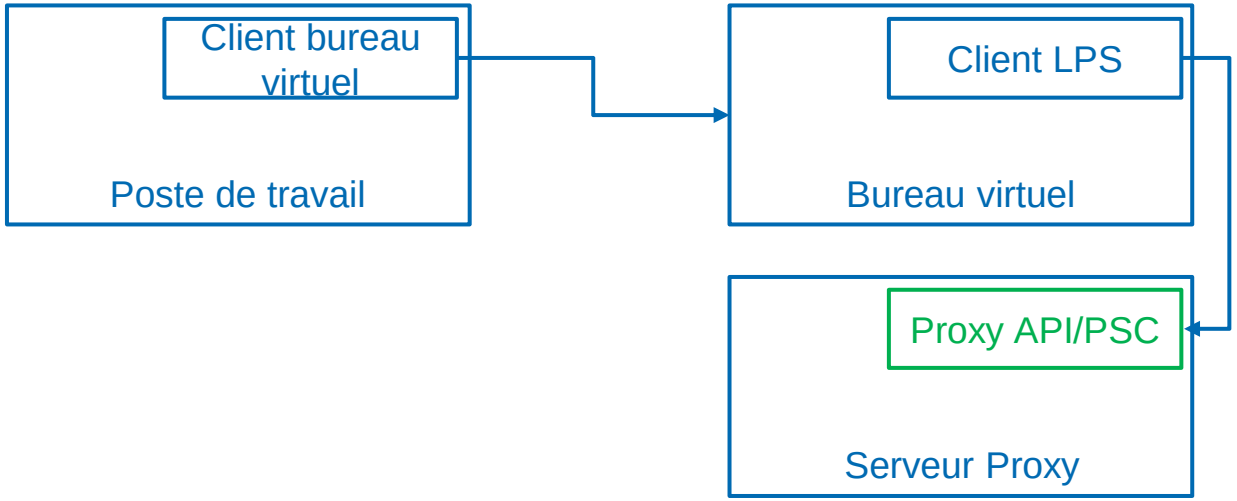
# Synthèse des cas d'usage et des solutions proposées

| | Cas d'usage | Solution |
|---|---|---|
| #1 | Applications **mutualisées** (mode SaaS) | Proxies **intégrés** |
| | | Proxy **mutualisé** |
| | | Proxy **externalisé** |
| #2 | Applications **dédiées** (cas des centres hospitaliers, des grands groupes de cliniques et d'EHPAD) | Proxy **mutualisé** |
| | | Proxies **intégrés** |
| #3 | Applications **locales** (cas des médecins libéraux) | Proxy **mutualisé** |
| #4 | Applications **dédiées hors SI** (cas des officines) | |

Les architectures avec des proxys mutualisés sont préconisées.

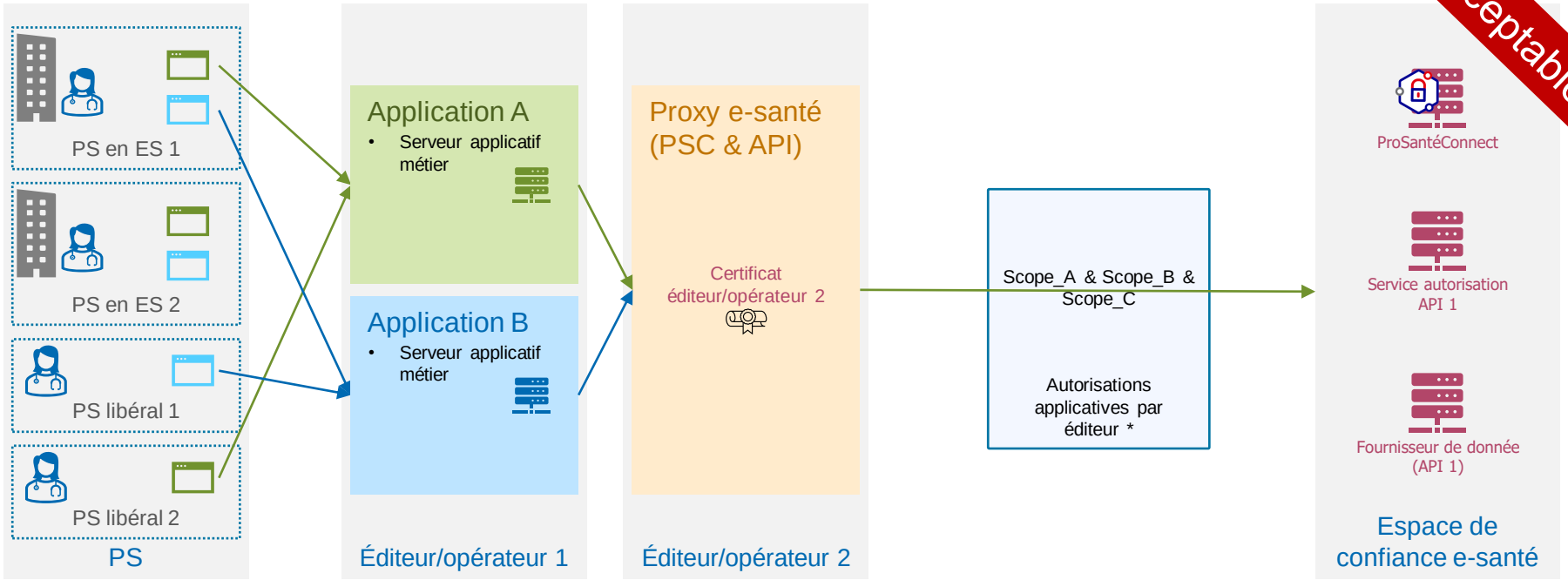
# Cas des bureaux virtuels (TSE/RDP/CITRIX)

Un bureau virtuel ne doit pas être pas être utilisé pour hébergé le proxy API/PSC. Il est donc important d'installer ce dernier sur un composant serveur dédié.



# Exemple 1 d'architecture non acceptée

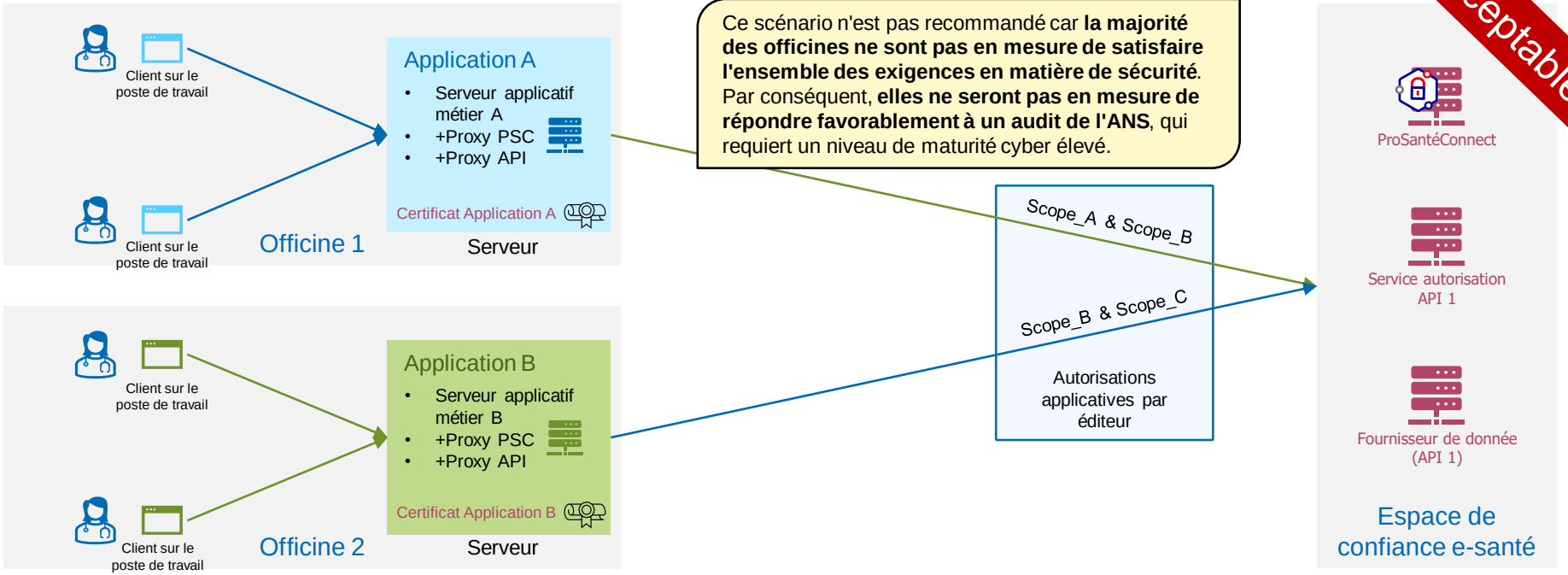
Non acceptable




- Application métier opéré par l'éditeur 1
- Proxy mutualisé et proposé en tant que services à d'autres éditeurs (porté et opéré par l'éditeur 2)
- **Non compatible avec la règle nécessitant de disposer d'1 certificat pour 1 application**

# Exemple 2 d'architecture non acceptée

Non acceptable




- L'hébergement des applications est réalisé sur un serveur installé dans l'officine. Les proxy API et PSC sont intégrés (sous formes de modules) à chaque application.
- 1 certificat = 1 client id = 1 instance de l'application.
- Une contractualisation est nécessaire avec **chaque officine.**
- **Une officine ne disposant pas d'un SI dédié ou ayant un niveau de maturité cyber suffisant, ce type de déploiement ne saurait répondre au cadre d'exigence définit et/ou à un audit commandité par l'ANS.**

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

# Introduction vers un Espace de Confiance

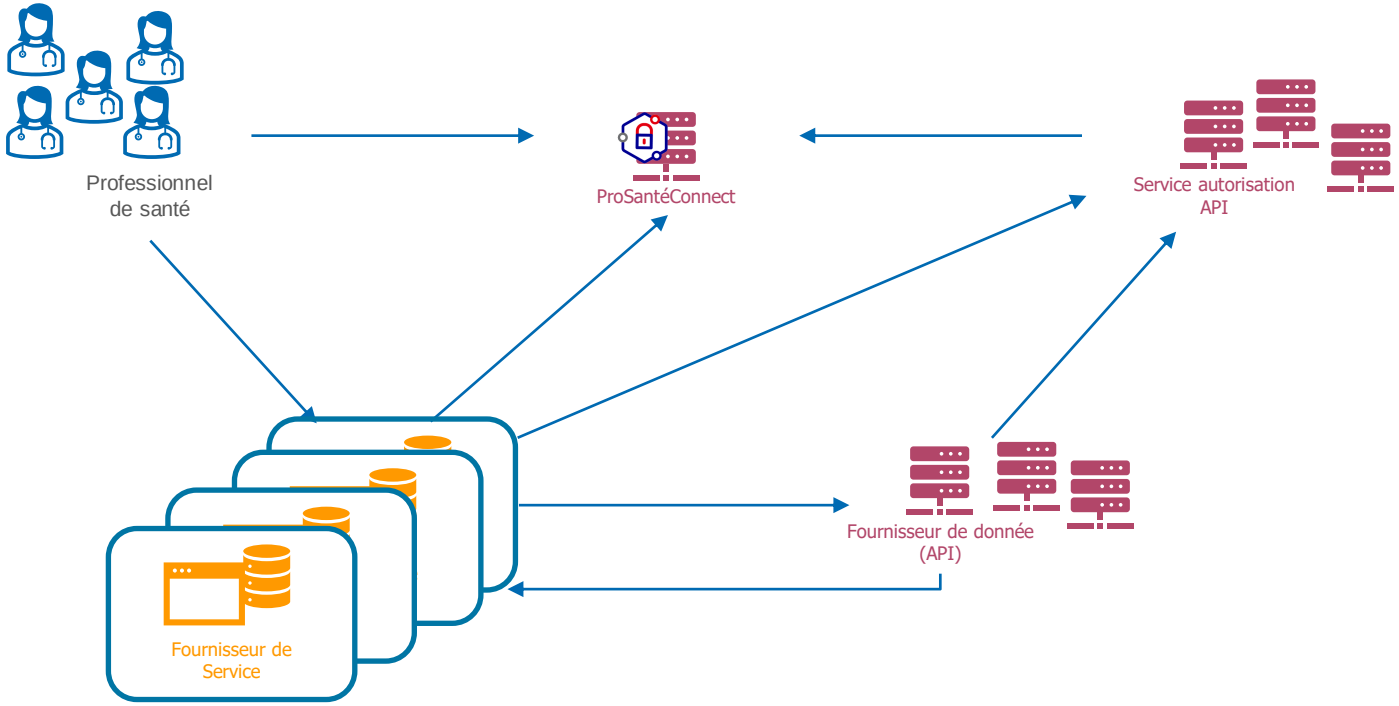
# Introduction

**L’ensemble des travaux nous permettent d’identifier de nouveaux composants de l’écosystème technique du Numérique en Santé qui sont les Proxy e-Santé (serveurs intermédiaires).**

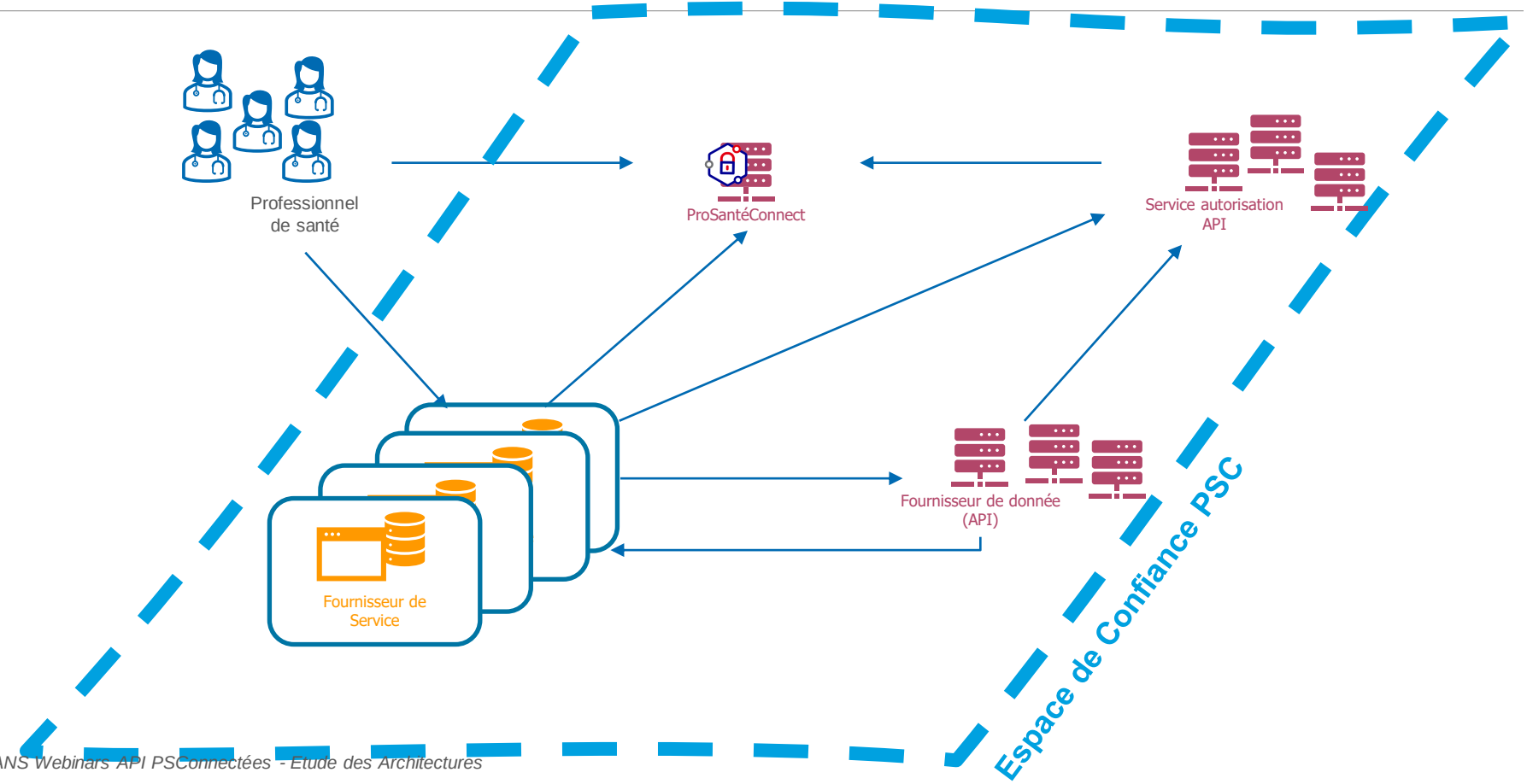
**Ces Proxy e-Santé sont opérés par des Entreprises du Numérique en Santé et/ou des Structures de Santé.**

**Dans le but de maintenir une relation de confiance dans la durée avec ces opérateurs et afin de garantir les niveaux de sécurité attendus, nous vous proposons d’introduire une notion d’Espace de Confiance autour de Pro Santé Connect.**

# Introduction



# Introduction



# Espace de Confiance Pro Santé Connect

## Cet Espace de Confiance doit s'articuler autour de 3 approches :

1. Une contractualisation unifiée des acteurs ENS et Structure
2. Un référentiel Pro Santé Connect à 2 niveaux de conformité
3. Une animation de l'Espace de Confiance afin de maintenir son niveau de sécurité dans le temps

# Contractualisation et Référentiel PSC

## Une nouvelle version de référentiel sera axée autour d'une approche à 2 niveaux de conformité demandée lors de la contractualisation avec l'ANS :

- **Niveau « Communauté » :**
  - équivalent à l'actuel référentiel, pour les industriels qui utilisent PSC uniquement en Fournisseur d'Identité
- **Niveau « Espace de confiance » :**
  - pour les industriels entrant dans le cadre de CI-SIS
  - intégrant un 1ier ensemble d'exigences de sécurité supplémentaire

## La mise en concertation est prévue fin octobre.

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

## esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante