Microsoft logo white text versionMise en œuvre Pro Santé Connect avec Microsoft Entra ID

Zzz

Guide de configuration Microsoft Entra Private Access à destination des établissements de santé

Version 0.4a - Septembre 2024

Cette page est intentionnellement laissée vide.

Avertissement

Les informations contenues dans le présent document, y compris les URL et autres références à des sites Internet, sont susceptibles d'être modifiées sans préavis. Sauf indication contraire, les exemples de sociétés, d'organisations, de produits, de noms de domaine, d'adresses électroniques, de logos, de personnes, de lieux et d'événements décrits dans le présent document sont fictifs et aucune association avec une société, une organisation, un produit, un nom de domaine, une adresse électronique, un logo, une personne, un lieu ou un événement réel n'est voulue ou ne doit être déduite. Il incombe à l'utilisateur de se conformer à toutes les lois applicables en matière de droits d'auteur.

A drawing of a face

Description automatically generated

Attribution 4.0 International (CC BY 4.0)

Microsoft et tous les contributeurs vous accordent une licence pour ce document sous la licence [Creative Commons Attribution 4.0 International Public License](https://creativecommons.org/licenses/by/4.0/legalcode), Cf. fichier [LICENSE](https://github.com/microsoft/prosanteconnect/blob/main/LICENSE-CODE), et vous accordent une licence pour tout code dans le référentiel sous la licence MIT, Cf. fichier [LICENSE-CODE](https://github.com/microsoft/prosanteconnect/blob/main/LICENSE-CODE).

Microsoft, Windows, Microsoft Azure et/ou d'autres produits et services Microsoft référencés dans le document peuvent être des marques commerciales ou des marques déposées de Microsoft aux États-Unis et/ou dans d'autres pays. La licence de ce document ne vous donne pas le droit d'utiliser les noms, logos ou marques de Microsoft. Les directives générales de Microsoft en matière de marques sont disponibles à l'adresse suivante : <http://go.microsoft.com/fwlink/?LinkID=254653>.

Des informations sur la protection de la vie privée sont disponibles à l'adresse suivante : <https://privacy.microsoft.com/fr-fr/>

Microsoft et tous les contributeurs se réservent tous les autres droits, que ce soit au titre de leurs droits d'auteur, de leurs brevets ou de leurs marques respectives, que ce soit de manière implicite, par préclusion ou de toute autre manière.

Content

[1 Introduction 5](#_Toc176967559)

[1.1 Objectifs du guide 5](#_Toc176967560)

[1.2 Non-objectifs du guide 6](#_Toc176967561)

[2 TBD 7](#_Toc176967562)

[2.1 TBD 7](#_Toc176967563)

# Introduction

Pro Santé Connect (PSC) est le fédérateur d’identités des professionnels des secteurs sanitaire, médico-social et social enregistrés au Répertoire Partagé des Professionnels de Santé (RPPS). Ce service socle est proposé par l’Agence du Numérique en Santé (ANS) en sa qualité d’autorité compétente.

Il leur offre une manière simple, sécurisée et unifiée de se connecter à tous leurs services numériques en santé, en pouvant passer de l’un à l’autre de manière particulièrement fluide.

Ces derniers peuvent implémenter gratuitement ce service socle basé sur des technologies standardisées. PSC leur permet :

* Une sécurisation de l’identification électronique des professionnels, protégeant les données de santé éventuellement traitées, et leur garantissant une conformité réglementaire sur le niveau de garantie de l’identification électronique de leurs usagers professionnels.

A date la carte CPS et la e-CPS sont les seuls moyens d’identification électroniques (MIE) aujourd’hui pris en charge par PSC ;

* Un engagement de leurs utilisateurs, familiers de ce mode d’identification électronique commun à de nombreux services ;
* De récupérer les attributs de l’identité sectorielle (profession, savoir-faire, situation d’exercice, …) pour en faire la vérification et éventuellement automatiser leur contrôle d’accès sur cette base.

Le fédérateur d’identités PSC permet la délégation de l’authentification auprès de fournisseurs d’identités (FI) tiers. Pour plus d’informations, nous invitons le lectorat à consulter le Portail Industriels de l’ANS :

* Délégation à un fournisseur d'identité local : <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/delegation-un-fournisseur-d-identite-local> ;
* Liste des fournisseurs d’identités déjà supportés par Pro Santé Connect : <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/documentation-technique-idp-externe> ;
* Travaux en cours : <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/travaux-en-cours>.

Une telle mise en œuvre et les capacités nouvelles ainsi proposées constituent un premier niveau de livrable du projet Pro Santé Connect sans couture.

## Objectifs du guide

La délégation de l’authentification PSC auprès du fournisseur d’identités (FI) tiers Microsoft Entra ID (anciennement connu sous le nom d’Azure AD) autorise une expérience d’authentification unique ou SSO (Single Sign-On) depuis une session ouverte depuis une session de terminal Windows pour l’accès à une application ou un service numérique déléguant l’authentification à PSC.

L’objectif de ce guide est d’expliciter la configuration permettant une telle expérience ainsi que les prérequis éventuels associés.

## Non-objectifs du guide

La configuration de la délégation de l’authentification PSC auprès du FI tiers Microsoft Entra ID n’est pas couverte dans ce guide. Cette dernière fait l’objet du Guide de configuration de Pro Santé Connect à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

Cela suppose par ailleurs d’avoir déployé et configuré un ou plusieurs moyens d’identification électroniques (MIE) conformes avec les exigences établies par l’ANS. La mise en œuvre de ces MIE pour les appareils Windows 10 (et ultérieur) est couverte dans les guides suivants :

* Guide de configuration des cartes CPx à destination des établissements de santé ;
* Guide de configuration des clés de sécurité FIDO2 à destination des établissements de santé ;
* Guide de configuration des Microsoft Authenticator à destination des établissements de santé ;
* Guide de configuration de Windows Hello Entreprise à destination des établissements de santé.

Nous invitons le lectorat à s’y reporter.

Microsoft Entra ID propose par ailleurs des mécanismes permettant une navigation sans couture dès l’ouverture de session sur un appareil Windows pour l’accès à une application ou un service numérique déléguant l’authentification à PSC. Si les prérequis pour la mise en place de ces éléments pour cette navigation sans couture ne font pas partie du cadre minimum défini par l’ANS, ceux-ci sont néanmoins couverts dans ce même guide. Nous invitons le lectorat à s’y reporter.

Enfin, l’accès à PSC depuis une session Entra ID ouverte avec un MIE conforme, est permis au travers d’un accès conditionnel afin d’assurer le respect d’un ensemble d’exigences comme la force d’authentification requise. Un tel accès conditionnel est indépendant de la configuration de la navigation sans couture.

La mise en œuvre des politiques d’accès conditionnel attendues est couverte dans le Guide de configuration de l’accès conditionnel à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

# TBD

## TBD

Ceci conclut le présent guide.