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

Zzz

Guide de configuration des clés de sécurité FIDO2 à destination des établissements de santé

Version 0.4b - 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.

Contenu

[1 Introduction 5](#_Toc176967478)

[1.1 Objectifs du guide 6](#_Toc176967479)

[1.2 Non-objectifs du guide 6](#_Toc176967480)

[2 Configuration des clés de sécurité FIDO2 au niveau des appareils 8](#_Toc176967481)

[3 Configuration de l’authentification avec une clé de sécurité FIDO2 dans Microsoft Entra ID 11](#_Toc176967482)

[3.1 Autorisation de la configuration en libre-service ​ 11](#_Toc176967483)

[3.2 Ajout de l’authentification par clé de sécurité FIDO2 en libre-service​ 11](#_Toc176967484)

[3.3 Ajout d’un nouvel objet Kerberos Server dans le domaine Active Directory 12](#_Toc176967485)

[4 Provisionnement administratif des clés de sécurité FIDO2 14](#_Toc176967486)

# 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.

Dans le cadre du déploiement de PSC, différents retours terrains ont mis en lumière la nécessité de faire évoluer le service pour simplifier les parcours d’accès aux services connectés à PSC ; notamment dans les contextes des ES.

L’objectif du projet Pro Santé Connect sans couture est d’étudier, de définir puis d’implémenter des mesures organisationnelles et techniques permettant de fluidifier l’accès à ces services numériques dans le contexte des ES.

Pour fluidifier la navigation, une fédération/délégation peut être ainsi mise en place entre le fournisseur d’identités (FI) local de l’ES et PSC selon les contextes. Microsoft Entra ID

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

Le POC technique prend en charge la délégation de l’authentification à Microsoft Entra ID. 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>.

Dans ce contexte, et cette logique, une clé de sécurité FIDO2 constitue un moyen d’identification électronique (MIE) retenu dans le périmètre du POC technique afin de pouvoir offrir une sécurité renforcée, une expérience utilisateur améliorée, une réduction des risques de piratage et une conformité réglementaire accrue. (Le POC technique sécurisation cible plus spécifiquement cette utilisation. Dans ce cadre, la fourniture d’une clé de sécurité FIDO2 est à la charge de l’ES.)

L’authentification FIDO2 ou Fast ID Online v2.0 est un standard ouvert pour l’authentification sans mot de passe, Cf. <https://fidoalliance.org/>.

Ce standard permet aux PS et autres utilisateurs de se connecter à leurs appareils et applications à l’aide de l’authentification biométrique ou d’une clé de sécurité physique, sans avoir besoin d’un mot de passe traditionnel.

L’ouverte de session avec une clé de sécurité FIDO2 (clé USB, carte à puce, etc.) réalisée depuis un poste de travail Windows avec une jointure (hybride) à Entra ID permet au Professionnel de Santé (PS) de bénéficier d’un accès transparent à l’ensemble des applications raccordés au FI local ainsi qu’à l’ensemble de l’écosystème PSC et ses services numériques (SN) dans le cadre de cette délégation de l’authentification.

Une telle session nominative avec son identité provenant d’un FI tiers déjà appairé (ici Microsoft Entra ID) autorise alors l’accès en authentification unique (SSO) à un SN connecté à PSC au même titre qu’à une application de type client riche. Il s’agit de permettre une expérience de navigation sans couture à PSC aux applications web et lourds, dès l’ouverture de la session Windows au travers de mécanismes natifs de l’environnement Windows.

Le POC technique et les retours terrain et métier permettront d’affiner les exigences quant à la définition d’un MIE 2FA conforme de type clé FIDO2.

En fonction des résultats, il pourra être par exemple envisager de permettre à chaque utilisateur d’associer clé de sécurité FIDO2 à son Identité Nationale de Santé (IdNat, RPPS) et de gérer facilement cette association. A ce titre, une première intégration est désormais effective dans l’application PSC\_BAS.

Une image contenant texte, capture d’écran, Police, Page web

Description générée automatiquement

Pour plus d’informations, et pour suivre les dernières avancées, nous invitons le lectorat à consulter le Portail Industriels de l’ANS : Travaux en cours : <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/travaux-en-cours>.

## Objectifs du guide

L’objectif de ce guide est d’expliciter dans ce contexte les éléments de configuration des clés de sécurité FIDO2.

## Non-objectifs du guide

La configuration de la délégation de l’authentification PSC auprès du FI tiers Microsoft Entra ID n’est pas couverte en tant que telle 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.

Les clés de sécurité FIDO2 (clé USB, carte à puce, etc.) ne sont pas le seul MIE conforme dans le cadre du POC technique. Les MIE suivants sont également retenus dans le périmètre du POC technique :

* Certificat X.509 avec une carte CPx physique ;
* Microsoft Authenticator ;
* Windows Hello Entreprise.

La configuration de ces MIE n’est pas couverte dans ce guide. Cette dernière fait l’objet des guides suivants :

* Guide de configuration des cartes CPx à destination des établissements de santé ;
* Guide de configuration de 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.

De plus, ce guide ne donne pas de préconisations sur la stratégie de déploiement à opérer au sein d’un ES pour par exemple déployer ces nouveaux MIE auprès de ses PS et autres utilisateurs ; celle-ci étant sous la responsabilité de l’ES.

Il pourra le cas échéant renvoyer le lectorat sur les guides de planification disponibles dans la documentation Microsoft.

Par ailleurs, cette même expérience d’authentification unique peut être étendue à d’autres types de dispositifs comme les services de terminaux Windows. Ceci requiert la mise en œuvre additionnelle de Microsoft Entra Private Access, un produit de type ZTNA (Zero Trust Network Access) centré sur l'identité. Cette mise en œuvre est couverte dans le Guide de configuration de Microsoft Entra Private Access à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

Enfin, l’accès à PSC depuis une session Entra ID et/ou Windows ouverte avec un MIE conforme, est permis au travers d’un accès conditionnel Entra ID 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.

# Configuration des clés de sécurité FIDO2 au niveau des appareils

Le support d’une clé FIDO2 suppose les opérations suivantes depuis un appareil Windows 10 ou ultérieur. Le support depuis un appareil Android ou iOS n’est pas couvert dans la version courante de ce guide.

Depuis un appareil Windows 10 ou ultérieur, procéder comme suit :

1. A l’aide d’un compte d’administrateur local, ouvrir l’utilitaire Editeur de stratégie de groupe locale (*gpedit.exe*).​

Remarque : Pour un déploiement centralisé, il faudra bien entendu faire l’équivalent à travers un Group Policy Object dans Active Directory, ou une stratégie de type OMA-DM - Open Mobile Alliance" "Device Management"

Une image contenant texte, capture d’écran, logiciel, ordinateur

Description générée automatiquement

1. Activer la connexion par clé de sécurité :
   1. Naviguer vers Configuration ordinateur > Modèles d’administration > Système > Ouverture de session.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

* 1. Double-cliquer sur le paramètre Activer la connexion par clé de sécurité.
  2. Dans Activer la connexion par clé de sécurité, cliquer sur Activer.

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

* 1. Cliquer sur OK.

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Documentation Microsoft :

* Connexion Windows par clé de sécurité sans mot de passe : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/howto-authentication-passwordless-security-key-windows>.

# Configuration de l’authentification avec une clé de sécurité FIDO2 dans Microsoft Entra ID

## Autorisation de la configuration en libre-service ​

Procéder comme suit :

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com>, puis sur la vue d’ensemble Identité de Microsoft Entra ID. L’adresse <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView> peut être utilisée pour un accès direct.
2. Se diriger dans l’onglet Protection > Méthodes d’authentification > Stratégies.
3. Cliquer sur Clé de sécurité FIDO2.
4. Activerla clé de sécurité FIDO2 pour Tous les utilisateurs.
5. Dans l’onglet Configurer,Autoriser la configuration libre-service**.** L’attestation et la restriction de clés sont optionnelles mais recommandées :
   1. Appliquer l’attestation : Les métadonnées de clé FIDO doivent être publiées et vérifiées auprès de la FIDO Alliance et également passer d’autres tests de validation par Microsoft.
   2. Appliquer les restrictions de la clé : Autorise ou interdit certaines clés FIDO selon leur AAGUID (identifiant indiquant le fabriquant et le modèle de la clé)

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Documentation Microsoft :

* Enable passkeys for your organization (preview) : <https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-passkey-fido2>.

## Ajout de l’authentification par clé de sécurité FIDO2 en libre-service​

Pour les utilisateurs de test du POC technique sécurisation, procéder comme suit :

1. Se connecter sur le site <https://mysignins.microsoft.com> et se rendre dans Information de sécurité.
2. Cliquer sur Ajouter une méthode, sélectionner clé de sécurité et suivre la procédure d’enrôlement.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

## Ajout d’un nouvel objet Kerberos Server dans le domaine Active Directory

Cette section ne concerne QUE l’ES disposant d’un environnement Active Directory (AD) en local avec des appareils avec jointure hybride Microsoft Entra et des comptes synchronisés entre cet environnement et Microsoft Entra ID.

Les appareils avec jointure hybride Microsoft Entra sont des appareils membres d’un AD et qui sont également liés à Microsoft Entra ID en effectuant une jointure hybride Microsoft Entra, Cf. Planifier la mise en œuvre de votre jointure hybride Microsoft Entra : <https://learn.microsoft.com/fr-fr/entra/identity/devices/hybrid-join-plan>.

Microsoft Entra ID peut émettre des ticket-granting tickets (TGT) Kerberos pour un ou plusieurs de domaines Active Directory de l’ES. Cette fonctionnalité permet aux utilisateurs de se connecter à Windows avec des informations d’identification modernes telles qu’une clé de sécurité FIDO2 pour accéder à des ressources Active Directory traditionnelles. Les tickets de service Kerberos et l’autorisation continuent d’être contrôlés par les contrôleurs de domaine Active Directory locaux de l’ES.

Un objet serveur Kerberos Microsoft Entra doit être créé dans l’instance Active Directory locale de l’ES, puis publié en toute sécurité sur le locataire Microsoft Entra ID de l’ES. L’objet n’est associé à aucun serveur physique. Il s’agit simplement d’une ressource que Microsoft Entra ID peut utiliser afin de générer des TGT Kerberos pour le domaine Active Directory considéré.

### Installation du module AzureADHybridAuthenticationManagement

Le module AzureADHybridAuthenticationManagement fournit des fonctionnalités de gestion FIDO2 pour les administrateurs.

Procéder comme suit :

1. Ouvrir une invite PowerShell à l’aide de l’option Exécuter en tant qu’administrateur.
2. Installer le module AzureADHybridAuthenticationManagement :

# First, ensure TLS 1.2 for PowerShell gallery access.

[Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor [Net.SecurityProtocolType]::Tls12

# Install the AzureADHybridAuthenticationManagement PowerShell module.

Install-Module -Name AzureADHybridAuthenticationManagement -AllowClobber

### Création de l’objet serveur Kerberos

Procéder comme suit :

1. Préciser les informations d’identification cloud à l’aide de l’authentification moderne
   1. Spécifier le domaine Active Directory en local. Le nouvel objet Serveur Kerberos sera créé dans ce domaine.

PS C:\> $domain = $env:USERDNSDOMAIN

* 1. Spécifier le nom d’utilisateur principal (UPN) de l’administrateur global. Remplacer *administrator@contoso.onmicrosoft.com* par l’UPN d’un administrateur général de l’ES.

PS c:> $userPrincipalName = "administrator@contoso.onmicrosoft.com"

* 1. Préciser les informations d’identification correspondantes.

PS C:> $domainCred = Get-Credential

1. Créer l’objet serveur Kerberos dans Active Directory et le publier ensuite dans Entra ID

PS C:\> Set-AzureADKerberosServer -Domain $domain -UserPrincipalName $userPrincipalName -DomainCredential $domainCred

Remarque : Depuis un appareil joint à un domaine avec un compte disposant de privilèges d’administrateur de domaine et que l’ES protège la connexion par mot de passe et applique des méthodes d’authentification modernes telles que l’authentification multifacteur, FIDO2 ou la technologie de carte à puce, il est nécessaire d’utiliser le paramètre -UserPrincipalName avec le nom d’utilisateur principal (UPN) d’un administrateur global. Le paramètre -DomainCredential peut être ignoré.

1. Afficher et vérifier l’objet serveur Kerberos Microsoft Entra. Préciser les informations d'identification de domaine au format UPN lorsqu’inviter à le faire.

PS C:\> Get-AzureADKerberosServer -Domain $domain -UserPrincipalName $userPrincipalName -DomainCredential (get-credential)

Documentation Microsoft :

* Activer la connexion par clé de sécurité sans mot de passe à des ressources locales à l’aide de Microsoft Entra ID : <https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-passwordless-security-key-on-premises#install-the-azureadhybridauthenticationmanagement-module> ;
* How-to: Password-less FIDO2 Security Key Sign-in to Windows 10 HAADJ Devices : <https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/how-to-password-less-fido2-security-key-sign-in-to-windows-10/ba-p/1434583>. ;

# Provisionnement administratif des clés de sécurité FIDO2

Au-delà des éléments de configuration décrits précédemment pour permettre aux utilisateurs d’enregistrer leurs propres clés de sécurité, de nouvelles API de provisionnement FIDO2 (<https://aka.ms/passkeyprovision>) dans Entra ID permettent aux ES de gérer ce provisionnement pour le compte de leurs utilisateurs, en fournissant ainsi une authentification sécurisée et transparente dès le premier jour.

Bien que les ES puissent toujours déployer des clés de sécurité dans leur configuration par défaut pour leurs différents utilisateurs, comme les professionnels de Santé (Ps), ou autoriser ces dernier à apporter leurs propres clés de sécurité - ce qui nécessite une inscription en libre-service par l’utilisateur - les API ‘actuellement en aperçu public) permettent aux clés d’être préconfigurées pour les populations ciblées, de sorte que ces utilisateurs bénéficient d’une expérience plus facile lors de la première utilisation.

 Avec ces API de provisionnement FIDO2, les ES sont ainsi à même de créer leurs propres solutions de provisionnement d’administration ou s’associer à l’un des nombreux principaux fournisseurs de systèmes de gestion des informations d’identification (CMS) qui ont intégré ces API dans leurs offres.

Il est ainsi désormais possible de demander des options de création WebAuthn à partir d’Entra ID et d’utiliser les données renvoyées pour créer et enregistrer des informations d’identification de clé d’accès au nom d’un utilisateur.

Pour simplifier ce processus, trois étapes principales sont requises pour enregistrer une clé de sécurité au nom d’un utilisateur :

image miniature 1 de l’article de blog intitulé 
 
Préversion publique : API d’approvisionnement Microsoft Entra ID FIDO2 

1. Demander les *creationOptions* pour un utilisateur: Le locataire Entra ID renverra les données nécessaires à l’appelant pour provisionner un identifiant d’identification de clé de sécurité FIDO2. Il s’agit notamment d’informations telles que les informations sur l’utilisateur, la partie de confiance, les exigences de la politique d’identification, les algorithmes, etc.
2. Provisionner les informations d’identification de la clé de sécurité FIDO2 avec les *creationOptions*: À l’aide des options de création, utiliser un client ou un script qui prend en charge le protocole CTAP (Client to Authenticator Protocol) pour provisionner les informations d’identification. Au cours de cette étape, une clé de sécurité FIDO2 doit être insérée et un code PIN défini.
3. Enregistrer les informations d’identification provisionnées avec le locataire Entra ID: À l’aide du résultat du processus de provisionnement, fournir au locataire Entra ID les données nécessaires pour enregistrer les informations d’identification de clé de sécurité FIDO2 pour l’utilisateur ciblé.

En plus de fournir les outils ci-dessus, Microsoft a également collaboré avec 10 fournisseurs de premier plan dans le domaine des CMS pour intégrer ces nouvelles API de provisionnement FIDO2.

image miniature 2 de l’article de blog intitulé 
 
Préversion publique : API d’approvisionnement Microsoft Entra ID FIDO2 

Ces fournisseurs ont effectué des tests rigoureux et connaissent parfaitement les nouvelles API, et sont disponibles pour aider le cas échéant les ES dans leur parcours de provisionnement si la création d’une intégration en propre n’est pas souhaitée.

**Ce partenariat souligne notre engagement à fournir un écosystème sécurisé et interopérable à nos clients. Ces fournisseurs représentent une gamme variée de solutions CMS, chacune apportant des connaissances et une expertise uniques. Leur implication a permis de s’assurer que les API sont robustes, polyvalentes et prêtes à relever les défis du monde réel.**

Il convient de souligner qu’en l’état des travaux, si aucune vérification n’est effectuée quant à l’appartenance d’une clé de sécurité FIDO2 utilisée à la liste des produits certifiés par l’ANSSI, cette fonctionnalité sera développée ultérieurement par l’ANS.

Documentation Microsoft :

* Enable passkeys for your organization (preview) - Microsoft Entra ID : <https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-passkey-fido2> ;
* fido2AuthenticationMethod resource type - Microsoft Graph beta : <https://learn.microsoft.com/en-us/graph/api/resources/fido2authenticationmethod?view=graph-rest-beta>.

Ceci conclut le présent guide.