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

Zzz

Guide de configuration des moyens d’identification électronique (MIE) et de la navigation sans couture à destination des établissements de santé

Version 0.3 - Février 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](#_Toc158807547)

[1.1 Présentation succincte du projet Pro Santé Connect sans couture 5](#_Toc158807548)

[1.2 Objectifs du guide 7](#_Toc158807549)

[1.3 Non-objectifs du guide 7](#_Toc158807550)

[2 Prise en charge des MIE conformes aux exigences de l’ANS dans Entra ID 8](#_Toc158807551)

[2.1 Utilisation des certificats X.509 de la carte CPx physique 8](#_Toc158807552)

[2.2 Utilisation d’une clé de sécurité FIDO2 8](#_Toc158807553)

[2.3 Utilisation de Windows Hello Entreprise 8](#_Toc158807554)

[2.4 Utilisation de Microsoft Authenticator 8](#_Toc158807555)

[2.5 Non prise en charge de la carte e-CPS 8](#_Toc158807556)

[2.6 MIE et navigation sans couture 8](#_Toc158807557)

[2.7 Axes d’extensibilité futurs prévisibles 9](#_Toc158807558)

[3 Configuration des MIE au niveau des appareils 10](#_Toc158807559)

[3.1 Activation du support des certificats X.509 de la carte CPx physique 10](#_Toc158807560)

[3.2 Activation du support des clés de sécurité FIDO2 13](#_Toc158807561)

[3.3 Activation de Windows Hello Entreprise 14](#_Toc158807562)

[3.4 Activation de Microsoft Authenticator 14](#_Toc158807563)

[4 Configuration des MIE dans Microsoft Entra ID 15](#_Toc158807564)

[4.1 Configuration des moyens d’authentification approuvés 15](#_Toc158807565)

[4.2 Configuration de l’authentification par certificats Microsoft Entra ID 15](#_Toc158807566)

[4.3 Configuration de l’authentification avec une clé de sécurité FIDO2 18](#_Toc158807567)

[4.4 Configuration de l’authentification avec Windows Hello Entreprise 19](#_Toc158807568)

[4.5 Configuration de l’authentification avec Microsoft Authenticator 19](#_Toc158807569)

# 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.

## Présentation succincte du projet Pro Santé Connect sans couture

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.

Dans le cadre des POC techniques raccordement et sécurisation, un professionnel de santé (PS) peut ouvrir une session Microsoft Entra ID depuis un navigateur de son appareil Windows. Il utilise pour cela typiquement un moyen d’identification électronique (MIE) conforme avec les exigences établies par l’ANS et reconnu comme mécanisme d’authentification au niveau de ce locataire.

L’activation des différents MIE vis-à-vis desquels l’ANS invite les ES à conduire une évaluation ainsi que leur support dans Microsoft Entra ID sont couvert dans la suite de ce document.

A diagram of a computer application

Description automatically generated

Ainsi, lorsque le PS accède à ce service numérique, il est renvoyé vers PSC qui le redirige alors de façon transparente avec la délégation en place vers Microsoft Entra ID.

Dans le cadre des tests préliminaire, l’application de test PSC\_BAS, c.à.d. le portail de gestion des utilisateurs Bac à sable est mise à disposition à cette fin ; elle est accessible à l’adresse Internet <https://wallet.bas.psc.esante.gouv.fr/login-page>.

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

Description générée automatiquement

Le lancement de la cinématique avec Microsoft Entra ID peut être effectuée en cliquant sur le bouton S’Identifier avec EntraID. Une fois automatiquement authentifié par Microsoft Entra ID, avec le ou les MIE conforme configurés, et sur la base éventuellement d’une ouverture de session Windows avec la navigation sans couture, le PS est renvoyé vers PSC.

D’un point de vue technique, le protocole utilisé dans ces redirections et échanges est le standard de l’industrie OpenID Connect (OIDC) avec le flux de code d’autorisation (authorization code flow). (Le flux de code d'autorisation permet à l'application d'échanger un code d'autorisation contre des jetons d'ID pour représenter l'utilisateur authentifié et des jetons d'accès nécessaires pour appeler des API protégées.)

A ce stade, le PS n’accède pas directement au service numérique mais voit un écran intermédiaire lui demandant de confirmer sa volonté de continuer en utilisant le compte Microsoft Entra ID qui lui a été attribué par l’ES. Le PS peut alors choisir de continuer avec cette identité, ou de s’authentifier d’une autre façon (avec un autre MIE PSC par exemple).

Note concernant le parcours sans couture :il est en effet apparu préférable que le PS n’accède pas de façon totalement transparente au service numérique, afin de faciliter la gestion des sessions utilisées.

Exemple de cas d’usage : dans ce contexte, une secrétaire médicale pourrait laisser un accès rapide à son appareil à un des PS de son service : lors de l’accès au service numérique, la secrétaire choisirait sur l’écran intermédiaire de ne pas se connecter via son compte appairé, mais choisirait une authentification PSC. Cela permettrait au PS d’utiliser le poste de la secrétaire pour réaliser une tâche rapide et de se déconnecter par la suite.

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

Description générée automatiquement

Pour plus d’informations, nous invitons le lectorat à consulter la page suivante sur le site de l’ANS : TBD.

## Objectifs du guide

L’objectif de ce guide est d’expliciter les éléments de configuration de Microsoft Entra ID associés aux MIE suivants :

* Certificat basée sur Microsoft Entra ID avec une carte CPx physique ;
* Clé de sécurité FIDO2 (clé USB, carte à puce, etc.) ;
* Windows Hello Entreprise ;
* Microsoft Authenticator.

L’ensemble de ces MIE offrent à minima une authentification de type multifacteur (MFA).

Ce guide ne donne pas de préconisation sur la stratégie de déploiement à opérer au sein d’un ES pour par exemple déployer ces nouveaux MIE auprès de ses 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.

Ce guide vise également à couvrir de façon additionnelle les mécanismes additionnels 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 un appareil Windows 10 ou ultérieur est en effet enregistré auprès du locataire Microsoft Entra ID de l’ES, c.à.d. joint à Entra ID, de tels MIE peuvent également servir à l’ouverture d’une session nominative.

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 service numérique 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.

Il est à noter que 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.

## 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 tel 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.

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.

# Prise en charge des MIE conformes aux exigences de l’ANS dans Entra ID

## Utilisation des certificats X.509 de la carte CPx physique

Comme décrit précédemment en introduction de ce document, un PS peut utiliser le certificat X.509 de sa carte de professionnel de santé, ou carte CPx pour s’authentifier sur son locataire Entra ID et ainsi accéder à des services numériques connectés à PSC sans avoir besoin de se réauthentifier.

Le POC technique raccordement cible plus spécifiquement cette utilisation.

Documentation : carte d’identité professionnelle électronique du secteur de la santé : [<https://industriels.esante.gouv.fr/produits-services/cps-et-socle-technique/caracteristiques-de-la-cps3>](https://industriels.esante.gouv.fr/produits-services/cps-et-socle-technique/caracteristiques-de-la-cps3)

## Utilisation d’une clé de sécurité FIDO2

De la même façon, un PS peut utiliser une clé de sécurité FIDO2.

Le POC technique sécurisation cible plus spécifiquement cette utilisation. Dans ce cadre, la fourniture d’une clé FIDO2 est à la charge de l’ES. Windows Hello Entreprise peut être utilisé à cet effet dans ce contexte.

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 dans le cadre de la Task Force MIE.

## Utilisation de Windows Hello Entreprise

Windows Hello Entreprise peut être également utilisé à cet effet dans ce contexte comme clé FIDO2.

## Utilisation de Microsoft Authenticator

L’application Microsoft Authenticator peut enfin être utilisée dans ce contexte comme MIE 2FA conforme.

## Non prise en charge de la carte e-CPS

La carte e-CPS n’est PAS prise en charge dans le cadre proposé. Le flux « découplé » CIBA (Client-Initiated Backchannel Authentication, <https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html>) n’est en effet PAS pris en charge par la plateforme d’identité Microsoft Entra ID.

L’extension CIBA du protocole OpenID Connect (OIDC) n’est pas en effet pas intégré à date dans les environnements Microsoft.

Il convient de noter que la carte e-CPS reste cependant disponible que PSC pour réaliser l’appairage.

Documentation : OpenID Connect on the Microsoft identity platform : <https://learn.microsoft.com/fr-fr/entra/identity-platform/v2-protocols-oidc>

## MIE et navigation sans couture

Il est possible de plus de tirer parti à la fois de l’authentification Microsoft Entra ID avec ces MIE et de la possibilité de jointure (hybride ou non) des appareils Windows 10 ou ultérieur avec un locataire Microsoft Entra ID pour offrir une navigation sans couture afin d’accéder à un service numérique connecté à PSC.

Ainsi, par exemple, l’ouverture de session Windows par carte à puce avec les cartes CPx physiques délivrées par l’ANS aux PS est utilisée par de (très) nombreux ES. Le projet Pro Santé Connect sans couture vise donc naturellement à capitaliser à la fois sur ce mécanisme et l’expérience utilisateur associée.

Pour autant, et comme déjà indiqué, les prérequis pour cette navigation sans couture ne font pas partie du cadre minimum défini par l’ANS. Ils sont néanmoins couvert dans la suite de ce document.

## Axes d’extensibilité futurs prévisibles

L’intégration courante de PSC avec Microsoft Entra ID telle que décrite dans ses modalités opérationnelles dans le cadre de cette expérimentation vise à établir une fondation technique pérenne qui pourra être étendue tant d’un point de vue fonctionnel que technique afin de répondre aux attentes exprimées par les ES et PS.

Ainsi, l’ouverture de session et la capacité de navigation sans couture résultante pourront être étendues par la suite après qualification et validation. Ainsi, par exemple, l’ouverture de session avec Microsoft Entra ID pourra être effectuée depuis une session de terminal Windows à distance avec les fonctionnalités proposées par Microsoft Entra Private Access pour l’intégration étendue avec les environnements existants en local.

La version courante du présent document n’aborde pas cette dimension et ce qu’elle suppose en termes de mise en œuvre. Nous invitons pour cela le lectorat à se reporter d’une façon générale au site de l’ANS pour une information à jour ainsi que vis-à-vis de la seconde dimension au Guide de configuration de Microsoft Entra Private Access à destination des établissements de santé pour les éléments de configuration associés et éventuels prérequis.

# Configuration des MIE au niveau des appareils

## Activation du support des certificats X.509 de la carte CPx physique

La carte CPx physique comme MIE permet d'adopter une authentification résistante à l’hameçonnage (phishing) et de s’authentifier avec un certificat X.509 émis par l'infrastructure de gestion de la confiance du secteur santé-social français, dite « IGC-Santé », c.à.d. l’infrastructure de gestion de clés cryptographiques (IGC) opérée par l'ANS.

Sa prise en charge suppose les opérations suivantes depuis un appareil Windows 10 ou ultérieur.

### Lecture de la carte CPx par Cryptolib

La « Cryptolib CPS (Windows) » un logiciel qui permet l’interfaçage entre des applications informatiques et la carte CPx. L’installation de la « Cryptolib CPS (Windows) » permet ici à Windows de lire la carte physique CPx.

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

1. A l’aide d’un compte d’administrateur local, installer le logiciel Cryptolib comme décrit sur le lien suivant : <https://esante.gouv.fr/services/espace-cps/telechargements-libres/cryptolib-cps-windows>.
2. Vérifier la lecture effective du certificat du PS dans CPS Gestion :

Une image contenant texte, Appareils électroniques, capture d’écran, nombre

Description générée automatiquement

### Lecture des champs du certificat de la carte CPS

Certificat présent sur la carte CPS

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

Description générée automatiquement

Lecture du Principal Name (PN)

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

Description générée automatiquement

Lecture du Subject Key Identifier

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

Description générée automatiquement

Documentation :

* Certificats logiciels : <https://esante.gouv.fr/produits-services/certificats-logiciels>.

### Lecture de la carte CPx à l’ouverture de session Windows

Pour la navigation sans couture, la lecture de la carte CPS à l’ouverture de session Windows suppose un paramétrage du registre de Windows.

Ce paramétrage permet aux utilisateurs de voir apparaître un champ pour remplir un nom d’utilisateur lors de l’ouverture ou du déverrouillage de la session Windows par carte à puce. Ceci établit le lien entre l'identité enregistrée dans la carte CPS, représentée par le certificat X.509, et la paire de clés présente sur la carte, ainsi que l'identité utilisée au niveau de Windows.

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

1. Exécuter l’éditeur du Registre(regedit.exe) depuis la barre Windows.
2. Se diriger vers : Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Polices\Microsoft\Windows.
3. Créer un nouveau dossier : SmartCardCredentialProvider.
4. Une fois le dossier créé, créer un nouveau fichier DWORD (32-bit) Value.
5. Renommer ce fichier X509HintsNeeded, puis passer la Value dataà 1.

Remarque : cette opération peut être automatisé au travers de la définition d’un fichier .reg à exécuter directement depuis un invite de commande avec l’éditeur de registre (regedit.exe).

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

Description générée automatiquement

Un champ apparait alors lors de la connexion par carte à puce, pour renseigner un nom d’utilisateur

Une image contenant peinture, texte, montagne, plein air

Description générée automatiquement

## Activation du support des clés de sécurité FIDO2

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 Local Group Policy Editor.​   
   (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, nombre

Description générée automatiquement

1. Dans Computer Configuration > Administrative Templates > System > Logon, activer le paramètre Turn on security key sign-in.​

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>.

## Activation de Windows Hello Entreprise

La prise en charge de Windows Hello Entreprise suppose les opérations suivantes depuis un appareil Windows 10 ou ultérieur.

<A décrire>

## Activation de Microsoft Authenticator

La prise en charge de Microsoft Authenticator suppose les opérations suivantes depuis un appareil Android ou iOS.

<A décrire>

# Configuration des MIE dans Microsoft Entra ID

Microsoft Entra ID propose différents MIE pour gérer l’authentification de ces utilisateurs. De nombreuses méthodes peuvent être ainsi utilisées pour l’authentification multifacteur (MFA).

## Configuration des moyens d’authentification approuvés

Vous pouvez effectuer votre choix parmi la liste des méthodes d’authentification disponibles, en évaluant chacune d’elles sur le plan de la sécurité, de la facilité d’utilisation et de la disponibilité.

A ce propos, l’ES doit s’assurer que ces méthodes correspondent à des MIE autorisés et dûment configurés afin de permettre l’accès transparent à PSC et ses services.

L’ES aura à cible la charge de faire homologuer si nécessaire les MIE qu’il souhaite déployer et de leur compatibilité avec Microsoft Entra ID et les méthodes d’authentification proposées.

Afin de gérer les moyens d’authentifications autorisés pour les PS :

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.

Cette page permet de configurer les différents moyens d’authentification du projet Pro Santé Connect sans couture à intégrer dans le cadre des POC technique raccordement vs. sécurisation

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

Description générée automatiquementUne image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

C’est l’objet des sections suivantes.

Documentation Microsoft :

* Planifier un déploiement d'authentification multifacteur Microsoft Entra : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/howto-mfa-getstarted>

## Configuration de l’authentification par certificats Microsoft Entra ID

L’authentification basée sur les certificats Microsoft Entra permet d'authentifier les PS à l’aide de certificats X.509 sur leurs cartes à puce CPS3 directement auprès de Microsoft Entra ID quand ils ouvrent une session sur leur appareil Windows 10 ou ultérieur joint (en hybride) à Microsoft Entra. Aucune configuration spéciale n’est nécessaire sur l’appareil Windows pour accepter l’authentification par carte à puce au-delà de ce qui a été précisé précédemment, Cf. section 2.1 Utilisation des certificats X.509 de la carte CPx physique.

Prérequis :

* Les versions Windows des appareils Windows 10 ou ultérieurs prises en charge sont celles décrites pour la jointure à Microsoft Entra.

Cette prise en charge dans le cadre du projet Pro Santé Connect sans couture suppose l’application préalables des correctifs suivants selon les versions de Windows concernées :

* + [Windows 11 - KB5017383](https://support.microsoft.com/topic/september-20-2022-kb5017383-os-build-22000-1042-preview-62753265-68e9-45d2-adcb-f996bf3ad393) : <https://support.microsoft.com/topic/september-20-2022-kb5017383-os-build-22000-1042-preview-62753265-68e9-45d2-adcb-f996bf3ad393> ;
  + [Windows 10 - KB5017379](https://support.microsoft.com/topic/20-september-2022-kb5017379-os-build-17763-3469-preview-50a9b9e2-745d-49df-aaae-19190e10d307) : <https://support.microsoft.com/topic/20-september-2022-kb5017379-os-build-17763-3469-preview-50a9b9e2-745d-49df-aaae-19190e10d307> ;
  + [Windows Server 20H2- KB5017380](https://support.microsoft.com/topic/20-september-2022-kb5017380-os-builds-19042-2075-19043-2075-og-19044-2075-preview-59ab550c-105e-4481-b440-c37f07bf7897) : <https://support.microsoft.com/topic/20-september-2022-kb5017380-os-builds-19042-2075-19043-2075-og-19044-2075-preview-59ab550c-105e-4481-b440-c37f07bf7897> ;
  + [Windows Server 2022 - KB5017381](https://support.microsoft.com/topic/20-september-2022-kb5017381-os-build-20348-1070-preview-dc843fea-bccd-4550-9891-a021ae5088f0) : <https://support.microsoft.com/topic/20-september-2022-kb5017381-os-build-20348-1070-preview-dc843fea-bccd-4550-9891-a021ae5088f0> ;
  + [Windows Server 2019 - KB5017379](https://support.microsoft.com/topic/20-september-2022-kb5017379-os-build-17763-3469-preview-50a9b9e2-745d-49df-aaae-19190e10d307) : <https://support.microsoft.com/topic/20-september-2022-kb5017379-os-build-17763-3469-preview-50a9b9e2-745d-49df-aaae-19190e10d307>

Documentation Microsoft :

* Présentation de l'authentification basée sur les certificats : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication>

### Configuration de l’authentification multifacteur (MFA)

Procéder comme suit :

1. Depuis la page Stratégies des Méthodes d’authentification, cliquer sur Authentification basée sur un certificat.
2. Activer l’authentification basée sur un certificatpour Tous les utilisateurs.
3. Pour considérer l’authentification par certificat comme une authentification multifacteur (MFA)**,** choisir authentification multifacteur dans la partie Niveau de protection.
4. Il est ensuite possible d’indiquer l’ordre de priorité des champs à rechercher dans un certificat pour authentifier l’utilisateur. Ici on utilisera le PrincipalName en priorité 1.

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

Description générée automatiquement

### Déclaration des autorités de certification (AC)

Cette partie est obligatoire pour l’authentification basée sur un certificat /

Procéder comme suit :

1. Se diriger dans l’onglet Protection > Centre de sécurité.
2. Cliquer sur Autorités de certification.
3. Charger ensuite tous les certificats de la chaîne de confiance menant au certificat racine de l'infrastructure de gestion de la confiance du secteur santé-social français, dite « IGC – Santé », c.à.d. l’infrastructure de gestion de clés cryptographiques (IGC) opérée par l'ANS. L’IGC est ici celle de test pour le POC technique raccordement et le bac à sable PSC.

Il s’agit ici du certificat intermédiaire qui signe les certificats des cartes CPS et du certificat racine de l’AC.

* 1. Cliquer sur Charger pour charger le fichier de certificat.

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

Description générée automatiquement

* 1. Renseigner les champs et cliquer sur Ajouter.

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

Description générée automatiquement

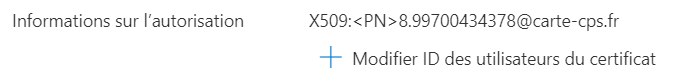
Documentation :

* Infrastructure de gestion de la confiance « IGC-Santé » : <http://igc-sante.esante.gouv.fr/PC%20TEST/>

### Déclaration de l’attribut du certificat souhaité pour l’appairage utilisateur

Procéder comme suit :

1. Retourner dans la vue d’ensemble de Microsoft Entra ID.
2. Dans Utilisateurs, cliquer sur Tous les utilisateurs, puis dans la page sur un utilisateur cible pour le POC technique raccordement.
3. Cliquer sur Modifier des propriétés.
4. Cliquer surInformations sur l’autorisation, puis sur Modifier ID des utilisateurs du certificats.
5. Ajouter l’attribut à rechercher dans le certificat selon la syntaxe ci-dessous. Ici, pour le PrincipalName (PN)



## Configuration de l’authentification avec une clé de sécurité FIDO2

### Autorisation de la configuration en libre-service ​

Procéder comme suit :

1. Depuis la page Stratégies des Méthodes d’authentification, cliquer sur Clé de sécurité FIDO2.
2. Activerla clé de sécurité FIDO2 pour Tous les utilisateurs.
3. 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

### 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

## Configuration de l’authentification avec Windows Hello Entreprise

TBD

## Configuration de l’authentification avec Microsoft Authenticator

TBD

Ceci conclut le présent guide.