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

Zzz

Guide de configuration des cartes CPx à destination des établissements de santé

Version 0.4b - Juin 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](#_Toc168328672)

[1.1 Objectifs du guide 6](#_Toc168328673)

[1.2 Non-objectifs du guide 6](#_Toc168328674)

[2 Configuration des cartes CPx au niveau des appareils 7](#_Toc168328675)

[2.1 Activation du support des certificats X.509 de la carte CPx physique sur les appareils Windows 7](#_Toc168328676)

[2.2 Lecture de la carte CPx à l’ouverture de session Windows 13](#_Toc168328677)

[3 Configuration de l’authentification par certificat en local 18](#_Toc168328678)

[3.1 Mise en place des prérequis 18](#_Toc168328679)

[3.2 Configuration de nouveaux comptes d’utilisateur en local 19](#_Toc168328680)

[3.3 Appairage manuel d’utilisateurs existants 20](#_Toc168328681)

[3.4 Résolution des problèmes de certificats et de configuration 22](#_Toc168328682)

[4 Configuration de l’authentification par certificat dans Microsoft Entra ID 23](#_Toc168328683)

[4.1 Activation de l’authentification basée sur certificat sur le locataire de l’ES 24](#_Toc168328684)

[4.2 Déclaration des autorités de certification (AC) 29](#_Toc168328685)

[4.3 Liaison des utilisateurs avec le certificat de la carte CPx physique 30](#_Toc168328686)

# 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. Cette dernière est décrite dans le Guide de configuration de Pro Santé Connect à destination des établissements de santé.

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

Dans ce contexte, un certificat X.509 d’une carte CPx physique constitue un moyen d’identification électronique (MIE) retenu dans le périmètre du POC technique. (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)

Ce MIE offre à minima une authentification de type multifacteur (MFA). Pour un appareil Windows 10 ou ultérieur enregistré auprès du locataire Microsoft Entra ID de l’ES, c.à.d. joint à Entra ID, la carte CPx physique peut ainsi servir à l’ouverture d’une session nominative.

L’ouverte de session par carte à puce avec une carte CPx réalisée depuis un poste de travail Windows avec une jointure (hybride) à Entra ID permet en effet de satisfaire aux exigences du Référentiel d’Identification Electronique (RIE) et 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.

## Objectifs du guide

L’objectif de ce guide est d’expliciter dans ce contexte les éléments de configuration de l’authentification par certificat X.509 basée sur Microsoft Entra ID avec une carte CPx physique.

## 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.

Un certificat X.509 sur une carte CPx physique n’est pas le seul MIE conforme dans le cadre du POC technique. Les MIE suivants sont également retenus dans le périmètre du POC technique :

* Clé de sécurité FIDO2 (clé USB, carte à puce, etc.) ;
* 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 clés de sécurité FIDO2 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 cartes CPx au niveau des appareils

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.

## Activation du support des certificats X.509 de la carte CPx physique sur les appareils Windows

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

### Prise en charge Plug-and-Play (PnP) de la carte CPx physique

Procéder comme suit :

1. Brancher le lecteur de carte à puce PC/SC (Personal Computer/Smart Card) v2 de type USBCCID. Lors du branchement, Windows détecte l'événement de branchement du lecteur, se rend compte qu'il est CCID (Chip Card Interface Device) et installe directement le pilote du périphérique ou bien qu'il n'a pas ledit pilote et se retourne alors vers Windows Update pour le récupérer puis l'installer.
2. Insérer la carte CPx dans le lecteur. Lors de l'insertion de la carte CPx dans le lecteur de cartes, l'évènement PC/SC "insertion carte" à Windows qui repart sur Windows Update récupérer et installer le mini-pilote intelligent carte CPx.

Le mini-pilote intelligent carte CPx fait office de pilote de la carte CPx physique auprès du système pour en arriver à un appareil Windows fonctionnel, c.à.d. prêt à utiliser la carte CPx pour PSC sans couture, accéder aux téléservices Assurance Maladie ou à toutes autres fonctions de sécurisation offerte par la carte CPx.

Le mini-pilote intelligent carte offre une alternative plus simple au développement d’un fournisseur de services de chiffrement (Cryptographic Services Provider ou CSP) hérité, Cf. section 2.1.2 Installation de la Cryptolib CPS (Windows) – Optionnel ci-dessous, en encapsulant la plupart des opérations de chiffrement complexes du développeur de mini-pilote carte.

Visuellement, pour le PS, le téléchargement des pilotes du lecteur de carte est automatique au branchement du lecteur. Il en est de même pour la carte CPx physique dès son insertion.

Si une erreur est rencontrée lors de l’installation du mini-pilote, il convient de désinstaller le mini-pilote CPx encore présent dans le système et de réinstaller le mini-pilote.

Procéder comme suit :

1. Cliquer sur Rechercher et taper « *cmd.exe* ».
2. Faire un clic droit et sélectionner Exécuter en tant qu’administrateur.
3. Dans l’invite de commandes, taper la commande suivante :

C:\> pnputil.exe -e

1. Noter le nom du fichier Oem#.inf où # est le numéro du mini-pilote CPx signé par l'ANS.
2. Taper la commande suivante :

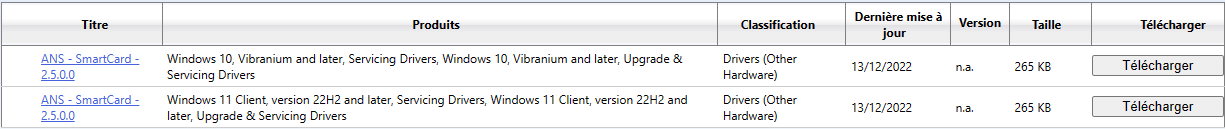
C:\> pnputil.exe -d Oem#.inf

1. Réinsérer la carte CPx et réinstaller le mini-pilote CPx.

Le mini-pilote CPx peut également être installé via le Catalogue Microsoft qui contient l’ensemble des pilotes qualifiés par Microsoft. Ce catalogue sert de base de pilotes à Windows Update et WSUS (Windows Server Update Services). Il permet aussi de récupérer manuellement des pilotes afin de les installer hors Windows Update ou de les déployer explicitement dans un WSUS local.

Pour installer le mini-pinote CPx depuis le Catalogue Microsoft, procéder comme suit :

1. Depuis un navigateur, aller sur le site <http://catalog.update.microsoft.com/v7/site/Home.asp>.
2. Taper « *ANS* » pour rechercher les dernières versions du mini-pilote CPx pour Windows 10 et ultérieur.



- ou –

Taper « *ASIP* » pour rechercher toutes les versions du mini-pilote CPx pour Windows.

Une image contenant texte, nombre, Police, ligne

Description générée automatiquement

1. Cliquer sur Télécharger pour la version correspondante à la plateforme cible. Un dialogue s’ouvre.

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

Description générée automatiquement

1. Cliquer sur le lien pour télécharger le mini-pilote.
2. Cliquer sur Fermer.

Documentation Microsoft :

* Mini-lecteur de carte à puce : <https://learn.microsoft.com/fr-fr/windows-hardware/drivers/smartcard/smart-card-minidrivers>.

Documentation ANS :

* Guide d'installation et d'utilisation du Minidriver CPS V2.1.0 du 03/12/2018 : <https://industriels.esante.gouv.fr/sites/default/files/media/document/ANS_PUSC_PSCE_Guide_installation_et_utilisation_du_Minidriver_CPS_20181203_v2.1.0.pdf>.

### Installation de la Cryptolib CPS (Windows) – Optionnel

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 également à Windows de lire la carte physique CPx.

Pour une utilisation de la carte physique CPx à des fins uniquement d’authentification, il n’est pas nécessaire de procéder à l’installation de la Cryptolib CPS (Windows) ; cette dernière est nécessaire uniquement pour la facturation.

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. Cliquer sur la flèche puis sur le lien INSTALLEUR 32 ET 64 BITS DE CRYPTOLIB CPS.

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

Description générée automatiquement

1. Une fois le fichier *CryptolibCPS-5.1.9.exe* téléchargé, l’ouvrir.
2. Lorsqu’invité à le faire, confirmer la modification par cette application de l’appareil. Cliquer sur Oui.
3. Le dialogue Composants Cryptographiques CPOS v5.1.9 (x64) s’ouvre.

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

Description générée automatiquement

1. Suivre les instructions de l’assistant pour l’installation de la « 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

Procéder comme suit :

1. Insérer la carte CPx dans le lecteur de carte à puce.
2. Depuis le bureau Windows, ouvrir le dialogue Exécuter. Taper Touche Windows + R pour cela
3. Dans Ouvrir, taper la commande "*mmc.exe certmgr.msc*".

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

Description générée automatiquement

1. Cliquer sur OK. Le Gestionnaire de certificats utilisateur s’ouvre.

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

Description générée automatiquement

1. Naviguer sous Certificats - Utilisateur actuel > Personnel > Certificats.
2. Deux certificats utilisateur sont présents sur la carte CPx et publiés dans le magasin de certificats utilisateur.

Sélectionner et afficher le certificat contenant les OID suivants :

* + Ouverture de session par carte à puce (Smart Card Logon) : 1.3.6.1.4.1.311.20.2.2
  + Garantit votre identité auprès d’un ordinateur distant (Proves your identity to a remote computer), c.à.d. Authentification du client : 1.3.6.1.5.5.7.3.2.

Remarque : seul l’OID Authentification du client est requis pour l’ouverture de session par carte à puces !

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

Description générée automatiquement

* 1. Lire le Principal Name (PN). Le PN est précisé dans le champ Subject Alternative Name (SAN) présent dans ce certificat (depuis mars 2011) qui sert à faire le lien avec un compte utilisateur dans Active Directory. Ce PN est construit selon le format ID\_utilisateur@carte-cps.fr. Par exemple :

8.99700434378@carte-cps.fr

ID\_utilisateur est construit sous la forme <Type d’identifiant>.<ID registre national>/<ID registre structure> ; ceci correspond au champ CN (= identifiant PS) du champ Objet présent dans les certificats de la carte CPx.

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

Description générée automatiquement

* 1. Lire l’extension x509 Subject Key Identifier (SKI) qui permet d’identifier une certificat contenant une clé publique particulière, Cf. <https://www.rfc-editor.org/rfc/rfc3280#section-4.2.1.2>. Par exemple 6e5f6d9917798ba271f83c704f8d0e422a21b402.

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

Description générée automatiquement

Documentation ANS :

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

### Utilisation de la carte CPS sur le site de test TLS de l’ANS

Procéder comme suit :

1. Insérer la carte CPx dans le lecteur de carte à puce.
2. Depuis un navigateur, aller à l’adresse suivante : <https://testssl.eservices.esante.gouv.fr/>.
3. Valider l’authentification client par certificat depuis la carte insérée.

**Les étapes de configuration suivantes supposent que cette opération est concluante. Dans le cas contraire, il est impératif de revoir la configuration réalisée et d’en résoudre le ou les problèmes rencontrés.**

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

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

### Utilisation d’indices (hint)

Ce paramétrage permet aux utilisateurs de voir apparaître un champ pour l’utilisation d’indices (hint) lors de l’ouverture ou du déverrouillage de la session Windows par carte à puce.

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 :

* Un fichier de registre .reg peut être défini. Ce dernier est alors à exécuter directement depuis un invite de commande avec l’éditeur de registre (regedit.exe)

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Polices\Microsoft\Windows\SmartCardCredentialProvider] "X509HintsNeeded"=dword:00000000

- ou -

* Pour un appareil Windows membre d’un domaine Active Directory, cette opération peut être automatisée au travers de l’application d’une stratégie de groupe (Group Policy Object ou GPO) de carte à puce.

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

Description générée automatiquement

Un champ pour une indication de connexion du nom d’utilisateur (X509UserNameHint) apparait alors lors de la connexion par carte à puce, pour renseigner un nom d’utilisateur. La valeur fournie doit être au format UPN (Universal Principal Name).

Une image contenant peinture, texte, montagne, plein air

Description générée automatiquement

Cette indication de connexion du nom d’utilisateur permet notamment d’utiliser le mappage dynamique avec un compte AD afin d’établir le lien entre l'identité enregistrée dans la carte CPx, représentée par le certificat X.509, et la paire de clés présente sur la carte, et l'identité utilisée au niveau de Windows. Celui-ci intègre le mappage implicite et le mappage explicite et y ajoute 4 autres méthodes fondées sur les extensions du certificat :

1. Le mappage implicite (ou mode UPN) se fonde sur la valeur UPN présente dans le champ Subject Alternative Name du certificat du PS, par exemple 8.99700434378@carte-cps.fr.
2. Le mappage explicite se fonde sur l’attribut altSecurityIdentities du compte d’utilisateur dans AD, Cf. section 3.2 Appairage manuel d’utilisateurs existants ci-dessous.

Cette indication de connexion du nom d’utilisateur (X509UserNameHint) est par ailleurs envoyé à Microsoft Entra ID si celle-ci est fournie.

En l’absence de cette information, Windows envoie :

* Pour les appareils joints à Microsoft Entra, le nom principal (UPN) et, s’il n’est pas présent, le RFC822Name à partir de champs Subject Alternative Name (SAN) du certificat utilisé pour se connecter à Windows. (Cependant, si aucun n’est présent, il est nécessaire de fournir une indication du nom d’utilisateur...)
* Pour les appareils avec une jointure hybride à Microsoft Entra, le nom principal (UPN) AD comme une connexion doit d’abord s’effectuer au domaine AD considéré.

Si l’ES conserve des valeurs UPN différentes et parfois non routables dans AD (par exemple utilisateur@es.local), la valeur envoyée par Windows peut dans ces cas ne pas correspondre à l’UPN du comptes Microsoft Entra des PS. Pour prendre en charge ces scénarios où Microsoft Entra ID ne trouve pas de correspondance avec la valeur envoyée par Windows, une recherche ultérieure est effectuée pour un utilisateur avec une valeur correspondante dans son attribut onPremisesUserPrincipalName. Si la connexion réussit, Windows met en cache l’UPN Microsoft Entra des utilisateurs et l’envoie dans les connexions suivantes.

Comme résumé dans le tableau suivant :

|  |  |  |
| --- | --- | --- |
| Connexion | Appareil joint à Microsoft Entra | Appareil avec jointure hybride à Microsoft Entra |
| Première connexion | Extrait du certificat | UPN AD ou 509UserNameHint |
| Connexion suivante | Extrait du certificat | UPN Microsoft Entra mis en cache |

### Non-utilisation du SAN pour le nom d’ouverture de session

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

Pour les appareils avec une jointure hybride à Microsoft Entra, l’ouverture de session utilise par défaut le champ subjectAltName (SAN) du type prefixe@carte-cps.fr, p. ex. 8.99700434378@carte-cps.fr, du certificat pour authentifier l’utilisateur.

Pour mémoire, la logique suivante est utilisée pour mapper un compte utilisateur :

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

Description générée automatiquement

Si le nom d’ouverture de session n’utilise pas ce format dans l’ES, il est donc nécessaire de désactiver l’usage du subjectAltName (SAN).

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

1. Depuis l’éditeur du Registre(regedit.exe), se diriger vers : Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\kdc.
2. Créer un nouveau fichier DWORD (32-bit) Value.
3. Renommer ce fichier UseSubjectAltName, puis passer la Value dataà 0.
4. se diriger vers : Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters.
5. Créer un nouveau fichier DWORD (32-bit) Value.
6. Renommer ce fichier UseSubjectAltName, puis passer la Value dataà 0.

Remarque :

* Un fichier de registre .reg peut être défini. Ce dernier est alors à exécuter directement depuis un invite de commande avec l’éditeur de registre (regedit.exe)

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\kdc] "UseSubjectAltName"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters] "UseSubjectAltName"=dword:00000000

- ou -

* Pour un appareil Windows membre d’un domaine Active Directory, cette opération peut être automatisée au travers de l’application d’une stratégie de groupe (Group Policy Object ou GPO) de carte à puce.

Documentation Microsoft :

* Paramètres de Registre et de stratégie de groupe de carte à puce : <https://learn.microsoft.com/fr-fr/windows/security/identity-protection/smart-cards/smart-card-group-policy-and-registry-settings> ;
* Autoriser l’indicateur de nom d’utilisateur (clé de registre X509HintsNeeded) : <https://learn.microsoft.com/fr-fr/windows/security/identity-protection/smart-cards/smart-card-group-policy-and-registry-settings#allow-user-name-hint> ;
* Exigences et énumération des certificats : <https://learn.microsoft.com/fr-fr/windows/security/identity-protection/smart-cards/smart-card-certificate-requirements-and-enumeration>.

# Configuration de l’authentification par certificat en local

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>.

Passer cette section pour des appareils joints à Microsoft Entra avec l’utilisation de comptes utilisateur cloud déclarés dans Entra ID pour les PS et suivre directement les étapes de configuration de la section 4 Configuration de l’authentification par certificat dans Microsoft Entra ID ci-dessous.

La connexion de jointure hybride doit d’abord se s’effectuer au domaine AD. Dans ce contexte, l’ouverture de session Windows par certificat au niveau AD impose un ensemble de prérequis qui doivent être impérativement satisfaits.

## Mise en place des prérequis

Prérequis :

* AD doit disposer dans le magasin Enterprise NTAuth de l’autorité de certification (AC) émettrice 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, pour authentifier les utilisateurs auprès d’Active Directory. L’IGC considérée est ici celle de test pour le POC technique raccordement et le bac à sable PSC.

Le magasin Enterprise NTAuth d’Active Directory est stocké dans la partition de configuration de l’Active Directory :

CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=<forêt>,DC=<suffixe>

Pour publier manuellement un certificat d’AC tiers dans le magasin NTAuth, nous invitons le lectorat à se reporter aux procéder aux instructions sur comment importer des certificats d’autorité de certification tierce dans le magasin Enterprise NTAuth, Cf. ci-dessous.

Après avoir placé ce certificat dans le magasin NTAuth, une stratégie de groupe stratégie de groupe (Group Policy Object ou GPO) place une clé de registre (avec l’empreinte du certificat) à l’emplacement suivant sur tous les membres du domaine :

HKEY\_LOCAL\_MACHINE\Software\Microsoft\EnterpriseCertificates\NTAuth\Certificates

Cette clé est actualisée toutes les huit heures, c.à.d. l’intervalle d’application classique d’une stratégie de groupe.

* Tous les contrôleurs de domaine doivent être configurés avec un certificat de contrôleur de domaine pour authentifier les utilisateurs de carte à puce :
  + Pour des certificats émis par le service Active Directory Certificates Service (AD CS), ceux-ci doivent être basés sur l’un des 3 gabarits natifs suivants : Domain Controller, Domain Controller Authentication ou Kerberos Authentication. Nous invitons le lectorat à se reporter à la configuration requise pour les certificats de contrôleur de domaine provenant d’une autorité de certification tierce, Cf. ci-dessous.
  + Pour des certificats émis par une IGC tierce comme par exemple « IGC – Santé », nous invitons le lectorat à se reporter aux instructions pour activer l’ouverture de session smart carte auprès d’autorités de certification tierces, Cf. ci-dessous.
* Tous les contrôleurs de domaine se sont vus appliquer les modifications d’authentification basées sur des certificats décrites dans l’article de la base de connaissance Microsoft KB5014754. Cf. KB5014754 : modifications apportées à l’authentification basée sur les certificats sur les contrôleurs de domaine Windows : <https://support.microsoft.com/fr-fr/topic/kb5014754-modifications-apport%C3%A9es-%C3%A0-l-authentification-bas%C3%A9e-sur-les-certificats-sur-les-contr%C3%B4leurs-de-domaine-windows-ad2c23b0-15d8-4340-a468-4d4f3b188f16>.
* Tous les appareils avec jointure hybride Microsoft Entra voir tous les membres du domaine doivent disposer du certificat de l’AC racine de l’« IGC – Santé » dans leur magasin des autorités de certification racines de confiance. Active Directory peut être configuré pour distribuer ce certificat à tous les membres du domaine à l’aide d’une stratégie de groupe (GPO).

Ces prérequis doivent être satisfait avant de passer à la section 3 Configuration de l’authentification par certificats dans Microsoft Entra ID.

Documentation Microsoft :

* Instructions pour activer l’ouverture de session smart carte auprès d’autorités de certification tierces : <https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/certificates-and-public-key-infrastructure-pki/enabling-smart-card-logon-third-party-certification-authorities> ;
* Comment importer des certificats d’autorité de certification tierce dans le magasin Enterprise NTAuth : <https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/certificates-and-public-key-infrastructure-pki/import-third-party-ca-to-enterprise-ntauth-store> ;
* Configuration requise pour les certificats de contrôleur de domaine provenant d’une autorité de certification tierce : <https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/active-directory/requirements-domain-controller>.

Documentation ANS :

* Infrastructure de gestion de la confiance « IGC-Santé de test » : <https://igc-sante.esante.gouv.fr/PC_TEST/> ;
* Infrastructure de gestion de la confiance « IGC-Santé » : <https://igc-sante.esante.gouv.fr/PC>.

## Configuration de nouveaux comptes d’utilisateur en local

Lors de la déclaration d’un nouveau comptes d'utilisateur, le nom d’ouverture de session de l’utilisateur à déclarer dans l’AD doit donc correspondre au Principal Name (PN) précisé dans le champ Subject Alternative Name (SAN). Comme déjà indiqué, ce PN est construit selon le format ID\_utilisateur@carte-cps.fr. Par exemple : 8.99700434378@carte-cps.fr

Ceci permet d’attribuer l'UPN de la carte CPx correspondante au compte d’utilisateur. Il s’agit d’un mappage de type 1:1.

### Paramétrage de comptes d’utilisateur préexistants

L’ANS met à disposition un canevas de script PowerShell de déploiement de ces UPN pour l’AD en local. La modification des utilisateurs se base sur une liste d’utilisateurs existants, reformatée dans un fichier texte dont la grammaire est fournie.

Ce script est à adapter en fonction de l’environnement existant :

1. Compte d’utilisateur stockés dans des unités d’organisation (Organizational Unit ou OU) particuliers ;
2. Connexion à AD différente ;
3. Modification d’autres attributs des comptes d’utilisateur ;
4. Etc.

Documentation ANS :

* Guide de mise en œuvre d’un Smartcard logon avec une carte CPS version 2.5 : <https://esantegouv.sharepoint.com/:b:/s/GRP-PoCProSantConnectsanscoutureEntraID/Ebz79nLukSxIhsWunea5-agBrviciPjEJa2iROSjwnJVjw?e=rkpjFU>.

### Déclaration du suffixe carte-cps.fr dans AD

Le suffixe carte-cps.fr doit être déclaré dans l’AD en local. Si le suffixe de l’UPN n’apparait pas dans la liste des noms de domaines connus, une relation d’approbation avec le domaine existant doit préalablement être créée.

Procéder comme suit :

1. Dans Outils d’administration, exécuter Domaines et approbations Active Directory.
2. Faire un clic droit sur Domaines et approbations Active Directory puis choisir Propriétés.
3. Ajouter « carte-cps.fr ».
4. Cliquer sur OK.

## Appairage manuel d’utilisateurs existants

AD en local prend en charge l’authentification basée sur des certificats et plusieurs liaisons de nom d'utilisateur.

A cette fin, l’attribut altSecurityIdentities des objets utilisateur dans AD permet d’utiliser différentes méthodes de mappage. Un indicateur (hint) est utilisé lors de la connexion pour diriger AD vers le compte souhaité afin de vérifier la connexion, Cf. section 2.2 Lecture de la carte CPx à l’ouverture de session Windows ci-dessus.

Cette approche alternative permet d’assurer le mappage, sans avoir à éditer/modifier le nom d’ouverture de session utilisateur.

Il existe six valeurs prises en charge pour cet attribut, avec trois mappages considérés comme faibles (non sécurisés) et les trois autres considérés comme forts. En général, les types de mappage sont considérés comme forts s’ils sont basés sur des identificateurs que vous ne pouvez pas réutiliser. Par conséquent, tous les types de mappage basés sur les noms d’utilisateur et les adresses e-mail sont considérés comme faibles.

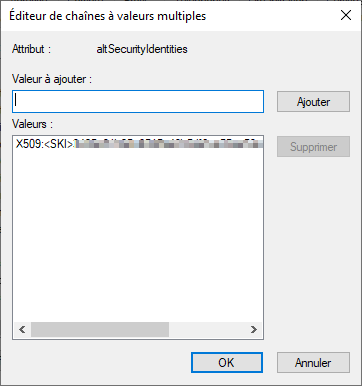
Procéder comme suit :

1. Dans Outils d’administration, exécuter Utilisateurs et ordinateurs Active Directory.
2. Dans Affichage, sélectionner Fonctionnalités avancées.
3. Sélectionner le compte d’utilisateur à mapper.
4. Faire un clic droit et cliquer sur Mappages des noms. Le dialogue Mappage des identités de sécurité s’ouvre.
5. Sélectionner l’onglet Certificats X.509.
6. Cliquer sur Ajouter.
7. Dans Editeur de chaînes à valeurs multiples :
   1. Préciser la valeur à ajouter. Cf. article de la base de connaissance Microsoft KB5014754.

|  |  |
| --- | --- |
| Champ du certificat X.509 | altSecurityIdentities |
| RFC822Name | X509:<RFC822>8.99700434378@carte-cps.fr |
| SKI | X509 :<SKI>6e5f6d9917798ba271f83c704f8d0e422a21b402 |
| SHA1PublicKey (condensat SHA1 de la valeur de SKI) | X509:<SHA1-PUKEY>ed913fa41377dbfb8eac2bc6fcae71ecd4a974fd |
| Emetteur et numéro de série | X509:<I>ValeurEmetteurEnFormatInversé<SR>ValeurNumeroSérieEnFormatInversé  Pour obtenir la valeur du numéro de série, exécuter la commande suivante et enregistrer la valeur indiquée dans l’attribut CertificateUserIds du compte d'utilisateur : certutil –dump –v [~cheminCertificat~] >> [~cheminFichier~]  Par exemple: certutil -dump -v utilisateur1.cer >> CertDump1.txt  X509:<I> DC=fr,DC=ANS,CN=TEST AC IGC-SANTE ELEMENTAIRE PERSONNES <SR>b24134139f069b49997212a86ba0ef48 |
| Emetteur et objet | X509:<I>ValeurEmetteurEnFormatInversé<S>ValeurSujetEnFormatInversé  X509:<I>DC=fr,DC=ANS,CN=TEST AC IGC-SANTE ELEMENTAIRE PERSONNES<S>DC=fr,DC=es,OU=UserAccounts,CN=psctest |
| Sujet | X509:<S>ValeurSujetEnFormatInversé  X509:<S>DC=fr,DC=es,OU=UserAccounts,CN=psctest |

Il s’agit typiquement du champ SKI pour une telle configuration.

* 1. Cliquer sur Ajouter.



* 1. Répéter les étapes a et b si nécessaires.
  2. Cliquer sur OK.

1. Cliquer sur OK.

Cette opération d’« enrôlement » manuelle est automatisable.

Pour mettre à jour cet attribut altSecurityIdentities à l’aide de PowerShell, la commande suivante peut être utilisée avec des privilèges d’administration pour par exemple préciser ici l’extension x509 Subject Key Identifier (SKI):

PS C:\> set-aduser 'DomainUser' -replace @{altSecurityIdentities="X509:<SKI>6e5f6d9917798ba271f83c704f8d0e422a21b402"}

Documentation Microsoft :

* HowTo: Map a user to a certificate via all the methods available in the altSecurityIdentities attribute : <https://learn.microsoft.com/fr-fr/archive/blogs/spatdsg/howto-map-a-user-to-a-certificate-via-all-the-methods-available-in-the-altsecurityidentities-attribute>.

## Résolution des problèmes de certificats et de configuration

La configuration à réaliser tant pour le respect des prérequis que pour celle des comptes revêt de multiples dimensions et peut conduire à une situation non fonctionnelle pour l’ouverture de session par carte à puces.

Le message d’erreur remonté est alors du type : « Vos informations d’identification n’ont pas pu être vérifiées ».

Il s’agit d’une erreur générique qui peut être le résultat d’un ou plusieurs des problèmes répertoriés.

Ces différents problèmes et leur résolution sont décrits dans la section [Problèmes de certificat et de configuration](https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/certificates-and-public-key-infrastructure-pki/enabling-smart-card-logon-third-party-certification-authorities#certificate-and-configuration-problems) de l’article [Activation de l’ouverture de session carte intelligente - Windows Server.](https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/certificates-and-public-key-infrastructure-pki/enabling-smart-card-logon-third-party-certification-authorities#possible-issues)

Nous invitons le lectorat à s’y reporter.

# Configuration de l’authentification par certificat dans Microsoft Entra ID

L’authentification basée sur certificat dans Microsoft Entra ID permet d'authentifier les PS à l’aide de certificats X.509 présents sur les cartes CPx directement auprès de Microsoft Entra ID quand ils ouvrent une session sur leur appareil Windows 10 ou ultérieur joint (en hybride) à Microsoft Entra ID.

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 Configuration des cartes CPx au niveau des appareils.

Pour les appareil Windows 10 ou ultérieur avec une jointure hybride à Microsoft Entra, une connexion de jointure hybride doit d’abord s’effectuer au domaine Active Directory, Cf. section .

Après une ouverture de session réussie, les utilisateurs reçoivent un jeton de rafraîchissement primaire (Primary Refresh Token ou PRT) de Microsoft Entra ID. Dans la configuration mise en œuvre ci-dessous, le PRT contient la revendication multifacteur.

Prérequis :

* Les versions Windows des appareils Windows 10 ou ultérieurs prises en charge sont celles décrites pour les appareils joints à Microsoft Entra ou ceux avec une jointure hybride 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>

Si la version de Windows de l’appareil ne prend pas en charge l’authentification par certificate Entra ID, une l’erreur NGC suivante apparait lors de l’exécution de la commande “dsregcmd /status”:

+----------------------------------------------------------------------+

AzureAdPrt : No

AzureAdPrtAuthority : https://login.microsoftonline.com/{tenantID}

AcquirePrtDiagnostics : PRESENT

Previous Prt Attempt : 2024-04-23 18:39:23.330 UTC

Attempt Status : 0xc000006d

User Identity : username@ans.fr

Credential Type : Certificate

Correlation ID : 72f070db-dfe6-4255-9418-763948153346

Endpoint URI : https://login.microsoftonline.com/{tenantID}/oauth2/token/

HTTP Method : POST

HTTP Error : 0x0

HTTP status : 400

Server Error Code : invalid\_requestServer Error Description : AADSTS130004: UserPrincipal doesn't have the NGC key configured.

* Le point de terminaison de l’authentification par certificat certauth de Microsoft Entra ID \*.certauth.login.microsoftonline.com doit être accessible pour l’environnement cloud de l’ES. L’inspection TLS doit de plus être désactiver sur ce point de terminaison certauth afin de vérifier que la demande de certificat client a bien abouti dans le cadre de la connexion TLS.

Documentation Microsoft :

* Présentation de l'authentification basée sur les certificats : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication> ;
* Comment configurer l’authentification Microsoft Entra basée sur certificat : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/how-to-certificate-based-authentication>.

## Activation de l’authentification basée sur certificat sur le locataire de l’ES

L’authentification basée sur certificat dans Microsoft Entra permet à l’ES de configurer son locataire Microsoft Entra pour autoriser ou demander aux utilisateurs de s’authentifier avec des certificats X.509 créés par l’infrastructure de gestion de la confiance « IGC-Santé » précédente afin de se connecter à PSC sans couture.

### Activation de l’authentification basée sur un certificat pour les utilisateurs ciblés

L’authentification basée sur les certificats Microsoft Entra peut être à facteur unique (SFA) ou multifacteur (MFA) en fonction de la configuration du locataire Entra ID.

L’activation de l’authentification basée sur les certificats rend un utilisateur potentiellement capable d’effectuer une authentification multifacteur. C’est cette approche qui est retenue dans la configuration présente.

Procéder comme suit :

1. Depuis la page Stratégies des Méthodes d’authentification, cliquer sur Authentification basée sur un certificat.
2. Sous Activer et cibler, sélectionner Activer.
   1. Sous Inclure, cliquer sur Sélectionner des groupes pour sélectionner des groupes spécifiques.
   2. Cliquer sur Ajouter des groupes.

Remarque : Nous ne recommandons PAS l’application à tous les utilisateurs. En effet, tous les utilisateurs déclarés dans le locataire ne disposant pas forcément d’une carte CPx, ce paramètre pourrait donc rendre certains comptes inaccessibles…

1. Sélectionner le ou les groupes cibles, Cf. Guide de configuration de l’accès conditionnel pour les établissements de Santé.
2. Cliquer sur Sélectionner.

Remarque : Une fois l’authentification basée sur les certificats activée sur le locataire Entra ID, tous les utilisateurs du locataire voient l’option de se connecter avec un certificat. Seuls les utilisateurs qui sont activés pour l’authentification basée sur les certificats peuvent s’authentifier à l’aide du certificat X.509.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. Prendre connaissance du message et cliquer sur J’accepte.

### Configuration de la stratégie de la liaison d’authentification

La stratégie de liaison d’authentification permet de définir la force de l’authentification sur un facteur (SFA), ou sur plusieurs (MFA).

Le niveau de protection par défaut pour les certificats sur le locataire est l’authentification à facteur unique. La configuration avec les carte CPx suppose de modifier la valeur par défaut en passant d’une authentification à facteur unique à une authentification multifacteur (et configurer des règles de stratégie personnalisées).

Pour configurer la liaison d’authentification, procéder comme suit :

1. Depuis la page Stratégies des Méthodes d’authentification, cliquer sur Authentification basée sur un certificat.
2. Cliquer sur Configurer.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. Dans Liaison d’authentification, pour Niveau de protection, sélectionner Authentification multifacteur afin de considérer l’authentification par certificat comme une authentification multifacteur (MFA) et remplacer la valeur par défaut.
2. A ce stade, il est possible de définir également des règles de liaison d’authentification personnalisées pour aider à déterminer le niveau de protection pour les certificats X.509 clients.

Création de règles de liaison d’authentification personnalisées

Des règles de liaison d’authentification personnalisées peuvent être configurées à l’aide des champs émetteur du certificat (Certificate issuer) et/ou OID de stratégie (Policy OID) dans le certificat X.509.

Elles mappent ainsi les attributs de certificat (émetteur de certificat ou OID de stratégie) à une valeur, et sélectionnent le niveau de protection par défaut pour cette règle. Plusieurs règles peuvent être ainsi créées pour aider à déterminer le niveau de protection pour les certificats client.

Pour ajouter des règles personnalisées, procéder comme suit :

1. Sélectionnez Ajouter une règle.
2. Pour créer une règle vis-à-vis de l’émetteur du certificat, c.à.d. l’« IGC-Santé » :

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

Description générée automatiquement

* 1. Sélectionner Émetteur de certificat.
  2. Dans Identificateur de l’émetteur de certificat, sélectionner CN=TEST AC IGC-SANTE pour l’« IGC-Santé de test ».
  3. Dans Force de l’authentification, sélectionner Authentification multifacteur.
  4. Dans Liaison d’affinité, sélectionner Basse.
  5. Cliquer sur Ajouter. Lorsqu’invité à le faire, cliquer sur J’accepte pour terminer l’ajout de la règle.

- ou -

Pour créer une règle vis-à-vis de l’OID de stratégie :

1. Sélectionner OID de stratégie.
2. Dans OID de stratégie, préciser l’OID approprié.
3. Dans Force de l’authentification, sélectionner Authentification multifacteur.
4. Dans Liaison d’affinité, sélectionner Basse.
5. Cliquer sur Ajouter. Lorsqu’invité à le faire, cliquer sur J’accepte pour terminer l’ajout de la règle.

Remarque importante : Il existe un problème connu lorsqu’une règle de liaison d’authentification personnalisée est configurée à l’aide de l’émetteur de certificat ET de l’OID de stratégie, ce qui a un impact direct sur certains scénarios des scénarios relatifs au POC technique, comme notamment l’inscription de clés de sécurité FIDO2 ou celle de Windows Hello Entreprise pour les MIE autorisés. Une telle règle personnalisée ne doit pas être créée en l’état. Nous œuvrons à corriger ce problème.

En laissant de côté les règles d’émetteur + OID de stratégie, les étapes suivantes sont utilisées pour déterminer le niveau de protection de l’authentification lorsque des règles personnalisées se chevauchent :

1. Les règles d’OID de stratégie prévalent sur les règles d’émetteur de certificat.
2. Les règles personnalisées utilisant des OID de stratégie sont évaluées. En cas de conflit entre plusieurs OID de stratégie - Par exemple, lorsqu’un certificat a deux OID de stratégie, l’un lié à l’authentification à un facteur (SFA) et l’autre à plusieurs (MFA) -, le certificat est traité comme authentification à un facteur.
3. Ensuite, les règles personnalisées utilisant l’autorité de certification de l’émetteur sont évaluées.
4. Si un certificat correspond à la fois à l’OID de stratégie et aux règles de l’émetteur, l’OID de stratégie est toujours vérifié en premier, et si aucune règle de la stratégie n’est trouvée, les liaisons de l’émetteur sont vérifiées. L’OID de stratégie a une priorité de liaison d’authentification forte supérieure à celle de l’émetteur.
5. Si une autorité de certification est liée à MFA, tous les certificats utilisateur émis par l’autorité sont éligibles comme MFA. La même logique s’applique à une authentification à un facteur.
6. Si un OID de stratégie est lié à MFA, tous les certificats utilisateur qui incluent cet OID de stratégie comme un des OID - un certificat utilisateur peut avoir plusieurs OID de stratégie - sont éligibles comme MFA.

Documentation Microsoft :

* Configurer la stratégie de liaison d’authentification : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/how-to-certificate-based-authentication#step-3-configure-authentication-binding-policy>.
* Comment Microsoft Entra ID résout plusieurs règles de liaison de stratégie d’authentification : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication-technical-deep-dive#how-microsoft-entra-id-resolves-multiple-authentication-policy-binding-rules>.

### Définition de la stratégie de liaison de nom d’utilisateur

La stratégie de liaison de nom d’utilisateur permet de valider le certificat de l’utilisateur présenté à Entra ID et de le mapper à un compte d’utilisateur Entra ID.

Par défaut, le nom alternatif du sujet (Subject Alternative Name ou SAN) dans le certificat est mappé à l’attribut UserPrincipalName de l’objet utilisateur pour déterminer l’utilisateur. Il est possible de remplacer la valeur par défaut et de créer un mappage personnalisé.

Les types de mappage basés sur les noms d’utilisateur et les adresses e-mail (RFC822Name) sont considérés comme ayant une affinité basse. Microsoft Entra ID implémente trois mappages considérés comme à affinité basse en fonction des identificateurs réutilisables. Les autres sont considérés comme des liaisons à affinité haute.

Procéder comme suit :

1. Depuis la configuration précédente, Cf. section précédente, naviguer vers Liaison de nom d’utilisateur.

Une image contenant texte, ligne, Police, nombre

Description générée automatiquement

1. Dans Liaison de nom d’utilisateur, indiquer l’ordre de priorité des champs à rechercher dans un certificat pour authentifier l’utilisateur. On utilisera ici le PrincipalName en priorité 1.
2. Préciser le cas échéant l’attribut à utiliser.

|  |  |
| --- | --- |
| Champ du certificat X.509 | Attribut(s) du compte d’utilisateur |
| PrincipalName | userPrincipalName, onPremisesUserPrincipalName, certificateUserIds (recommandé) |
| RFC822Name | userPrincipalName, onPremisesUserPrincipalName, certificateUserIds (recommandé) |
| SKI | certificateUserIds |
| SHA1PublicKey (condensat SHA1 de la valeur de SKI) | certificateUserIds |
| Emetteur et numéro de série | certificateUserIds |
| Emetteur et objet | certificateUserIds |
| Sujet | certificateUserIds |

1. A titre d’illustration, et de façon non obligatoire pour le POC technique, pour ajouter une règle personnalisée, sélectionner Ajouter une règle.

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

Description générée automatiquement

* 1. Dans Champ Certificat, sélectionner le ou les champs souhaités dans la liste proposée selon les affinités associées.
  2. Valider le cas échéant l’attribut du compte d’utilisateur à utiliser. L’attribut IDs des utilisateurs du certificat, ou certificateUserIds est le seul attribut utilisateur qui peut être mappé aux champs du certificat, Cf. section 4.3 Liaison des utilisateurs avec le certificat de la carte CPx physique ci-dessous.
  3. Cliquer sur Ajouter. Lorsqu’invité à le faire, cliquer sur J’accepte pour terminer l’ajout de la règle.

1. Cliquer sur Enregistrer pour enregistrer les modifications.

Microsoft Entra ID résout plusieurs règles de liaison de nom d’utilisateur de la façon suivante en utilisant la liaison de priorité la plus élevée (nombre le plus bas) :

1. Recherche de l’objet utilisateur à l’aide du nom d’utilisateur ou du nom d’utilisateur principal.
2. Obtention de la liste de toutes les liaisons de nom d’utilisateur configurées par l’ES classées selon l’attribut « priorité ».
3. Si la liaison à affinité élevée est activée ou si les valeurs du certificat correspondent à une règle personnalisée exigeant une liaison à affinité élevée, suppression de la liste toutes les liaisons à affinité faible.
4. Évaluation de chaque liaison dans la liste jusqu’à ce qu’une authentification réussie se produise.
5. Si le champ du certificat X.509 de la liaison configurée se trouve sur le certificat présenté, correspondance de la valeur du champ du certificat à la valeur d’attribut de l’objet utilisateur.
6. Si une correspondance est trouvée, l’authentification de l’utilisateur réussit.
7. Si aucune correspondance n’est trouvée, passez à la liaison de priorité suivante.
8. Si le champ du certificat X.509 ne se trouve pas sur le certificat présenté, passage à la liaison de priorité suivante.
9. Validation de toutes les liaisons de nom d’utilisateur configurées jusqu’à ce que l’une d’elles entraîne une correspondance et que l’authentification utilisateur réussisse.
10. Si aucune correspondance n’est trouvée sur l’une des liaisons de nom d’utilisateur configurées, échec de l’authentification utilisateur.

Documentation Microsoft :

* Présentation de la stratégie de liaison de nom d’utilisateur : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication-technical-deep-dive#understanding-the-username-binding-policy>.
* Comment configurer l’authentification Microsoft Entra basée sur certificat : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/how-to-certificate-based-authentication>.

## Déclaration des autorités de certification (AC)

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

Les certificats X.509 présents sur les cartes CPx sont émis par l’infrastructure de gestion de la confiance « IGC-Santé ». L’autorité de certification (AC) émettrice et les AC intermédiaires de cette infrastructure doivent être configurées dans Microsoft Entra ID.

### Configuration des autorités de certification

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 Autorités de certification.
4. 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 » 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. Dans URL de la liste de révocation de certificats, renseigner la valeur suivante pour le point de distribution configuré de la liste de révocation de l’autorité de confiance considérée :
* "http://igc-sante.esante.gouv.fr/CRL/ACI-EL-PP-TEST.crl" pour l’« IGC-Santé de test » ;

- ou -

* "http://igc-sante.esante.gouv.fr/CRL/ACI-EL-PP.crl" pour l’« IGC-Santé ».

Remarque importante : comme souligné ci-avant, dans le cadre du POC technique, la valeur à considérer est celle de pour l’« IGC-Santé de test ».

* 1. Laisser URL de la liste de révocation de certificats Delta. L’« IGC-Santé » ne propose pas de listes Delta.
  2. Cliquer sur Ajouter.

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

Description générée automatiquement

Documentation ANS :

* Infrastructure de gestion de la confiance « IGC-Santé de test » : <http://igc-sante.esante.gouv.fr/PC_TEST/> ;
* Infrastructure de gestion de la confiance « IGC-Santé » : <https://igc-sante.esante.gouv.fr/PC>.

### Validation des autorités de certification

Il est important de s’assurer que le résultat des étapes de configuration ci-dessus est la capacité d’Entra ID i) à valider la chaîne de confiance de ces autorités et ii) à obtenir correctement la liste de révocation de certificats (à partir du point de distribution.

Pour faciliter cette tâche, procéder comme suit :

1. Installer le module PowerShell MSIdentityTools depuis le dépôt GitHub <https://github.com/AzureAD/MSIdentityTools>.
2. Ouvrir un invite PowerShell et exécuter le cmdlet PowerShell Test-MsIdCBATrustStoreConfiguration : <https://github.com/AzureAD/MSIdentityTools/wiki/Test-MsIdCBATrustStoreConfiguration>.

PS C:\> Test-MsIdCBATrustStoreConfiguration

Ce cmdlet PowerShell examine la configuration de l'autorité de confiance du client Entra et fait apparaître le cas échéant des erreurs et des avertissements pour les problèmes courants rencontrés de mauvaise configuration.

## Liaison des utilisateurs avec le certificat de la carte CPx physique

Les objets utilisateurs dans Microsoft Entra ID ont un attribut nommé IDs des utilisateurs du certificat, ou certificateUserIds.

A l’instar de l’attribut altSecurityIdentities des objets utilisateur dans AD en local, Cf. section 3.2 Appairage manuel d’utilisateurs existants ci-dessus, cet attribut permet d’utiliser différentes méthodes de liaison de façon à associer un certificat à un utilisateur. Nous ne considérons ici que le mappage d’un certificat à un compte d’utilisateur Entra (1:1).

Remarque : Il existe des scénarios où un ES peut vouloir prendre en charge plusieurs certificats pour une identité unique (M:1) ou inversement un même certificat pour plusieurs comptes d’utilisateurs Entra (1:M). Bien que supportés, ces scénarios ne sont pas considérés dans le présent guide. Cf. Sécurisation de la configuration Microsoft Entra avec plusieurs liaisons de nom d’utilisateur : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication-technical-deep-dive#securing-microsoft-entra-configuration-with-multiple-username-bindings>.

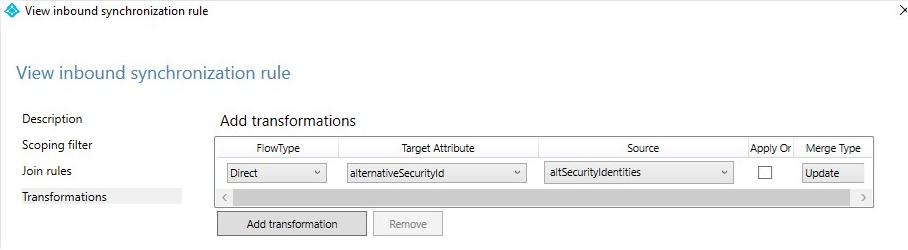
Prérequis :

* Pour des utilisateurs cloud uniquement, le rôle Administrateur d’authentification privilégiée (Privileged Authentication Administrator) est nécessaire pour mettre à jour l’attribut certificateUserIds. Le Centre d’administration Microsoft Entra, l’API Microsoft Graph (requêtes ou commandes PowerShell) peuvent être utilisées à cette fin.
* Pour des utilisateurs synchronisés, le rôle Administrateur d’identité hybride (Hybrid Identity Administrator) est nécessaire.
* Seul Microsoft Entra Connect peut être utilisé pour mettre à jour cet attribut en synchronisant la valeur sur site lors de la synchronisation des utilisateurs hybrides si celle-ci est en place dans l’ES entre son annuaire Active Directory en local et son locataire Entra ID. Cf. section Synchronisation d’annuaire avec un environnement Active Directory existant dans Socle technique minimal pour la mise en œuvre de PSC avec Microsoft Entra ID : <https://github.com/microsoft/prosanteconnect/blob/main/PREREQUISITES.md>.

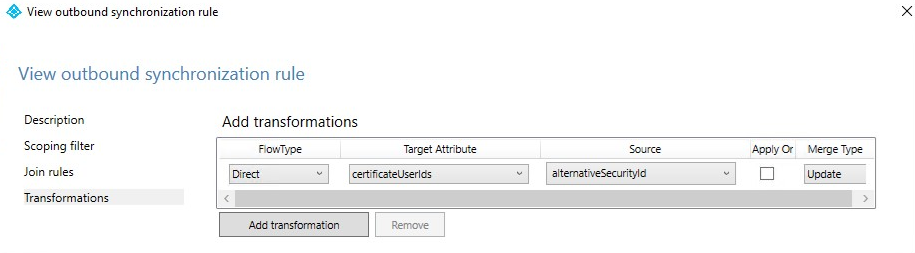
L’application Microsoft Entra Connect ou la synchronisation cloud Microsoft Entra Connect peuvent être utilisée à cet effet. Dans le premier cas, la dernière version disponible de l’application doit être utilisée. Celle-ci est téléchargeable depuis l’adresse Internet : <https://www.microsoft.com/download/details.aspx?id=47594>.

Pour les utilisateurs cibles, il s’agit alors de définir typiquement les règles suivantes de façon à ce que l’attribut altSecurityIdentities des objets utilisateur dans AD en local soit remonté au niveau Microsoft Entra ID dans l’attribut certificateUserIds des objets utilisateurs correspondants :

1. Règle de synchronisation en entrée :



1. Règle de synchronisation en sortie :



Documentation Microsoft :

* Mappage à l’attribut certificateUserIds dans Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication-certificateuserids>.

### Déclaration de l’attribut du certificat souhaité pour des utilisateurs cloud uniquement

Seule l’utilisation du Centre d’administration Microsoft Entra est illustrée dans la suite de cette section.

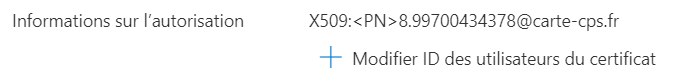
Pour celle de Microsoft Graph et de l’objet utilisateur (<https://learn.microsoft.com/en-us/graph/api/resources/user>), nous invitons le lectorat à se reporter à la documentation Microsoft :

* Mettre à jour certificateUserIds au moyen de requêtes Microsoft Graph : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication-certificateuserids#update-certificateuserids-using-microsoft-graph-queries> ;
* Mettre à jour certificateUserIds à l’aide des commandes PowerShell : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication-certificateuserids#update-certificateuserids-using-powershell-commands>.

Pour configurer un mappage de type 1:1 pour les utilisateurs cibles, procéder comme suit :

1. Retourner dans la vue d’ensemble de Microsoft Entra ID.
2. Dans Utilisateurs, cliquer sur Tous les utilisateurs.
3. Cliquer sur un utilisateur cible pour le POC technique raccordement, puis sur Modifier des propriétés.
4. Cliquer surInformations sur l’autorisation, puis sur Modifier les ID des utilisateurs du certificat.
5. Cliquer sur Ajouter. Entrer l’attribut à rechercher dans le certificat comme champ de mappage de certificat, puis cliquer sur Enregistrer.

Ici, pour le PrincipalName (PN) : X509 :<PN>. Par exemple 8.99700434378@carte-cps.fr



Les formats pris en charge pour certificateUserIds sont les suivants. Conformément à ce qui est illustré précédemment, le champ SKI sera typiquement utilisé dans la configuration.

|  |  |
| --- | --- |
| Champ du certificat X.509 | Format et/ou exemple de valeur |
| PrincipalName | X509:<PN>userPrincipalName  X509:<PN>8.99700434378@carte-cps.fr |
| RFC822Name | X509:<RFC822>8.99700434378@carte-cps.fr |
| SKI | X509 :<SKI>6e5f6d9917798ba271f83c704f8d0e422a21b402 |
| SHA1PublicKey (condensat SHA1 de la valeur de SKI) | X509:<SHA1-PUKEY>ed913fa41377dbfb8eac2bc6fcae71ecd4a974fd |
| Emetteur et numéro de série | X509:<I>ValeurEmetteurEnFormatInversé<SR>ValeurNumeroSérieEnFormatInversé  Pour obtenir la valeur du numéro de série, exécuter la commande suivante et enregistrer la valeur indiquée dans l’attribut CertificateUserIds du compte d'utilisateur : certutil –dump –v [~cheminCertificat~] >> [~cheminFichier~]  Par exemple: certutil -dump -v utilisateur1.cer >> CertDump1.txt  X509:<I> DC=fr,DC=ANS,CN=TEST AC IGC-SANTE ELEMENTAIRE PERSONNES <SR>b24134139f069b49997212a86ba0ef48 |
| Emetteur et objet | X509:<I>ValeurEmetteurEnFormatInversé<S>ValeurSujetEnFormatInversé  X509:<I>DC=fr,DC=ANS,CN=TEST AC IGC-SANTE ELEMENTAIRE PERSONNES<S>DC=fr,DC=es,OU=UserAccounts,CN=psctest |
| Sujet | X509:<S>ValeurSujetEnFormatInversé  X509:<S>DC=fr,DC=es,OU=UserAccounts,CN=psctest |

Remarque : jusqu’à 5 valeurs peuvent ainsi être précisées. Chaque valeur doit avoir moins de 1 024 caractères et doit être unique. Une fois qu’une valeur est présente sur un compte d'utilisateur, elle ne peut pas être écrite dans un autre compte d'utilisateur dans le même locataire Entra ID de l’ES.

### Déclaration de l’attribut du certificat souhaité pour des utilisateurs synchronisés

Comme indiqué précédemment, Microsoft Entra Connect prend en charge la synchronisation des valeurs de l’attribut certificateUserIds lors de la synchronisation des utilisateurs cibles hybrides si celle-ci est en place dans l’ES entre son annuaire AD en local et son locataire Entra ID. L’attribut altSecurityIdentities des objets utilisateur dans AD est utilisé à cette fin.

Remarque importante : cet attribut altSecurityIdentities ne fait pas partie de l’ensemble des attributs synchronisés par défaut. Il est nécessaire d’ajouter un nouvel attribut à l’objet personne (person) dans le Métaverse, puis créer les règles de synchronisation appropriées pour relayer ces données vers l’attribut certificateUserIds dans Entra ID.

Pour éviter les erreurs de synchronisation :

1. S’assurer que les valeurs en cours de synchronisation suivent l’un des formats pris en charge pour l’attribut multivalué attribut ID des utilisateurs du certificat, ou certificateUserIds.
2. Vérifier que tous les comptes d’utilisateur synchronisés à partir de l’AD en local ont :
   1. 5 valeurs ou moins dans leurs attributs altSecurityIdentities.
   2. Aucune valeur avec plus de 1 024 caractères.
   3. Aucune valeur dupliquée.

Documentation Microsoft :

* Mappage à l’attribut certificateUserIds dans Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication-certificateuserids> ;
* Synchroniser X509 :<PN>PrincipalNameValue : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication-certificateuserids#synchronize-x509pnprincipalnamevalue>.
* Synchroniser l'attribut altSecurityIdentities d'Active Directory avec le certificateUserIds de Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication-certificateuserids#synchronize-altsecurityidentities-attribute-from-active-directory-to-microsoft-entra-id-certificateuserids>.

### Déploiement par étapes pour le POC technique

Dans le cadre du POC technique, le déploiement par étapes (staged rollout features) permet à l’ES de tester des (groupes d’)utilisateurs de manière sélective avec des fonctionnalités d’authentification cloud comme l’authentification multifacteur sur la base du certificat de la carte CPx physique, l’accès conditionnel, etc.

Pour les utilisateurs cibles hybrides, et de façon préférentielle sur la base de groupe(s) d’utilisateurs, au-delà de l’authentification basée sur un certificat, Cf. section , il s’agira également d’activer typiquement :

* La synchronisation du hachage de mot de passe (Password Hash Sync ou PHS) – ceci s’effectue au niveau des fonctionnalités facultatives de Microsoft Entra Connect -,
* L’authentification unique fluide (Seamless Sign-On) pour fluidifier l’authentification.
* La réécriture de mot de passe (Password Write Back) afin que si un utilisateur change son mot de passe dans le locataire Entra ID de l’ES, cette modification soit répercutée dans Active Directory en local.

Pour cela, procéder comme suit :

1. Se connecter au Centre d’administration Microsoft Entra au moins en tant qu'[administrateur d’identité hybride](https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference#hybrid-identity-administrator).
2. Accéder à Identité > Gestion hybride > Microsoft Entra Connect > Connect Sync.
3. Dans Microsoft Entra Connect, sous Déploiement par étapes de l’authentification cloud, sélectionner Activer le déploiement par étapes pour la connexion utilisateur managée.

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

Description générée automatiquement

1. Dans Activer la fonctionnalité de déploiement par étapes, sélectionner les fonctionnalités à activer, typiquement :
   1. Synchronisation du hachage du mot de passe,
   2. Authentification unique fluide,
   3. Authentification basée sur un certificat.

Faire glisser les contrôles correspondant sur Activé.

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

Description générée automatiquement

1. Ajouter des groupes aux fonctionnalités sélectionnées. Pour chacune d’elles :
   1. Cliquer sur Gérer les groupes.
   2. Cliquer sur Ajouter des groupes.
   3. Dans Sélectionner un groupe, sélectionner le ou les groupes à ajouter.
   4. Cliquer sur Sélectionner.

Pour éviter les problèmes de délai d’expiration, vérifier que les groupes de sécurité ne contiennent pas plus de 200 membres au départ.

Remarques importantes : Les membres d’un groupe sont automatiquement activés pour le déploiement par étapes. Les groupes dynamiques et imbriqués ne sont pas pris en charge pour le déploiement par étapes.

Quand vous ajoutez un nouveau groupe, les utilisateurs du groupe (jusqu’à 200 utilisateurs pour un nouveau groupe) sont mis à jour pour utiliser l’authentification managée immédiatement. La prise en compte de la modification d’un groupe (ajout ou suppression d’utilisateurs) peut prendre jusqu’à 24 heures.

L’authentification unique fluide s’applique seulement si les utilisateurs se trouvent dans le groupe Authentification unique fluide et également dans un groupe Synchronisation du hachage du mot de passe (PHS) ou Authentification directe (Passthrough Authentication ou PTA).

Documentation Microsoft :

* Migrer vers l’authentification cloud avec un déploiement par étapes : [Microsoft Entra Connect : authentification cloud par le biais du déploiement par étapes - Microsoft Entra ID | Microsoft Learn](https://learn.microsoft.com/fr-fr/entra/identity/hybrid/connect/how-to-connect-staged-rollout) ;
* Qu’est-ce que la synchronisation de hachage du mot de passe avec Microsoft Entra ID ? : <https://learn.microsoft.com/fr-fr/entra/identity/hybrid/connect/whatis-phs> ;
* Authentification unique fluide Microsoft Entra : <https://learn.microsoft.com/fr-fr/entra/identity/hybrid/connect/how-to-connect-sso> ;
* Tutoriel : activer la réécriture et la réinitialisation de mot de passe en libre-service Microsoft Entra dans un environnement local : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/tutorial-enable-sspr-writeback>.

A titre de compléments, nous invitons le lectorat à consulter la série de guides « Active Directory from on-premises to the cloud – Entra ID whitepapers » disponible sur le Centre de téléchargement Microsoft à l’adresse <https://www.microsoft.com/en-us/download/details.aspx?id=36391>.

Ceci conclut le présent guide.