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

Zzz

Guide de configuration de Microsoft Authenticator et des clés d’accès à destination des établissements de santé

Version 1.0 - Novembre 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](#_Toc184310796)

[1.1 Objectifs du guide 5](#_Toc184310797)

[1.2 Non-objectifs du guide 5](#_Toc184310798)

[2 Configuration de Microsoft Authenticator au niveau des appareils 7](#_Toc184310799)

[2.1 Installation de l’application Microsoft Authenticator 7](#_Toc184310800)

[2.2 Activation de Microsoft Authenticator 7](#_Toc184310801)

[3 Configuration de l’authentification avec Microsoft Authenticator dans Microsoft Entra ID 9](#_Toc184310802)

[4 Configuration additionnelle pour l’authentification avec les clés d’accès dans Microsoft Entra ID 10](#_Toc184310803)

[4.1 Activation des clés d’accès dans Microsoft Authenticator 10](#_Toc184310804)

[4.2 Inscription d’une clé d’accès dans Microsoft Authenticator 12](#_Toc184310805)

[4.3 Connexion avec une clé d’accès dans Microsoft Authenticator 16](#_Toc184310806)

# 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

La délégation à un fournisseur d'identité local permet désormais aux PS et utilisateurs de se connecter à PSC en utilisant l'identité numérique fournie par leur établissement de Santé (ES) d'origine. Nous nous intéressons ici à la délégation de l’authentification à Microsoft Entra ID. Pour plus d’informations, nous invitons le lectorat à consulter le Portail Industriels de l’ANS : Délégation à un fournisseur d'identité local : <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/delegation-un-fournisseur-d-identite-local>.

Dans ce contexte, l’application Microsoft Authenticator peut enfin être utilisée comme un moyen d’identification électronique (MIE) 2FA conforme.

## Objectifs du guide

L’objectif de ce guide est d’expliciter dans ce contexte les éléments de configuration de Microsoft Authenticator.

## 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.

Microsoft Authenticator n’est pas le seul MIE conforme dans le cadre de cette mise en œuvre technique. Les MIE suivants sont également retenus dans le périmètre de celle-ci :

* Certificat X.509 avec une carte CPx physique ;
* Clé de sécurité FIDO2 (clé USB, carte à puce, etc.) ;
* Windows Hello Entreprise.

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

* Guide de configuration des cartes CPx à destination des établissements de santé ;
* Guide de configuration des clés de sécurité FIDO2 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 de Microsoft Authenticator au niveau des appareils

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

## Installation de l’application Microsoft Authenticator

Procéder comme suit :

1. Depuis votre appareil mobile, télécharger l’application. L’application Microsoft Authenticator est téléchargeable sur :

* Les appareils Android depuis le store Google Play à l’adresse Internet suivante : <https://go.microsoft.com/fwlink/p/?linkid=2168850&clcid=0x40c&culture=fr-fr&country=fr>.

Ce QR code peut être scanné à cet effet :

Une image contenant motif, texte, point, monochrome

Description générée automatiquement

* Les appareils iOS depuis l’Apple Store à l’adresse Internet suivante : <https://go.microsoft.com/fwlink/p/?linkid=2168643&clcid=0x40c&culture=fr-fr&country=fr> .

Ce QR code peut être scanné à cet effet :

Une image contenant motif, point, pixel, mots croisés

Description générée automatiquement

1. Procéder à l’installation de l’application.

## Activation de Microsoft Authenticator

Procéder comme suit :

1. Ouvrir l'application Microsoft Authenticator et sélectionner le bouton + pour ajouter un compte.
2. Choisir Compte professionnel ou scolaire et suivre les instructions pour se connecter avec le compte Microsoft Entra ID souhaité. Vous pouvez ajouter votre compte en vous connectant avec vos informations d'identification de compte professionnel ou scolaire, en scannant un code QR, ou en vous connectant avec vos informations d'identification.
3. Une fois le compte ajouté, un message s’affiche demandant d'appuyer sur un numéro dans l'application. Entrer le numéro sir l'écran de connexion dans la boîte de dialogue Microsoft Authenticator.
4. Choisir Approuver et fournir votre code confidentiel ou votre biométrie pour terminer le processus de connexion.
5. À ce stade, vous pouvez être invité à scanner un code QR fourni par l’ES pour configurer un compte d'authentification multifacteur dans l'application. Suivre les instructions fournies pour compléter cette étape.

A ce stade, il est nécessaire d’ activer la connexion par téléphone. Procéder comme suit :

1. Dans **Microsoft Authenticator**, sélectionner le compte enregistré ci-dessus.
2. Sélectionner **Activer la connexion par téléphone**.
3. Suivre les instructions de l’application pour terminer de s’inscrire à la connexion sans mot de passe.

Une fois ces étapes terminées, Microsoft Authenticator peut être utilisé pour se connecter au compte Entra ID configuré sans avoir besoin d'un mot de passe traditionnel.

Pour utiliser l'authentification sans mot de passe avec Microsoft Authenticator, certaines conditions préalables doivent être remplies, notamment l'installation de la dernière version de Microsoft Authenticator sur des appareils exécutant Android ou iOS, et l'activation de l'authentification multifacteur (MFA) Microsoft avec les notifications Push autorisées comme méthode de vérification.

Documentation Microsoft :

* Activer la connexion sans mot de passe avec Microsoft Authenticator :  
  <https://learn.microsoft.com/fr-fr/entra/identity/authentication/howto-authentication-passwordless-phone>
* Ajouter votre compte professionnel ou scolaire à l’application Microsoft Authenticator : <https://support.microsoft.com/fr-fr/account-billing/ajouter-votre-compte-professionnel-ou-scolaire-%C3%A0-l-application-microsoft-authenticator-43a73ab5-b4e8-446d-9e54-2a4cb8e4e93c> ;
* Vous connecter à vos comptes à l’aide de l’application Microsoft Authenticator : <https://support.microsoft.com/fr-fr/account-billing/vous-connecter-%C3%A0-vos-comptes-%C3%A0-l-aide-de-l-application-microsoft-authenticator-582bdc07-4566-4c97-a7aa-56058122714c>.

# Configuration de l’authentification avec Microsoft Authenticator dans Microsoft Entra ID

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. Sous Microsoft Authenticator, choisir les options suivantes :
   1. Activer - Oui ou Non.
   2. Cible - Tous les utilisateurs ou les utilisateurs sélectionnés.
4. Chaque groupe ou utilisateur ajouté est activé par défaut pour utiliser Microsoft Authenticator dans les modes de notifications sans mot de passe et push (mode « Tout »). Pour modifier le mode, pour chaque ligne pour le Mode d’authentification, choisir Tout ou Sans mot de passe. Le choix d’une notification Push empêche l’utilisation des informations d’identification de connexion par téléphone
5. Pour appliquer la nouvelle stratégie, cliquer sur Enregistrer.

# Configuration additionnelle pour l’authentification avec les clés d’accès dans Microsoft Entra ID

Cette section décrit les étapes permettant d’activer et d’appliquer l’utilisation de clés d’accès (*passkeys*) dans Microsoft Authenticator pour un locataire Microsoft Entra ID d’un ES. .

Les clés d’accès offrent non seulement une expérience utilisateur (UX) améliorée avec Microsoft Authenticator en vous permettant de se connecter plus rapidement avec son visage, son empreinte digitale ou son code PIN, mais elles ne sont pas non plus susceptibles d’être exposées aux mêmes types d’attaques que les mots de passe. De plus, les clés d’accès éliminent les mots de passe oubliés et les codes à usage unique et réduisent les appels d’assistance.

Documentation Microsoft : Qu’est-ce qu’une clé d’accès ? : <https://www.microsoft.com/security/business/security-101/what-is-passkey>.

La mise en œuvre de cette fonctionnalité suppose :

1. Au niveau d’un ES de mettre à jour la stratégie des méthodes d’authentification afin permettre aux utilisateurs finaux de s’inscrire et de se connecter avec des clés d’accès dans Microsoft Authenticator.

La définition de la stratégie des méthodes d’authentification conformément aux exigences de la plateforme Pro Santé Connect sont couvertes dans le Guide de configuration des stratégies d’accès conditionnel à destination des établissements de santé. Nous invitons le lectorat à s’y reporter. Cette stratégie de force d’authentification d’accès conditionnel est ensuite appliquer la connexion à l’application PSC, par exemple PSC\_BAS pour le Bac à sable.

1. Pour les PS et autres utilisateurs de l’ES ciblés :
   1. d’inscrire une clé d’accès à l’aide de Microsoft Authenticator sur leur appareil iOS ou Android - L’appareil mobile doit exécuter iOS version 17 resp. Android version 14 ou ultérieure - en se connectant directement à l’application Microsoft Authenticator ou en utilisant le site Mes informations de sécurité (<https://aka.ms/mysecurityinfo>).

Le moyen le plus simple et le plus rapide d’ajouter une clé d’accès consiste à l’ajouter directement dans l’application Microsoft Authenticator. Une seule clé d’accès pour Microsoft Entra ID peut être associée à chaque compte dans Authenticator.

* 1. De par exemple ensuite se connecter à Microsoft Entra ID sur un autre appareil avec une clé de passe dans Microsoft Authenticator sur l’appareil mobile précédent.

## Activation des clés d’accès dans Microsoft Authenticator

La stratégie Microsoft Authenticator ne donne pas la possibilité d’activer les clés d’accès dans Microsoft Authenticator. Au lieu de cela, pour activer les clés d’accès dans Microsoft Authenticator, il est nécessaire de modifier la stratégie de Méthodes d’authentification par clé de sécurité FIDO2.

Procéder comme suit :

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com> (au moins en tant qu’[Administrateur de stratégie d’authentification](https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference#authentication-policy-administrator)), 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 la méthode Clé de sécurité FIDO2.
4. Sous l’onglet Activer et cibler :
   1. Cliquer sur Activer, puis sélectionner Inclure.
   2. Laisser Tous les utilisateurs sélectionné ou cliquer sur Sélectionner des groupes, puis sur Ajouter des groupes. Seuls les groupes de sécurité sont pris en charge.
   3. Dans le panneau Ajouter des groupes, cocher les groupes spécifiques au sein de l’ES qui sont concernés par cette méthode en termes de déploiement.
   4. Cliquer sur Sélectionner.
5. Sous l’onglet Configurer,
   1. Sous Général :
      * Définir Autoriser la configuration libre-service sur Oui. Si la valeur est défini sur Non, les PS et autres utilisateurs concernés de l’ES ne peuvent pas inscrire de clés d’accès via Mes informations de sécurité (<https://aka.ms/mysecurityinfo>), même si cette option est activée par la stratégie des méthodes d’authentification.
      * Définir Appliquer l’attestation sur Non pour l’aperçu public. La prise en charge de l’attestation est prévue pour la disponibilité générale.
   2. Sous Stratégie de restriction de clé :
      * Définir Appliquer des restrictions aux clés sur Oui. Ceci s’applique uniquement si l’ES souhaite autoriser ou interdire certaines clés d’accès identifiées par leur GUID d’attestation d’authentificateur (AAGUID). Il est possible d’entrer manuellement les AAGUID de l’application Microsoft Authenticator ou restreindre spécifiquement les appareils iOS ou Android ou iOS. Sinon, les AAGUID suivants peuvent être ajouté pour activer les clés d’accès Microsoft Authenticator :
        + Authenticator pour iOS: 90a3ccdf-635c-4729-a248-9b709135078f
        + Authenticator pour Android: de1e552d-db1d-4423-a619-566b625cdc84

Cf. Microsoft Authenticator ci-dessous.

* + - Définir Restreindre les clés spécifiques sur Autoriser. Les restrictions de clé définissent la facilité d’utilisation des clés d’accès spécifiques pour l’inscription et l’authentification.

Remarque importante : Si les restrictions de clé sont modifiées et un AAGUID précédemment autorisé supprimé, les utilisateurs qui ont précédemment inscrit une méthode autorisée ne peuvent plus l’utiliser pour la connexion. Si l’ES n’applique actuellement pas de restrictions de clé et dispose déjà d’une utilisation active de la clé d’accès, les AAGUID des clés utilisées à date doivent être collectés et ajoutés à la liste d’autorisation, ainsi que les AAGUID d’Authenticator, pour activer cette capacité. Cette tâche peut être effectuée via un script PowerShell automatisé qui analyse les journaux d’activité, tels que les détails de l’inscription et les journaux de connexion.

* + - Sélectionner Microsoft Authenticator si la case à cocher s’affiche dans le centre d’administration. Ce paramètre remplit automatiquement les AAGUID de l’application Authenticator dans la liste des restrictions de clé. Dans le cas contraire, ajouter manuellement les AAGUID précédents pour iOS et/ou Android pour activer les clés d’accès Microsoft Authenticator.

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

Description générée automatiquement

1. Une fois la configuration terminée, Cliquer sur Enregistrer.

Documentation Microsoft : Comment activer les clés d’accès dans Microsoft Authenticator pour Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/how-to-enable-authenticator-passkey>.

## Inscription d’une clé d’accès dans Microsoft Authenticator

Documentation Microsoft :

* Enregistrer les clés d’accès dans Authenticator sur les appareils iOS dans MySecurityInfo : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/how-to-register-passkey-authenticator?tabs=iOS> ;
* Enregistrer les clés d’accès dans Authenticator sur les appareils Android dans MySecurityInfo : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/how-to-register-passkey-authenticator?tabs=Android>.

### Inscription d’une clé d’accès directement depuis un même appareil

Un PS ou un autre utilisateur ciblé d’un ES peut se connecter à Microsoft Authenticator pour directement créer une clé d’accès dans l’application. Il s’agit du flux recommandé et préféré pour configurer une clé d’accès dans Authenticator.

Procéder comme suit :

1. Sur l’appareil mobile, ouvrir Microsoft Authenticator.
2. Appuyer sur Ajouter un compte ou sur le bouton +.
3. Sélectionner Compte professionnel ou scolaire, puis sur Se connecter. Préciser ou sélectionner le compte à utiliser pour continuer. Une authentification multifacteur (MFA) doit alors être effectuée.
4. Sélectionner Ouvrir les paramètres (iOS) ou Paramètres (Android) pour activer Authenticator en tant que fournisseur de clé d’accès.

Sous iOS :

* 1. Ouvrir Mots de passe, puis sélectionner Options de mot de passe.
  2. Vérifier que l’option Remplissage automatique des mots de passe et des clés d’accès est activée.
  3. Dans l’option Utiliser les mots de passe et les clés d’accès à partir de, vérifier qu’Authenticator est sélectionné.

– ou –

Sous Android :

* 1. Ouvrir Mots de passe et comptes.
  2. Dans Fournisseurs supplémentaires, vérifier qu’Authenticator est sélectionné.
  3. Revenir à l’application Authenticator, puis sélectionnez Terminer.

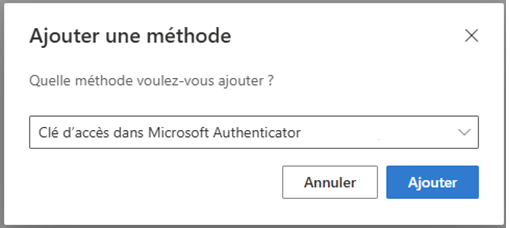
1. Authenticator configure l’authentification par clé d’accès, sans mot de passe et l’authentification MFA pour la connexion en fonction des stratégies de compte professionnel ou scolaire de l’ES.
2. Appuyer si besoin (iOS) sur Continuer pour terminer le processus d’inscription.

### Inscription d’une clé d’accès depuis Mes informations de sécurité

En guise d’alternative, il est également possible d’ajouter une clé d’accès à partir du navigateur de l’appareil mobile ou par le biais de l’inscription inter-appareils à l’aide d’un autre appareil, tel qu’un ordinateur portable.

Procéder comme suit :

1. Depuis un navigateur, aller sur Mes informations de sécurité à l’adresse <https://aka.ms/mysecurityinfo>, puis se connecter avec le compte utilisateur concerné.
2. Appuyer sur + Ajouter une méthode de connexion :
   1. Sélectionner Clé d’accès dans Microsoft Authenticator.



* 1. Cliquer sur Ajouter.

Une image contenant texte, capture d’écran, Système d’exploitation, logiciel

Description générée automatiquement

* 1. Se connecter avec l’authentification multifacteur (MFA), puis cliquer sur Suivant.

Une image contenant texte, capture d’écran, Système d’exploitation, logiciel

Description générée automatiquement

* 1. Si nécessaire, téléchargez Microsoft Authenticator, puis cliquer sur Suivant.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* 1. Sélectionner l’appareil mobile souhaité, par exemple, sur Android pour cette illustration.

Une image contenant texte, capture d’écran, Système d’exploitation, Police

Description générée automatiquement

* 1. Suivre les étapes pour activer Authenticator en tant que fournisseur de clé d’accès dans Paramètres sur l’appareil mobile (Android) :
* Sur l’appareil mobile, ouvrir Paramètres.
* Ouvrir Mots de passe et comptes.
* Sous Fournisseurs supplémentaires, activerAuthenticator.
* Revenir à [Mes informations de sécurité](https://aka.ms/mysecurityinfo), puis sélectionner Continuer.

Remarque :Les étapes d’activation d’un fournisseur de clé secrète sur Android peuvent varier selon les appareils mobiles. Rechercher les clés d’accès au niveau des paramètres de l’appareil ou demander auprès du support proposé pour l’appareil.

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

Description générée automatiquement

* 1. Vérifier que le Bluetooth est activé sur les deux appareils, puis cliquer sur Je suis prêt.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* 1. Dans la boîte de dialogue de sécurité qui s’ouvre sur votre appareil, sélectionner iPhone, iPad ou Appareil Android, puis sur Suivant.

Une image contenant texte, capture d’écran, motif, monochrome

Description générée automatiquement

Remarque :Pour accélérer la connexion, Android permet de mémoriser certains navigateurs et appareils Windows après avoir scanné le code QR WebAuthn. Dans ce cas, au lieu de scanner un code QR à chaque fois, l’appareil apparaît comme option sélectionnable et une notification est reçue sur l’appareil mobile considéré pour continuer l’authentification par clé d’accès.

* 1. L’appareil Android doit maintenant se connecter via Bluetooth à l’appareil avec lequel l’inscription a été démarrée. Ouvrir l’application système Appareil photo sur L’appareil mobile, ou appuyez sur Ajouter un compte professionnel ou scolairepuis Scanner le code QR pour utiliser l’appareil photo dans Authenticator.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Remarque :Bluetooth et une connexion Internet sont requis pour cette étape et les deux doivent être activés sur votre appareil mobile et distant.

* + - L’appareil ouvre une fenêtre de sécurité. La clé d’accès doit être enregistrée dans Authenticator en suivant les invites sur l’appareil.
    - Une fois la clé d’accès créée sur l’appareil, une redirection s’effectue vers [Mes informations de sécurité](https://aka.ms/mysecurityinfo).
    - Attribuer à la clé d’accès un nom facile à mémoriser, puis sélectionnez Terminer.
  1. Continuer sur l’appareil mobile en suivant les instructions affichées.

Remarque: Les instructions affichées peuvent varier selon le navigateur et l’appareil. Si l’appareil sur lequel a été démarré le processus d’inscription prend en charge les clés d’accès, vous êtes invité à enregistrer la clé d’accès sur cet appareil.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* 1. Cliquer sur OK.

Une image contenant texte, Police, ligne, logiciel

Description générée automatiquement

* 1. Renommer la clé d’accès et cliquer sur Suivant.

A ce stade, une clé d’accès est enregistrée dans Microsoft Authenticator sur l’appareil Android. Celle-ci peut être utilisée par un PS ou un autre utilisateur pour se connecter depuis un autre appareil.

## Connexion avec une clé d’accès dans Microsoft Authenticator

Procéder comme suit :

1. Sur l’autre appareil, accéder à la ressource à laquelle vous essayez d’accéder, par exemple, l’application PSC dans le bac à sable à l’adresse <https://wallet.bas.psc.esante.gouv.fr/login-page>, puis cliquer sur le bouton Pro Santé Connect.

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

Description générée automatiquement

1. Sélectionner Délégation, puis Entra ID et cliquer sur Se connecter via un fournisseur d’identité.
2. Au lieu d’entrer un nom d’utilisateur pour se connecter, cliquer sur Options de connexion pour se connecter plus facilement sans avoir à entrer un nom d’utilisateur. Sélectionner Visage, empreinte digitale, code PIN ou clé de sécurité.

Remarque : si vous avez utilisé pour la dernière fois une clé secrète pour vous authentifier la dernière fois, vous êtes automatiquement invité à vous authentifier avec une clé secrète.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

1. Pour démarrer l’authentification, suivre les étapes décrites dans l’invite de système d’exploitation ou de navigateur. Sur Windows 11 23H2 ou version ultérieure, sélectionner Appareil iPhone, iPad ou Android. Un code QR doit apparaître à l’écran.

Une image contenant texte, capture d’écran, motif, monochrome

Description générée automatiquement

1. Sur l’appareil mobile, ouvrir l’application de caméra système et scanner le code QR. Il est également possible d’utiliser la caméra dans Microsoft Authenticator. Accéder à la mosaïque du compte de clé d’accès, puis appuyer dessus. Sous Détails de clé d'accès, un bouton s’affiche dans le coin inférieur droit pour lire le code QR.

Remarque: Pour accélérer la connexion, Android permet de mémoriser certains navigateurs et appareils Windows après avoir scanné le code QR WebAuthn. Dans ce cas, au lieu d’avoir à lire un code QR à chaque fois, l’appareil apparaît comme une option sélectionnable et une notification est alors reçu sur l’appareil mobile pour continuer l’authentification par clé d’accès.

1. Pour sélectionner la clé secrète, suivre les étapes de la boîte de dialogue du système d’exploitation Android. Vérifier qu'il s'agit bien de la bonne personne en scannant le visage, l’empreinte digitale ou en saisissant le code PIN de l’appareil ou le geste de déverrouillage.

A ce stade, le PS ou l’utilisateur considéré est maintenant connecté à Microsoft Entra ID sur l’autre appareil.

Ceci conclut le présent guide.