18 - Guide d'authentification des utilisateurs

Introduction

En fonction du risque identifié (connexion depuis le réseau Renault ou depuis internet ou du niveau de confidentialité de l'application), le processus d'authentification pourra comporter une ou deux étapes :

- **Une étape**
  - Dans ce cas, l'utilisateur peut utiliser les mécanismes d'authentification suivants :
    - Mot de passe (géré dans l'annuaire Arca ou Renault Net),
    - certificat (Intune / ACE2 / USB token)
    - Authentification transparente basée sur la session Windows (Kerberos),

- **Deux étapes (Multi factor authentication i.e MFA)**
  - Si le risque est considéré comme important, cette seconde étape est nécessaire.
  - L'utilisateur devra utiliser l'un de ces mécanismes :
    - Validation Push Mobile au travers de l'application Okta Verify (MFA)
    - Mécanisme Windows Hello disponible sur PC Windows (code PIN ou empreinte digitale)
  - Cette seconde étape permet d'associer un appareil à l'identité de l'utilisateur (sorte d'enrôlement)

Table of contents

01 - Enrôlement d'un appareil

Pourquoi ?

La seconde étape d'authentification consiste à vérifier que l'utilisateur est bien en possession d'un appareil précédemment enrôlé. Pour cela, l'appareil doit être associé à l'identité de l'utilisateur au travers du processus d'enrôlement de l'appareil en question.

Quand ?

Dès que possible afin d'être prêt dès qu'une authentification renforcée (deux étapes) est nécessaire.

Quel type d'appareil ?

L'utilisateur peut enrôler les appareils suivants :

- Un PC Renault ACE2
- Un PC disposant d'un système d'exploitation Windows 10+ ou un Mac disposant de MacOS 11+
- Un téléphone (ou une tablette) équipé d'Android 8+ ou d'iOS 14+

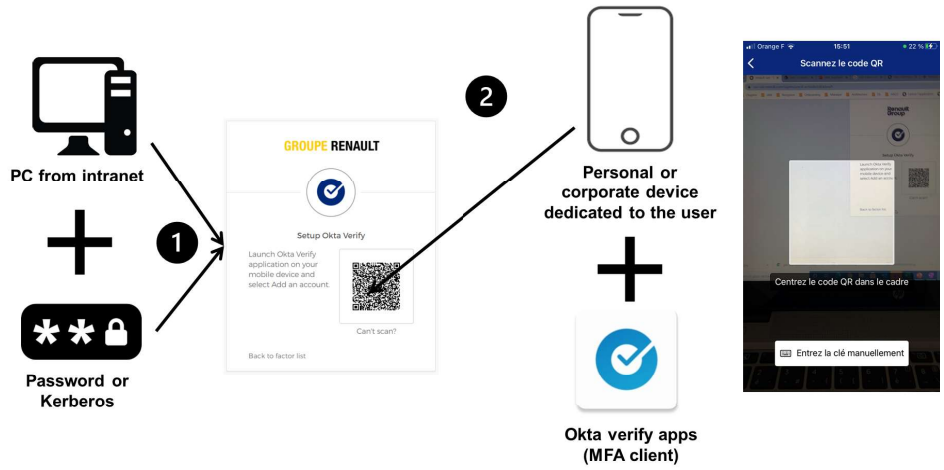
Voici la procédure détaillée à suivre pour enrôler chaque type d'appareil :

- Processus d'enrôlement d'un appareil mobile
- Processus d'enrôlement pour un PC
- Processus de réinitialisation de l'enrôlement

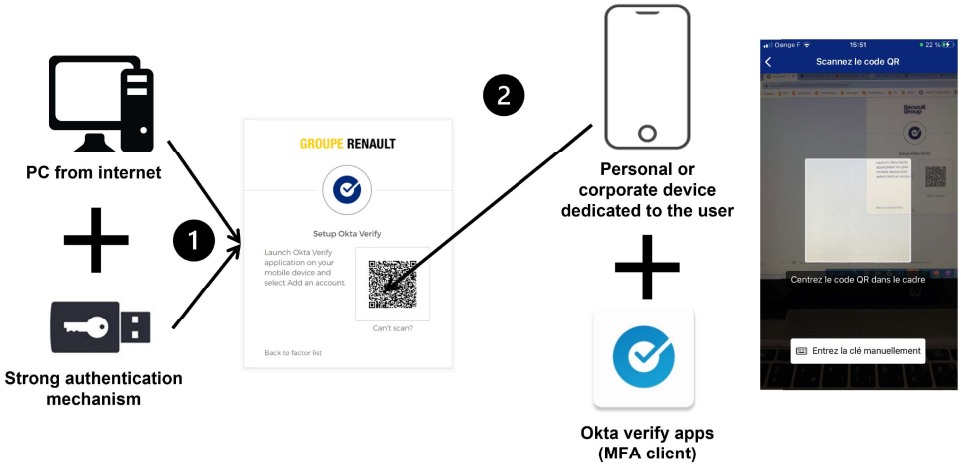
Processus d'enrôlement d'un appareil mobile

Il y a deux cas :

1. L'utilisateur initie l'enrôlement du terminal mobile depuis son PC connecté au réseau Renault (sur un site Renault ou à domicile au travers de l'accès VPN) :



2. L'utilisateur initie l'enrôlement du terminal mobile depuis son PC connecté à internet (hors site Renault office et sans accès VPN)



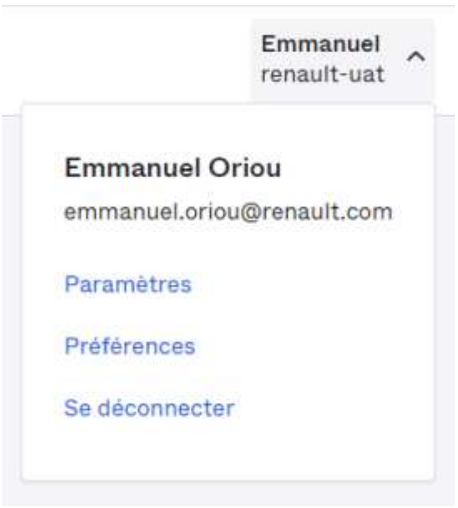
Dans ces deux cas, il y a deux étapes à suivre :

1. L'utilisateur se connecte au site Okta en utilisant le moyen d'authentification à l'un des deux cas décrits ci-dessus,
2. L'utilisateur accède aux paramètres Okta afin d'initier l'enrôlement de son appareil mobile,
3. L'utilisateur installe l'application Okta Verify (disponible dans le magasin d'application Apple App Store ou Google Play Store), puis lance l'application et scanne le QR code qui s'affiche en parallèle sur son PC.

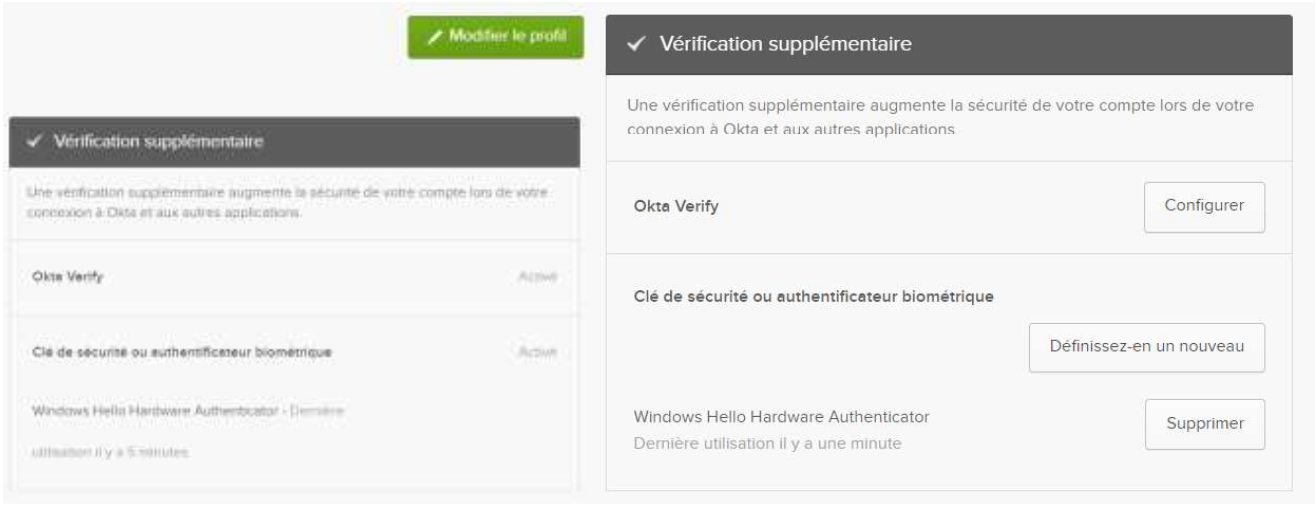
Voici la procédure détaillée :

La première partie du processus est initié depuis le PC :

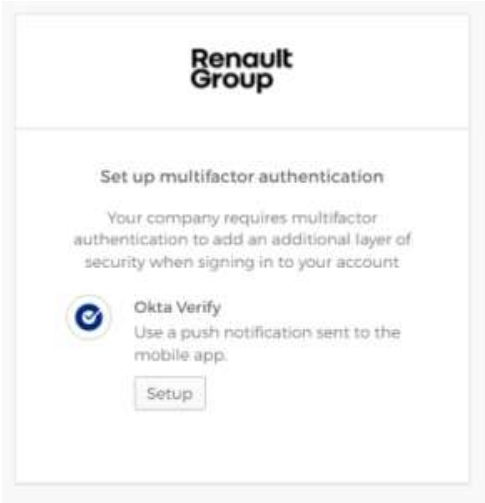
1. Accéder au site Okta dédié à Renault,
2. Cliquer sur son prénom en haut à droite de votre navigateur,
3. Cliquer sur le menu "Paramètres“



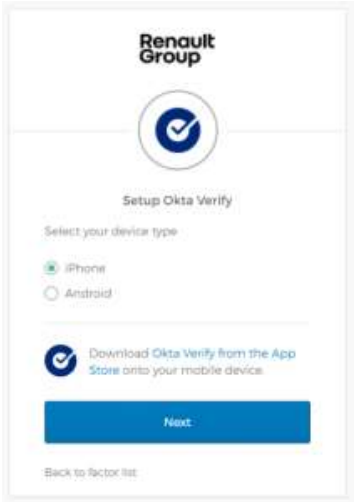
4. Cliquer sur le bouton "Modifier le profil" et ensuite sur le bouton "Configurer" situé à droite du texte "Okta verify" :



5. Cliquer sur le bouton “Setup” :



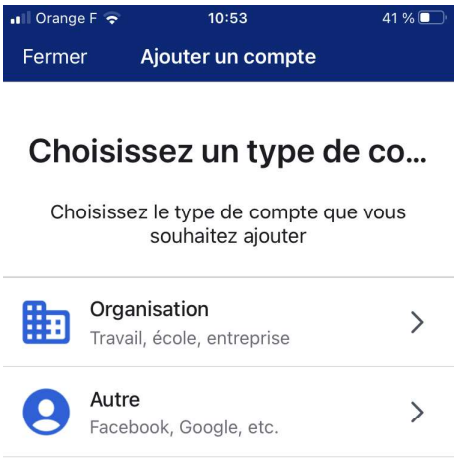
6. Sélectionner le type de votre appareil mobile et cliquer sur “Next”



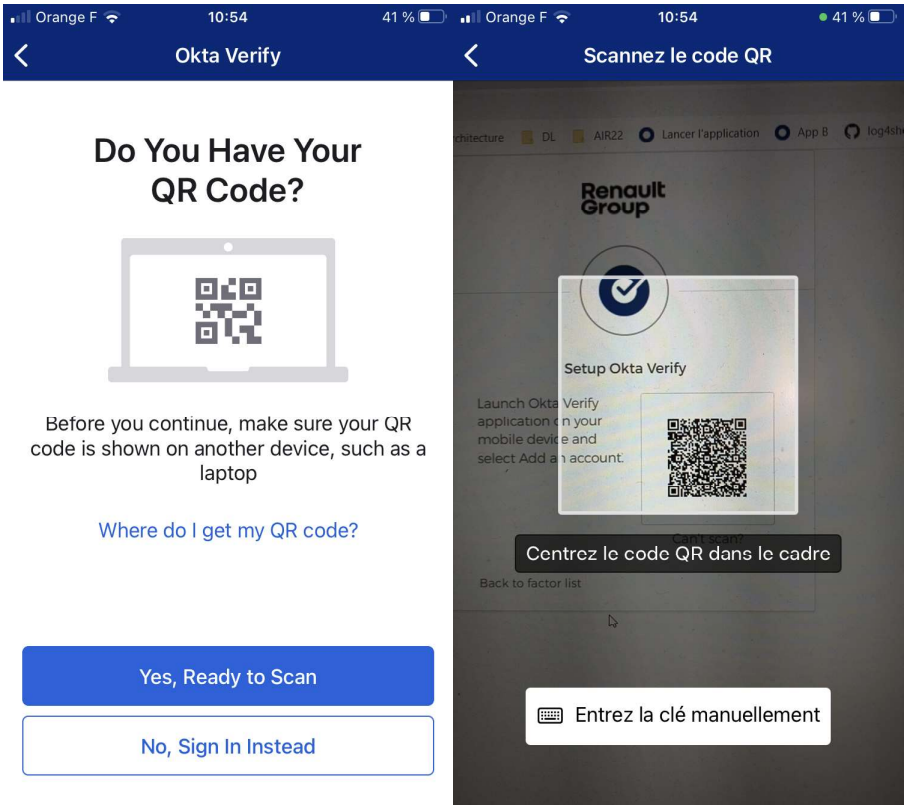
7. Enfin, scanner le QR code avec l'application Okta verify installée préalablement sur votre appareil mobile.

La seconde partie est à réaliser sur votre appareil mobile à enrôler :

1. Installer l'application Okta verify sur l'appareil,
2. Lancer l'application
3. Cliquer sur l'icone "+" située en haut à droit de l'écran,
4. Cliquer sur l'élément "Organisation"



5. Cliquer sur le bouton "Yes, Ready to Scan" et cibler le QR code qui est affiché dans le navigateur du PC :



6. L'enrôlement du terminal est terminé.


Orange F
10:55
40 %
Okta Verify
Compte ajouté
a184708
La connexion sécurisée aux applications de votre organisation est maintenant activée.
Pour poursuivre, retournez aux instructions de votre organisation.
Important: Gardez cette application installée sur votre appareil. Vous en aurez besoin pour vous connecter.
Terminé

Processus d'enrôlement pour un PC

Pour enrôler votre PC vis à vis de la solution Okta, il est nécessaire de configurer un facteur biométrique qui vous identifie et ensuite de l'associer à votre identité dans Okta.

Définition du facteur biométrique au niveau du système d'exploitation du PC

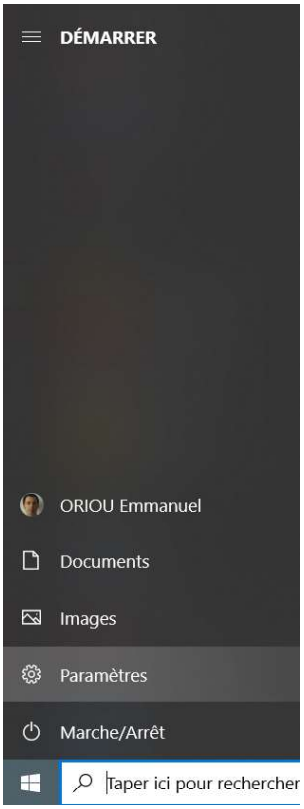
Vous avez deux options disponibles :

1. code PIN ,
2. Reconnaissance de l'empreinte digitale.

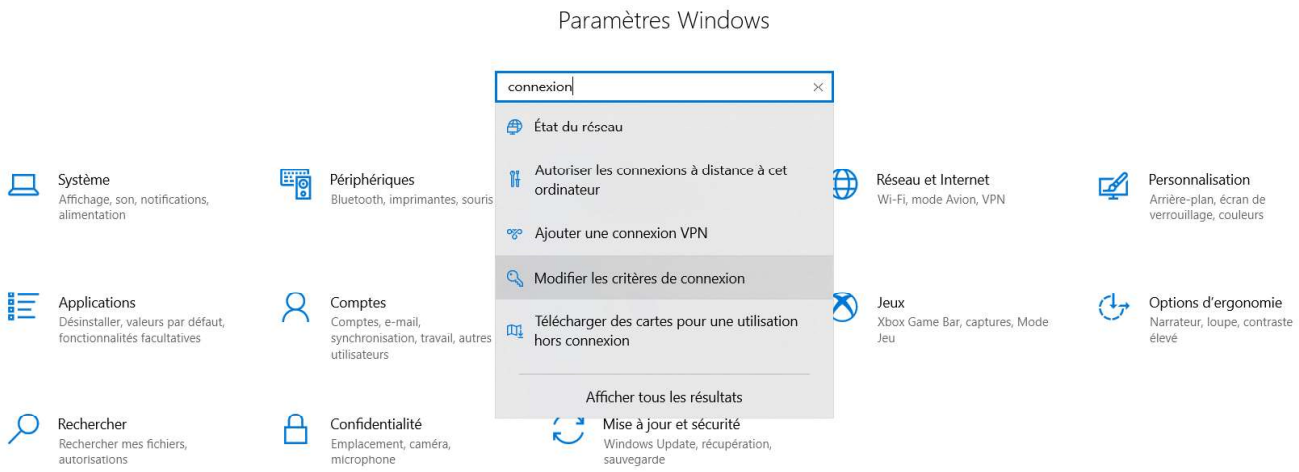
Attention, le code PIN est prérequis pour configurer le mécanisme de reconnaissance de reconnaissance de l'empreinte digitale.

La première partie de la procédure est commune aux deux options :

1. Cliquer sur le bouton "Windows" puis "Paramètres"



2. Puis chercher le bon menu en tapant le mot clé "connexion" et en sélectionnant le menu "Modifier les critères de connexion" :



Si vous pouvez également :

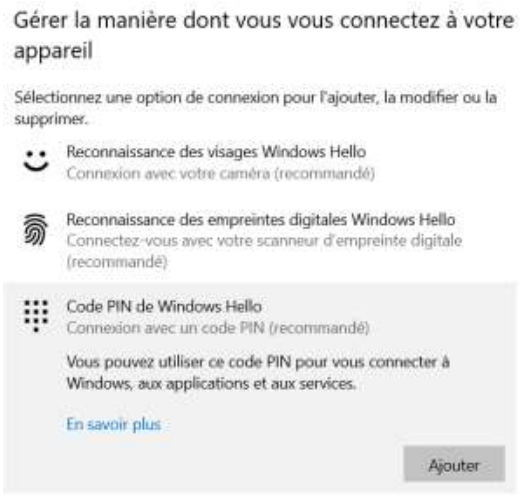
1. Taper la combinaison de touches Windows + R,
2. Copier et coller la commande "ms-settings:signinoptions" la popup qui apparaît et cliquer sur le bouton "Ok"

3. Sélectionner le facteur biométrique que vous voulez utiliser :

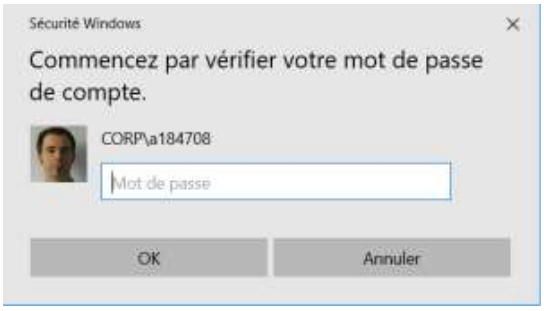
La seconde partie de la procédure dépend de quel facteur biométrique vous avez choisi :

Code PIN

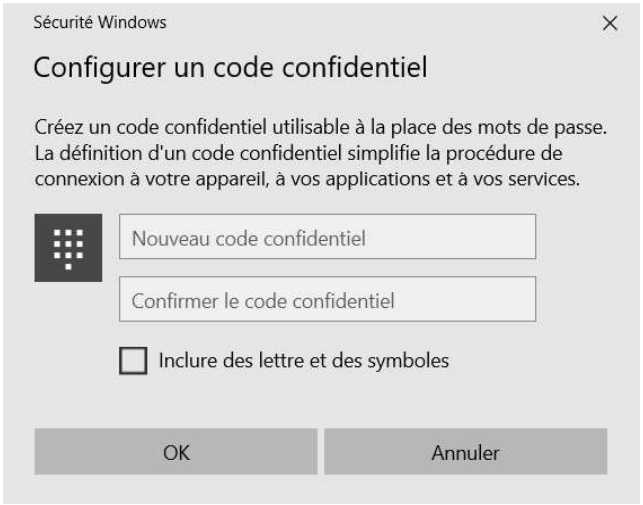
4. Dans ce cas, cliquer sur le menu "In this case, click on "Windows Hello PIN" menu item and then click on "Add" :



5. Entrer votre mot de passe ARCA :



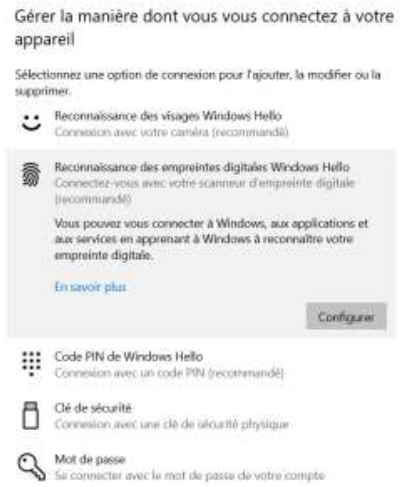
6. Choose your PIN code :



7. Vous devez obtenir cet écran

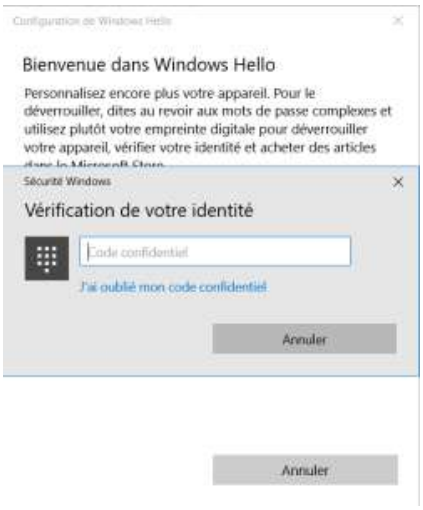
Empreinte digital

8. Dans ce cas, cliquer sur le menu "Reconnaissance des empreintes digitales Windows Hello " et cliquer ensuite sur le bouton "Configurer" :



9. Cliquer sur le boutton "Démarrer"

10. Saisir votre code PIN code que vous avez préalablement défini :



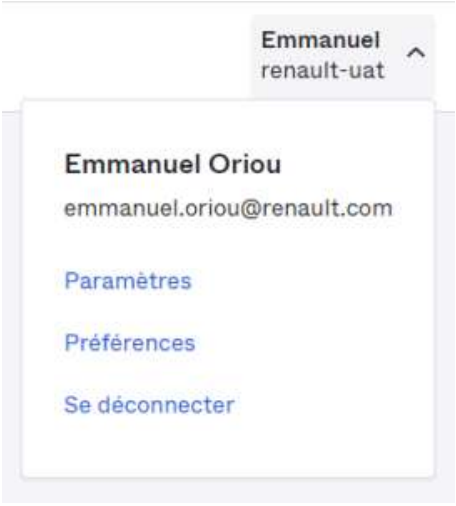
11. Toucher le lecteur d'empreintes digitales avec le doigt que vous voulez utiliser :

12. Continuez de toucher le lecteur avec votre doigt jusqu'à ce que vous obteniez cet écran :

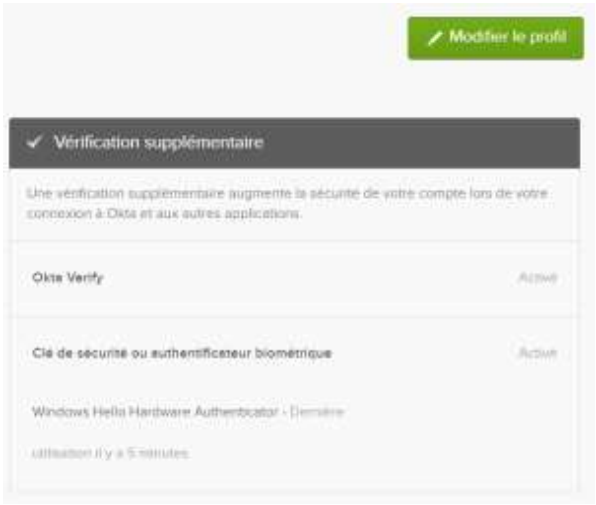
Association du facteur biométrique à votre identité dans Okta

Voici la procédure à suivre :

1. Accéder au site Okta dédié à Renault,
2. Cliquer sur son prénom en haut à droite de votre navigateur,
3. Cliquer sur le menu "Paramètres“

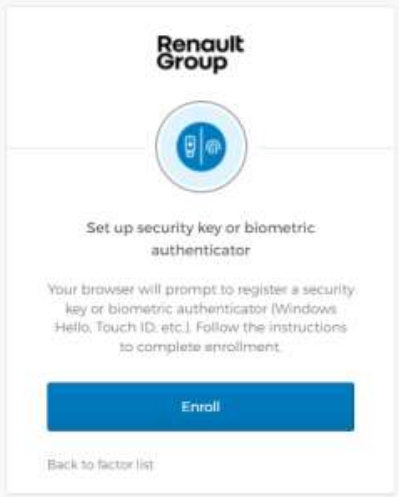


4. Cliquer sur le bouton "Modifier le profil" et ensuite sur le bouton "Configurer" situé à droite du texte "Clé de sécurité ou authentificateur biométrique" :



5. Cliquer sur le bouton "Setup" :

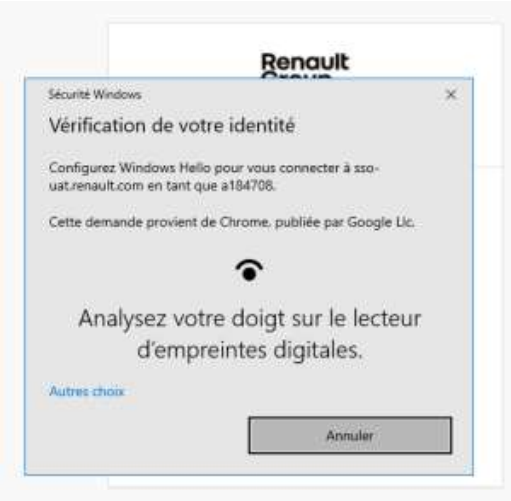
6. Puis cliquer sur le bouton "Enroll"



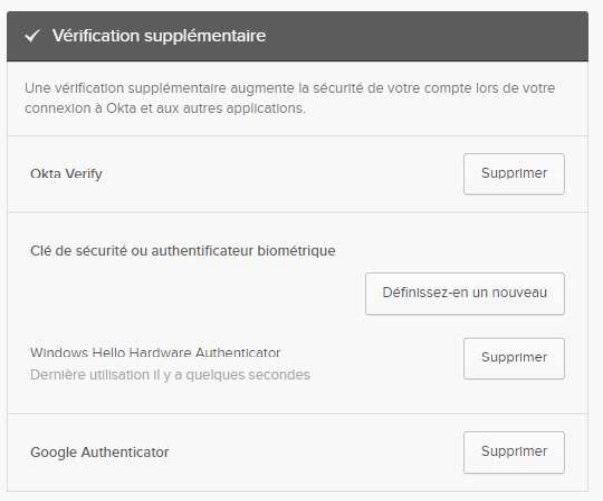
7. En fonction du type de facteur biométrique :

a. Saisir le code PIN

b. Toucher le lecteur d'empreinte digitale



8. Vous devez obtenir l'écran suivant :



Processus de réinitialisation de l'enrôlement

Vous devrez réinitialiser l'enrôlement de votre terminal (mobile or PC) dans les cas suivants :

1. Vous venez de changer de terminal,
2. Votre terminal est perdu ou volé.

Dans le premier cas, si vous disposez toujours de l'ancien terminal, c'est le cas le plus favorable car vous pouvez l'utiliser pour vous authentifiez au site Okta puis supprimer l'enrôlement existant et enfin initier l'enrôlement du nouveau terminal (Processus d'enrôlement d'un appareil mobile or Processus d'enrôlement pour un PC).

En particulier pour le second cas, il est fortement recommandé d'enrôler plusieurs terminaux pour garantir que vous disposez toujours d'au moins d'un terminal valide enrôlé et ainsi être en capacité de se connecter au site Okta pour supprimer le terminal volé / perdu et enfin initialiser l'enrôlement du nouveau terminal (Processus d'enrôlement d'un appareil mobile or Processus d'enrôlement pour un PC).

Si vous ne disposez plus d'aucun terminal valide enrôlé, vous devez contacter le support Helpdesk (+331768 11000) pour demander la réinitialisation de l'enrôlement du terminal précédent. Ensuite vous pouvez suivre de nouveau la procédure (Processus d'enrôlement d'un appareil mobile or Processus d'enrôlement pour un PC) pour enrôler un nouveau terminal.

02 - Employés & prestataires sur site

Il y a plusieurs cas fonction du type d'accès réseau utilisé et du type du niveau de confidentialité des données de l'application concernée.

Accès à une application très sensible (quelque soit l'accès réseau utilisé)

L'application nécéssite un moyen d'authentification fort car elle gère des données très confidentielles.

Voici une descriptions des différentes étapes de l'authentification de l'utilisateur à l'application :

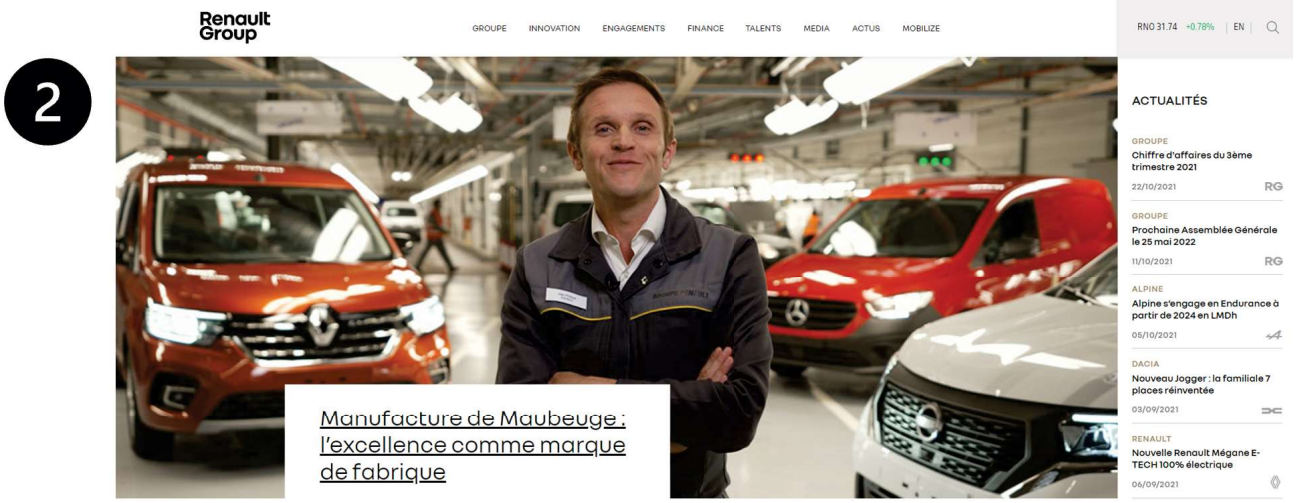
1. Connecter votre token USB à votre PC,

2. Vous êtes directement redirigé vers cet écran,

3. Choisir le bon certificat en sélectionnant le certificat de classe 2 (Emetteur Class 2 Authentication CA) stocké sur le token USB,

4. Entrer le code PIN du token USB,

5. Votre navigateur vous redirige automatiquement vers la page d'accueil de l'application une fois l'authentification validée



Vous pouvez également regarder la courte vidéo qui montre la séquence d'authentification :

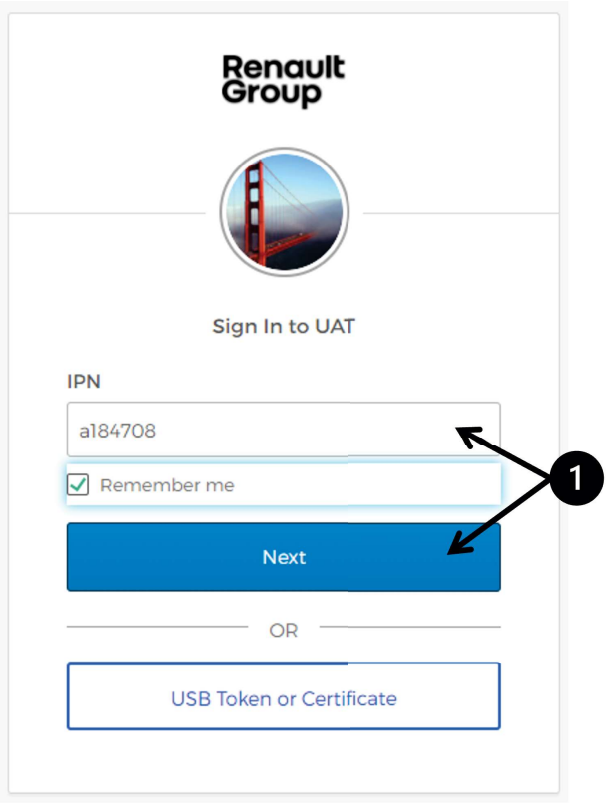
Accès depuis le réseau Renault (sur un site Renault ou à domicile au travers de l'accès VPN)

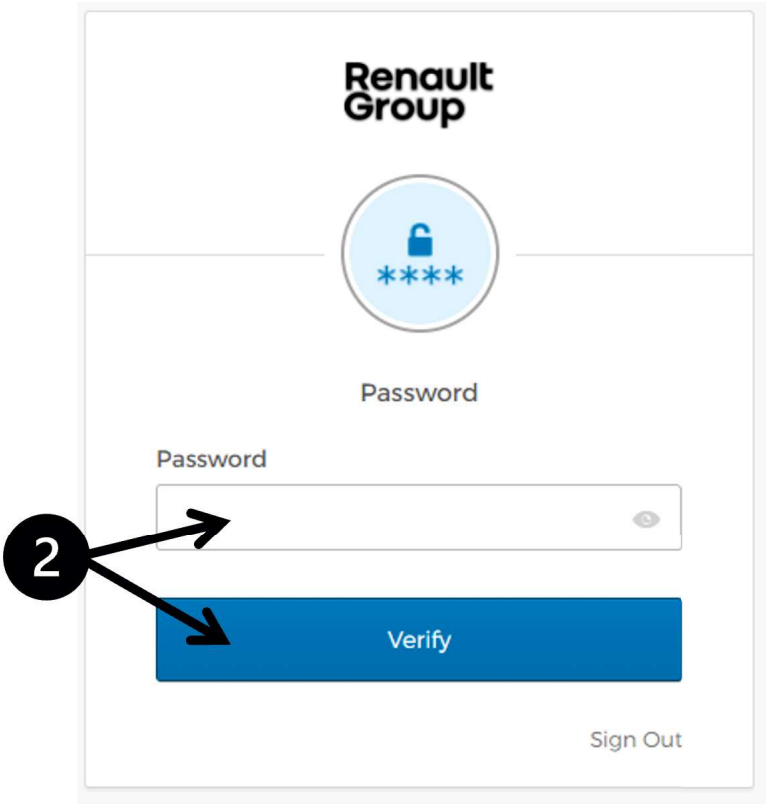
La plupart du temps, vous devriez être authentifié de manière transparente aux applications depuis cet accès réseau. Vous pouvez le visualiser au travers de cette vidéo :

Si vous n'utilisez pas un terminal fourni par l'entreprise (PC ACE2),

1.Saisir votre IPN et cliquer sur le bouton “Next”

2.Saisir votre mot de passe ARCA et cliquer sur le bouton "Verify"





Accès depuis l'extérieur au réseau Renault (Internet)

Habituellement, l'utilisateur est authentifié en suivant les deux étapes suivantes :

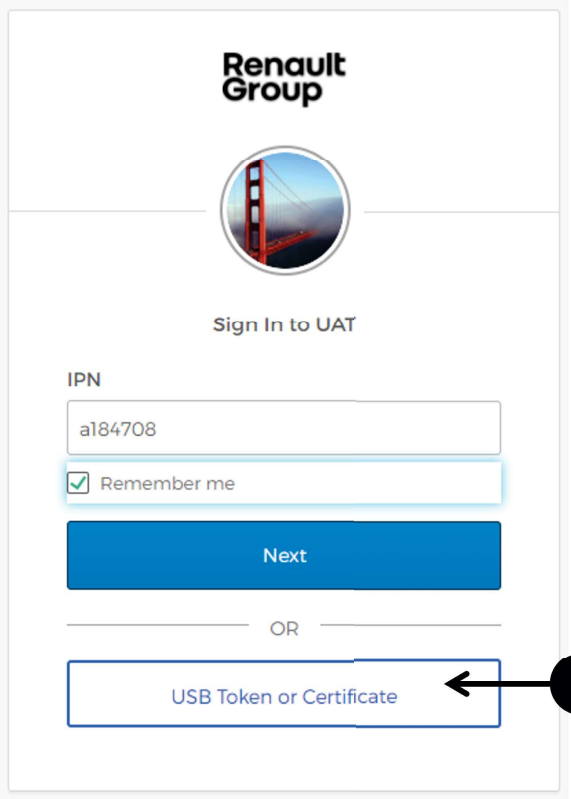
1. Authentification au travers d'un certificat installé sur le terminal,

2. Validation de l'identité au travers de l'application Okta verify installée sur votre terminal mobile ou au travers de votre PC en vous signant à l'aide du code PIN ou de la reconnaissance de votre empreinte digitale,

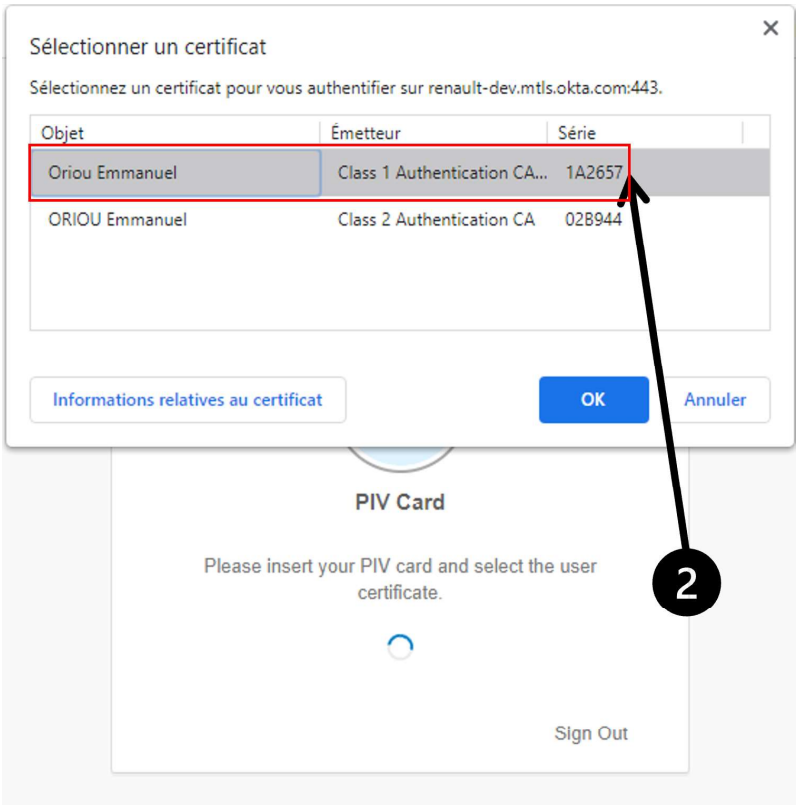
Dans les deux cas, ce processus nécéssite d'enrôler un terminal mobile ou un PC au préalable. Consulter cette section 01 - Enrôlement d'un appareil si vous ne l'avez pas déjà fait.

Pour la première étape, suivre la procédure :

1. Cliquer sur le boutton “USB Token or Certificate”

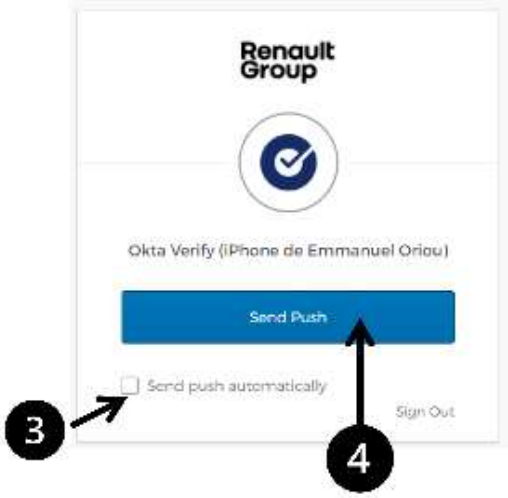


2. Puis choisir le bon certificat en sélectionnant le certificat de classe 1 (Emetteur : Class 1 Authentication CA) disponible sur votre terminal géré par l'entreprise (PC ou téléphone géré par Intune) :



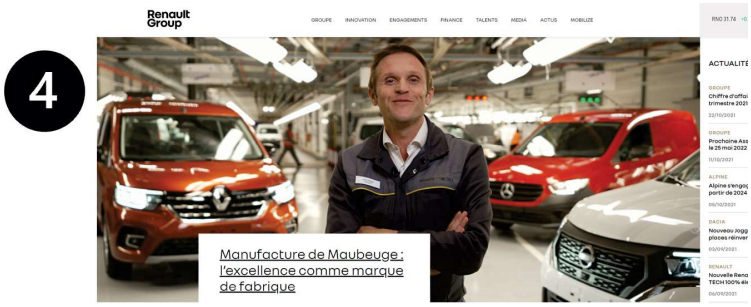
La seconde étape dépend de la façon de valider votre identité que vous avez choisi durant l'étape 01 - Enrôlement d'un appareil .

Validation de l'identité sur terminal mobile

Terminal accédant à l'application	Ce processus nécessite d'enrôler un terminal au préalable. Consulter la section 01 - Enrôlement d'un appareil si vous ne l'avez pas fait initialement. Dans cette partie, vous devez disposer du terminal enrôlé en plus du terminal que vous utilisez pour accéder à l'application. **Sur le terminal accédant à l'application** 3. Cliquer sur la case à cocher “Send push automatically” (si ce n'est pas déjà fait) 4. Cliquer sur “Send Push” afin de recevoir votre notification sur votre terminal enrôlé **Sur le terminal enrôlé (personel) utilisé pour valider votre identité** 5. Cliquer sur “Oui, c'est bien moi” **Sur le terminal accédant à l'application** 6. Votre navigateur va vous rediriger automatiquement vers la page d'accueil de l'application
	

Validation de l'identité sur PC

Code PIN défini sur PC	Dans cette section, vous avez besoin du PC enrôlé qui est aussi le terminal utilisé pou accéder à l'application. 3. Entrer votre code PIN code défini sur le PC ou placer votre doigt sur lecteur d'empr digitale 4. Votre navigateur va vous rediriger automatiquement vers la page d'accueil de l'application



03 - Fournisseurs

Il y a plusieurs cas fonction du type d'accès réseau utilisé et du type du niveau de confidentialité des données de l'application concernée.

Accès à une application très sensible (quelque soit l'accès réseau utilisé)

L'application nécéssite un moyen d'authentification fort car elle gère des données très confidentielles.

Voici une descriptions des différentes étapes de l'authentification de l'utilisateur à l'application :

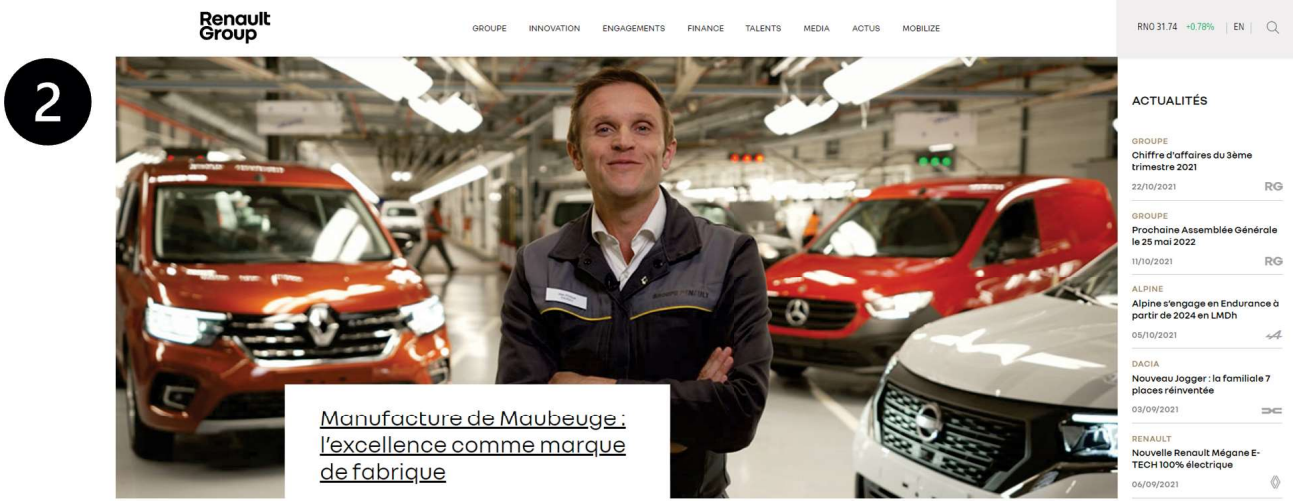
1. Connecter votre token USB à votre PC,

2. Vous êtes directement redirigé vers cet écran,

3. Choisir le bon certificat en sélectionnant le certificat de classe 2 (Emetteur Class 2 Authentication CA) stocké sur le token USB,

4. Entrer le code PIN du token USB,

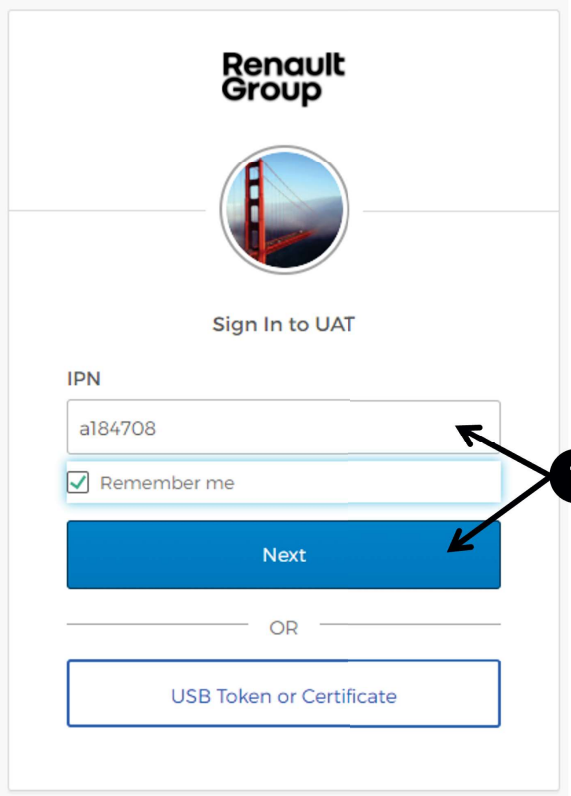
5. Votre navigateur vous redirige automatiquement vers la page d'accueil de l'application une fois l'authentification validée

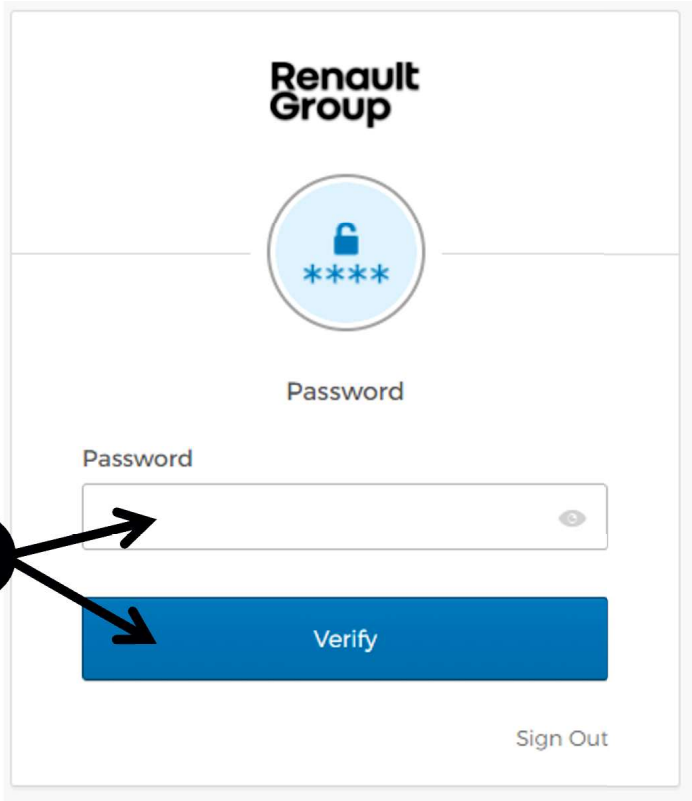


Accès aux applications standards

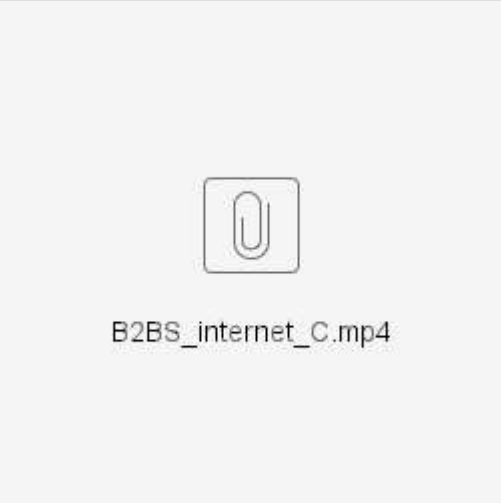
L'utilisateur est habituellement authentifié au travers de son mot de passe :

1. Entrer votre IPN et cliquer sur le bouton "Next",
2. Entrer votre mot de passe et cliquer sur le bouton "Verify"





Vous pouvez également regarder la courte vidéo qui montre la séquence d'authentification :



Accès à une application sensible

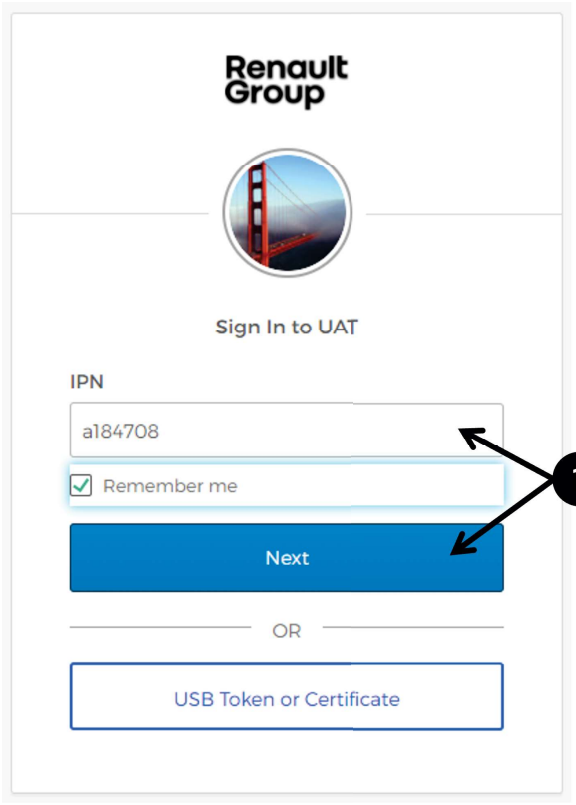
Habituellement, l'utilisateur est authentifié en suivant les deux étapes suivantes :

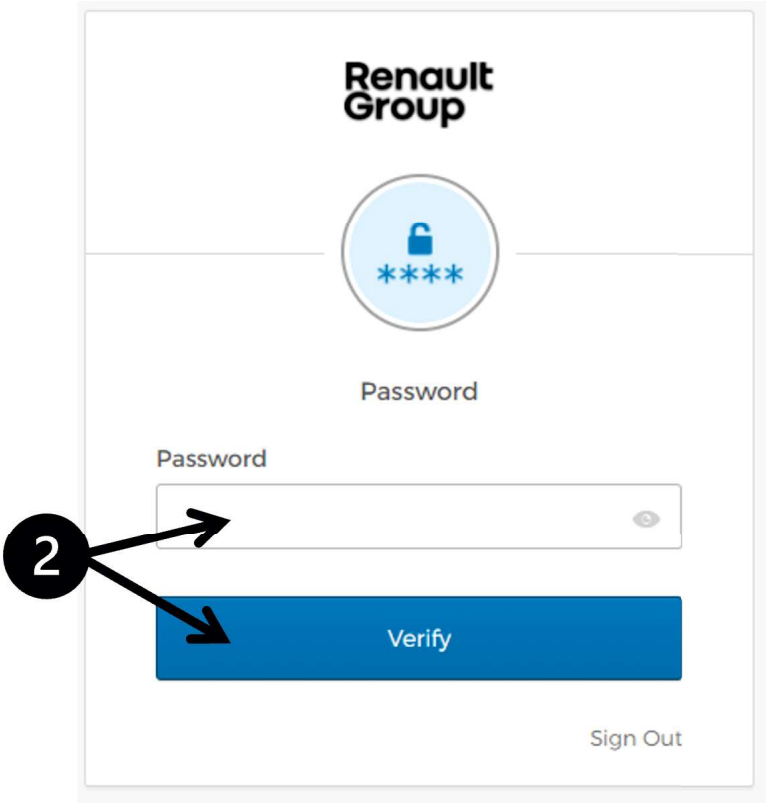
1. Authentification au travers du mot de passe de l'utilisateur,
2. Validation de l'identité au travers de l'application Okta verify installée sur votre terminal mobile ou au travers de votre PC en vous signant à l'aide du code PIN ou de la reconnaissance de votre empreinte digitale,

Dans les deux cas, ce processus nécéssite d'enrôler un terminal mobile ou un PC au préalable. Consulter cette section 01 - Enrôlement d'un appareil si vous ne l'avez pas déjà fait.

Suivre la procédure suivante pour la première étape :

1. Entrer votre IPN et cliquer sur le bouton “Next”
2. Entrer votre mot de passe et cliquer sur le bouton "Verify"

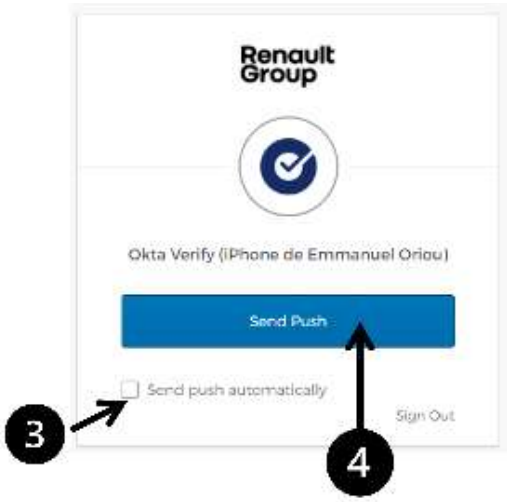




La seconde étape dépend de la façon de valider votre identité que vous avez choisi durant l'étape 01 - Enrôlement d'un appareil .

Validation de l'identité sur terminal mobile

Terminal accédant à l'application	Ce processus nécessite d'enrôler un terminal au préalable. Consulter la section 01 - Enrôlement d'un appareil si vous ne l'avez pas fait initialement.



Dans cette partie, vous devez disposer du terminal enrôlé en plus du terminal que vous utilisez pour accéder à l'application.

Sur le terminal accédant à l'application

3. Cliquer sur la case à cocher “Send push automatically” (si ce n'est pas déjà fait)

4. Cliquer sur “Send Push” afin de recevoir votre notification sur votre terminal enrôlé

Sur le terminal enrôlé (personel) utilisé pour valider votre identité

5. Cliquer sur “Oui, c'est bien moi”

Sur le terminal accédant à l'application

6. Votre navigateur va vous rediriger automatiquement vers la page d'accueil de l'application

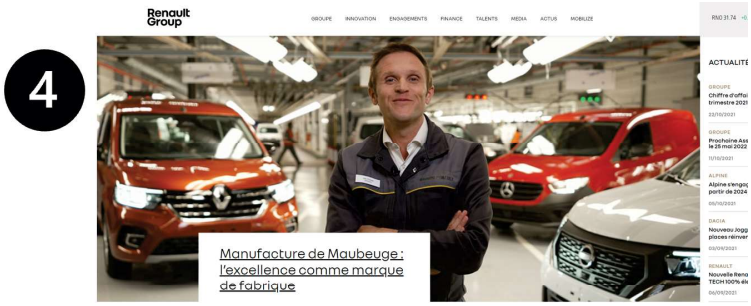
Validation de l'identité sur PC

Code PIN défini sur PC

Dans cette section, vous avez besoin du PC enrôlé qui est aussi le terminal utilisé pou accéder à l'application.

3. Entrer votre code PIN code défini sur le PC ou placer votre doigt sur lecteur d'empr digitale

4. Votre navigateur va vous rediriger automatiquement vers la page d'accueil de l'application



04 - Utilisateur du réseau commercial

There are multiples cases depending on which kind of application (web application or mobile native application).

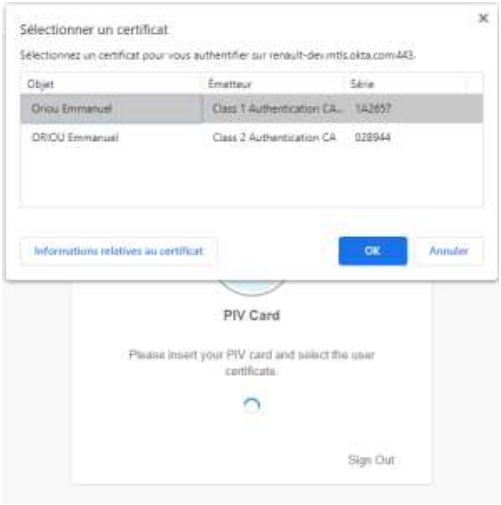
- Access to all applications (except application on mobile)
- Access to mobile applications
- Access specific to users from MRA

Access to all applications (except application on mobile)

The application requires a strong authentication mechanism as it manages very sensitive data.

Here is the steps of authentication,

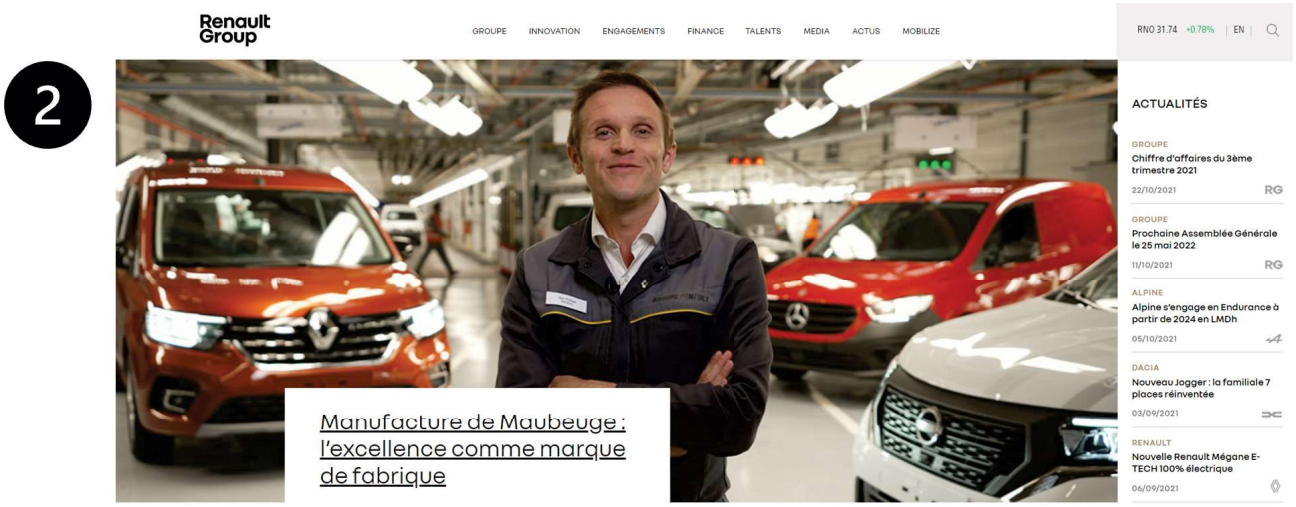
1. You are directly redirected to this screen,



2. Choose the right certificate by selecting Class 2 type to use certificate provided by USB token,

3. Enter PIN code of USB token

4. Your browser is automatically redirected to the application landing page



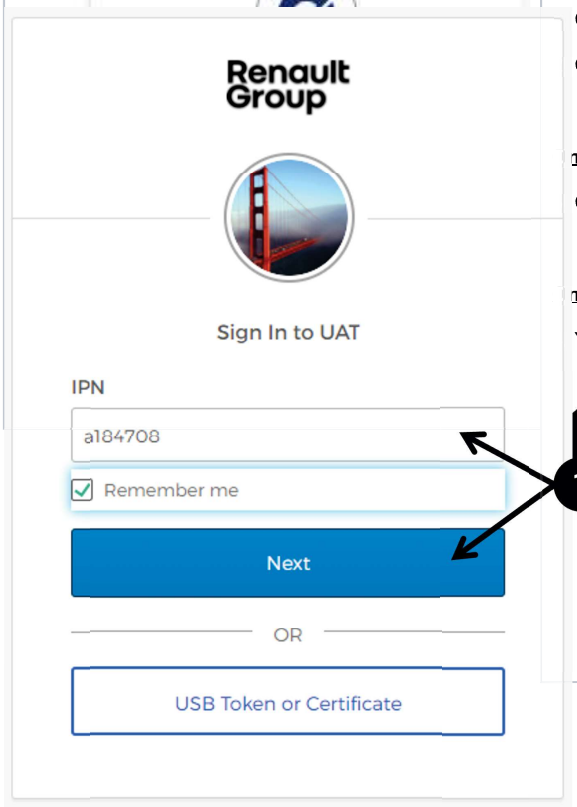
Access to mobile applications

Device accessing the application	This process requires to enroll the device first. Have a look to this section 01 - Device enrollment if you didn't do it initially.

Access specific to users from MRA

User uses to be authenticated throughhis password :

1. Fill in your IPN and click on "next" button
2. Fill in your password and click on Verify



In this section you need your enrolled device in addition to the device for accessing the application.

<u>On the device accessing the application</u>

Click on "Send push automatically" checkbox (if not already checked)

Click on "Send Push" to validate your identity

<u>n the enrolled device (personal) used to validate your identity</u>

Click on "Yes, it's me"

<u>n the device accessing the application</u>

Your browser is automatically redirected to the application landing page