Nicolas BOUGET
✉ nicolas.bouget@esial.net
3A TRS1

Marc PINHÈDE
✉ marc.pinhede@esial.net
3A LE

Julien GUÉPIN
✉ julien.guepin@esial.net
3A IL

Julien VAUBOURG
✉ julien@vaubourg.com
3A TRS2

SNACK

Documentation utilisateur

Société : B.H. Consulting
Intervenant industriel : Guillaume ROCHE
Intervenant universitaire : Jean-François SCHEID

Le 29 août 2013

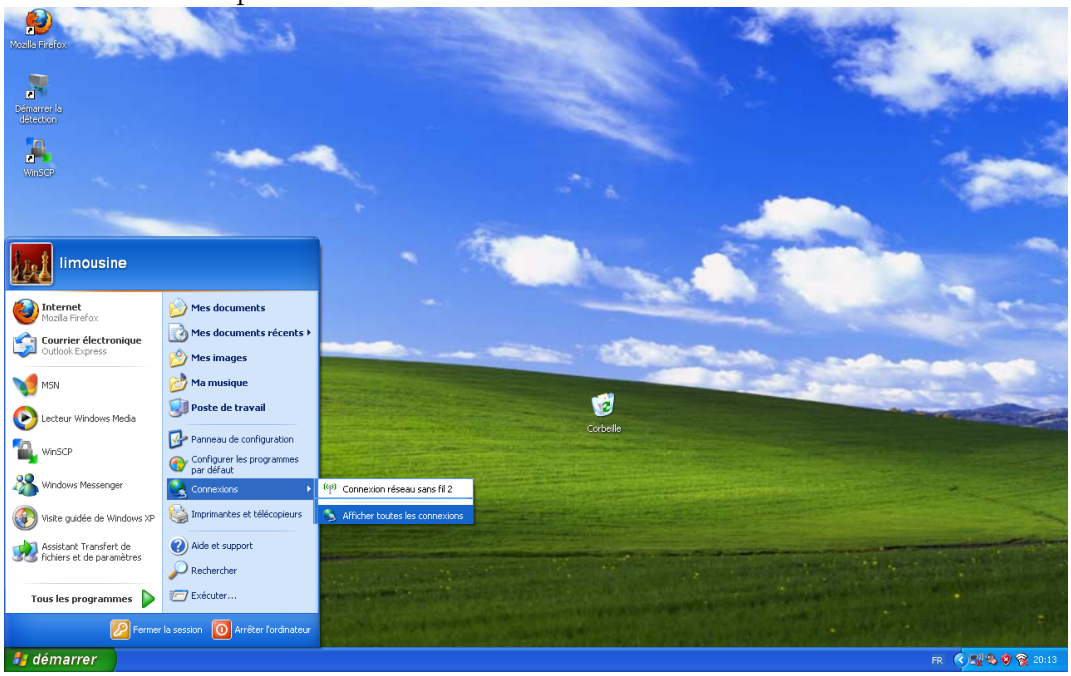
b. h. consulting

Table des matières

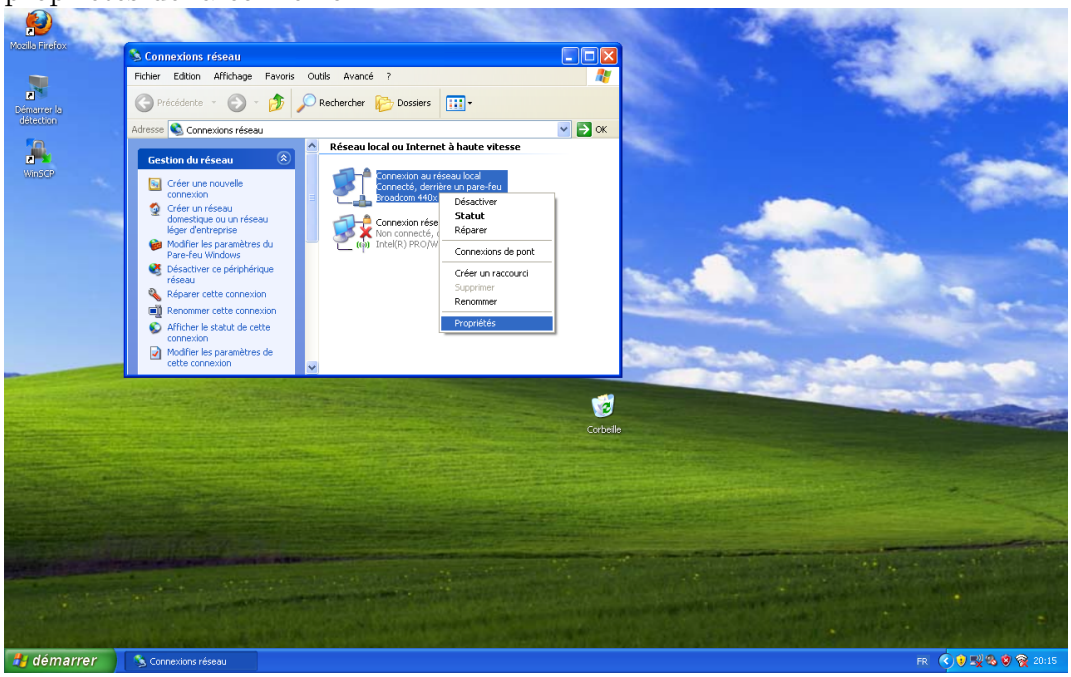
1 Windows

1.1 Connection en challenge-MD5

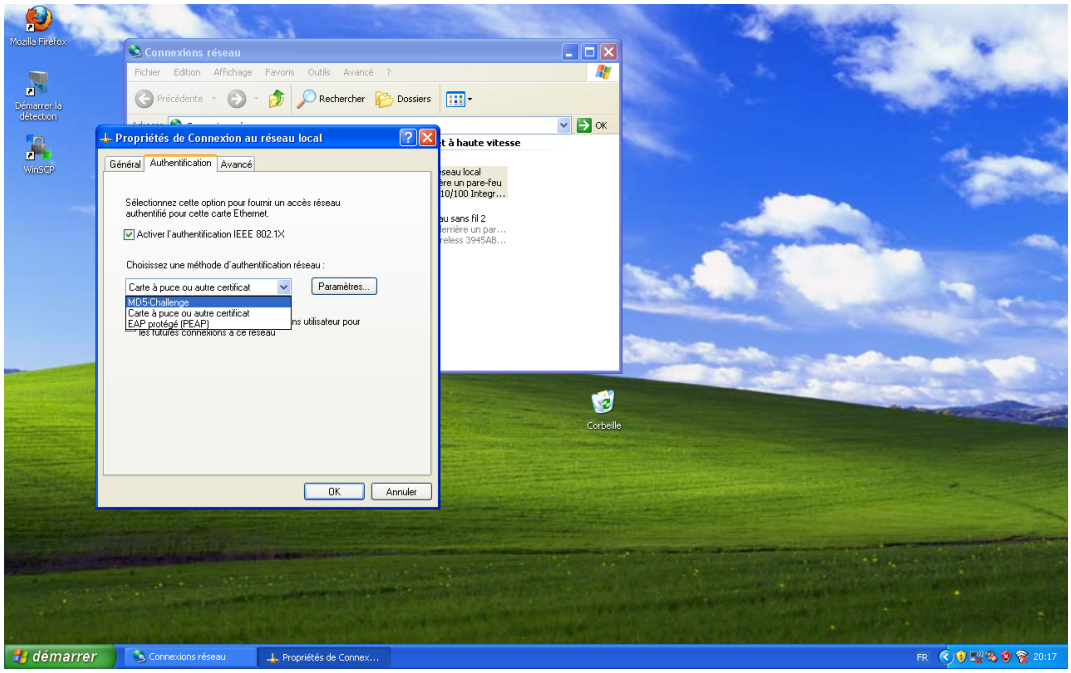
Allez dans le panneau des connections.



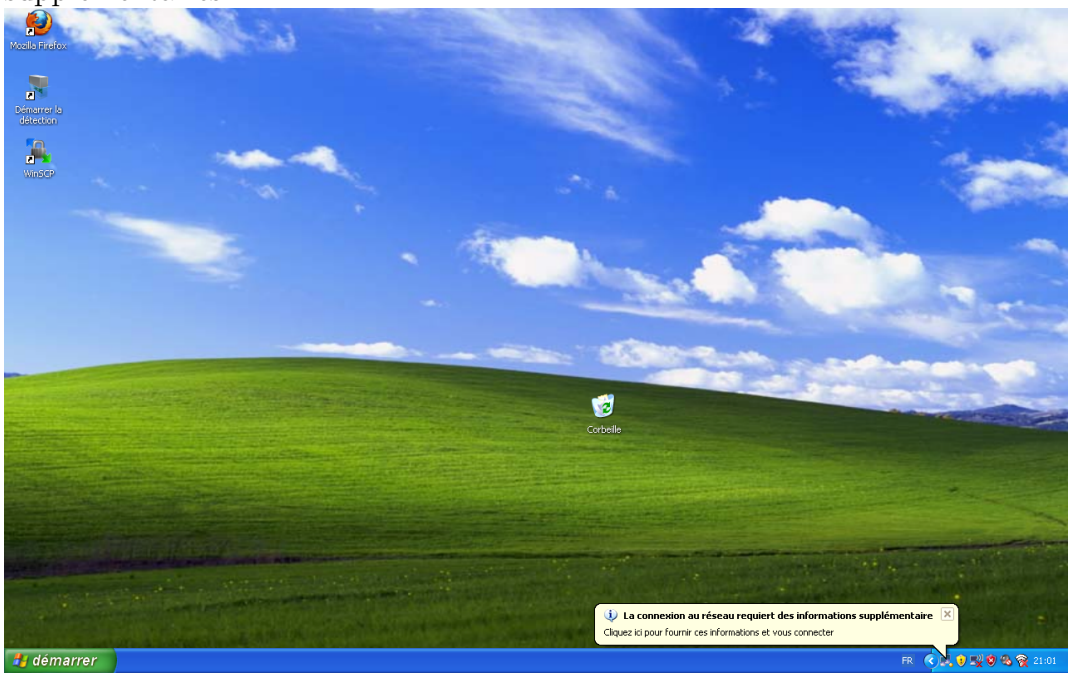
Puis effectuez un clic droit sur la connexion que vous utilisez pour accéder au reseaux, et ouvrez les propriétés de la connexion.



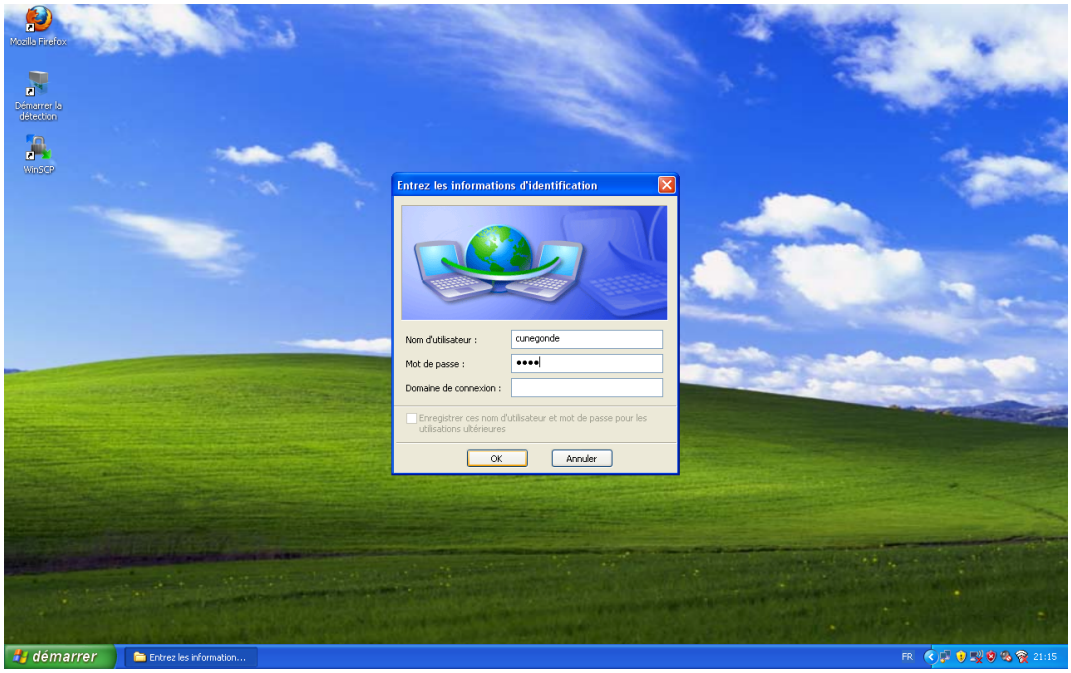
Choisissez alors 'challenge-MD5' dans l'onglet 'Authentification'.



Puis connectez-vous physiquement au reseau.
Une info-bulle windows doit apparaître, vous signifiant que l'accès au réseaux requiert des informations supplémentaires.



Après avoir cliqué sur l'info-bulle, il suffit de renseigner ses identifiants.

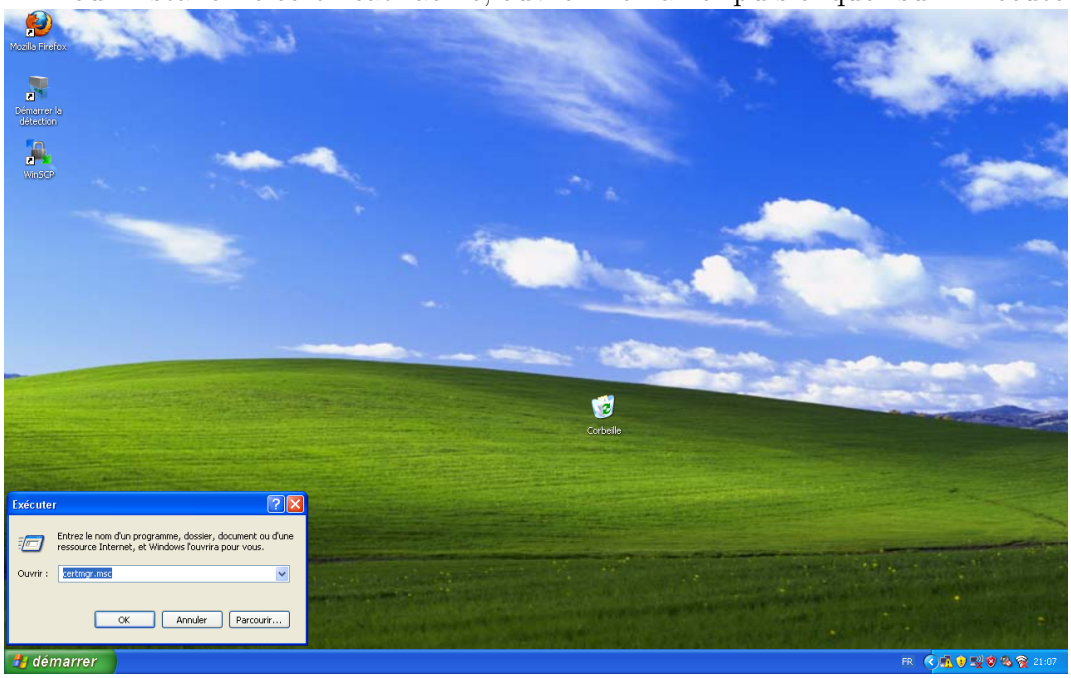


Après avoir validé, la connexion est établie.

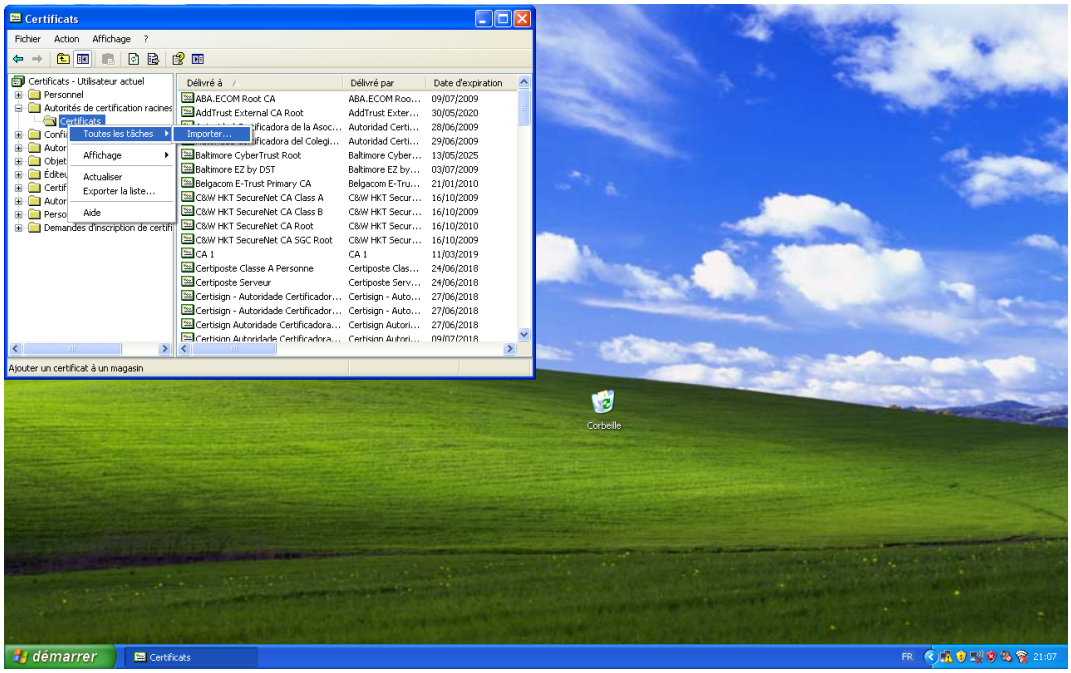
1.2 PEAP

1.2.1 Installation du certificat racine

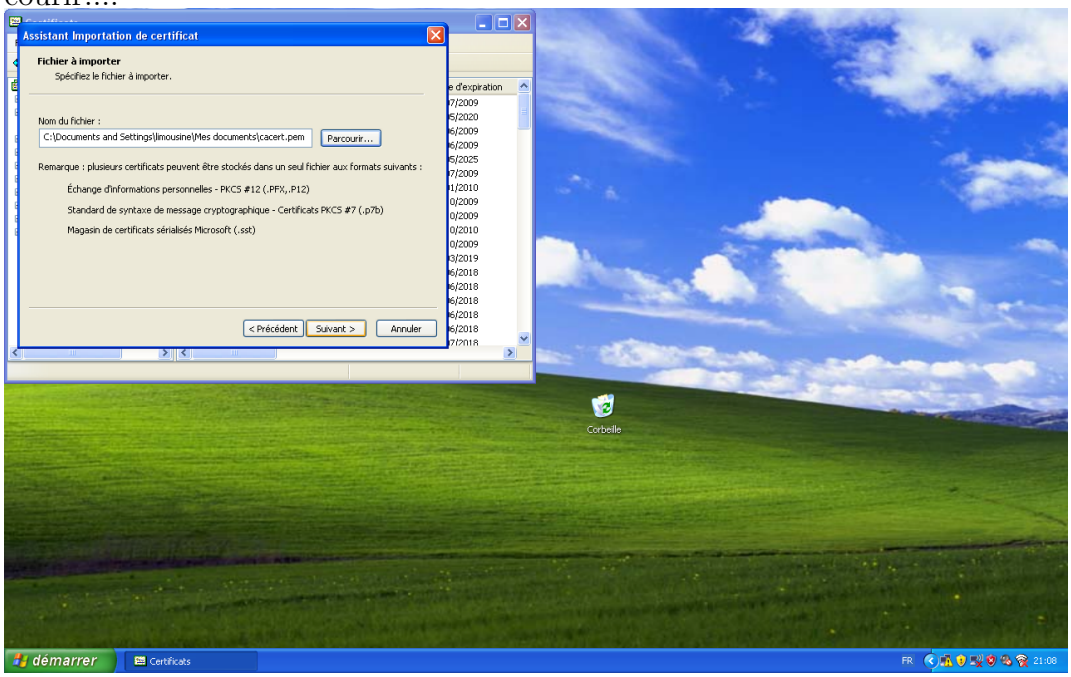
Pour installer le certificat racine, ouvrer Démarrer puis cliquez sur 'Exécuter' et lancez 'certmgr.msc'.



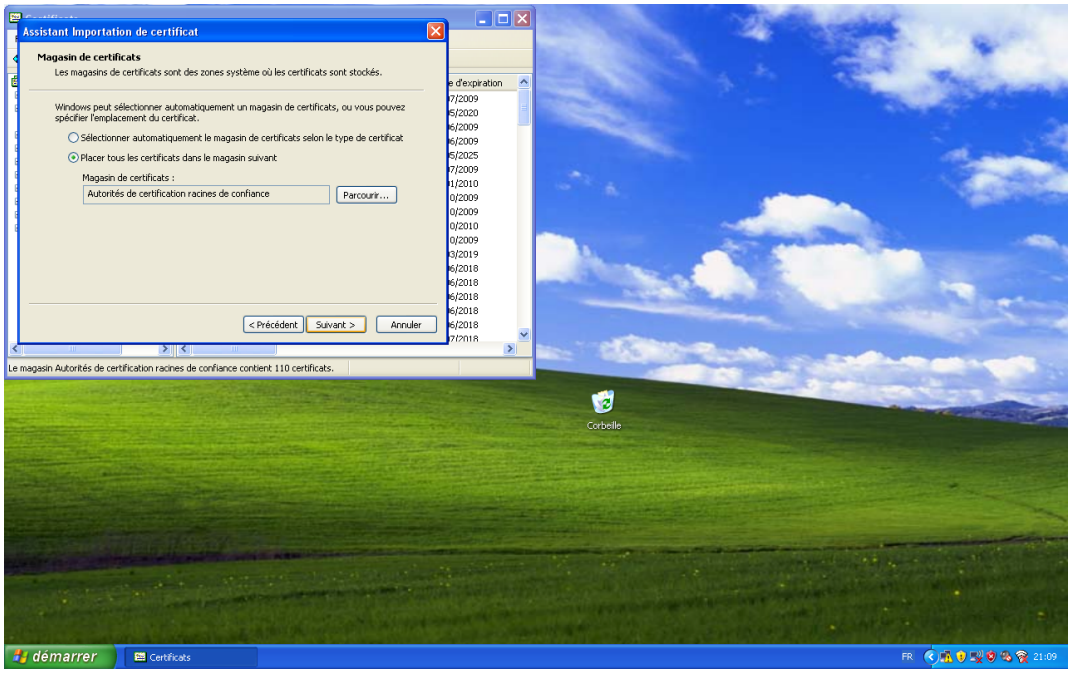
Double-cliquez ensuite sur les 'Authorités de certification racines de confiance' et faite un clic droit sur le sous-dossier 'Certificats', puis lancez 'toutes les tâches', 'Importer...'.



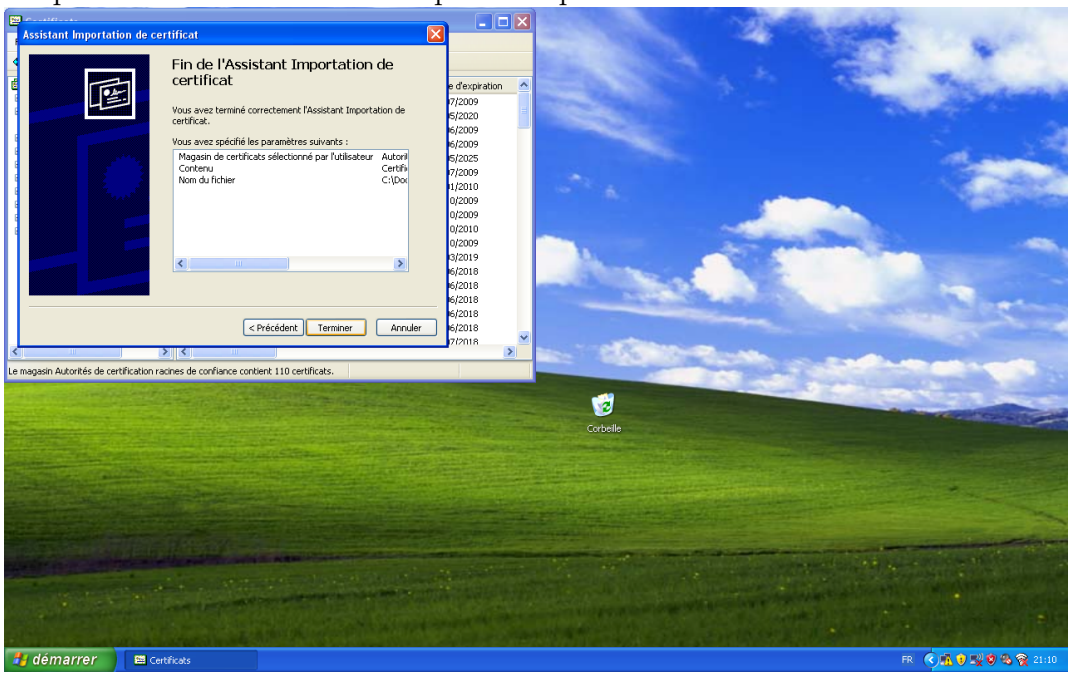
Cliquez suivant sur le premier panneau proposé. Puis sélectonnez votre fichier grâce au bouton 'Parcourir...'.



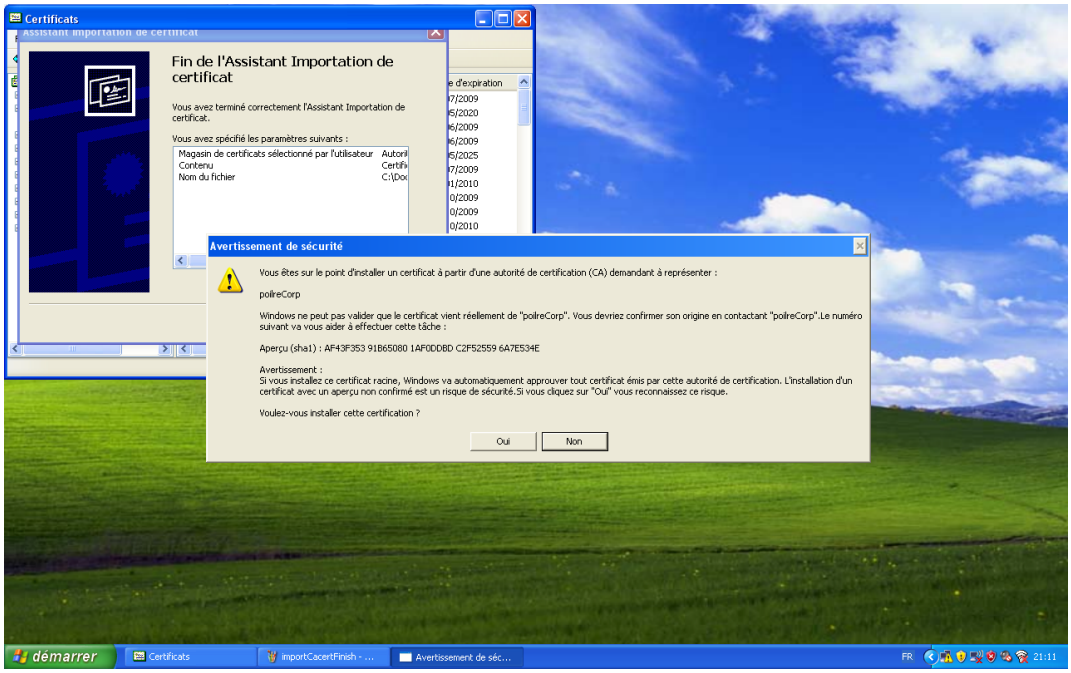
Cliquez sur suivant. Le panneau suivant vous demande de configurer le magasin dans lequel le certificat sera importé. Ici, le bon magasin est déjà choisi (Authorité de certification racines de confiance). Cliquez donc sur OK.



Cliquez sur suivant. Le dernier panneau permet de terminer l'installation. Cliquez donc sur Terminer.



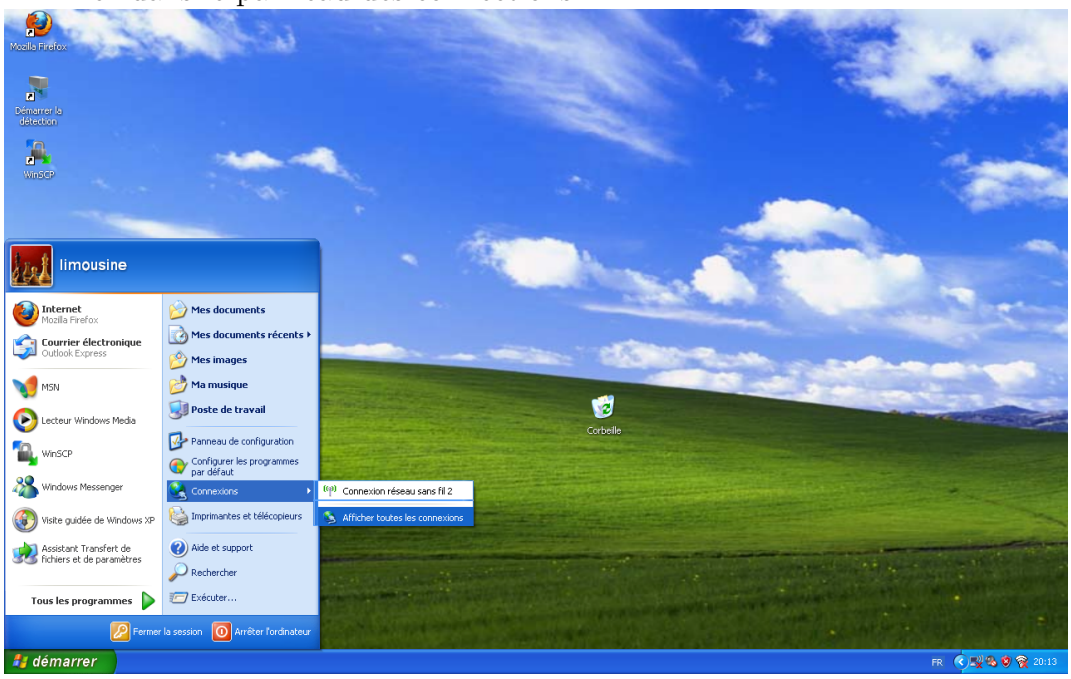
Un message d'alerte s'ouvre donc pour vous demander confirmation de l'import d'un nouveau certificat racine. Vous pouvez d'ailleurs voir apparaître le nom de l'autorité de certification. (Ici, PoilCorp).



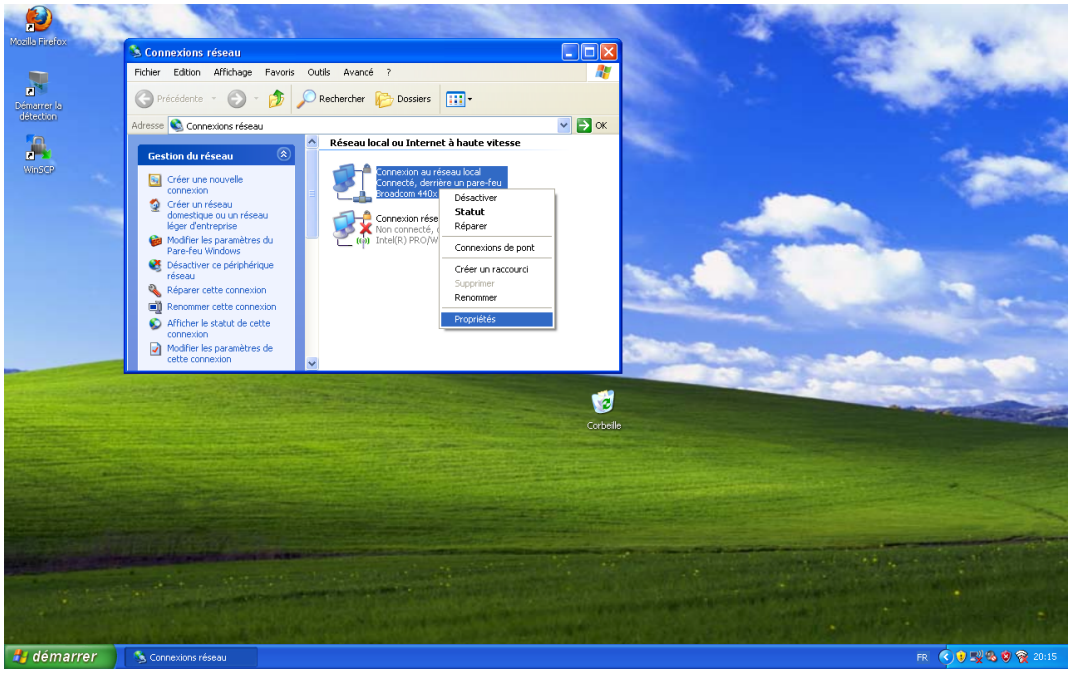
Authorisez cet import ('oui'). Puis validez et quittez toutes les fenêtres ouvertes.

1.2.2 Paramétrage du PEAP

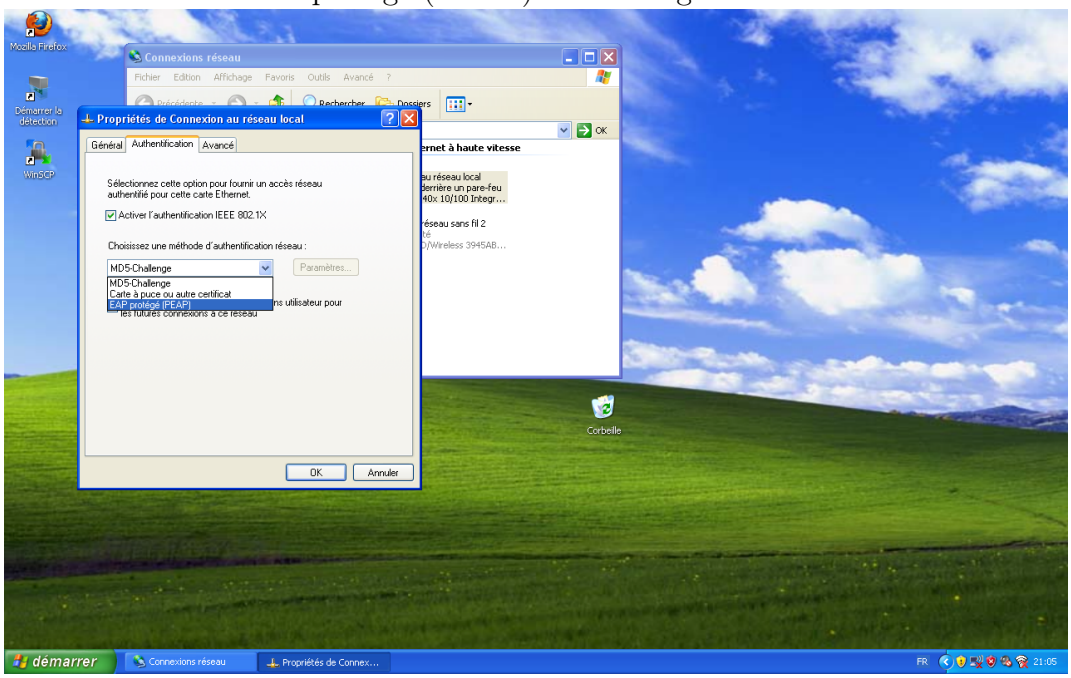
Allez dans le panneau des connections.



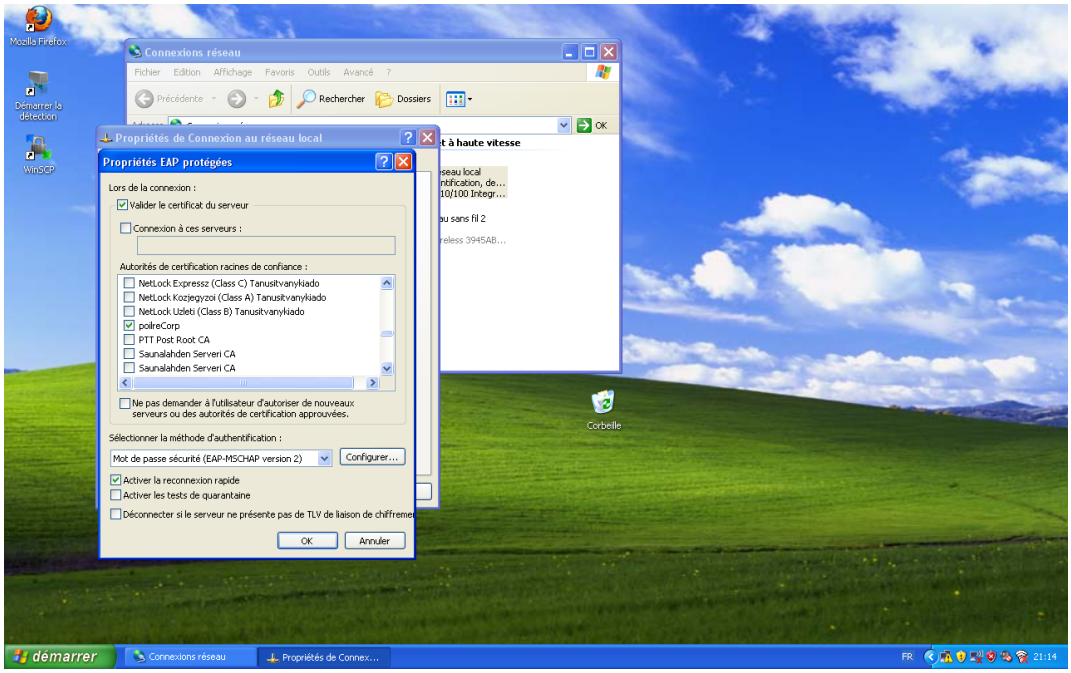
Puis effectuez un clic droit sur la connexion que vous utilisez pour accéder au reseaux, et ouvrez les propriétés de la connexion.



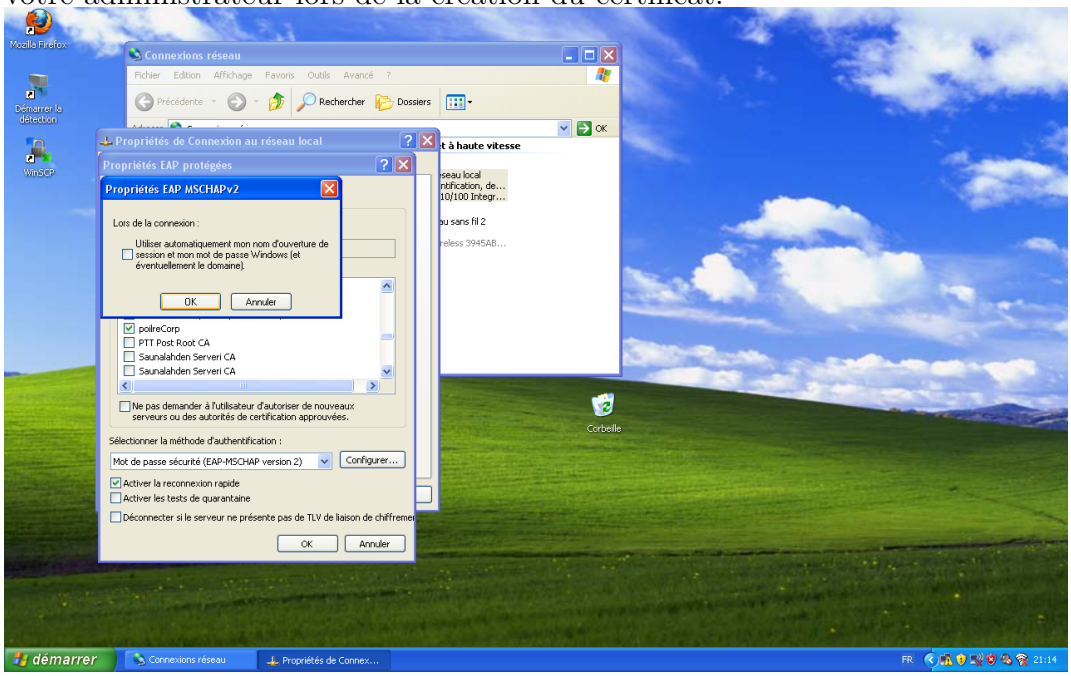
Choisissez alors 'EAP protégé (PEAP)' dans l'onglet 'Authentification'.



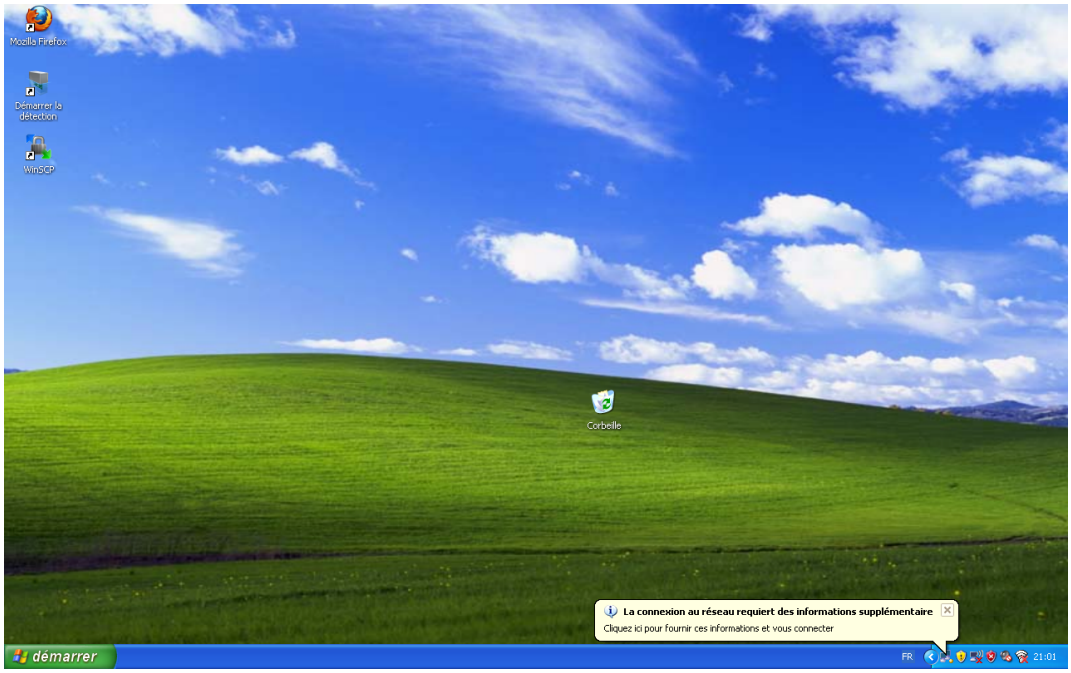
Cliquez ensuite sur le bouton 'Paramètres...' à coté de l'option PEAP et cochez votre authorité de certification dans la liste présentée.



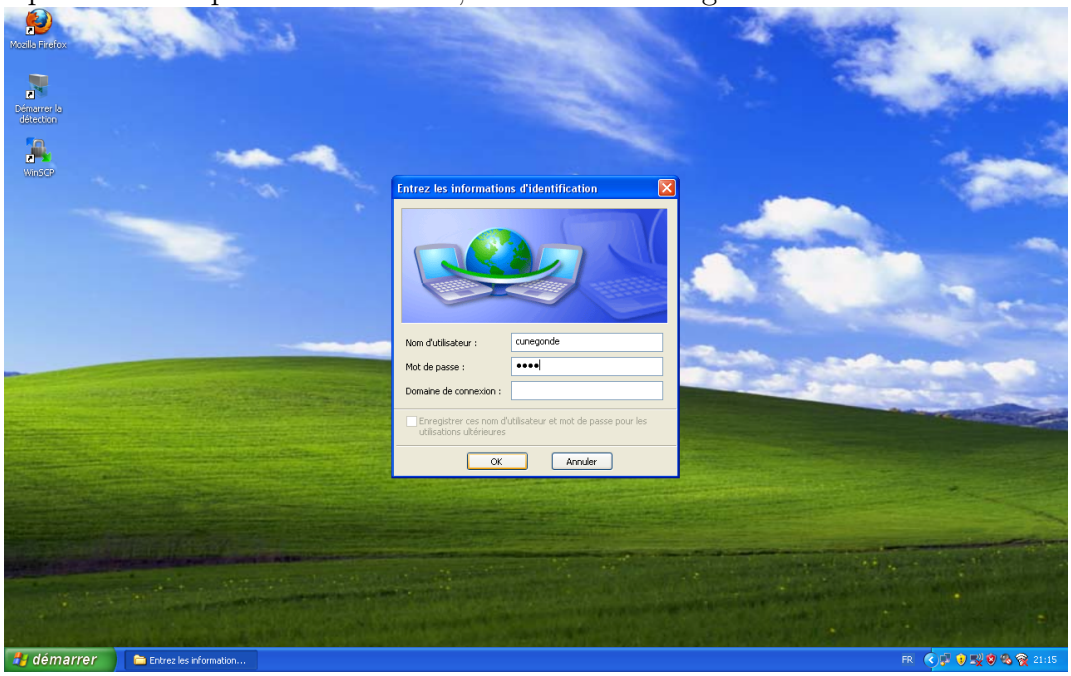
Cliquez ensuite sur le bouton 'Configurer...' à coté du champs présentant la méthode d'authentification (Mot de passe sécurité (EAP MSCHAP Version 2)).
Décochez alors l'utilisation du nom de session, à moins que celui-ci soit effectivement celui utilisé par votre administrateur lors de la création du certificat.



Puis validez et fermez toutes les fenêtres ouvertes. Connectez-vous physiquement au reseau.
Une info-bulle windows doit apparaître, vous signifiant que l'accès au réseaux requiert des informations supplémentaires.



Après avoir cliqué sur l'info-bulle, il suffit de renseigner ses identifiants.



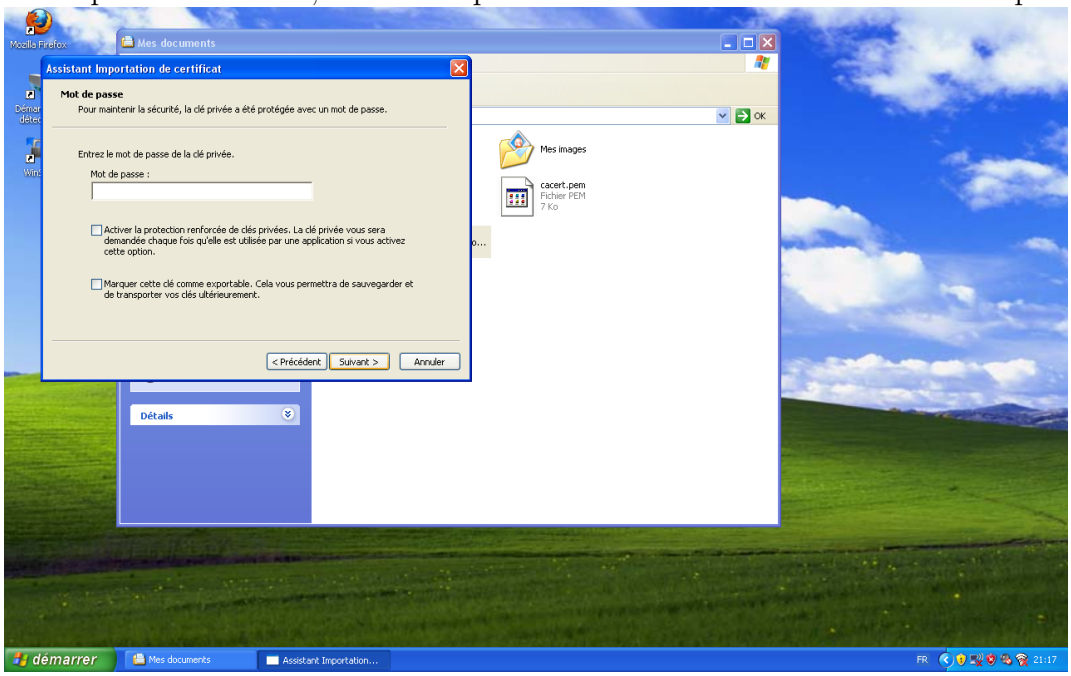
Après avoir validé, la connexion est établie.

1.3 TLS

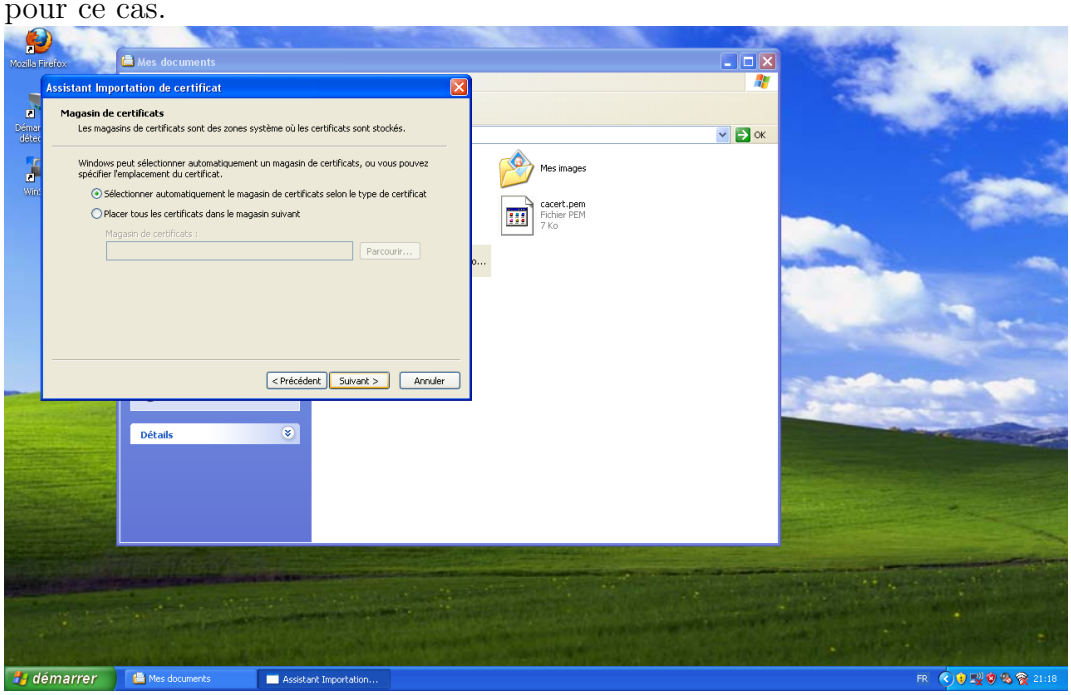
Si ce n'est pas fait, commencez par installer le certificat racine (ci-dessus, section PEAP).

1.3.1 Installation du certificat Client

Pour installer le certificat client au format p12, il vous suffit de double-cliquer dessus. Le même assistant que celui utilisé pour l'installation du certificat racine apparait.
Cliquez sur suivant lors du premier panneau. Cliquez sur suivant sur le panneau suivant (Le chemin du fichier est déjà bon).
Sur le panneau suivant, un mot de passe vous est demandé. Laissez le champs vide et cliquez sur suivant.



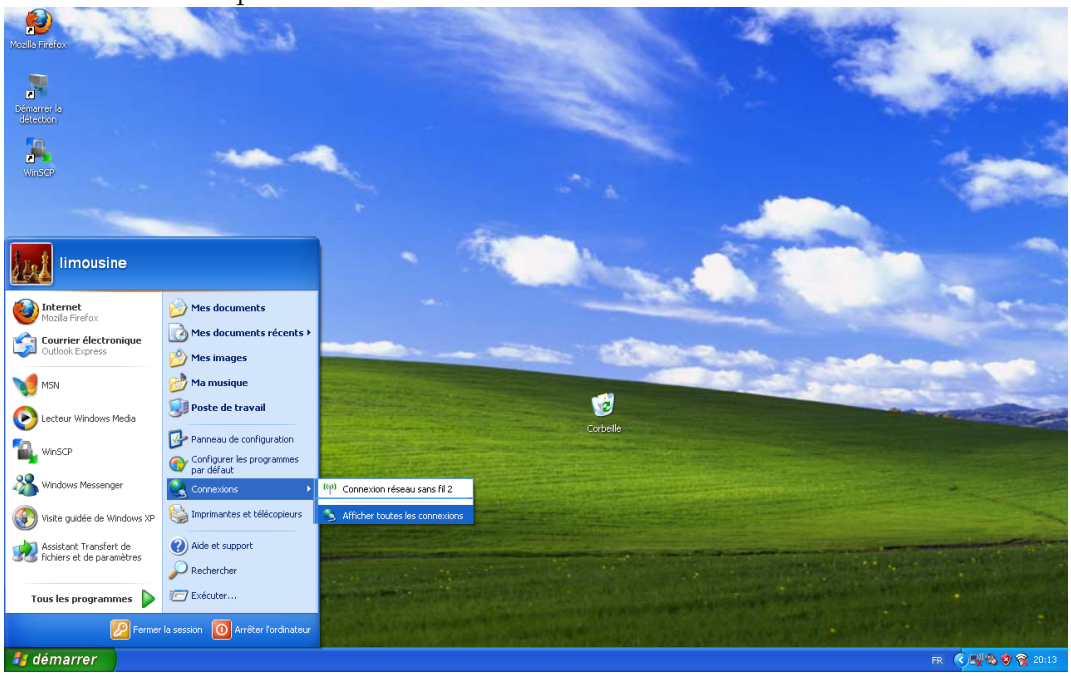
Cliquez ensuite sur suivant une nouvelle fois. La selection automatique du magasin est en effet adaptée pour ce cas.



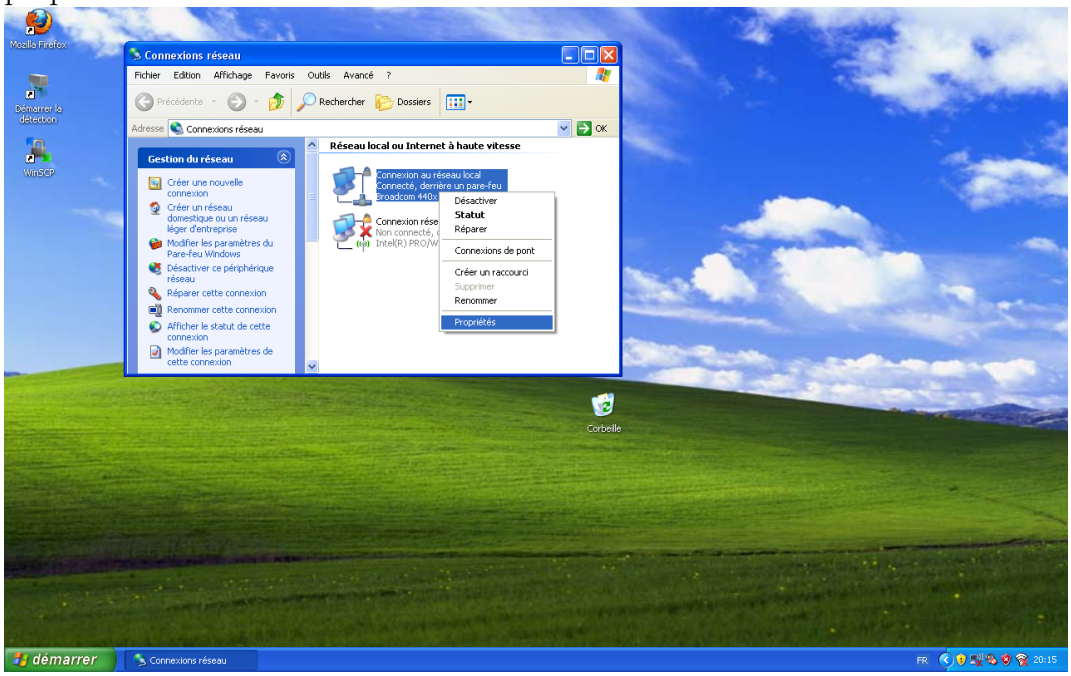
Cliquez enfin sur Terminer.

1.3.2 Paramétrage du TLS

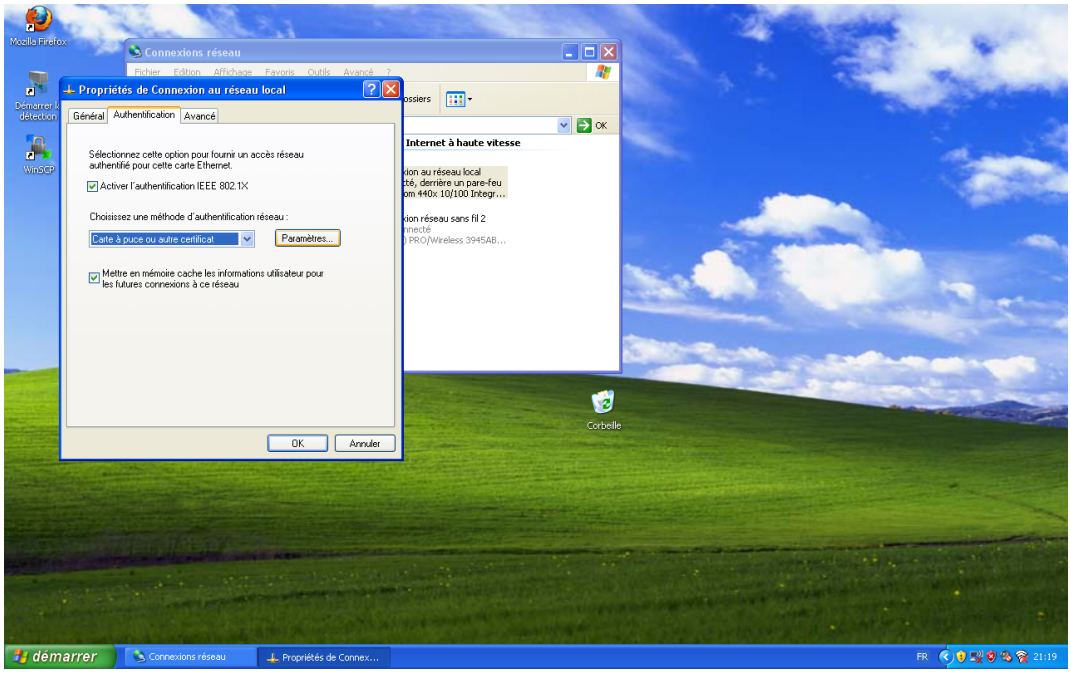
Allez dans le panneau des connections.



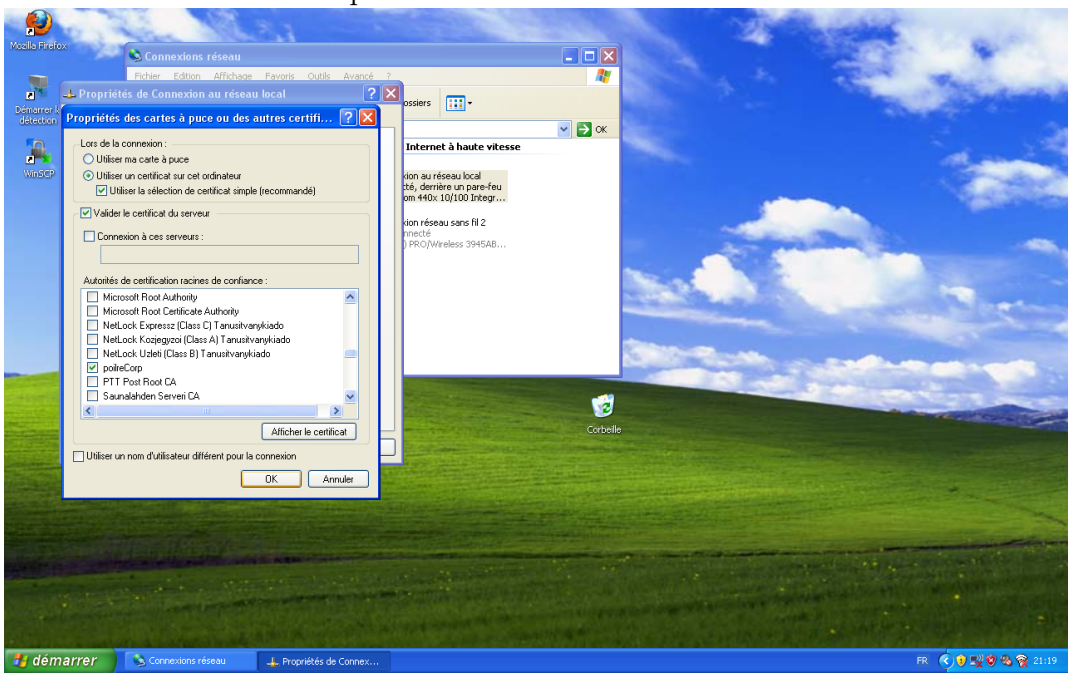
Puis effectuez un clic droit sur la connexion que vous utilisez pour accéder au reseaux, et ouvrez les propriétés de la connexion.



Choisissez alors 'Carte à puce ou autre certificat' dans l'onglet 'Authentification'.



Cliquez ensuite sur le bouton 'Paramètres...' à coté de l'option PEAP et cochez votre authorité de certification dans la liste présentée.



Validez et quitez enfin toutes les fenêtres ouvertes.
Connectez-vous physiquement au réseau. La connection est établie.

2 Linux

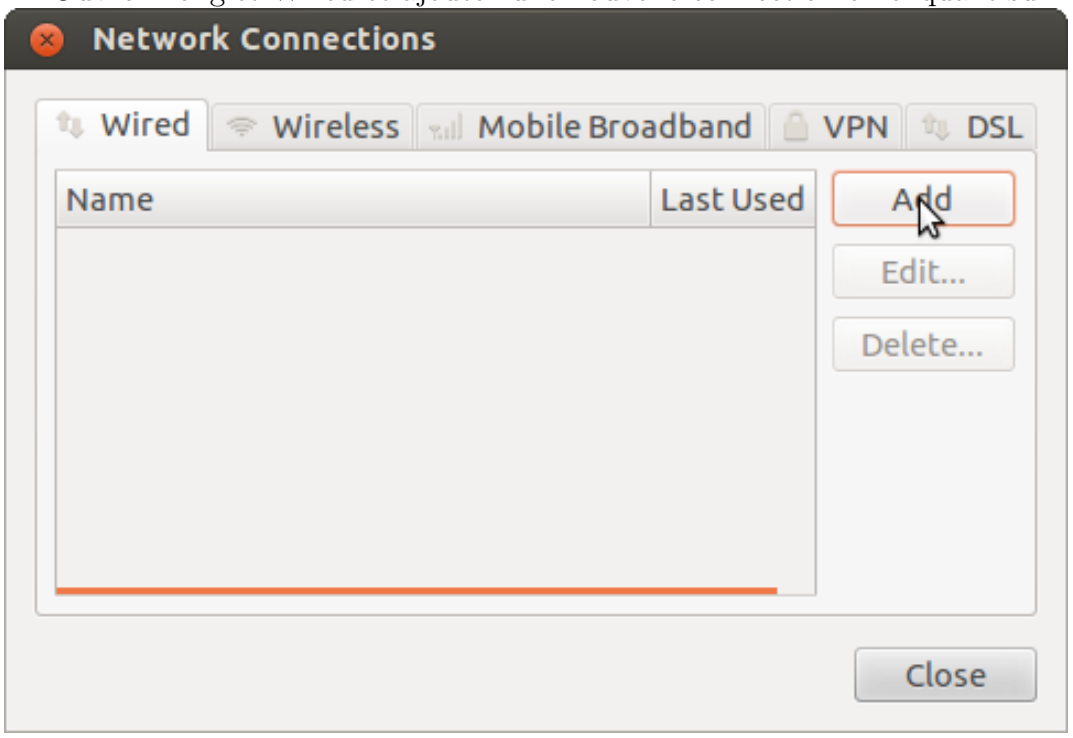
Nous supposerons que vous utilisez ubuntu et apt pour gestionnaire de paquets.

2.1 Avec Network-manager

Ouvrez Network-manager (nework connections).

2.1.1 Challenge-MD5

Ouvrez l'onglet Wired et ajoutez une nouvelle connection en cliquant sur 'Add'.



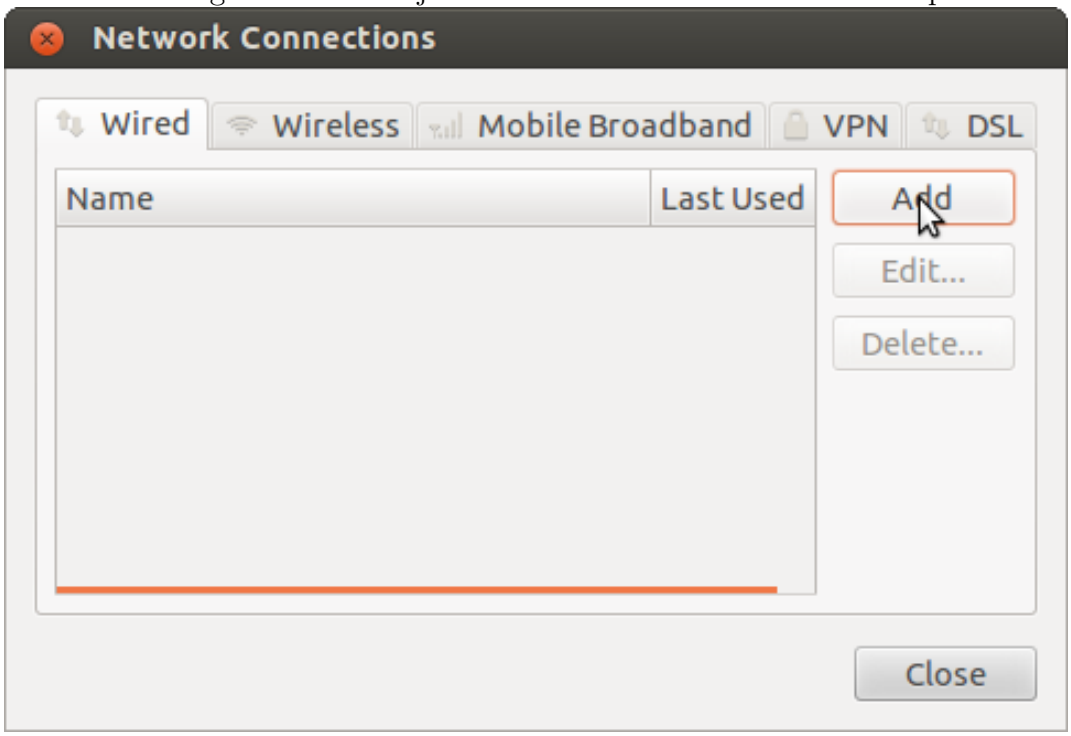
Dans l'onglet 'Wired' du nouveau panneau, choisissez votre MAC adresse dans le menu déroulant.

Puis dans l'onglet 802.1x, cochez 'Utiliser la sécurtité 802.1x pour cette connexion'.
Sélectionnez MD5 dans le menu déroulant 'Authentification'. Enfin remplissez les champs 'Username' et 'Password'

Cliquez ensuite sur 'sauvegarder' et fermez la fenêtre. Il ne reste alors plus qu'à se connecter physiquement au réseau.

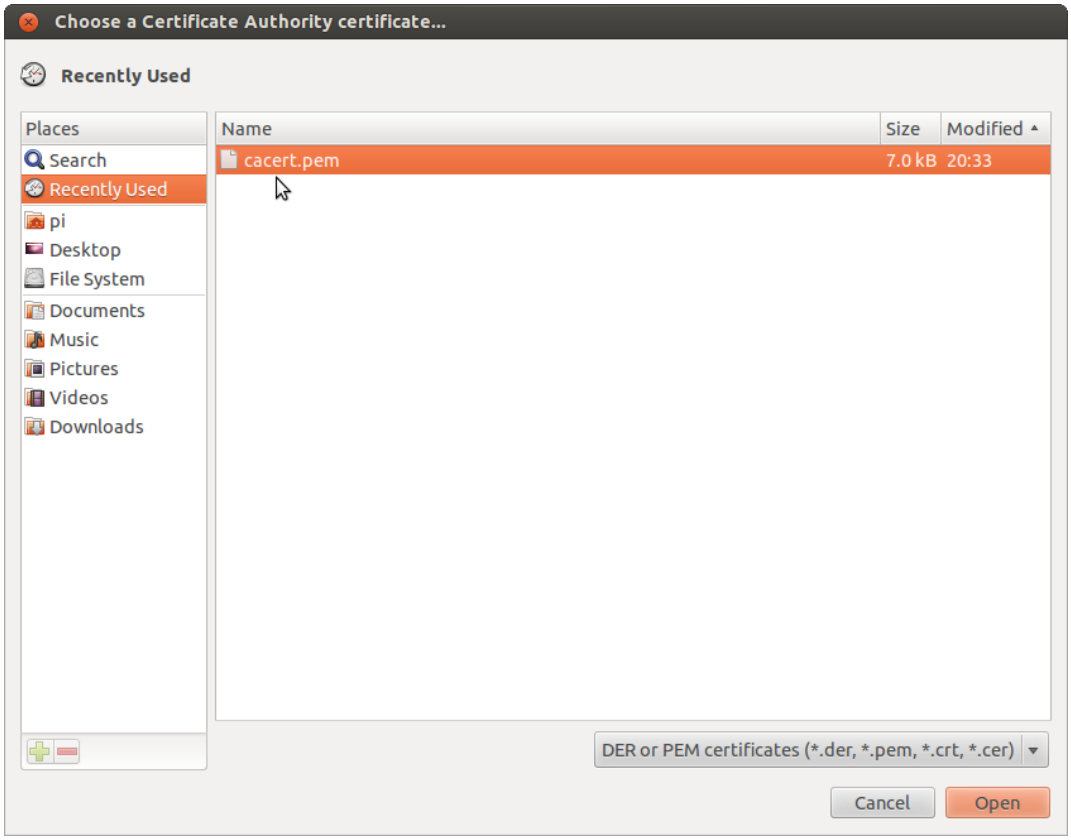
2.1.2 PEAP

Ouvrez l'onglet Wired et ajoutez une nouvelle connection en cliquant sur 'Add'.

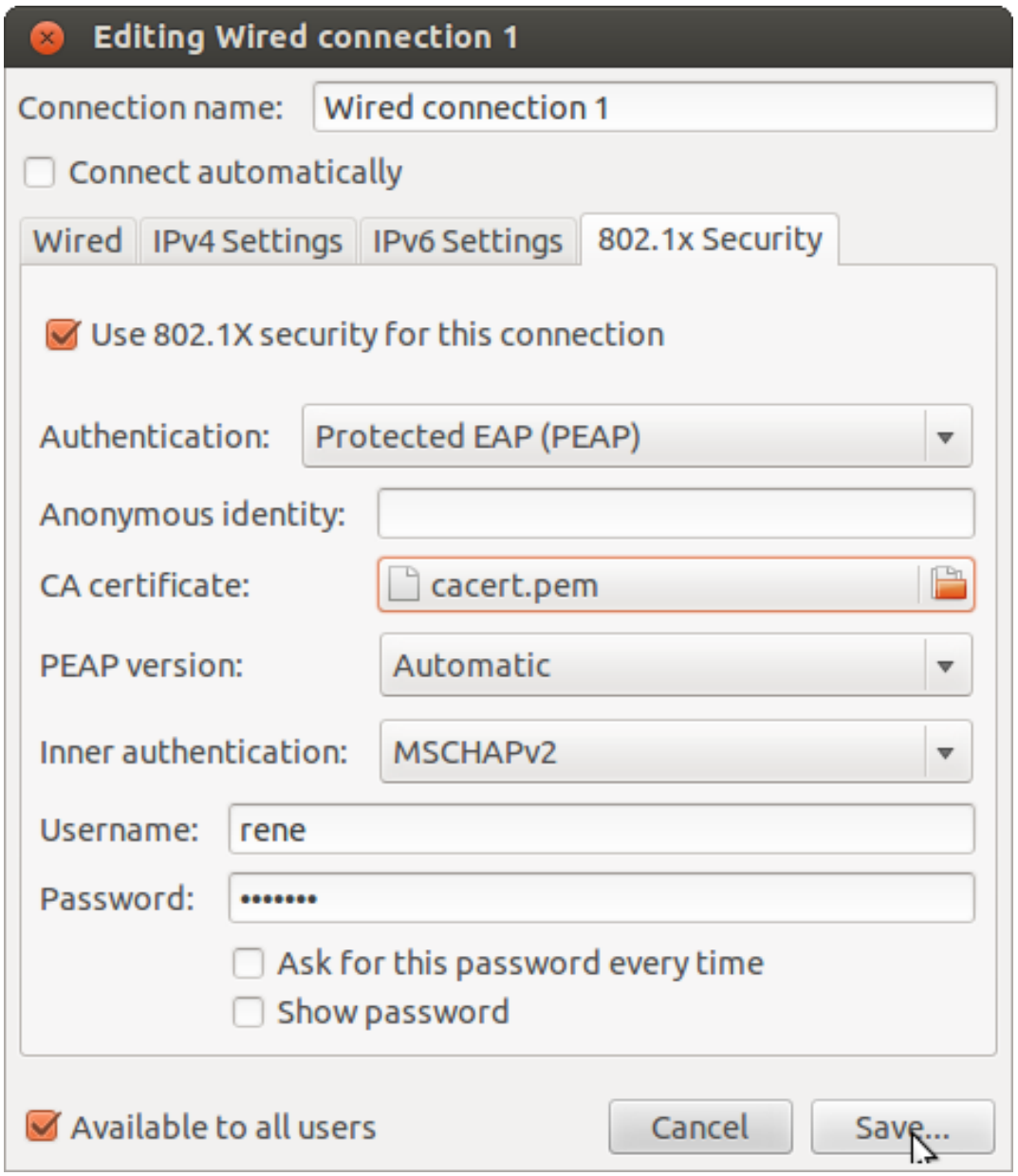


Dans l'onglet 'Wired' du nouveau panneau, choisissez votre MAC adresse dans le menu déroulant.

Puis dans l'onglet 802.1x, cochez 'Utiliser la sécurtité 802.1x pour cette connexion'.
Sélectionnez 'Protected EAP (PEAP)' dans le menu déroulant 'Authentification'. Cliquez sur le bouton à coté de CA certificate et choisissez votre certificat racine.



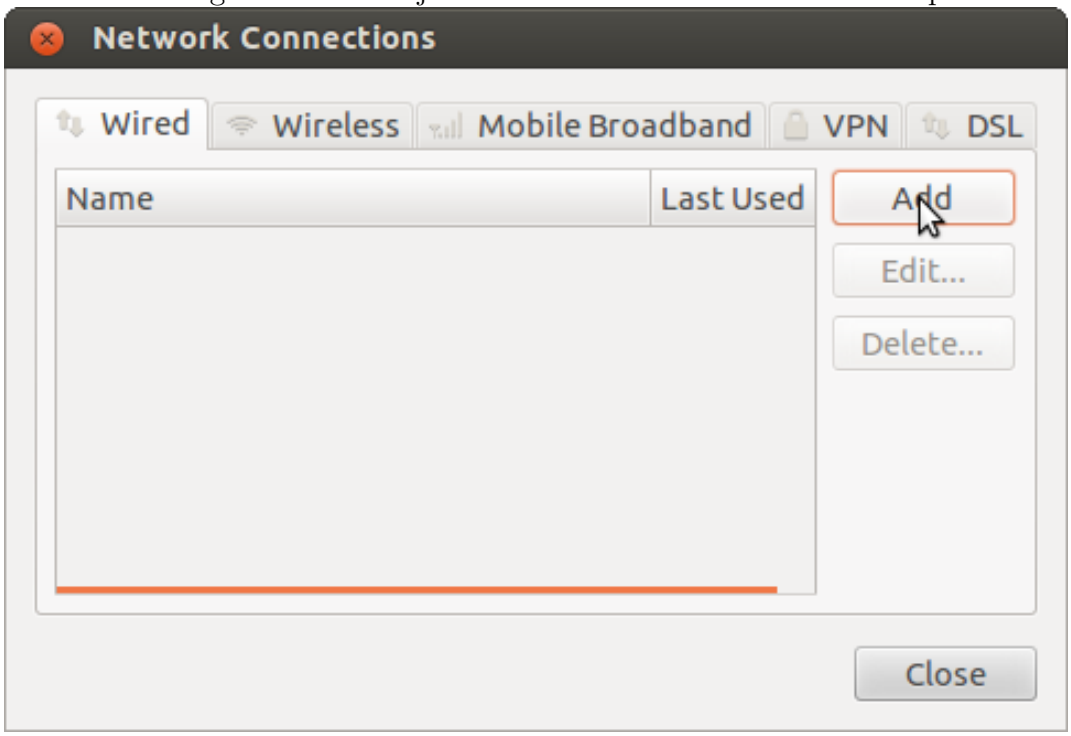
Remplissez les champs 'Username' et 'Password'.



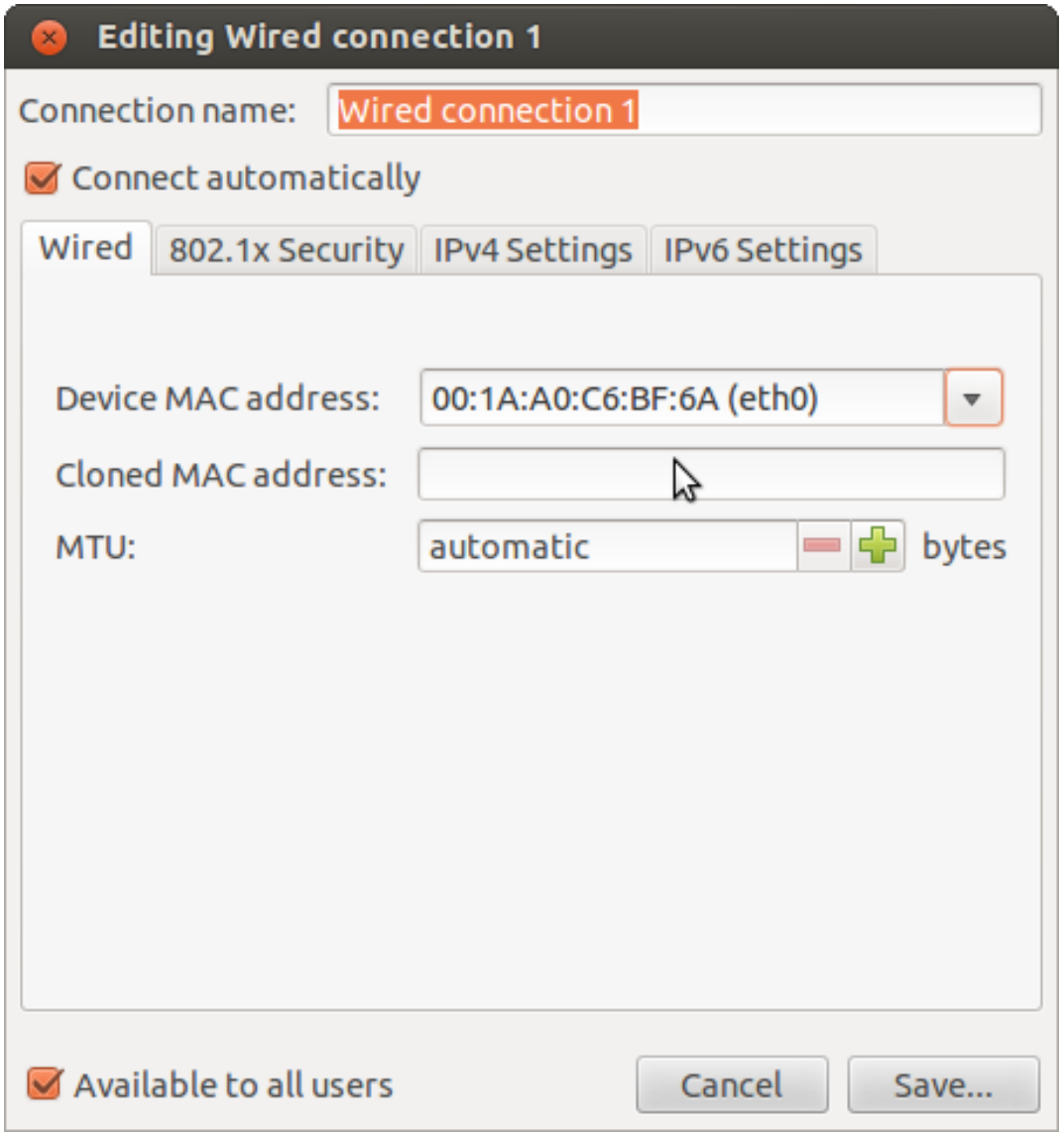
Cliquez ensuite sur 'sauvegarder' et fermez la fenêtre. Il ne reste alors plus qu'à se connecter physiquement au réseau.

2.1.3 TTLS

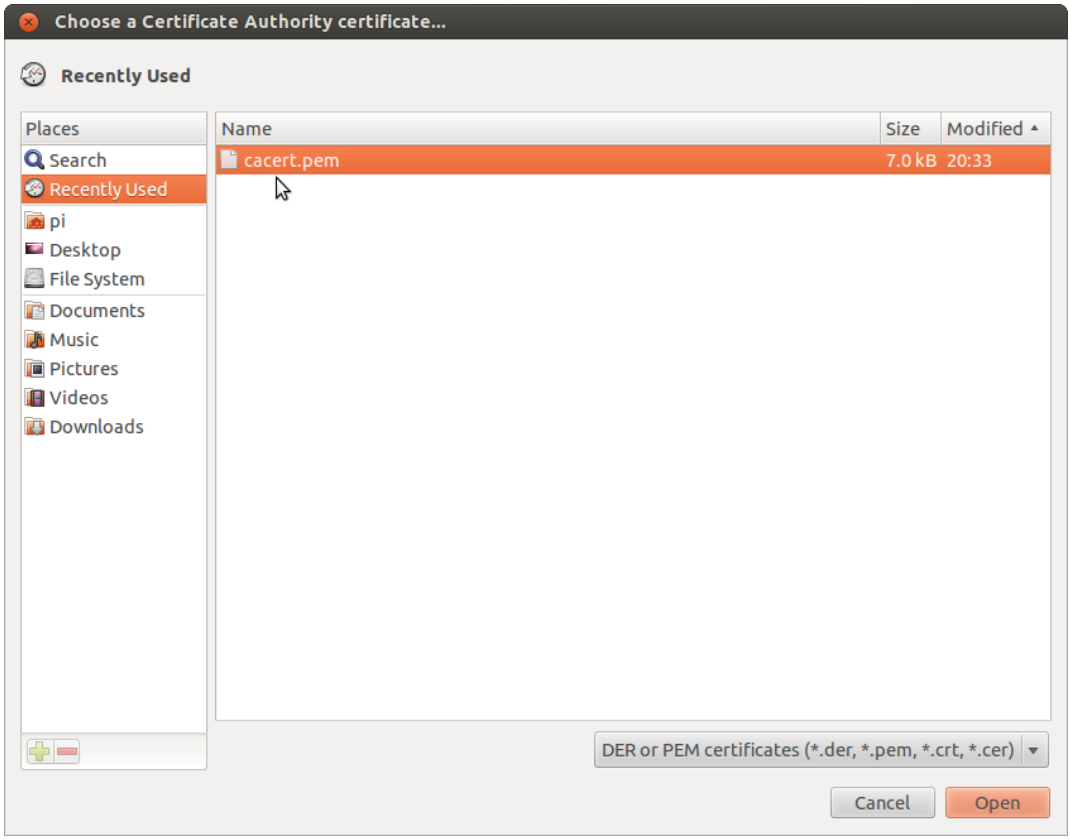
Ouvrez l'onglet Wired et ajoutez une nouvelle connection en cliquant sur 'Add'.



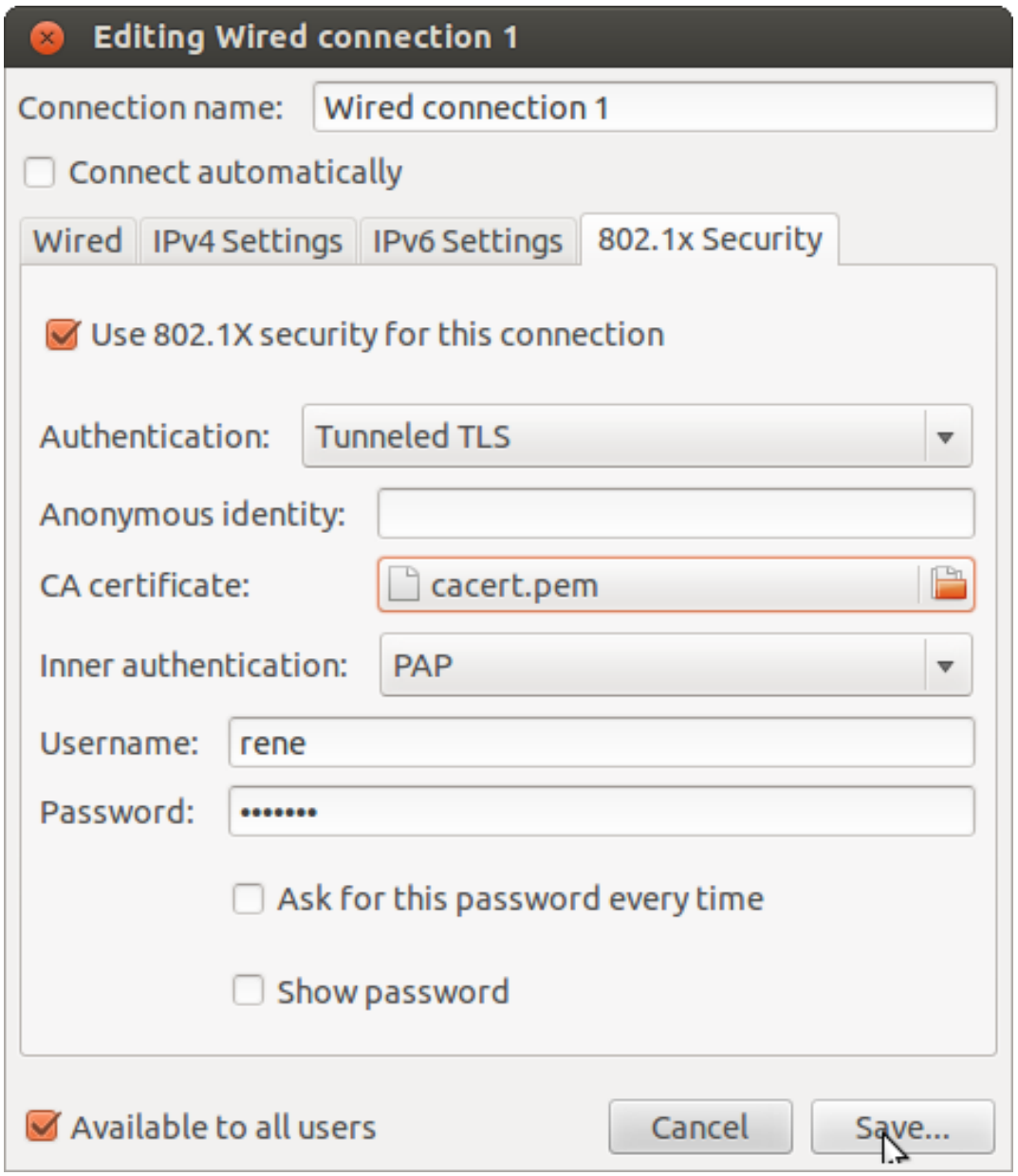
Dans l'onglet 'Wired' du nouveau panneau, choisissez votre MAC adresse dans le menu déroulant.



Puis dans l'onglet 802.1x, cochez 'Utiliser la sécurtité 802.1x pour cette connexion'.
Sélectionnez 'Tunneled TLS' dans le menu déroulant 'Authentification'. Cliquez sur le bouton à coté de CA certificate et choisissez votre certificat racine.



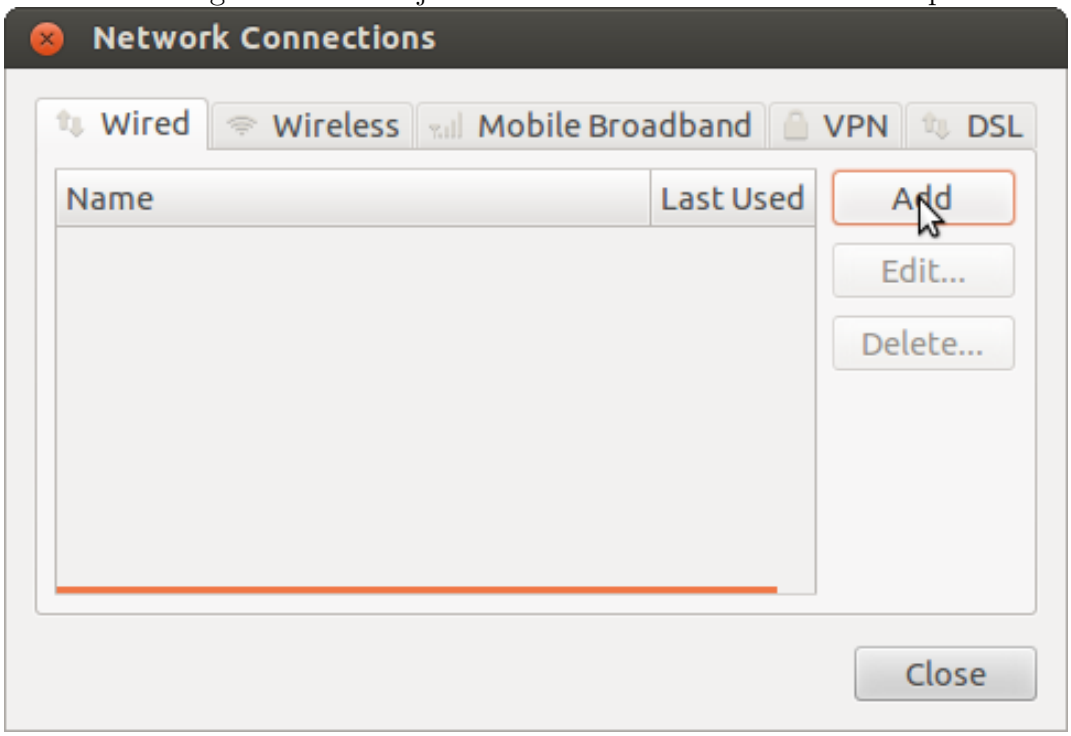
Remplissez les champs 'Username' et 'Password'.



Cliquez ensuite sur 'sauvegarder' et fermez la fenêtre. Il ne reste alors plus qu'à se connecter physiquement au réseau.

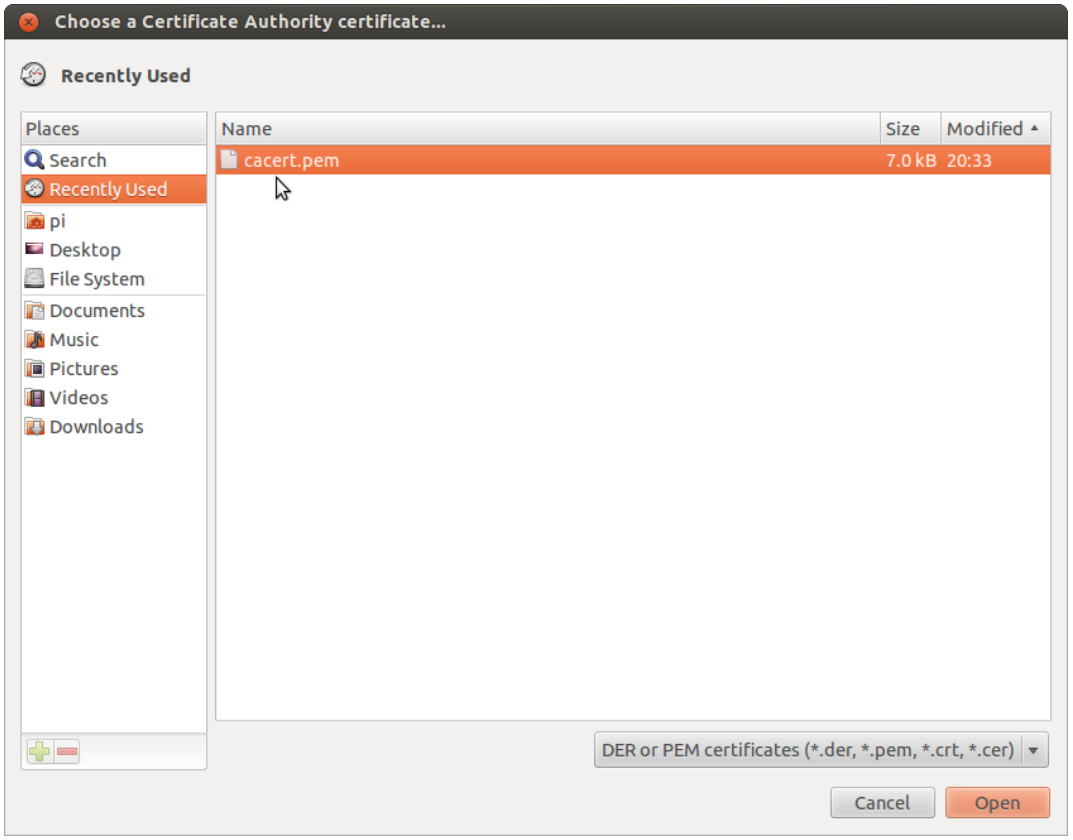
2.1.4 TLS

Ouvrez l'onglet Wired et ajoutez une nouvelle connection en cliquant sur 'Add'.

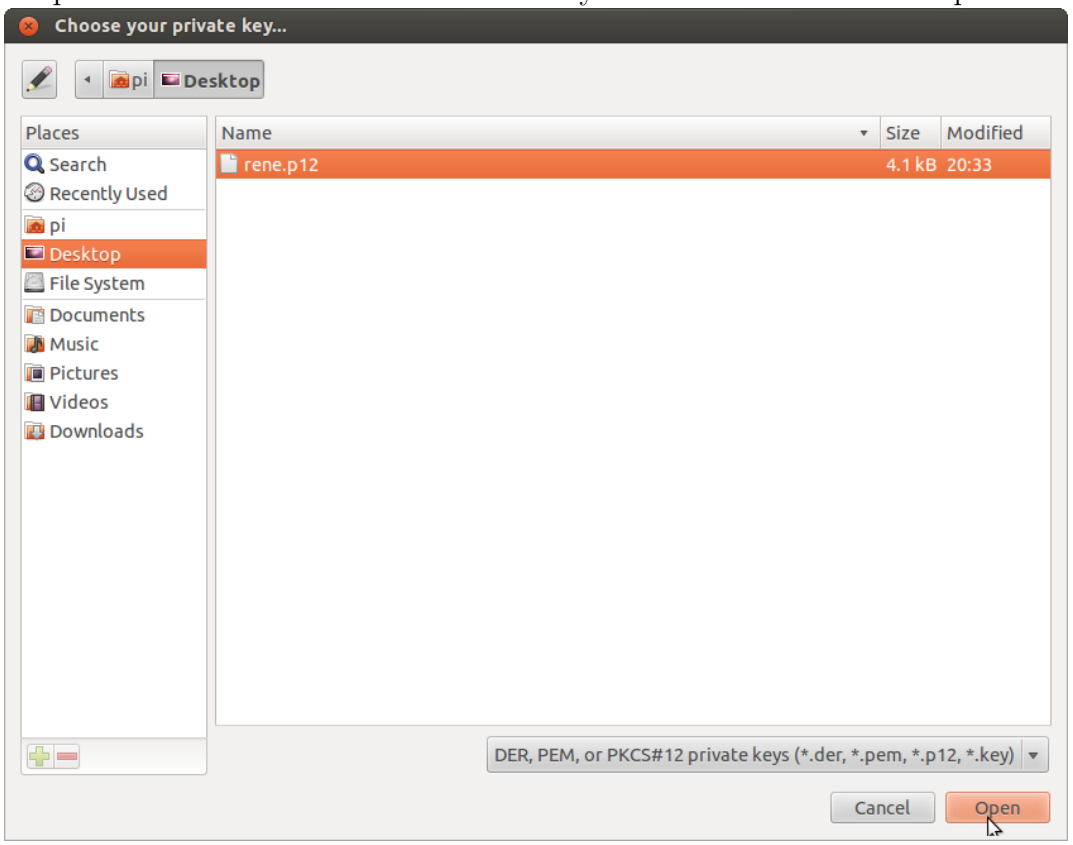


Dans l'onglet 'Wired' du nouveau panneau, choisissez votre MAC adresse dans le menu déroulant.

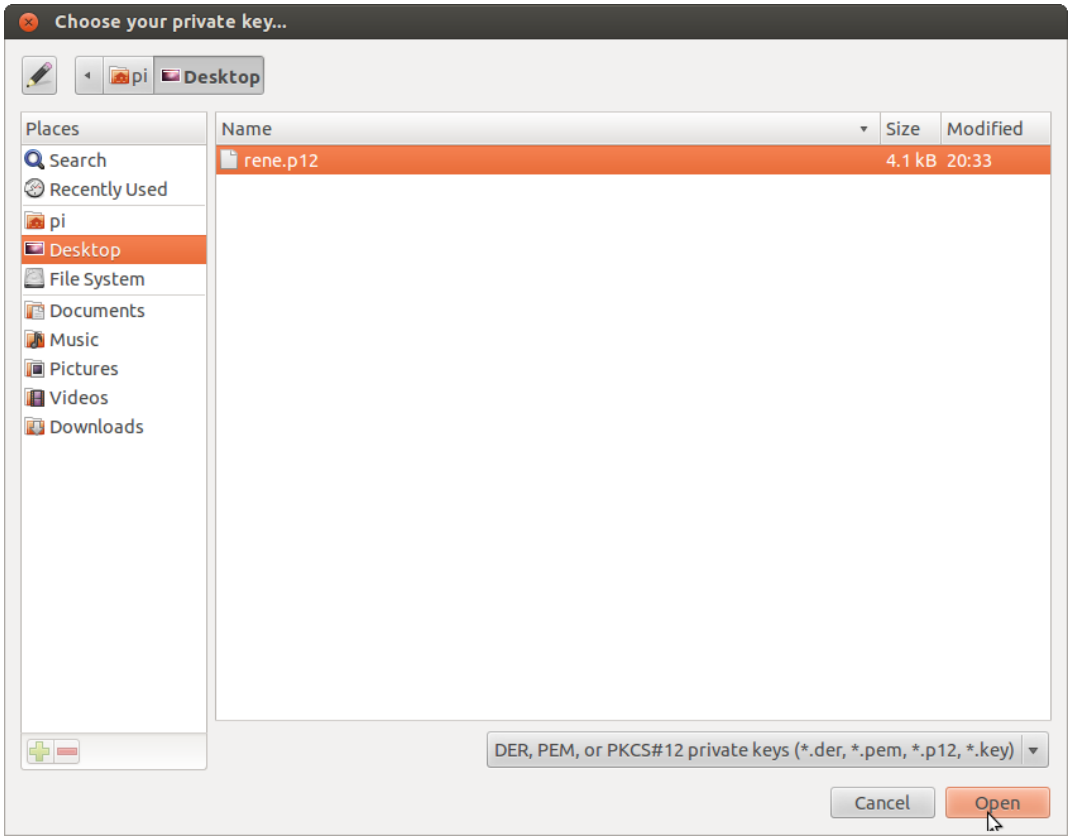
Puis dans l'onglet 802.1x, cochez 'Utiliser la sécurtité 802.1x pour cette connexion'.
Sélectionnez 'TLS' dans le menu déroulant 'Authentification'. Cliquez sur le bouton à coté de CA certificate et choisissez votre certificat racine.



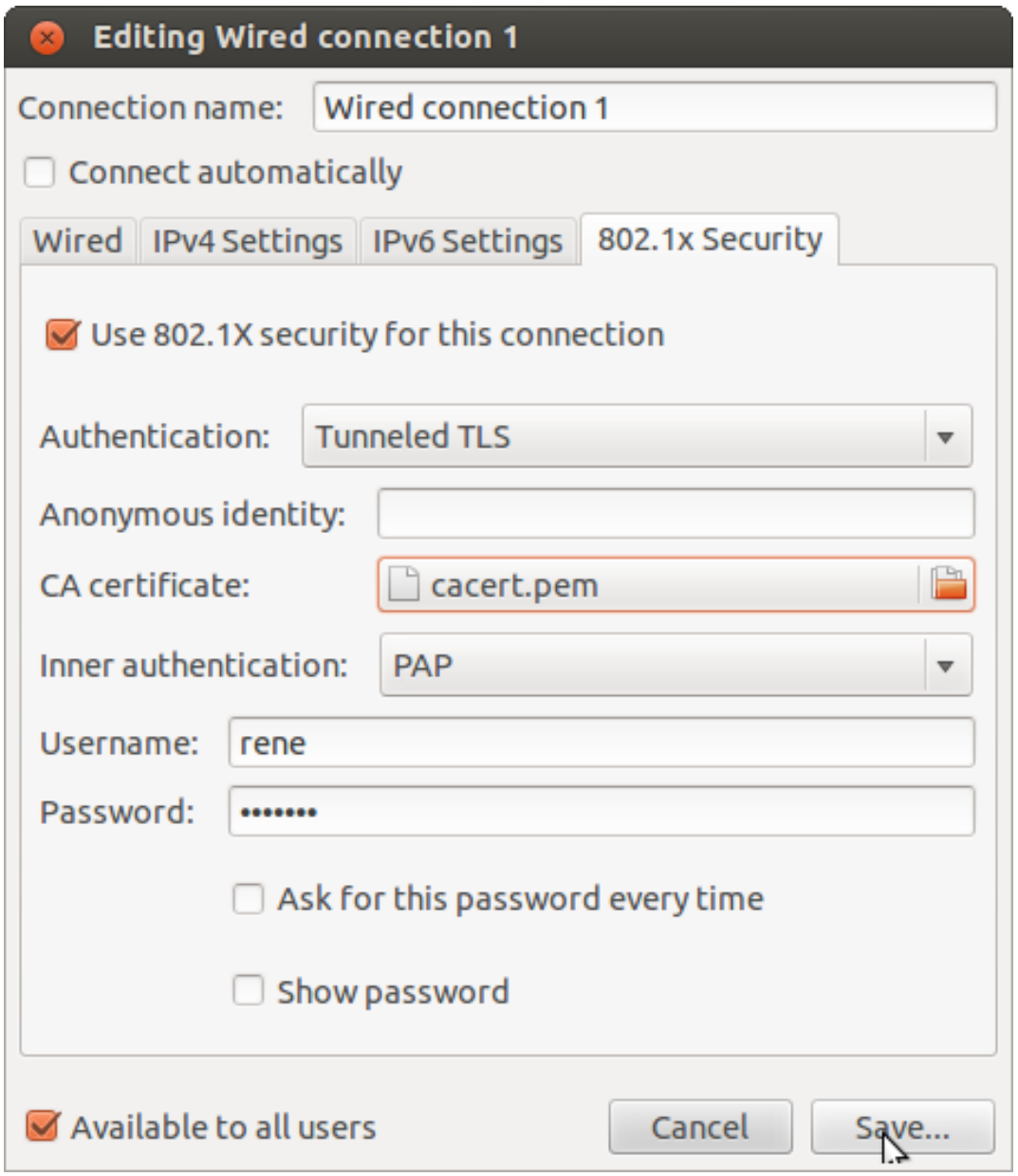
Cliquez sur le bouton à coté de Private key et choisissez votre fichier p12.



Cliquez sur le bouton à coté de User certificate et choisissez votre fichier pem.



Remplissez le champs 'Username'.



Cliquez ensuite sur 'sauvegarder' et fermez la fenêtre. Il ne reste alors plus qu'à se connecter physiquement au réseau.

2.2 Avec wpa-supplicant

Si vous ne l'avez pas déjà installé, installez wpa_supplicant.

```
1 $ sudo apt-get install wpa_supplicant
```

Il vous suffit alors d'utiliser un fichier l'un des fichier de configuration ci dessous. Vous pouvez alors lancer wpa_supplicant avec la commande suivante :

```
1 $ sudo wpa_supplicant -cpath/to/configuration/file.conf -ieth0 -Dwired -B
```

2.2.1 Challenge-MD5

```
network={
        key_mgmt=IEEE8021X
        eap=MD5
        identity="utilisateur1"
        password="pass_utilisateur1"
}
```

2.2.2 TLS

```
network={
    eap=TLS
    eapol_flags=0
    key_mgmt=IEEE8021X
    identity="utilisateur1"
    ca_cert="dossier_certs_utilisateur/cacert.pem"
    client_cert="dossier_certs_utilisateur/utilisateur1_cert.pem"
    private_key="dossier_certs_utilisateur/utilisateur1_key.pem"
}
```

Pour TLS, en utilsant un certificat au format p12 :

```
network={
    eap=TLS
    eapol_flags=0
    key_mgmt=IEEE8021X
    identity="utilisateur1"
    ca_cert="dossier_certs_utilisateur/cacert.pem"
    private_key="dossier_certs_utilisateur/utilisateur1.p12"
}
```

2.2.3 TTLS

Pour TTLS avec un chiffrement MD5 dans le tunnel :

```
network={
    eap=TTLS
    eapol_flags=0
    key_mgmt=IEEE8021X
    identity="utilisateur1"
    password="pass_utilisateur1"
    ca_cert="dossier_certs_utilisateur/cacert.pem"
    phase2="auth=MD5"
}
```

2.2.4 PEAP

Enfin, pour PEAP :

```
network={
    eap=PEAP
    eapol_flags=0
```

```
4       key_mgmt=IEEE8021X
5       identity="utilisateur1"
6       password="pass_utilisateur1"
7       ca_cert="dossier_certs_utilisateur/cacert.pem"
8       phase2="auth=MSCHAPV2"
9   }
```