COMMENT GARANTIR UN ACCÈS LÉGITIME AU SI PAR L'AUTHENTIFICATION À DOUBLE FACTEUR ?

Cyril Bras

Journée « Sécu »

Sommaire

- Contexte
- Pourquoi faire ?
- Comment ?
- Le matériel
- Au niveau d’Active Directory
- Configuration de la clef
- Résultat
- Limitations

Sommaire

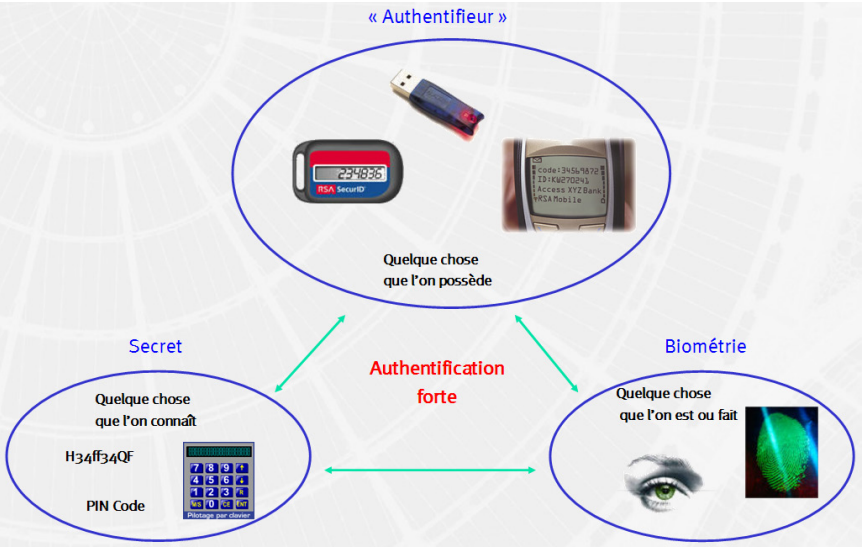
Contexte

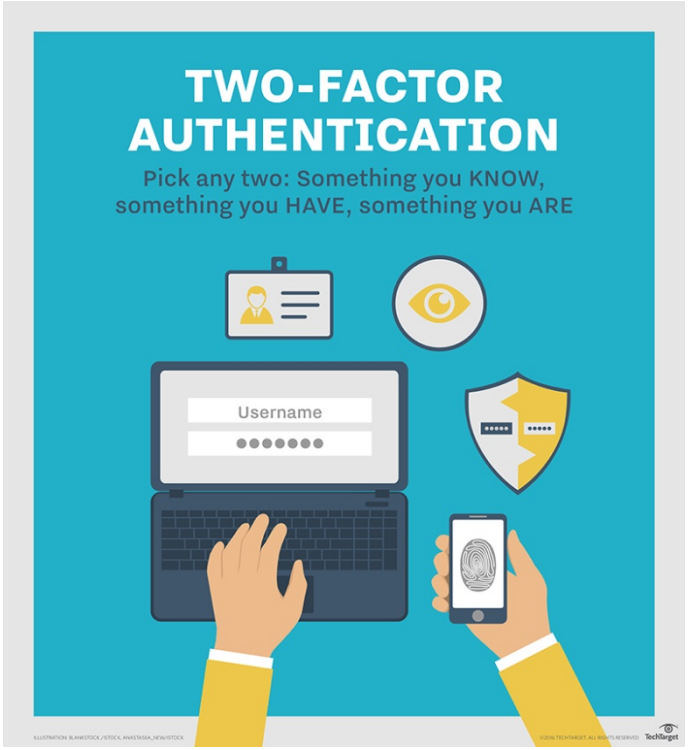
- Le CERMAV :
  - Unité Propre du CNRS
  - Situé sur le campus universitaire de Grenoble
  - Effectif : ~120 personnes
  - Service SI :
    - 3 personnes
    - 6 correspondants informatique
  - ~200 ordinateurs personnels (y compris instrumentation)
    - Principalement sous Microsoft Windows 10
  - ~30 serveurs dont certains en DMZ (Sites web, courriels, DNS)
    - Un domaine active directory avec autorité de certification

Sommaire

Pourquoi faire ?

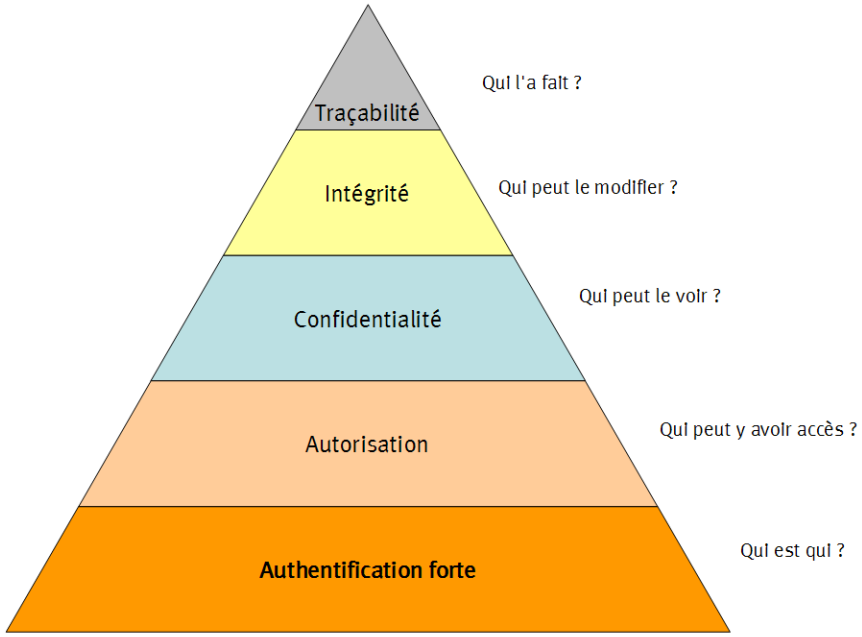
- Deux facteurs
  - Une chose possédée (ex : une carte bancaire), facteur matériel
  - Une chose connue (ex : le code PIN associé), facteur mémoriel
- Sans ces deux facteurs impossible d'utiliser le service protégé





Pourquoi faire ?

- Au CERMAV
  - Sécuriser l'ouverture de session
  - Garantir un accès légitime au réseau
  - Limiter les possibilités d'usurpation de comptes



Sommaire

Comment ?

- En s’appuyant sur :
  - Une carte à puce USB
  - Une structure Active Directory pour la gestion des comptes
  - Une autorité de certification (PKI)
  - Les fonctionnalités d’authentification par carte à puce des postes clients Microsoft Windows

Sommaire

Le matériel

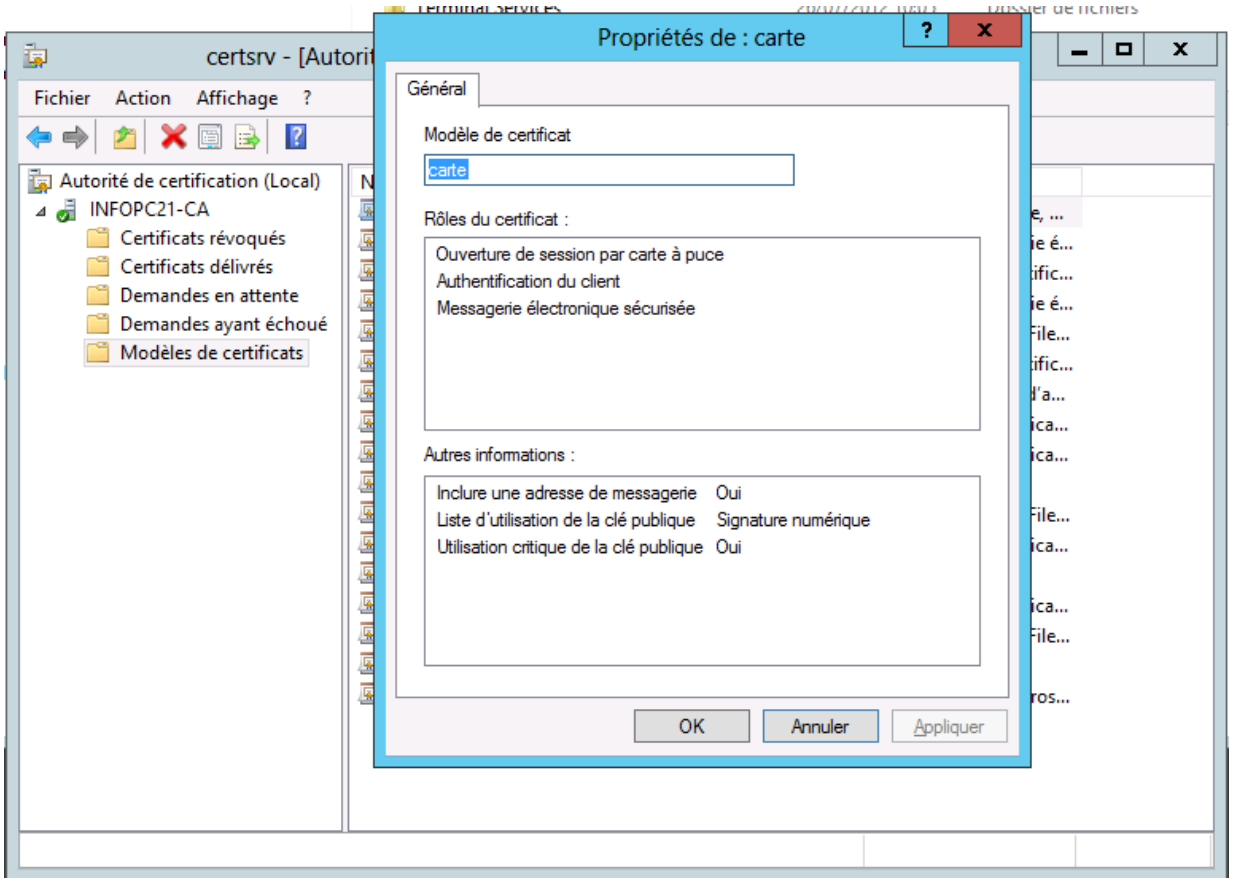
- Fabriquant : Yubico
- Modèle : Yubikey 4
- Prix : ~40€

Size	YubiKey 4
	18mm x 45mm x 3.3mm, 3g
Functions	**YubiKey 4**
Secure Static Passwords	●
Yubico OTP	●
OATH – HOTP (Event)	●
OATH – TOTP (Time)	●
Smart Card (PIV-Compliant)	●
OpenPGP	●
FIDO U2F (Universal Second Factor)	●
Secure Element	●

Sommaire

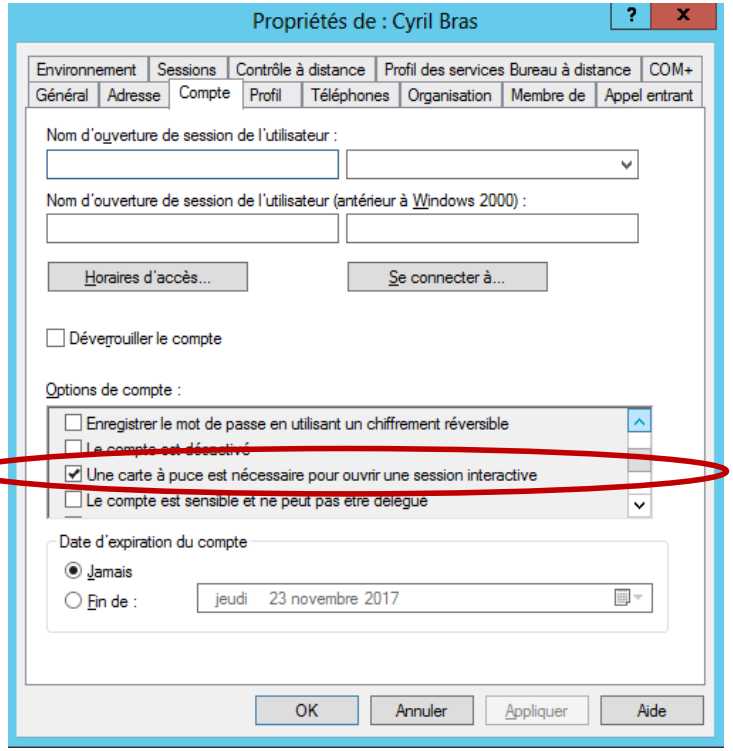
Au niveau d'Active Directory

- Configurer l'autorité de certification
  - Créer un modèle de certificat pour l'ouverture de session par carte à puce



Au niveau d'Active Directory

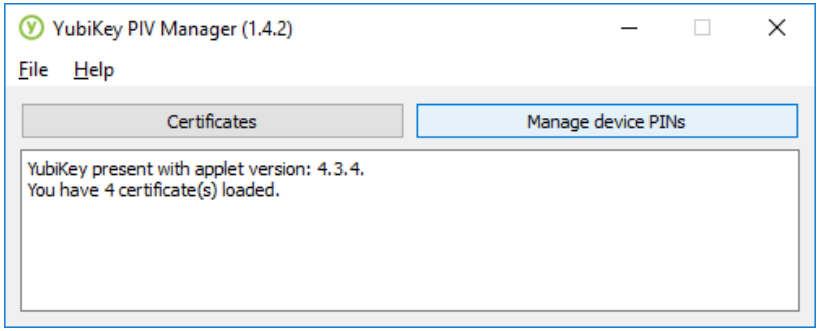
- Au niveau du compte utilisateur
  - Forcer l'ouverture de session par utilisation de carte à puce



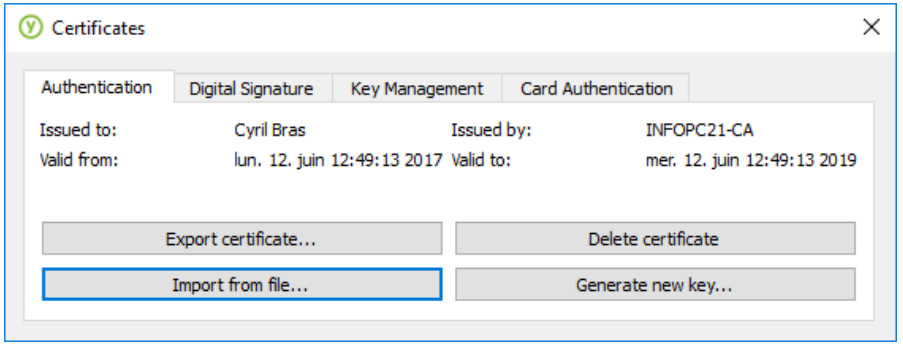
Sommaire

Configuration de la clef

- Nécessite le logiciel Yubikey PIV Manager
  - Définition d'un code PIN de protection

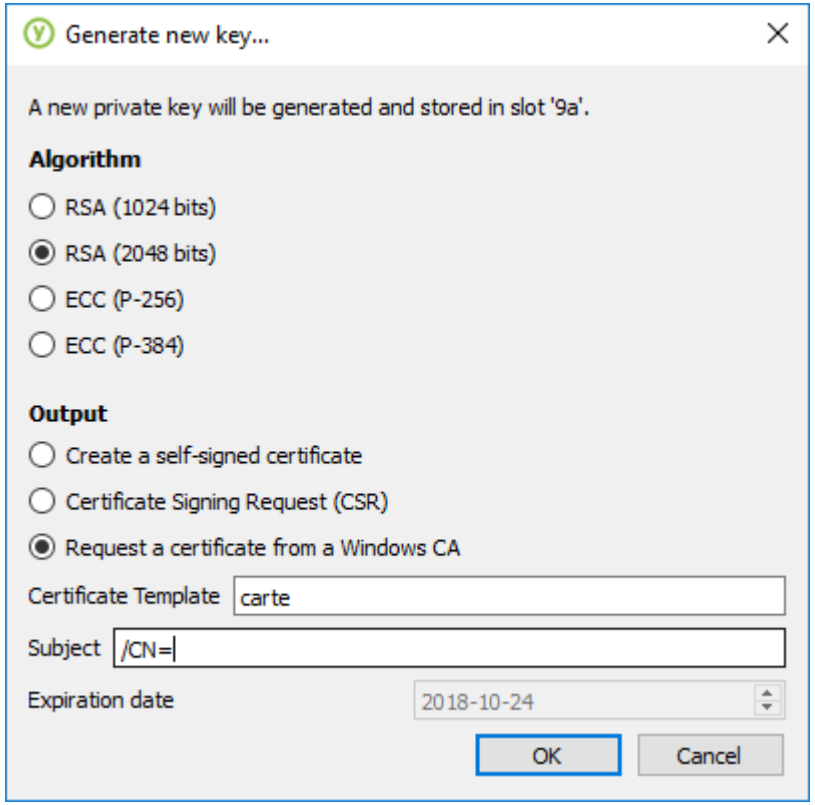


  - Installation d'un certificat
    - Soit depuis un fichier

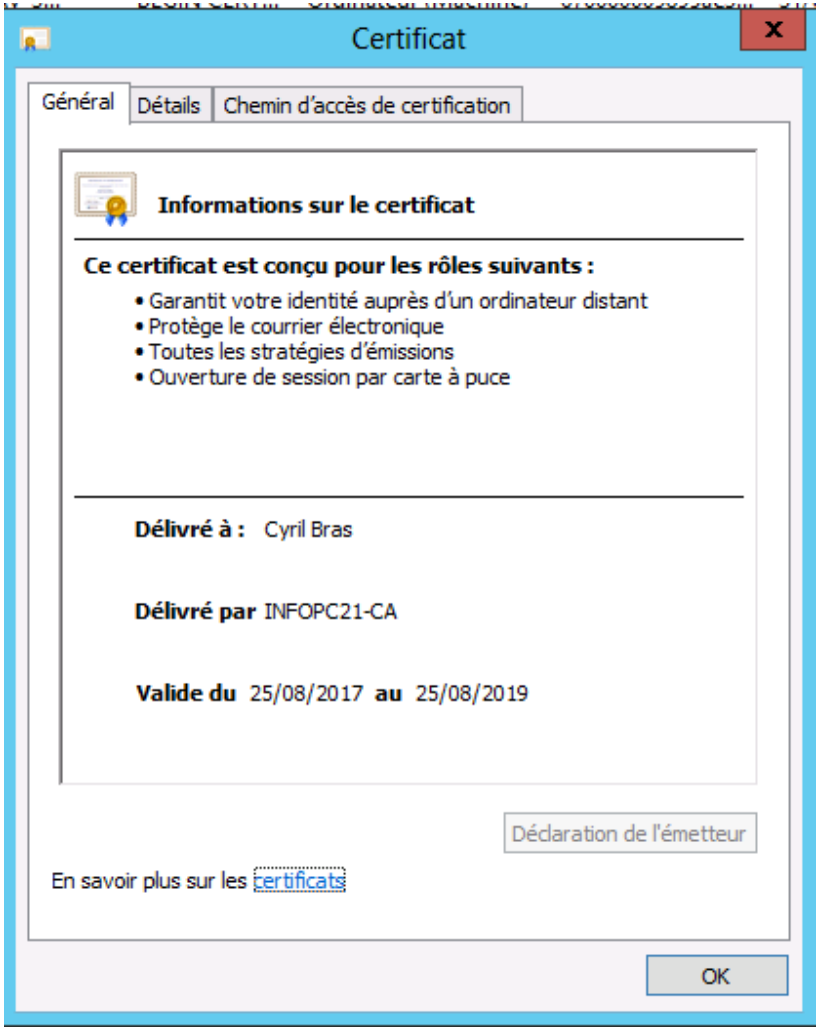


Configuration de la clef

- Soit en générant une demande directement depuis le logiciel

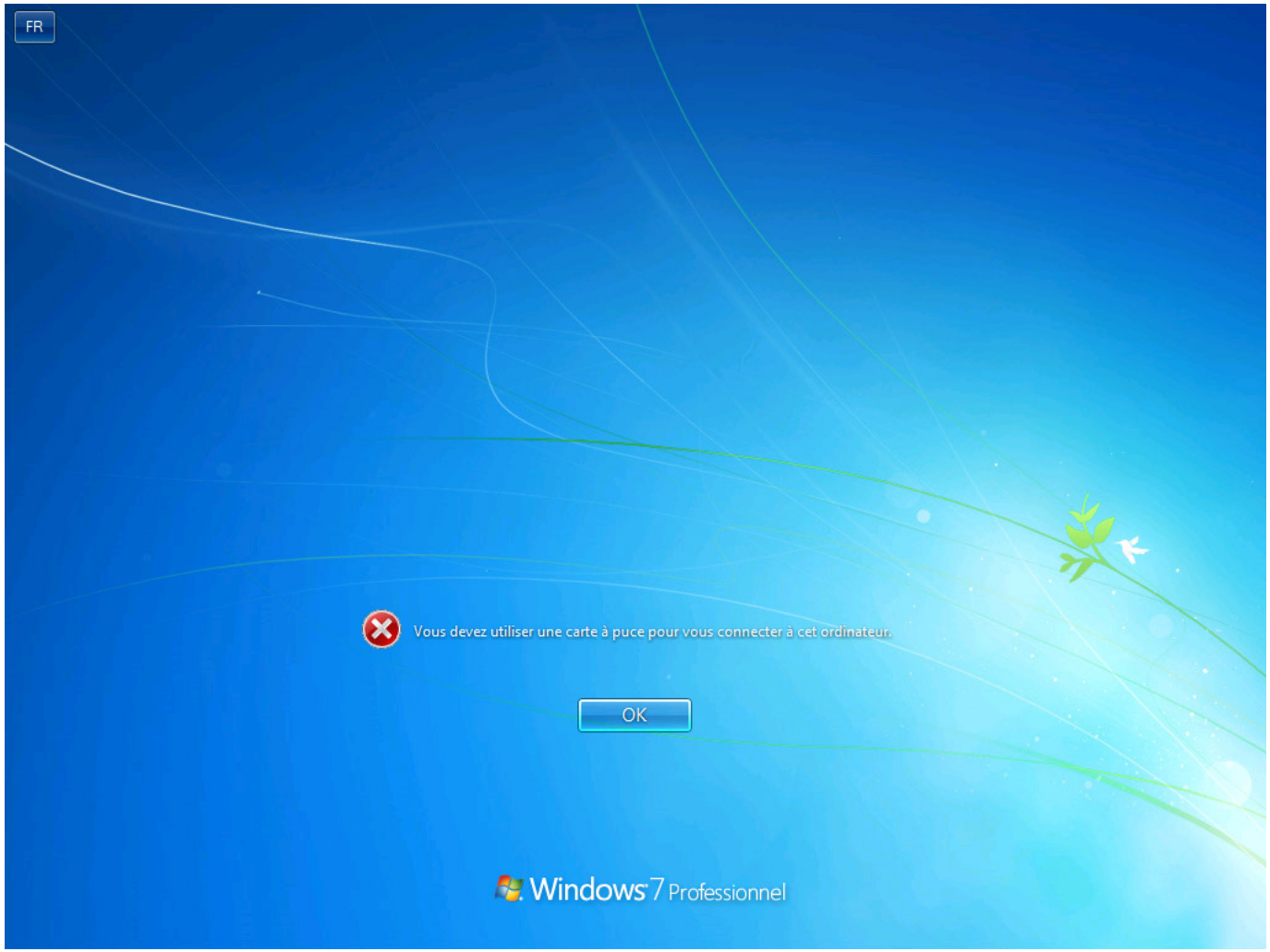


Configuration de la clef



Sommaire

Résultat


FR
Vous devez utiliser une carte à puce pour vous connecter à cet ordinateur.
OK
Windows 7 Professionnel

Résultat

- La saisie du login et d'un mot de passe ne permet plus l'ouverture de session

- L'ouverture de session n'est désormais possible que :
  - Si l'on saisit un nom de compte utilisateur valide
  - Si l'on introduit la clef carte à puce USB
  - Si l'on saisit le code PIN associé à la carte à puce

- En cas de perte de la clef
  - Le code PIN la protège
  - Il suffit de révoquer le certificat

Sommaire

- Contexte
- Pourquoi faire ?
- Comment ?
- Le matériel
- Au niveau d'Active Directory
- Configuration de la clef
- Résultat
- Limitations

Limitations

- Nécessite la présence d'un port USB disponible à l'ouverture de session
- Une connexion au réseau lors de la première utilisation de la clef
  - Ex : ne fonctionne pas sur une tablette puisque impossible d'avoir un port USB et un accès au réseau simultané
- Le code PIN est limité à 8 caractères

Questions ?