

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

Cyril Bras

Journée « Sécu »



Journée « Sécu » 13^{ème} Journée Thématique
du Réseau Min2RIEN



A word cloud graphic featuring various cybersecurity terms. At the top, there's a red padlock icon. Below it, the words 'ANALYSE DE DONNÉES', 'Expertise', 'alertes', 'Authentification', 'EternalBlue', 'Exploit', '2FA', 'Mirai', 'shadow brokers', 'MS7-010', 'PROXY', and 'certificat' are visible. A red key icon is positioned below the word cloud.

09 nov. 2017
Université Lille 1
IEMN - 09h00 à 17h00
Inscription gratuite
sur www.min2rien.fr



Sommaire

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

Sommaire

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

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

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

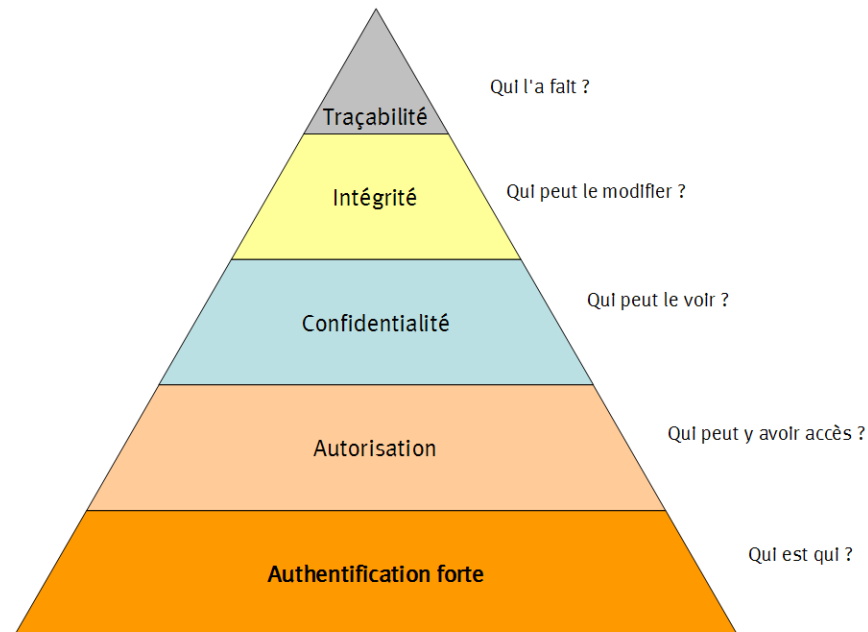
Pourquoi faire ?

- 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

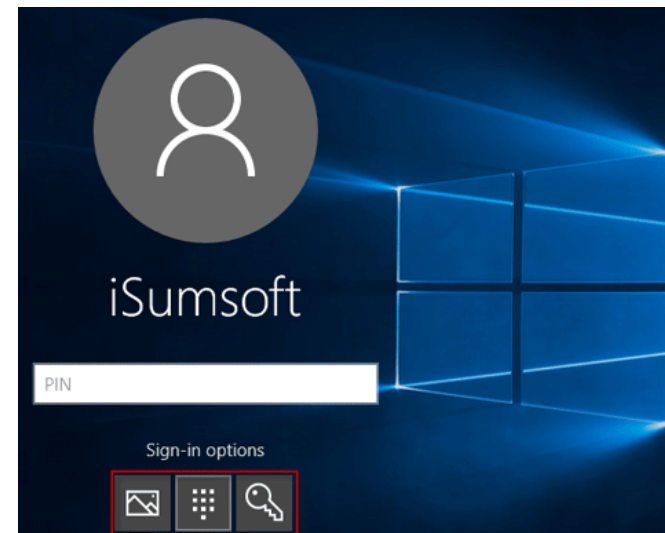


Sommaire

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

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

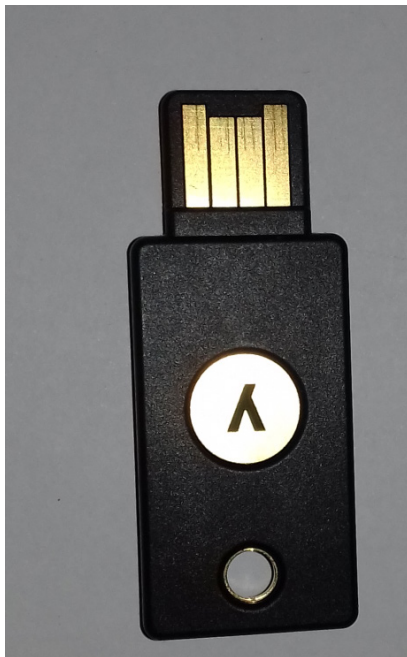


Sommaire

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

Le matériel

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



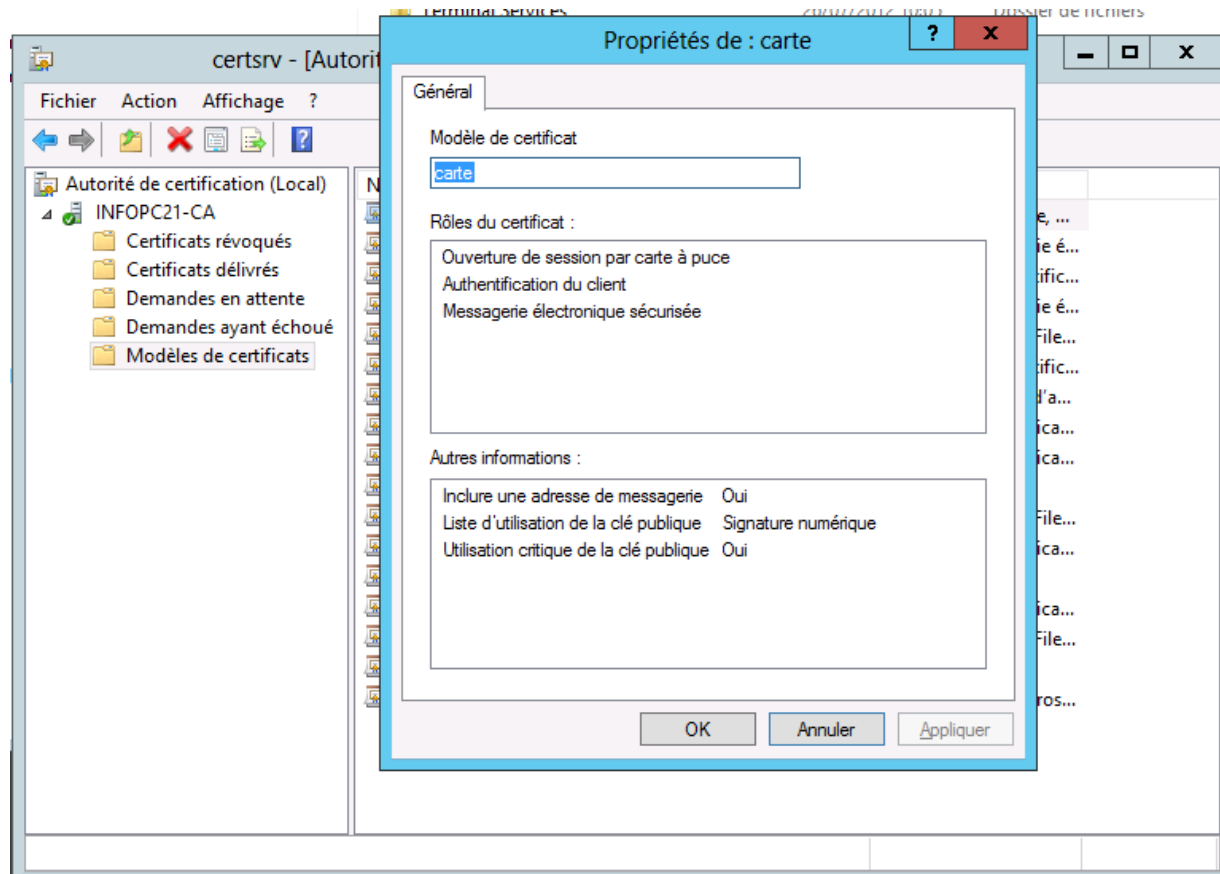
Size	YubiKey 4
	18mm x 45mm x 3.3mm, 3g
Functions	YubiKey 4
Secure Static Passwords	●
Yubico OTP	●
OATH – HOTP (Event)	●
OATH – TOTP (Time)	?
Smart Card (PIV-Compliant)	●
OpenPGP	●
FIDO U2F (Universal Second Factor)	●
Secure Element	●

Sommaire

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

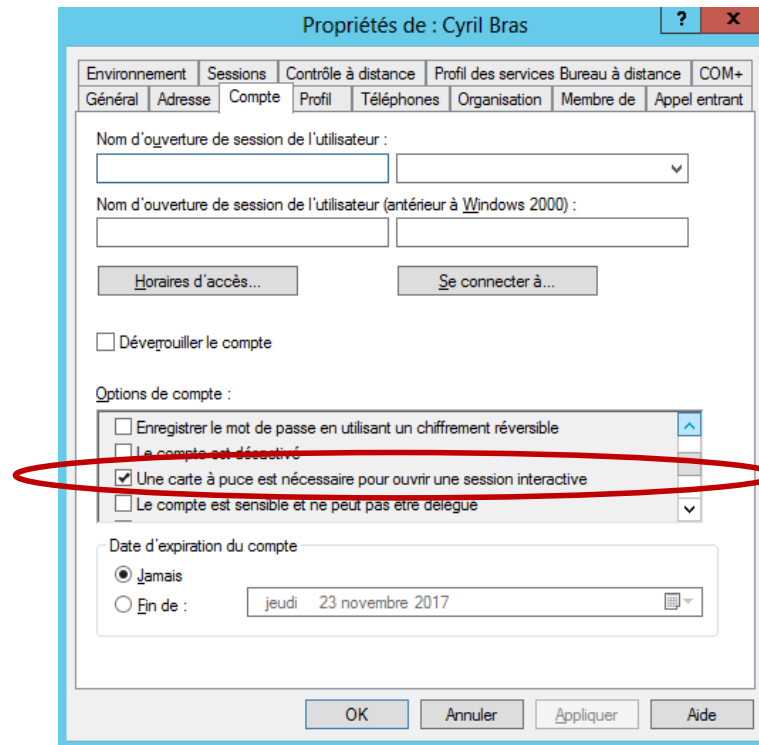
Au niveau d'Active Directory

- 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

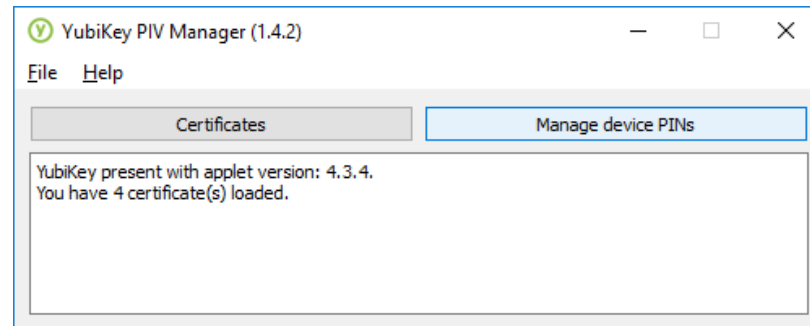


Sommaire

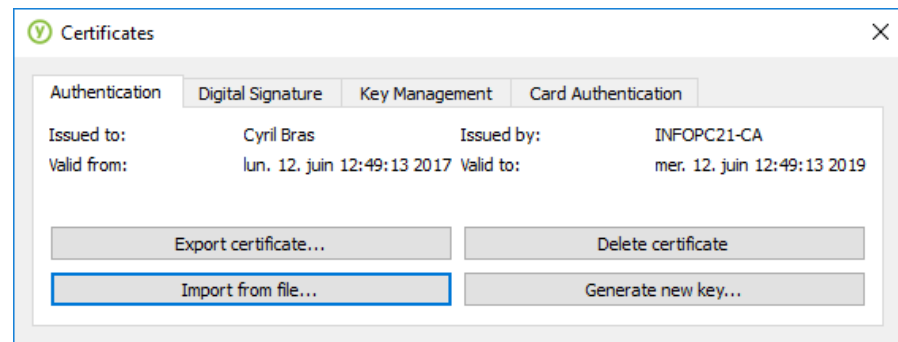
- Contexte
- Pourquoi faire ?
- Comment ?
- Le matériel
- Au niveau d'Active Directory
- Configuration de la clef
- Résultat
- Limitations

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

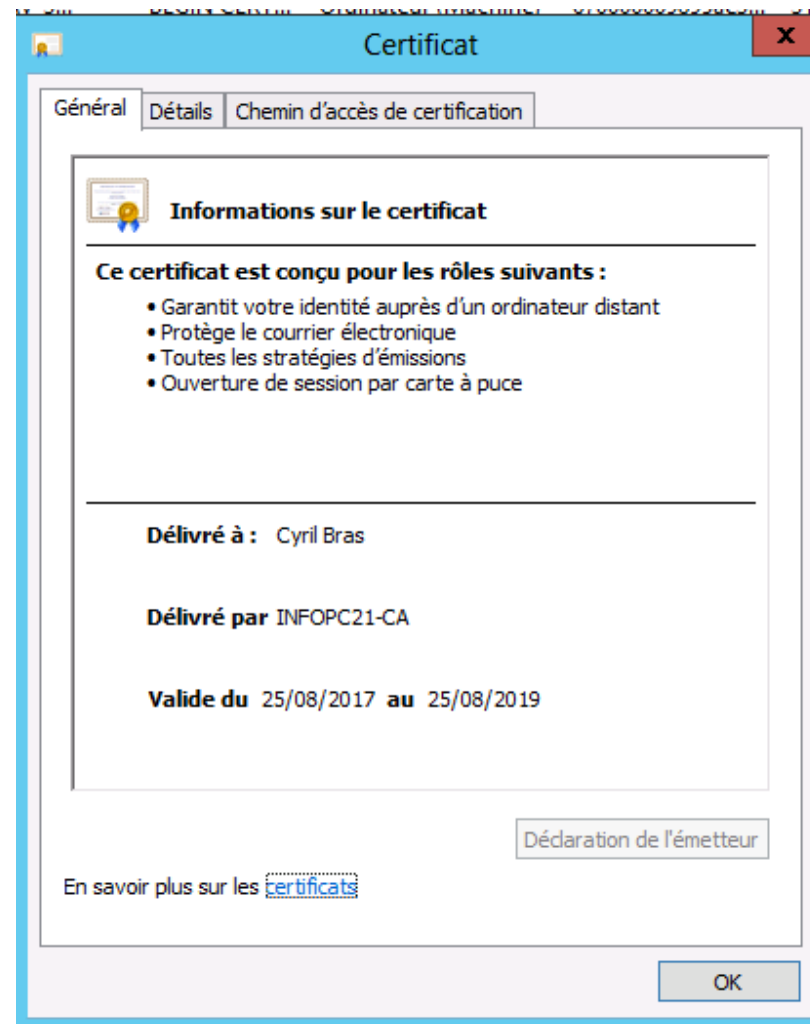


Configuration de la clef

- Soit en générant une demande directement depuis le logiciel

The screenshot shows a dialog box titled "Generate new key..." with a green checkmark icon in the top-left corner and a close button (X) in the top-right corner. The main text inside the dialog states: "A new private key will be generated and stored in slot '9a'". Below this, there are two sections: "Algorithm" and "Output". In the "Algorithm" section, there are four radio button options: "RSA (1024 bits)", "RSA (2048 bits)" (which is selected), "ECC (P-256)", and "ECC (P-384)". In the "Output" section, there are three radio button options: "Create a self-signed certificate", "Certificate Signing Request (CSR)", and "Request a certificate from a Windows CA" (which is selected). Below these options, there are three input fields: "Certificate Template" with the value "carte", "Subject" with the value "/CN=", and "Expiration date" with the value "2018-10-24". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

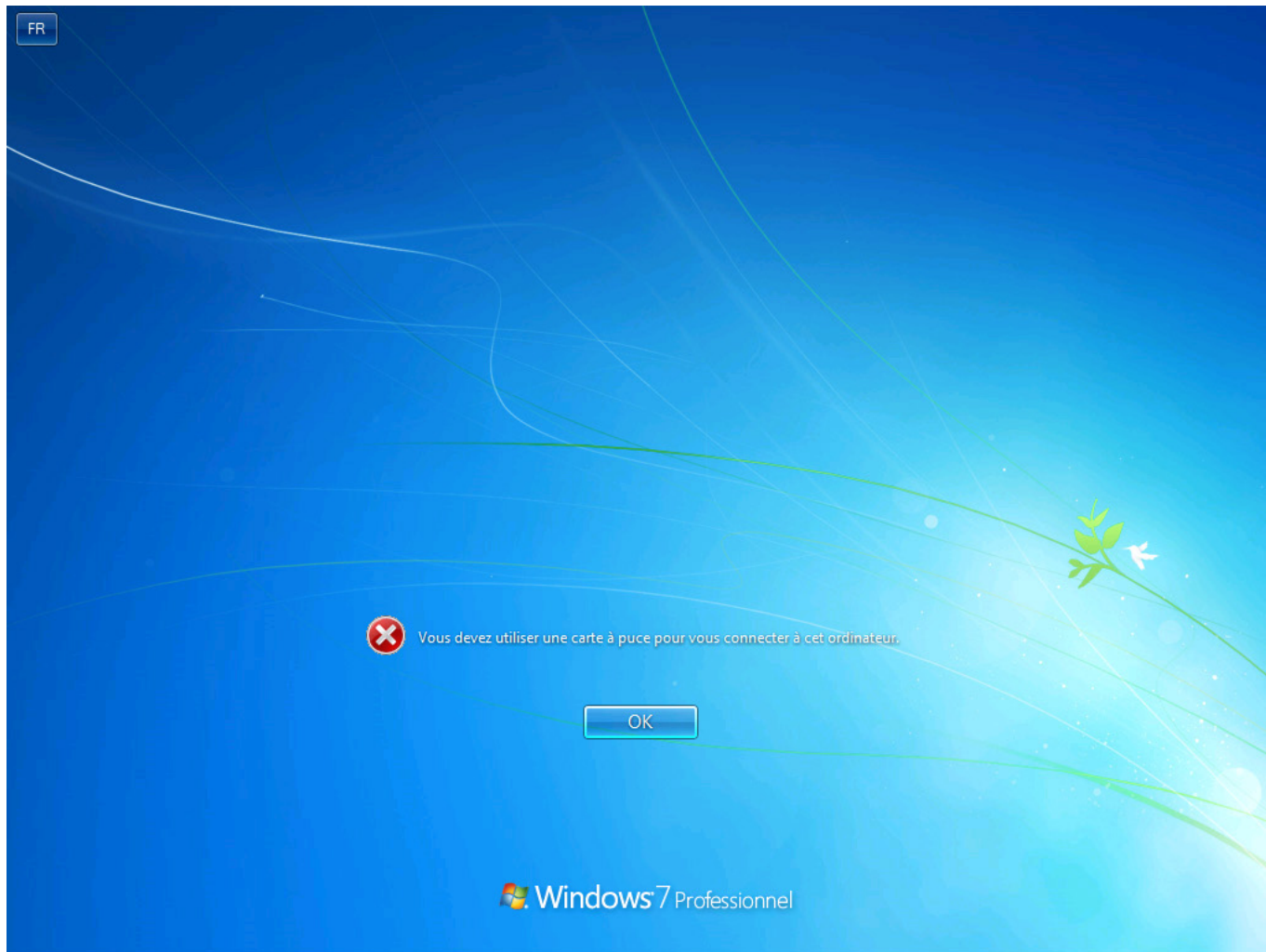
Configuration de la clef



Sommaire

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

Résultat



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 simultanément
- Le code PIN est limité à 8 caractères

Questions ?