Guide d'utilisation YubiKey 4

Master informatique parcours MIAGE

Rédigés par :

Thomas Pélissier

Naoual Mouzouri

Karim Jebara

Solutions matérielles de double authentification

Année 2015 / 2016

Monsieur Courtaud

Table des matières

La YubiKey 4

Définition de la Yubikey 4

La clé YubiKey est un dispositif matériel d'authentification fabriqué par Yubico, qui prend en charge les mots de passe uniques, chiffrement à clé publique et authentification, ceci en utilisant le protocole U2F développé par l'Alliance FIDO. Il permet aux utilisateurs de se connecter en toute sécurité à leurs comptes en émettant des mots de passe uniques ou en utilisant une paire base-FIDO publique / clé privée générée par le dispositif.

La clé YubiKey permet également de stocker des mots de passe statiques pour une utilisation sur des sites qui ne supportent pas les mots de passe uniques. Facebook utilise la clé YubiKey pour les informations d'identification de l'utilisateur, Google l’a prend également en charge. Certains gestionnaires de mot de passe utilisent également la clé YubiKey.

Les dispositifs mettent en œuvre le « One-Time Password », basé sur l’algorithme HMAC (de HOTP) et également sur le « One-Time » basé sur l’algorithme (TOTP). La YubiKey agit sur l’ordinateur comme un clavier qui fournit le mot de passe sur le protocole USB HID.

Les dispositifs de Neo et NEO-n mettent en œuvre le protocole OpenPGP de lecture carte à l'aide des clés RSA de 2048 bits. Ceci permet aux utilisateurs de signer, chiffrer et déchiffrer des messages sans exposer les clés privées pour le monde extérieur. Le dispositif NEO possède aussi un support NFC.

La 4ème génération YubiKey, lancé le 16 Novembre 2015, inclut le support pour OpenPGP avec des clés RSA 4096 bits et support PKCS # 11 pour PIV cartes à puce, une fonctionnalité qui permet la signature de code d'images Docker.

Fondée en 2007 par le PDG Stina Ehrensvärd, Yubico est une société privée avec des bureaux à Palo Alto, Seattle, Stockholm et Londres.

Guide de fonctionnement de la YubiKey 4 de l'entreprise Yubico

Au travers de ce guide, nous allons vous expliquer pas à pas comment configurer votre YubiKey sur un système d'exploitation Windows. Ceci dans l'objectif de verrouiller l'accès à votre session Windows grâce à la Yubikey. Nous vous détaillerons, également les fonctions de sécurité intégrées dans la YubiKey 4.

Configuration requise

Afin de pouvoir suivre ce guide, veuillez vérifier que vous disposez du matériel et dispositif suivant :

- Une clé YubiKey 4 représentée par l'imagine ci-contre.

- Un compte local (pas un compte cloud ou domaine) sur Windows 7, 8, ou 10. Les deux versions (32 comme 64 bits) sont gérées par les deux outils que nous allons utiliser.
  Un compte local signifie que vous vous connectez directement à votre session de l'ordinateur plutôt que de vous connecter à votre Outlook.com ou domaine/compte entreprise.
- Vous devez disposer des privilèges d'administrateur pour installer des applications.

Vous serez amené à redémarrer plusieurs fois votre ordinateur au cours de l'installation, la configuration et les paramétrages de votre YubiKey, veuillez bien respecter les moments où vous devez redémarrer votre ordinateur au risque que la procédure ne soit pas opérationnelle.

1. YubiKey Personalization Tool

1. Introduction

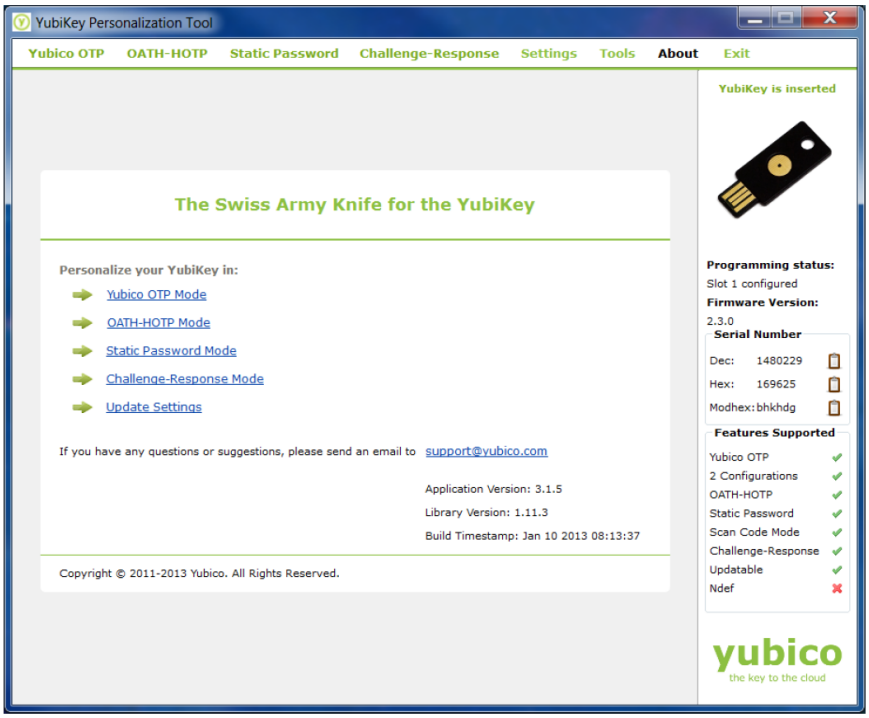
L'outil « Yubico Personalization Tool » (disponible sur le site web de Yubico (ici)) est un outil qui permet aux propriétaires de YubiKey de la configurer dans un format particulier, pour être par la suite utilisée par un autre logiciel (Windows Logon Tool).

Au travers de ce guide, nous allons vous détailler la démarche que nous avons suivie afin de configurer notre YubiKey avec l'aide de l'outil « Yubikey Personalization Tool ».

2. La configuration de la YubiKey

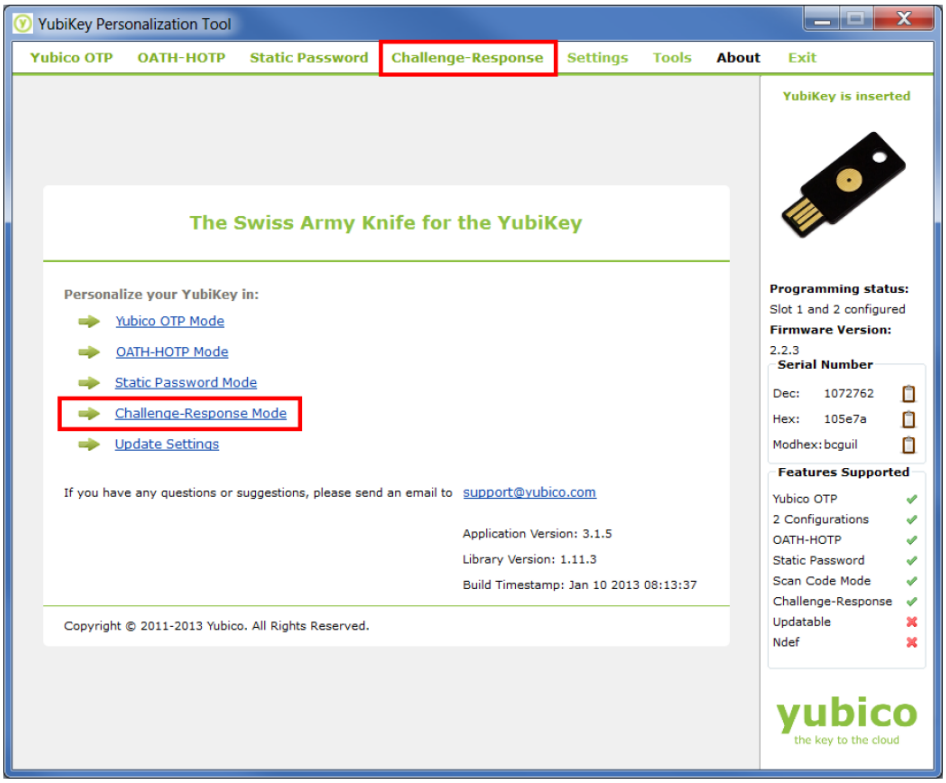
1. Dans un premier temps, si vous ne l'avez pas fait, veuillez télécharger l'outil « Yubikey Personalization Tool » présent sur le site de Yubico dans la rubrique téléchargement (ici). Il existe trois installeurs possibles, veuillez télécharger et installer celui qui correspond à votre système.

2. Une fois l'installation terminée, veuillez insérer votre clé YubiKey dans un port USB de votre ordinateur et lancer l'outil « YubiKey Personalization Tool ».

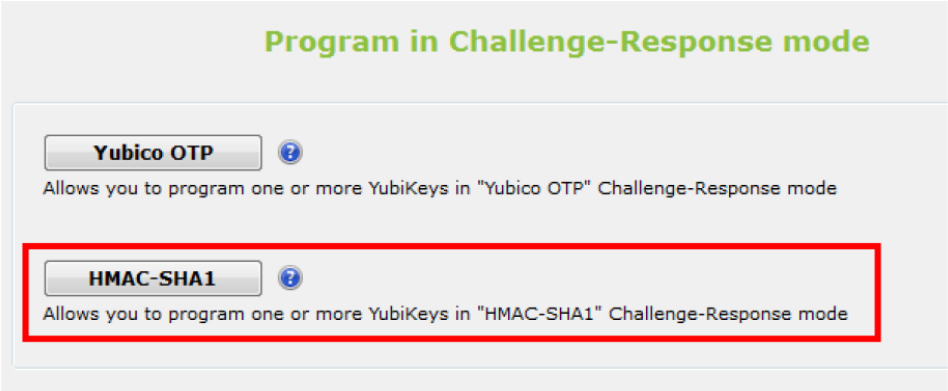


L'outil va détecter votre YubiKey est vous allez voir apparaitre des informations concernant votre YubiKey sur le côté droit de l'outil.

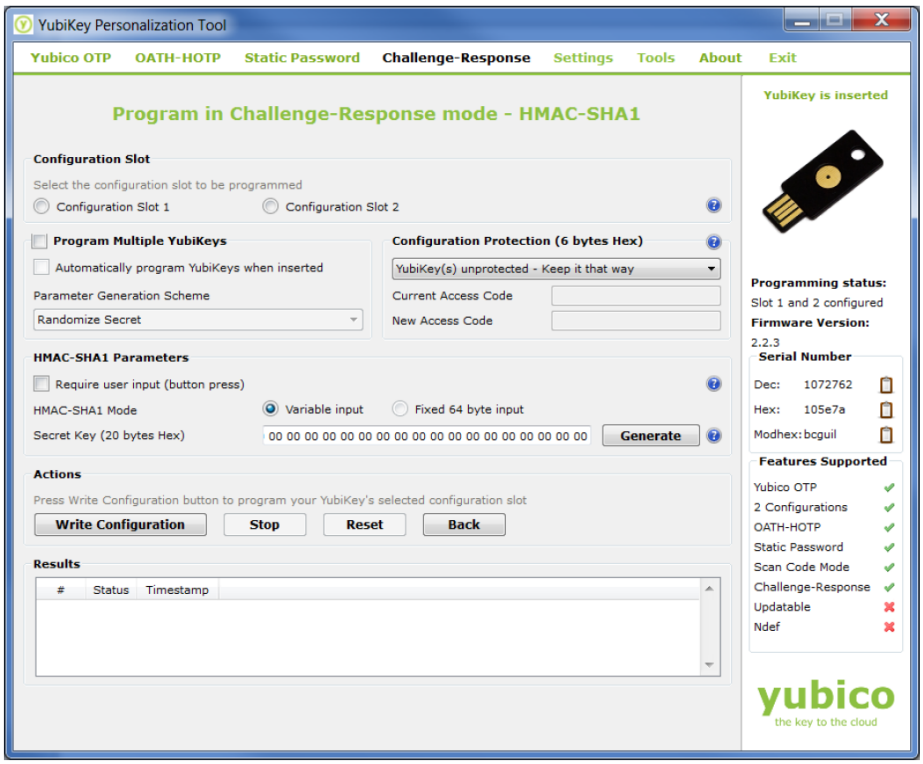
3. Cliquez dans le menu du haut « Challenge-Response » de l'outil ou « Challenge-Response Mode » situé sur la page centrale une fois votre clé YubiKey détectée par l'outil.



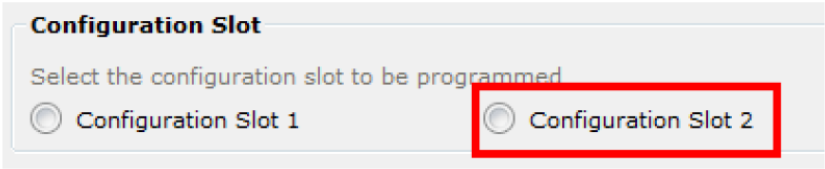
4. Dans le menu «Program in Challenge-Response mode », cliquez sur « HMAC-SHA1 ».



5. La fenêtre ci-dessous va apparaitre.



6. Dans la partie « Configuration Slot » sélectionnez « Configuration Slot 2 ».

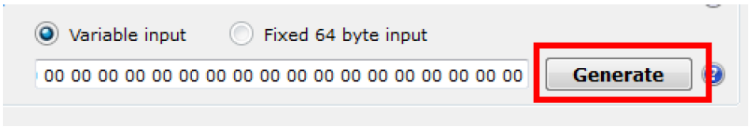


7. Dans la partie « HMAC-SHA1 Parameters » vérifiez que la case « Require user input (button press) est bien décochée.
   Attention : Si cette case est cochée, cela aura pour incidence de bloquer votre système lors de la configuration avec l'outil « Yubikey Logon Administration ».
   Si vous avez bloqué votre système, veuillez-vous référencer à la fin de ce guide.

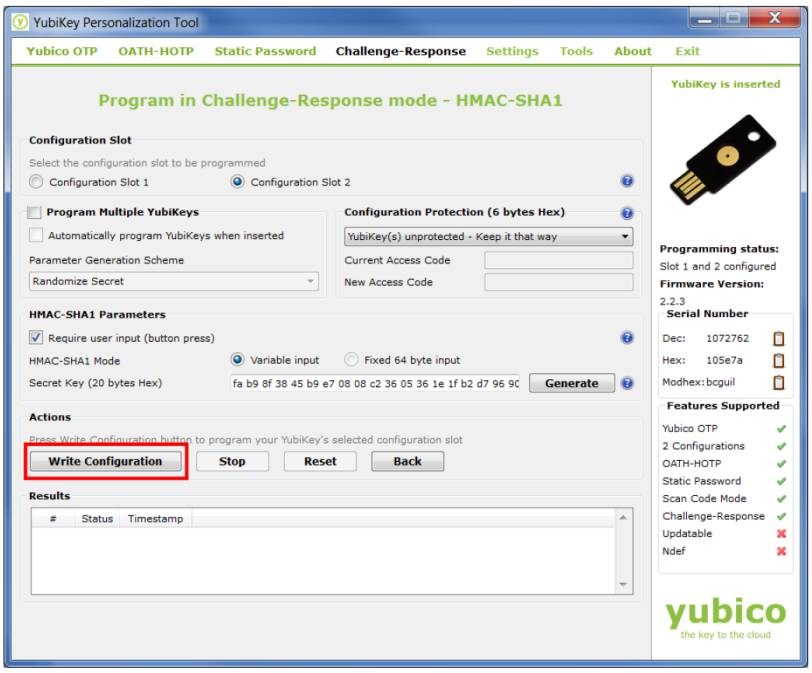
8. Toujours dans la partie « HMAC-SHA1 Parameters » vérifiez que « Variable input » est bien sélectionné.

9. Cliquez sur le bouton « Générer » sur la droite du menu « HMAC-SHA1 Parameters » sur la droite de « Secret Key (20 bytes Hex).

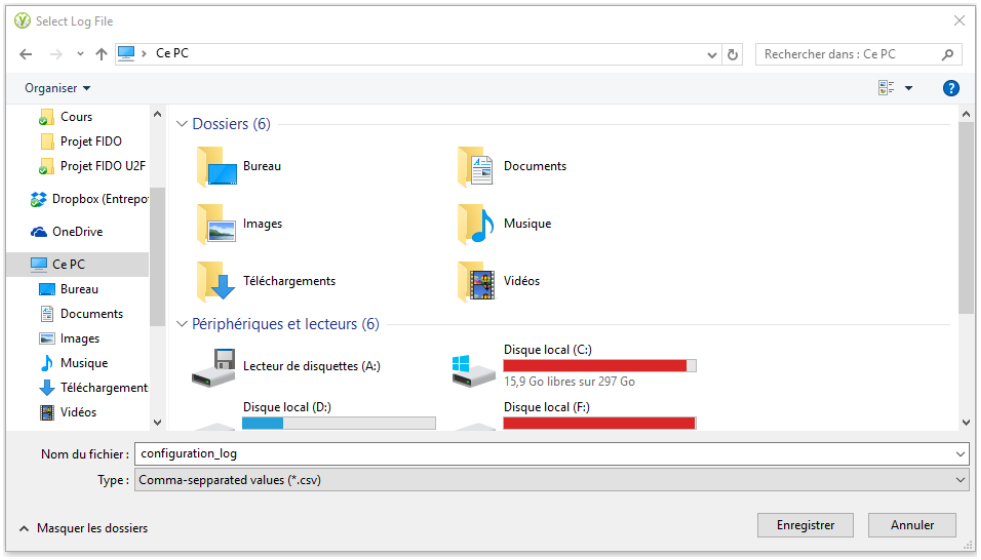
Remarque : Cette clé secrète est essentielle pour procéder à la sauvegarde de votre YubiKey. Veuillez noter cette valeur dans un endroit sûr pour pouvoir générer une YubiKey « backup ».



10. Enfin dans la partie « Actions », cliquez sur le bouton « Write Configuration ». Cela va configurer votre YubiKey pour pouvoir utiliser l'outil « Windows Logon Tool ».

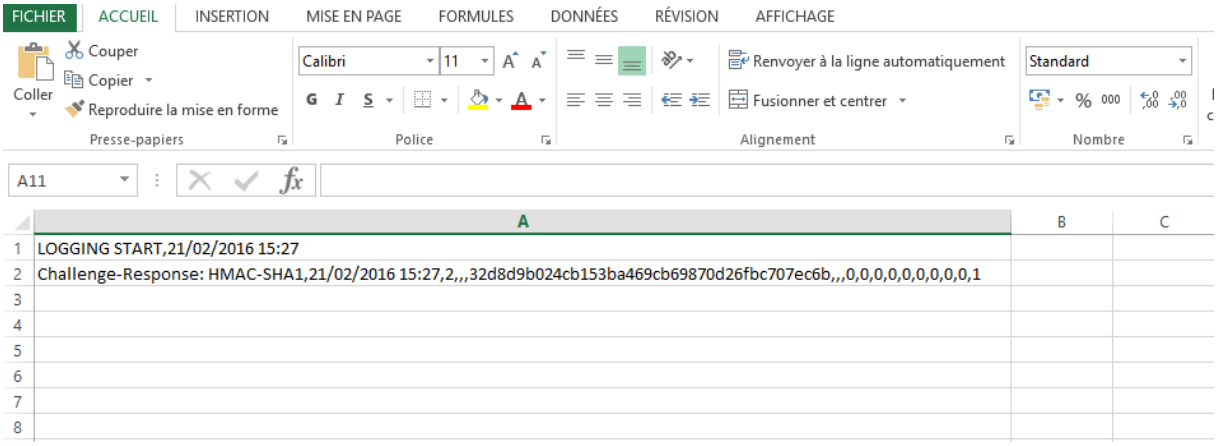


11. Lorsque vous allez cliquer sur « Write configuration » : une fenêtre d'enregistrement d'un fichier « configuration_log.csv » va s'ouvrir. Il est important pour vous de conserver ce document qui contient votre clé secrète générée par l'outil.
Conseil : conserver ce document dans un endroit sécurisé où seul vous avez accès.

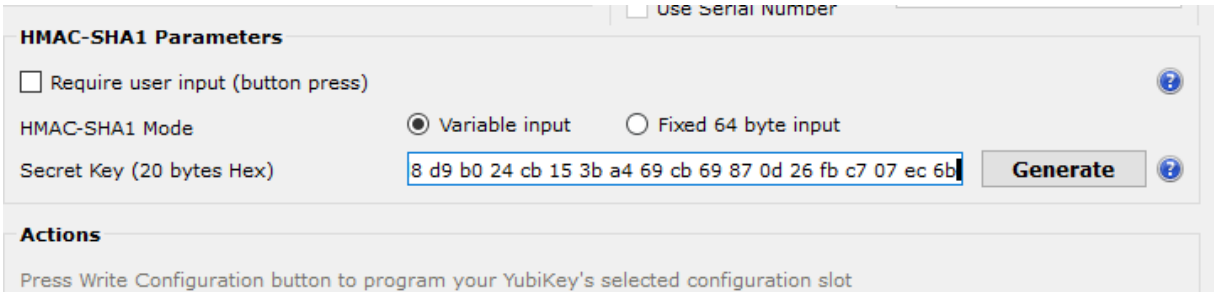


12. Le fichier se présente de la manière suivante :
    Dans notre cas : Challenge-Response:
    HMAC-SHA1,21/02/2016
    15:27,2,,,32d8d9b024cb153ba469cb69870d26fbc707ec6b,,,0,0,0,0,0,0,0,0,0,1

    La partie centrale de cette ligne de texte correspond à notre clé privée générée :
    32d8d9b024cb153ba469cb69870d26fbc707ec6b.



13. Nous vous conseillons de vérifier sur l'outil, que votre clé secrète généré par l'outil est bien la même correspondant à celle présente dans le fichier Excel.
    Ici dans notre cas nous retrouvons sur le fichier Excel et sur l'outil les codes correspondant à : 32d8d9b024cb153ba469cb69870d26fbc707ec6b. C'est donc correct.



2. La configuration de « backup / plusieurs YubiKeys »

Pour utiliser plusieurs YubiKey avec votre mot de passe Windows, ces dernières doivent être configurées avec la même clé secrète.

Pour créer votre backup, il faut appliquer la procédure comme si vous vouliez créer une YubiKey « Primaire » cependant, avant de cliquer sur le bouton « Write configuration » procéder aux ajouts suivants :

1) Dans la partie « Configuration Slot » veuillez cocher la case « Program Multiple YubiKeys ».
2) Cochez la case « Automatically Program YubiKeys when inserted »
3) Dans le menu « Parameter Generation Scheme », cliquez sur la flèche du menu déroulant et sélectionnez « Same Secret for all Keys ».
4) Cliquez sur le bouton « Write Configuration » afin de programmer votre YubiKey « primaire ».

5) Une fois cette YubiKey « Primaire » configurée, veuillez la retirer du port USB et insérer votre seconde YubiKey. Celle-ci sera programmée automatiquement.
6) Si vous désirez créer plus de YubiKeys, dans ce cas répétez l'étape 4 jusqu'à ce que toutes vos YubiKeys soient configurées.

3. Guide d'utilisation de « Windows Logon Tool »

1. Introduction

La société Yubico a créé un outil qui permet de garantir l'accès à une session Windows d'un ordinateur lorsque ce dernier est utilisé en conjonction d'une clé YubiKey ainsi qu'un mot de passe.

Lorsque vous avez correctement configuré votre YubiKey à l'aide de l'outil « Yubikey Personalization Tool » ainsi que vous avez associé un mot de passe à votre session Windows, vous allez pouvoir vous connecter à votre session Windows avec votre mot de passe ainsi qu'avec la clé YubiKey. Ces deux éléments deviennent obligatoires pour accéder au contenu de votre compte ce qui permet d'accroitre la sécurité d'authentification à votre session.

Exemple : nous pouvons imaginer que vous laissiez votre ordinateur sans surveillance dans votre chambre d'hôtel pendant un certain temps. Avant de partir vous avez pris soin de retirer votre clé YubiKey du port USB et la garder précieusement avec vous. Dans le cas extrême ou un individu parvient à rentrer dans votre chambre et tente de forcer votre mot de passe de session, grâce à cette solution, il aura beaucoup plus de difficulté à se connecter à votre session. Ce qui vous permet de garantir une véritable sécurité de vos données.

La société Yubico recommande aux utilisateurs de cette solution de posséder deux clés. Une première clé que l'on pourrait qualifier de YubiKey « primaire », c'est-à-dire celle que vous allez utiliser quotidiennement. Prenons le cas où votre clé devient défectueuse ou que vous l'a perdez. Dans ce cas-ci une seconde clé YubiKey que l'on qualifierait de « back-up » devient essentielle pour pouvoir continuer à vous connecter sur votre session.

2. Fonctionnalités de l'outil

L'outil « Windows Logon Tool » permet aux utilisateurs de verrouiller et sécuriser leur session Windows et empêcher tout accès sans l'utilisation de la bonne YubiKey.

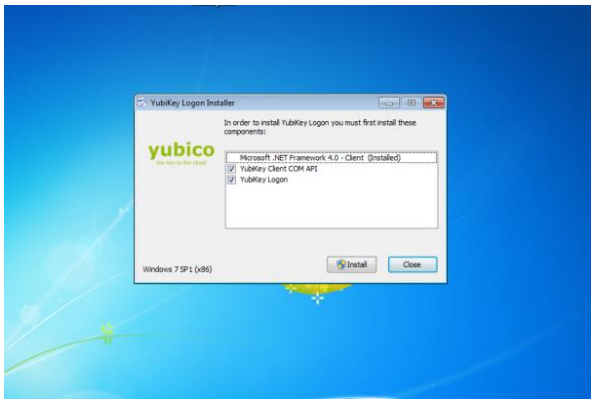
Cet outil permet également d'encrypter votre disque dur. Prenons le cas où vous perdiez votre ordinateur et qu'un individu tente de se connecter à votre session. Il s'aperçoit qu'il ne peut pas accéder à votre session Windows. Il décide alors de démonter votre disque dur pour le brancher sur son ordinateur. Grâce à cet outil, le BIOS de son ordinateur détectera qu'un disque dur est crypté et interrompra totalement la séquence de boot. Le message suivant apparait: "A disk read error occurred. Press Ctrl+Alt+Del to restart". Il devient impossible pour le pirate d'accès à vos données en passant par votre ordinateur ou par un autre et en branchant votre disque comme « slave » sur une carte mère.

4. Installation et configuration de l'utilitaire « Windows Logon Tool»

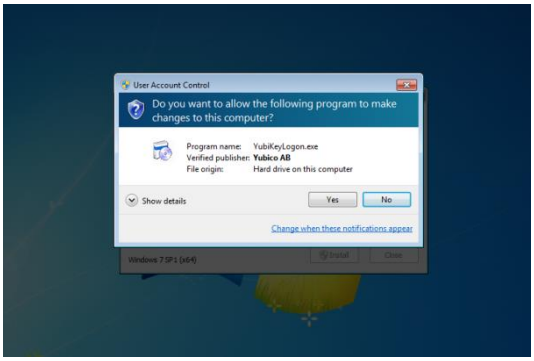
1. Configurez votre YubiKey pour définir le « challenge-response » qui utilise le mode « HMAC-SHA1 » avec entrée variable pour le slot2.

   Pour des raisons de sécurité : Veuillez noter qu'il est impossible de configurer votre YubiKey en mode « challenge-response » en slot 2 et de configurer un « static password » en slot 1 qui contiendrait votre mot de passe Windows. En effet, imaginons qu'une autre personne tente de se connecter à votre session Windows. Si vous avez laissé votre YubiKey dans un port USB, il lui suffirait alors d'appuyer sur le bouton de la YubiKey lorsqu'il est sur la page de connexion de session pour se connecter à votre session Windows, ce qui annule totalement la sécurité de votre authentification. Ainsi, il vous faut donc avoir votre YubiKey configuré dans ce mode ainsi qu'un mot de passe que vous connaissez.

2. Téléchargez le fichier d'installation « Windows Logon Tool » à partir de la page de téléchargement de Yubico en cliquant ici. Pour le moment, cet utilitaire n'est disponible que pour Windows. Il n'existe qu'un fichier d'installation valable pour les versions 7, 8 et 10 de Windows et pour les versions 32 ou 64 bits. Ouvrez maintenant le fichier d'installation et cliquez sur « Installer ».
   Remarque : Ce que vous devez installer est coché. Ces éléments sont installés automatiquement. Il faut impérativement que votre machine soit équipée de Microsoft .Net Framework. Si vous ne l'avez pas, il vous faudra le télécharger vous-même en cliquant ici.

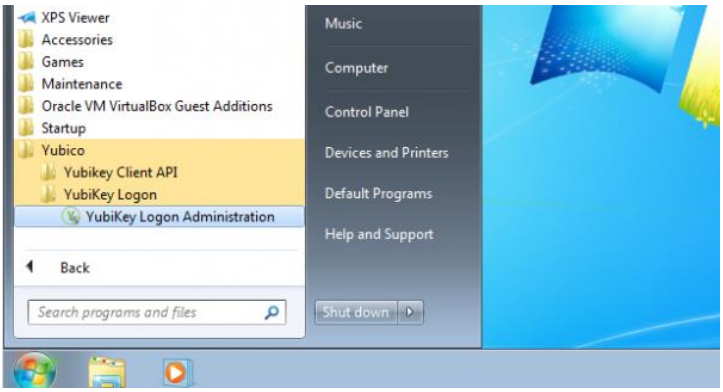


3. Cliquez sur « Oui » dans la fenêtre « User Account Control ».

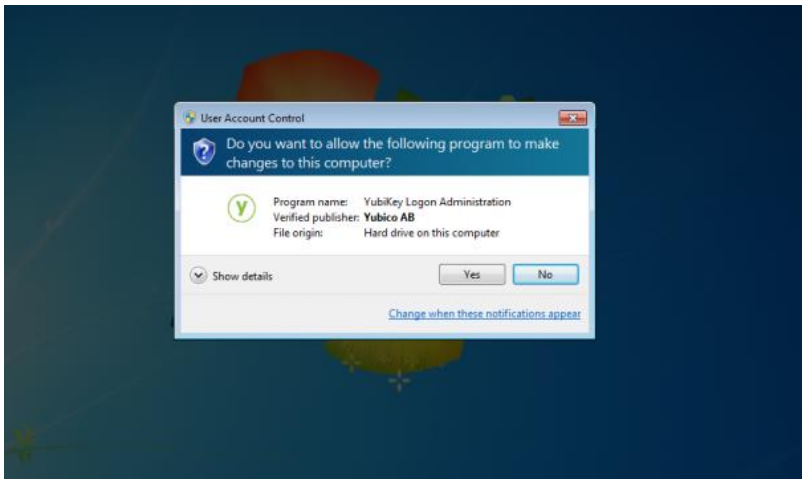


4. Poursuivez l'assistant d'installation.

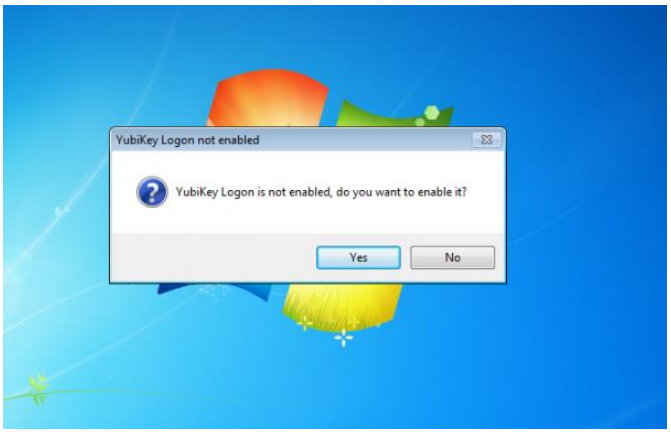
5. Lancez « YubiKey Logon Administration », qui est accessible depuis le menu Démarrer. Vous le trouverez dans le dossier Yubico -> YubiKey Logon -> « YubiKey Logon Administration ».



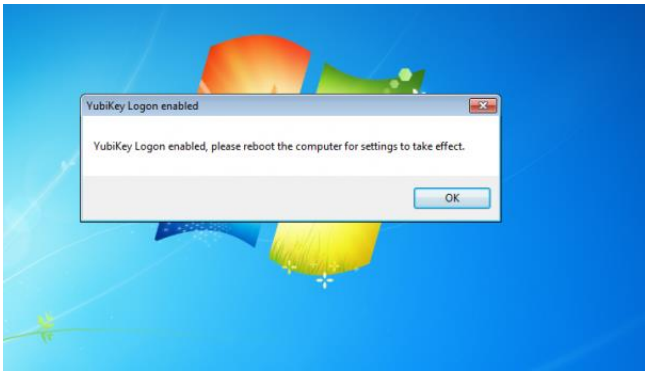
6. Cliquez sur « Oui » dans la fenêtre « User Account Control ».



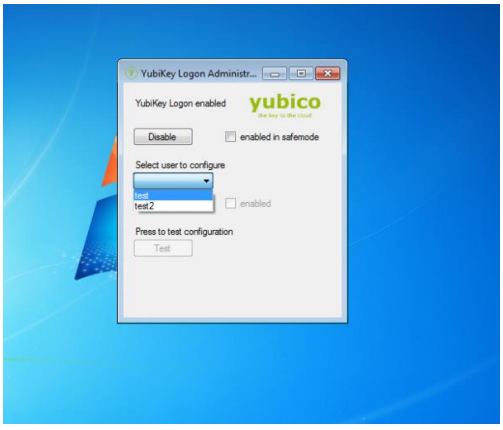
7. Cliquez sur « Oui » pour activer « YubiKey Logon Administration » sur votre ordinateur.



8. Choisissez de redémarrer maintenant ou après l'association de la clé YubiKey avec un utilisateur.

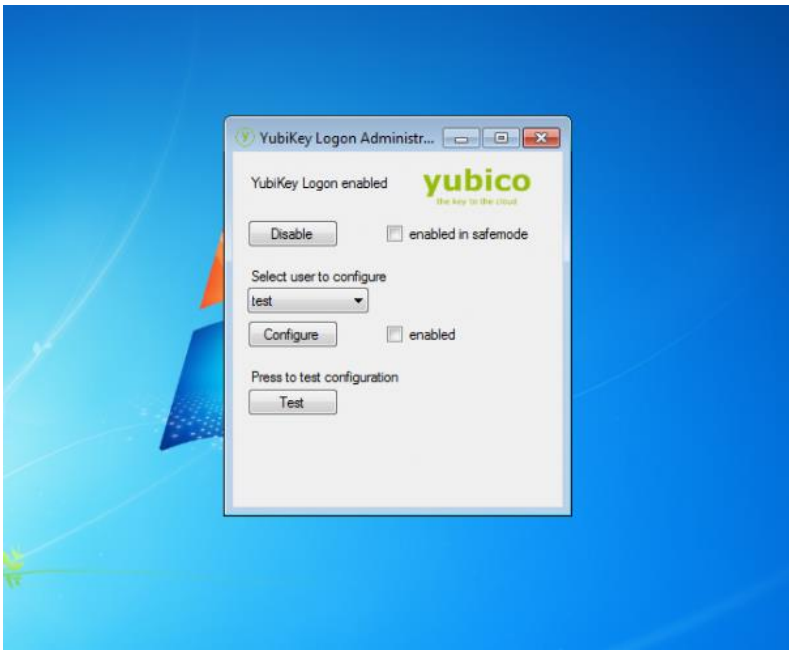


9. Cliquez sur la flèche pour sélectionner l'utilisateur que vous souhaitez configurer dans la fenêtre « YubiKey Logon Administation ».

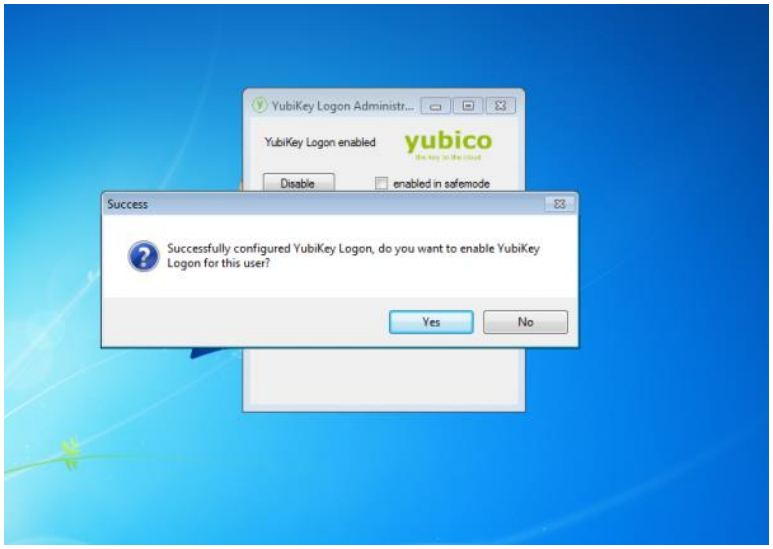


10. Si vous ne l'avez pas déjà fait, veuillez insérer votre YubiKey dans un port USB de votre ordinateur.

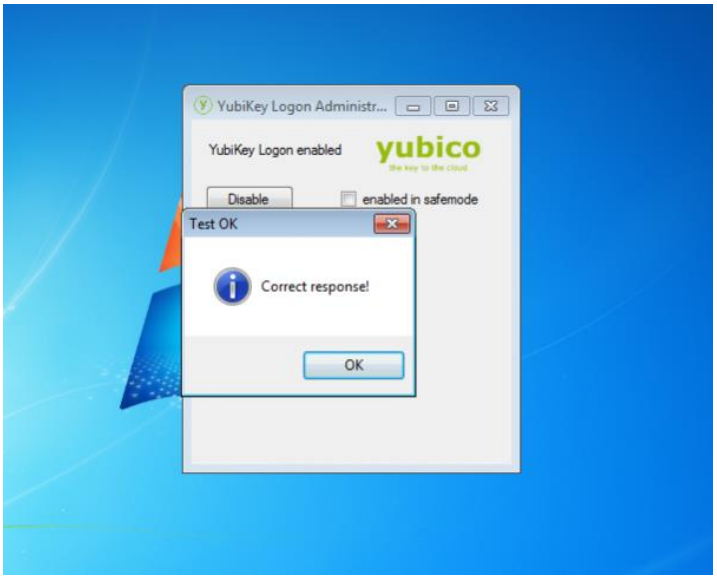
11. Cliquer sur « Configurer ». Il faut également appuyer avec votre doigt sur le bouton de la YubiKey pour que la configuration de votre clé soit réussie.



12. Cliquez sur « Oui » pour permette à « YubiKey Logon Administration » de s'appliquer sur l'utilisateur spécifié.



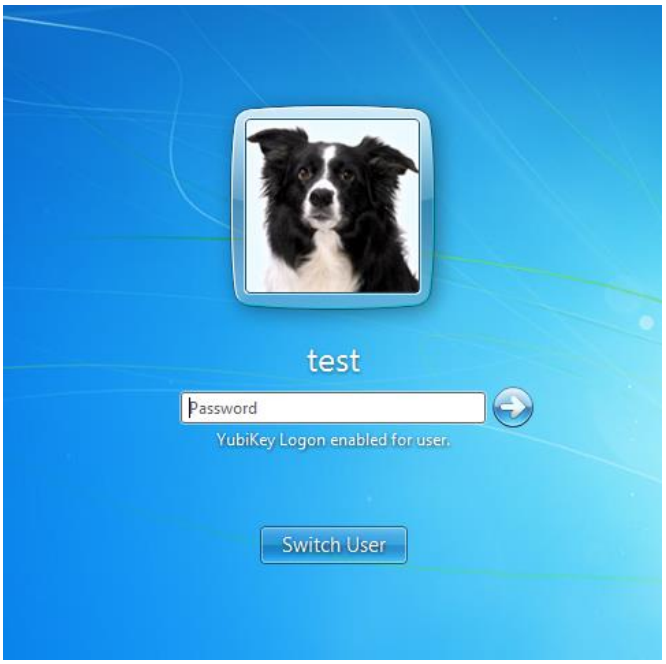
13. Facultatif : Cliquez sur « Test » pour effectuer un test avec la YubiKey. Ceci vérifiera que votre clé a bien été configurée.



14. Si vous ne l'avez pas déjà fait, redémarrer votre ordinateur.

15. Connectez-vous à votre session Windows avec la YubiKey insérer dans un port USB.

Remarque : Entrez votre mot de passe ordinaire et non un OTP de la YubiKey dans le champ de mot de passe. Le « challenge-responsive » aura lieu sans aucune intervention de l'utilisateur.



L'association de votre YubiKey avec votre mot de passe Windows est maintenant opérationnelle. Vous devrez donc vous connecter en saisissant votre mot de passe Windows et brancher votre YubiKey dans un port USB pour vous connecter à votre session.

5. Principe de fonctionnement des différentes configurations possibles de la YubiKey 4

1. Yubico OTP

Un mot de passe unique (OTP) est un mot de passe valable pour une seule utilisation et, une fois utilisé, ne peut pas être utilisé à nouveau pour l'authentification. Un Yubico OTP est une séquence unique de caractères générés chaque fois que le bouton YubiKey est touché. Le Yubico OTP est constitué d'une séquence de 32 caractères Modhex représentant des informations cryptées avec une clé 128 bits AES-128.
L'information qui constitue un Yubico OTP se compose de:

- Un compteur de session
- Un compteur d'horloge
- Un compteur d'utilisation
- Une clé AES interne

À chaque appui sur le bouton présent sur la clé, la YubiKey va émettre une chaine composée de son identifiant ainsi qu'un compteur de session. C'est-à-dire que chaque fois que l'on va brancher notre clé à notre port USB, un compteur va s'incrémenter.

Il y a également au sein de cette YubiKey un compteur « d'horloge ». C'est-à-dire que d'après la documentation technique disponible sur le site de Yubico, ce compteur d'horloge va s'incrémenter avec la caractéristique suivante : incrémentation de 8 toutes les secondes.

Enfin, un compteur d'utilisation de la clé est intégrer dans la YubiKey. Chaque fois que l'utilisateur appui sur le bouton de la clé, alors le compteur s'incrémente. Toutes ces informations sont vérifiées par un CRC16.

```
static unsigned short crc;

void initCrc(void)
{
    crc = 0xffff;
}

void updCrc(unsigned char val)
{
    int i, j;

    crc ^= val;
    for (i = 0; i < 8; i++) {
        j = crc & 1;
        crc >>= 1;
        if (j) crc ^= 0x8408;
    }
}

unsigned short getCrc(const unsigned char *bp, int bcnt)
{
    initCrc();
    while (bcnt--) updCrc(*bp++);

    return crc;
}

unsigned char verifyCrc(const unsigned char *bp, int bcnt)
{
    initCrc();
    while (bcnt--) updCrc(*bp++);

    return crc == 0xf0b8;
}
```

Figure 1 : Algorithme CRC16 conforme à la norme ISO 13239 utilisé par la YubiKey

2. OATH-HOTP

HOTP (HMAC-based One-Time Password) un algorithme défini par l'OATH puis par l'IEFT au sein de la RFC 4226.

HOTP a pour objectif de définir un algorithme d'OTP simple et robuste basé sur une fonction d'HMAC, elle-même basée sur SHA-1. HOTP vise à répondre aux objectifs suivants :

– être basé sur un compteur ou une séquence ;
– être simple à implémenter même avec des ressources limitées (carte à puce) ;
– être utilisable sur des dispositifs ne proposant pas d'entrée utilisateur ;
– produire une valeur générée facilement lisible et manipulable par l'utilisateur ;
– être simple à resynchroniser pour l'utilisateur ;
– être basé sur un secret partagé fort (ie. >= 160 bits).

3. Static Password

Le mot de passe statique est la méthode d'authentification la plus populaire. Il est également le moins sécurisé. Il s'agit par exemple d'un mot de passe que vous allez saisir lors de l'ouverture de votre session Windows / compte Facebook, Google, etc …

4. Challenge-Response :

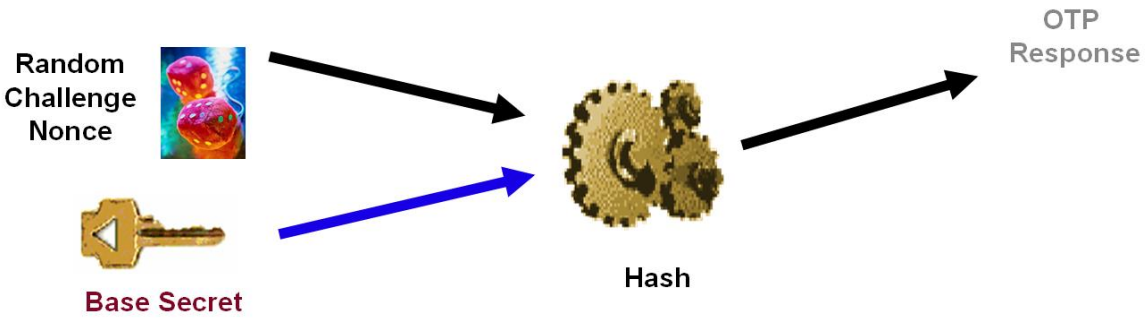


Figure 2 : Représentation du fonctionnement d'un authentifieur fondé sur un mécanisme « Challenge Response ».

Les authentifieurs « défi-réponse » (Challenge-Response) utilisent, en plus du secret partagé, un nombre aléatoire généré par le serveur d'authentification.

Le client reçoit ce « défi » ou « nonce » et répond à celui-ci au serveur. On utilise alors un Code NIP comme deuxième facteur d'authentification. Le code NIP peut être entré sur un clavier. Comme cette technologie utilise un secret partagé, ces authentifieurs ne sont pas capables d'offrir la non-répudiation.

Ces authentifieurs sont définis comme une technologie dite asynchrone, OCRA normalisée par l'« Initiative for Open Authentification» OATH.

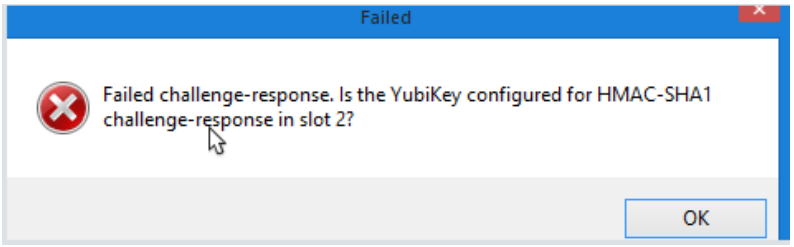
Le mode HMAC-SHA1 crée un HMAC sur 0-64 octet (0-512 bits). Le bloc de données utilise 20 octets (160 bits) de la clé secrète. Comme il n'y a pas de champs générés par le dispositif, la réponse est identique si un deuxième « défi » identique est utilisé.

Éventuellement, le mode « défi-réponse » peut être configurée pour nécessiter une interaction de l'utilisateur par le biais du dispositif en appuyant sur le bouton de la YubiKey afin que la réponse soit envoyée.

Mode défi-réponse ne peut pas être utilisé avec une voie normale OTP ou modes statiques. Lorsqu'il est configuré en mode défi-réponse, seul l'accès à l'API est disponible.

6. Comment désactiver l'application « Yubikey Logon Administration » ?

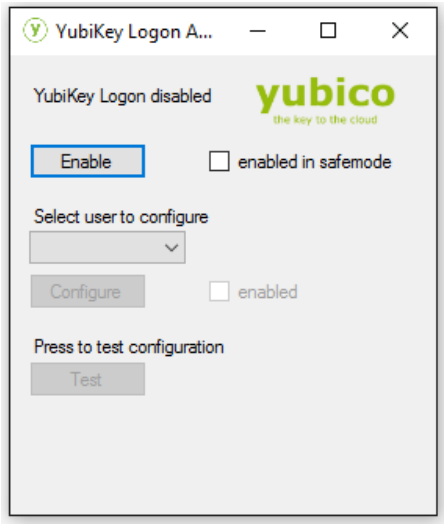
Dans le cas où vous ne parvenez plus à vous connecter à votre session Windows et que vous voyez apparaitre ce message lors de votre connexion :



Dans ce cas, pas de panique, identifiez et suivez l'un des deux cas suivant pour désactiver l'authentification à votre session Windows avec votre Yubikey.

1. Dans le cas où lors de la configuration « enabled in safemode » est désactivée

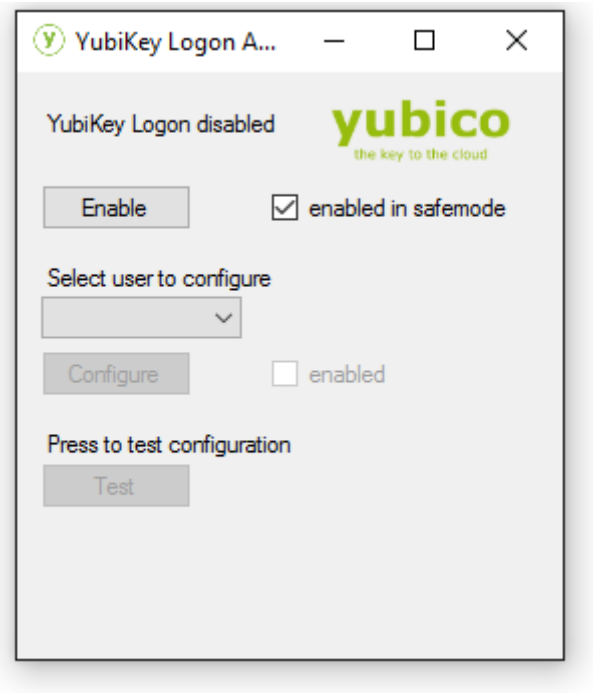
Lors de la configuration de votre Yubikey, si vous n'avez pas coché la case « Enabled in Safemode » comme en témoigne la capture d'écran ci-dessous. Veuillez exécuter la manipulation suivante :



1) Une fois que vous êtes sur la page d'ouverture de session. Maintenez la touche « Shift » et cliquer sur « Rédemarrer ». Vous allez avoir la possibilité de redémarrer votre système en mode sans échec.
2) Une fois que votre ordinateur a redémarré en mode sans échec, veuillez-vous connecter à votre session en utilisant votre mot de passe habituel.
3) Recherchez dans vos programmes, l'outil « Yubikey Logon Administration », exécutez-le.
4) Cliquez sur « Enable » pour désactiver l'outil puis redémarrer. Votre système ne sera plus sous le modèle d'authentification de la Yubikey mais redeviendra une authentification classique : nom d'utilisateur et mot de passe.

2. Dans le cas où lors de la configuration « enabled in safemode » est activée

Lors de la configuration de votre Yubikey, si vous avez coché la case « Enabled in Safemode » comme en témoigne la capture d'écran ci-dessous. Veuillez exécuter la manipulation suivante :



Désactivez YubiKey Logon Administration, lorsqu'il est activé en mode sans échec :

1. Démarrez votre ordinateur avec un disque / clé USB contenant un utilitaire pour modifier le Registre.
2. Mettez la clé "HKEY_LOCAL_MACHINE \ SOFTWARE \ Yubikey \ oauth \ settings \ permis" dans regedit à 0.
3. Redémarrez votre ordinateur et vous serez en mesure d'ouvrir une session sans utiliser votre YubiKey.
4. Lancez l'utilitaire YubiKey Logon administration.
5. Désactivez YubiKey Logon.

7. Des solutions complémentaires

1. La solution de l'entreprise Authasas

L'entreprise Authasas a mis au point un outil similaire à celui de « Windows Logon Tool ». Cet outil, une fois installé et configuré permet aux utilisateurs de YubiKey de s'identifier de la manière suivante :

1. Depuis la page d'ouverture de session Windows, l'utilisateur saisie son mot de passe ;
2. Une vérification du mot de passe va avoir lieux ;
3. Le système d'Authasas va par la suite demander à l'utilisateur d'appuyer sur le bouton de la YubiKey ;
4. Le système d'Authasas va ensuite vérifier après l'interaction avec le bouton de la YubiKey qu'il s'agit bien de la bonne clé YubiKey.

Vous pouvez avoir une visualisation concrète de son fonctionnement grâce au lien ci-dessous :

https://www.youtube.com/watch?v=s-4XSW4iQu

Nous avons tenté de télécharger cette application sur le lien ci-après, cependant il semble qu'à ce jour elle ne soit disponible que pour les entreprises et il est impossible de créer un compte.

http://www.authasas.com/

2. La solution Veracrypt / Truecrypt

Bien que votre disque dur soit crypté, lorsque vous activé votre système avec l'outil « Yubikey Logon Administration ». Vous avez pu constater qu'il est « très simple » de pouvoir désactiver son application.

Imaginons qu'un pirate mette la main sur votre ordinateur, ce dernier, peut avec du temps parvenir à déchiffrer votre mot de passe de session Windows et dans ce cas appliquer les méthodes décrites dans la partie 6 de ce rapport pour interrompre le fonctionnement de l'outil « Yubikey Logon Administration ».

Il existe à ce jour des solutions comme Veracrypt ou Truecrypt qui permette de crypter vos données. On peut facilement imaginer que face à de telles dispositions un pirate, n'arrivera pas ou extrêmement difficilement à décoder votre mot de passe et décrypter vos données.

D'après les informations que nous avons recueillies sur différents forum et sur les récentes documentations en ligne de Yubico (notamment celle-ci (ici)). La mise en place d'une solution avec Truecrypt est à ce jour possible. Cependant il n'est pas possible d'utiliser Truecrypt avec l'outil « Yubikey Logon Administration ». Ainsi, à ce jour il est possible de crypter vos données grâce à la YubiKey mais il n'est alors plus possible de pouvoir s'authentifier sur Windows avec elle. Il semblerait qu'aujourd'hui, une implémentation avec Veracrypt soit impossible ou extrêmement complexe à mettre en œuvre.

Conclusion

L'utilisation de la YubiKey est devenue une alternative très intéressante dans la sécurisation d'une authentification à une session Windows ainsi que la protection des données. Elle permet également de sécuriser les connexions sur des applications distantes comme l'authentification à votre compte Facebook / Google / Github / etc …

A ce jour nous avons cependant décelé des failles de sécurités très importantes. Comment est-il possible que les fonctions proposées par l'outil « Yubikey Logon Administration » soient si facilement désactivables ?

Cependant, nous avons constaté que les détenteurs de YubiKey n'étaient pas uniquement des simples utilisateurs. Comme peut en témoigner le forum de Yubico (ici), les détenteurs sont également acteurs de son développement. Beaucoup d'idées d'amélioration, de corrections d'anomalies sont présentes sur ce forum. On constate également que des entreprises s'intéressent de plus en plus à la YubiKey. C'est le cas de l'entreprise Authasas mais de très grands groupes comme Facebook / Google / Github / etc … qui ont d'ores et déjà implémentés cette solution dans leurs procédures d'authentifications sur leurs serveurs.

L'utilisation de la YubiKey est avant tout un changement d'habitude et des modifications en interne sur le verrouillage de votre session. En effet : un changement d'habitude car vous devez en permanence garder à l'esprit que sans votre YubiKey vous ne pouvez pas déverrouiller facilement votre session Windows. Toujours être conscient de ne jamais laisser votre YubiKey à porter de main d'un inconnu qui pourrait alors facilement s'authentifier sur votre session Windows mais également sur tous vos autres comptes avec lesquelles vous vous êtes synchronisé.
Des modifications internes de verrouillage de votre session : en effet, pour éviter qu'un individu ne puisse facilement se connecter sur votre session, il est intéressant de mettre en place un verrouillage de votre session au bout de quelques minutes d'inactivités.

Cette page de forum (ici) permet de témoigner de l'implication de l'évolution des fonctionnalités de la YubiKey par les utilisateurs. En effet, avec l'aide de l'équipe de Yubico, un utilisateur tente de mettre en place le verrouillage automatique de sa session Windows dès que ce dernier la retire d'un port USB.

Au travers de notre projet, nous avons travaillé sur la 4ème génération de YubiKey. Nous avons pu constater qu'au travers de nos recherches, un très grand nombre de nouvelles fonctionnalités / correctifs ont été amené depuis ces 4 générations.

Il est fort à parier, qu'avec l'intérêt et l'engouement que portent les utilisateurs ainsi que des très grandes entreprises du monde informatique, cette technologie continue à prospérer et dans les mois, années à venir parvient à apporter des fonctionnalités qui seront essentielles pour garantir une protection au quotidien.
La correction de la désactivation de l'outil « Yubikey Logon Administration » en mode sans échec et assurer un cryptage des données d'un disque dur de l'utilisateur ferait de cette solution, une solution incontournable pour des utilisateurs soucieux de protéger leurs données. On peut également envisager que des entreprises soient intéresser par cet apport de solutions. Ce pourquoi aujourd'hui des pontes des entreprises informatiques travaillent sur cette solution afin d'assurer la protection de leurs données afin d'éviter à l'avenir des cas comme Edward Snowden.