h e p i a
Haute école du paysage, d'ingénierie et d'architecture de Genève

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

# MISE A JOUR DES CERTIFICATS ROOT PAR MICROSOFT

**Stéphane Küng**

**19 juin 2014**

*Mise en évidence de l'installation automatique de certificats Root par Microsoft sur un ordinateur Windows 7 (toutes versions) de manière invisible pour l'utilisateur et sans son consentement explicite. Une option existe pour bloquer ce dispositif, mais n'est par défaut pas activée.*

# Table Des matières

## Introduction

Lors d'un test en entreprise, j'ai constaté que malgré l'absence d'un certificat **`Root`** dans le gestionnaire de certificats Windows pour un domaine nouvellement acheté, un site web pouvait quand même s'afficher avec un certificat valide et conforme. Après vérification, le certificat **`Root`** de l'autorité de certification (CA) avait magiquement apparu dans mon gestionnaire de certificats Windows, et ce sans en avoir été informé ou avoir donné mon aval sur son installation.

Le certificat du site web visité n'aurait tout simplement pas dû être validé, car mon ordinateur n'accordait aucune confiance à l'autorité de certification de ce domaine.

## Démonstration

La démonstration est ici effectuée sur ordinateur Windows 7 en version professionnelle équipé d'un Internet Explorer 8. Le site web utilisé ici est celui de la Bank of America https://www.bankofamerica.com en **`HTTPS`** (Figure 1). A noter que toutes les versions de Windows 7 (de Home à Ultimate) sont concernées.

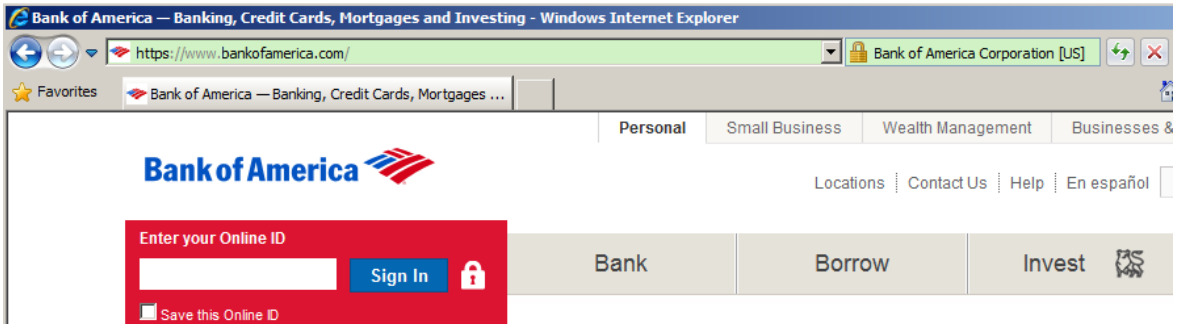


**Figure 1 - Site sécurisé de la Bank of America**

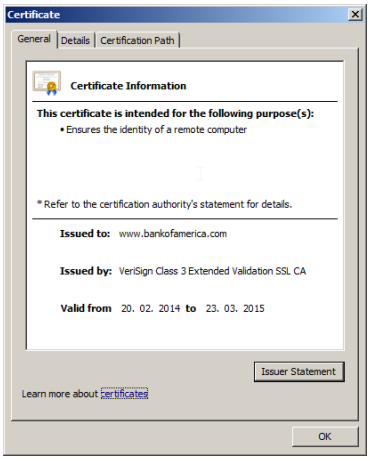


**Figure 2 - Certificat EV de la banque**

Nous commençons par constater que le certificat de ce site web est valide (Figure 2) et nous apercevons également son chemin de certification émanant de VeriSign (Figure 3). Il s'agit d'un certificat EV [1] qui n'est normalement délivré qu'après vérification de l'identité de l'organisme acquéreur.

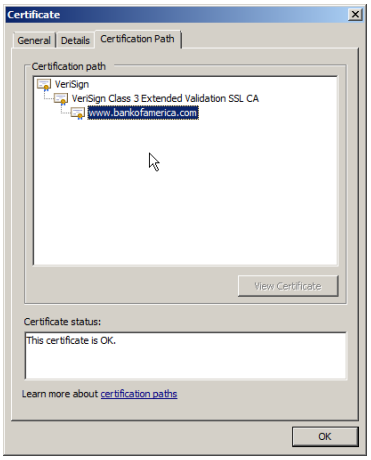


**Figure 3 - Chemin de certification**

Ce certificat **Root** (Figure 4) se trouve bien dans le gestionnaire de certificats Windows (Figure 5) de notre ordinateur. Ces certificats sont installés par défaut avec le système d'exploitation. Le gestionnaire de certificats Windows permet un aperçu global des certificats (du système et des utilisateurs) ce que l'outil d'aperçu des certificats **Root** d'Internet Explorer ne permet pas. Il permet également de créer des CSR ainsi que des certificats autosignés.

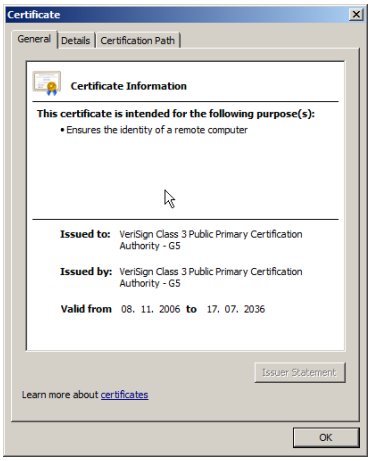


**Figure 4 – Certificat Root de VeriSign**

Nous sélectionnons ensuite tous les certificats **Root** se trouvant dans le **dossier Trusted Root Certification Authorities** et les supprimons (Figure 6).

```
Menu : Démarrer
Exécuter : certmgr.msc
```

**Figure 5 – Gestionnaire de certificat Windows**

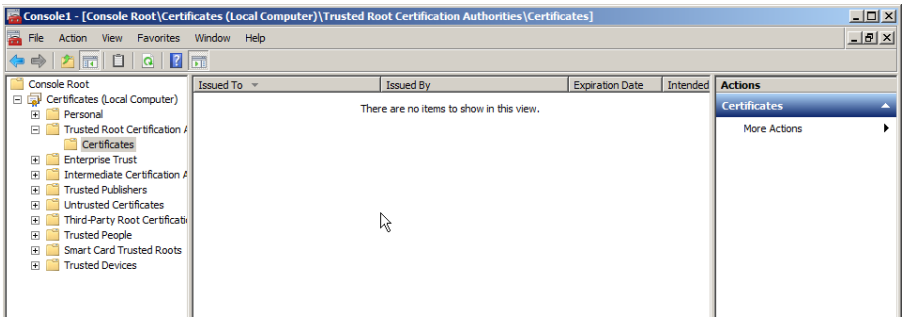


**Figure 6 - Dossier nettoyé des certificats Root (Thrusted Root Certification Authorities)**

[1] Extended Validation (Vérification de l'identité de l'acquéreur)

Nettoyons ensuite le cache SSL du navigateur Internet Explorer (Figure 7 et 8). Le but ici est de forcer le navigateur à revérifier le chemin de certification pour chaque site visité.

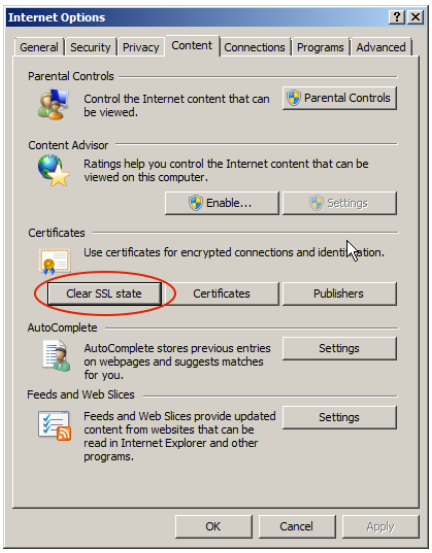


Figure 7 - Option pour vider le cache SSL

```
Menu : Outils
Options : Internet
Onglet : Contenu
Bouton : Vider le cache SSL
```

Figure 8 - Procédure pour vider le cache SSL d'Internet Explorer 8

Actualisons ensuite la page d'accueil du site https://www.bankofamerica.com. Nous constatons déjà qu'aucune erreur n'est apparue, que la barre d'adresse est verte (certificat EV valide) et que son certificat est validé. Rafraichissons le dossier **`Trusted Root Certification Authorities`** dans le gestionnaire de certificats Windows. Nous constatons immédiatement l'apparition de quatre nouveaux certificats **`Root`** : deux VeriSign, un Equifax et un DigiCert (Figure 9).

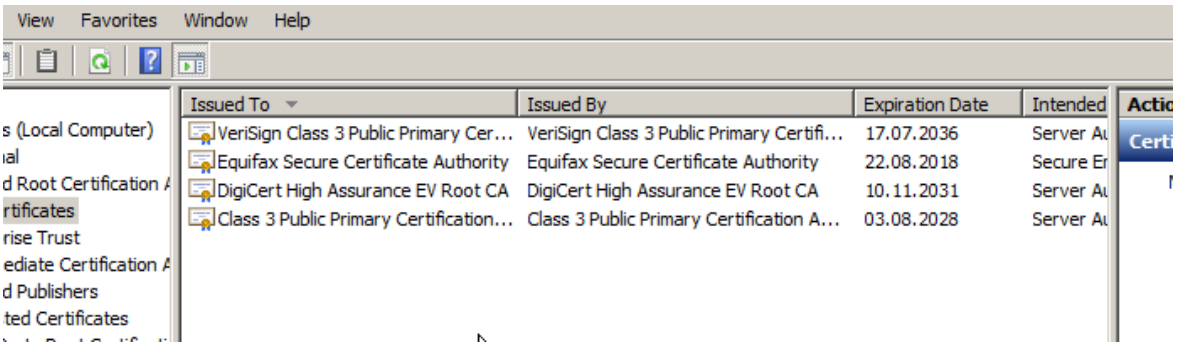


Figure 9 - Les quatre nouveaux certificats Root

## Fonctionnement

Lançons maintenant Wireshark pour analyser les paquets d'une requête **HTTPS** vers le site https://www.bankofamerica.com. Nous remarquons assez rapidement que notre ordinateur, lors de la requête, se connecte sur le site de VeriSign et reçoit un paquet (Paquet N° 50 sur la Figure 10) contenant 3 certificats de manière non chiffrée.

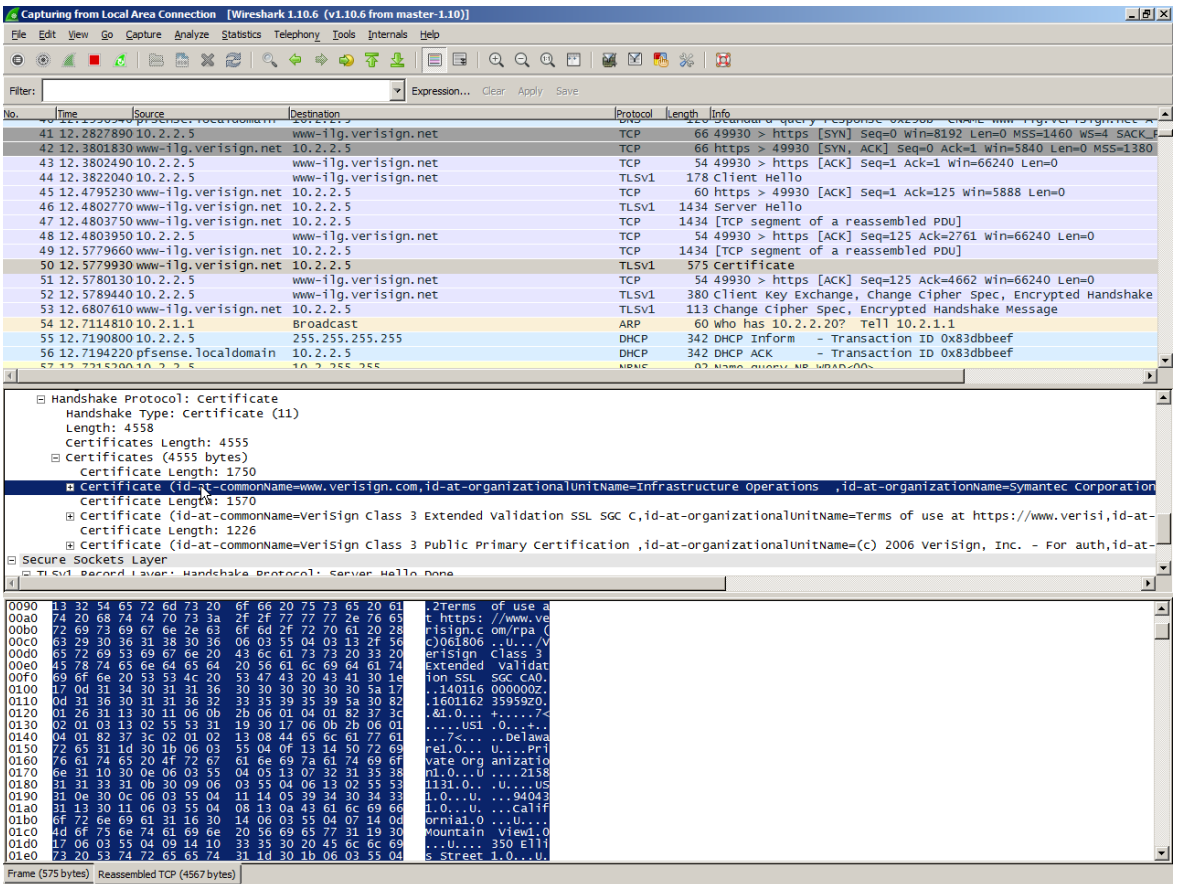


**Figure 10 - Réception des certificats Root**

Les paquets suivants étant chiffrés, nous supposons que le dernier certificat est récupéré ici.
Si aucun élément récupéré ici ne permet de montrer comment VeriSign est intervenu ici, nous pouvons penser qu'un lien vers le site de VeriSign est codé en dur dans la machine.

Deux points nous permettent d'affirmer ceci :

1. Il serait beaucoup trop facile d'autosigner un certificat pour un site web et d'inclure un lien qui forcerait Windows 7 à installer ce certificat **Root** dans son gestionnaire de certificats de manière transparente.
2. Si le CA n'est pas VeriSign, la procédure passe par un téléchargement du certificat au travers de Windows Update et non pas directement sur le site du CA.

En effet, après divers essais, nous avons constaté que si le certificat **Root** d'un domaine n'est pas VeriSign, mais par exemple GoDaddy[2], et que ce dernier n'existe pas dans le gestionnaire de certificats Windows ou qu'il a été supprimé par manque de confiance. Une connexion est directement établie vers le serveur www.download.windowsupdate.com pour récupérer le certificat **Root** manquant. Ce dernier est automatiquement installé dans le gestionnaire de certificats (Figure 11), et la page web s'ouvre ensuite sur le site web. Cette récupération du certificat se fait également au travers d'une connexion non chiffrée comme le laisse apercevoir la capture Wireshark (Packet N° 53 sur la Figure 12) sur lequel le lien de téléchargement est clairement visible et exploitable (Figure 14)

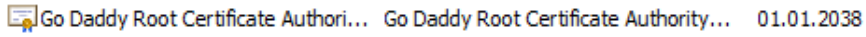


**Figure 11 - Le certificat Root GoDaddy est installé dans le gestionnaire de certificats Windows**

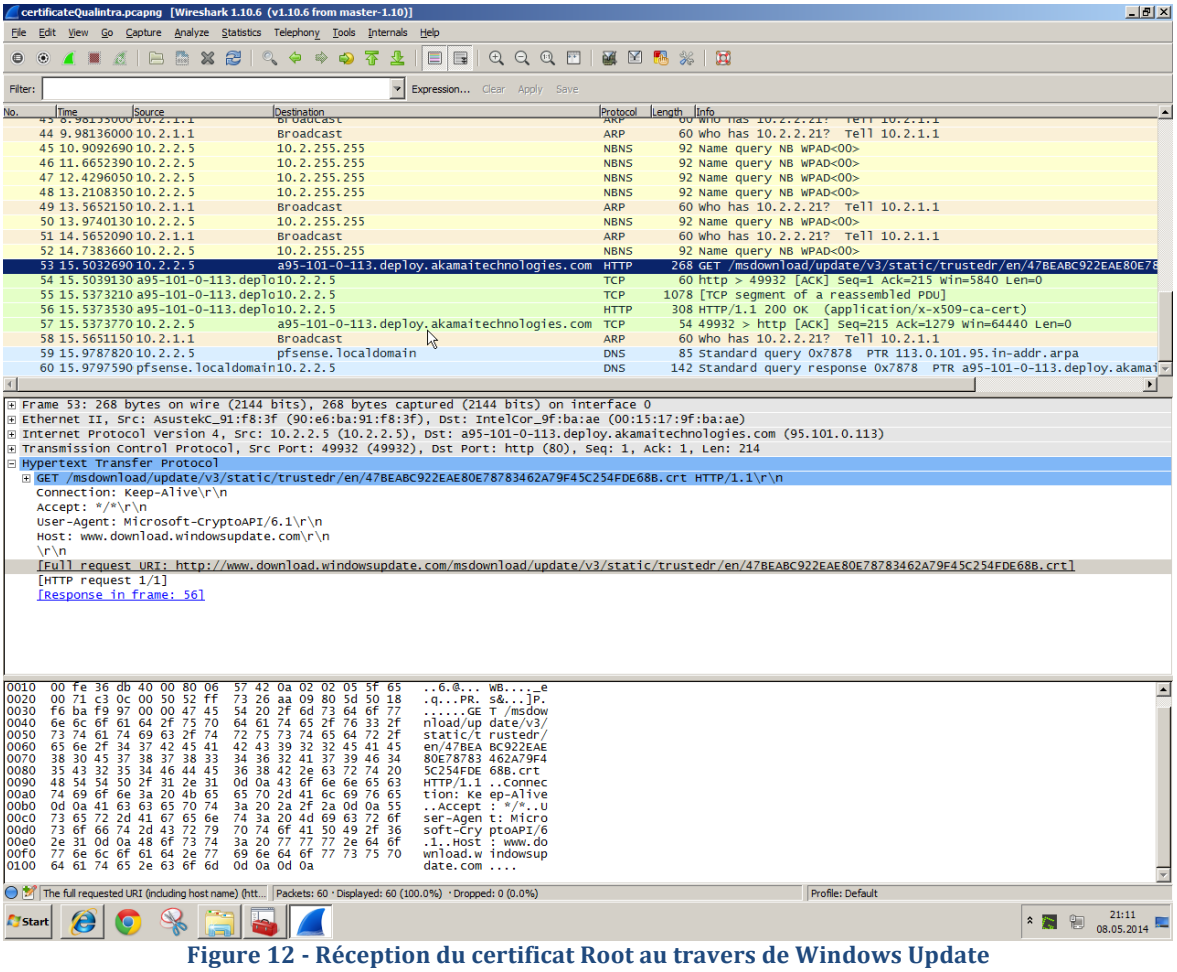


**Figure 12 - Réception du certificat Root au travers de Windows Update**

[2] GoDaddy : Prestataire de service internet ayant commencé la vente de certificats SSL après le lancement de Windows 7

Ouvrons ensuite ce certificat pour constater qu'il s'agit bien du certificat **`Root`** de GoDaddy (Figure 13).

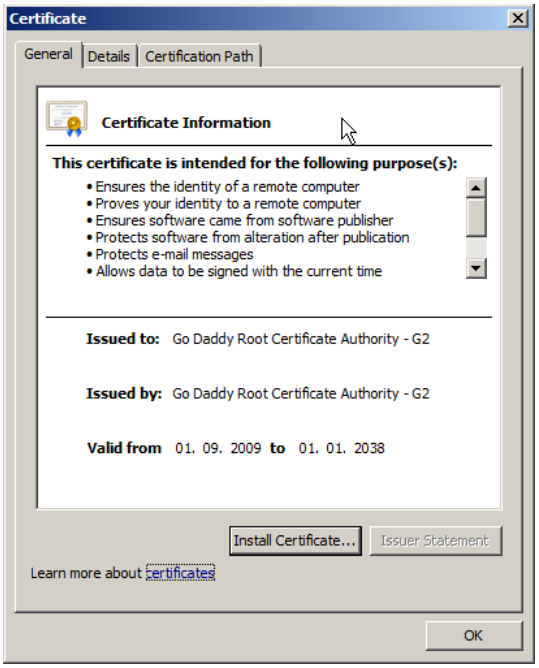


**Figure 13 - Le certificat Root GoDaddy Récupéré via Windows Update**

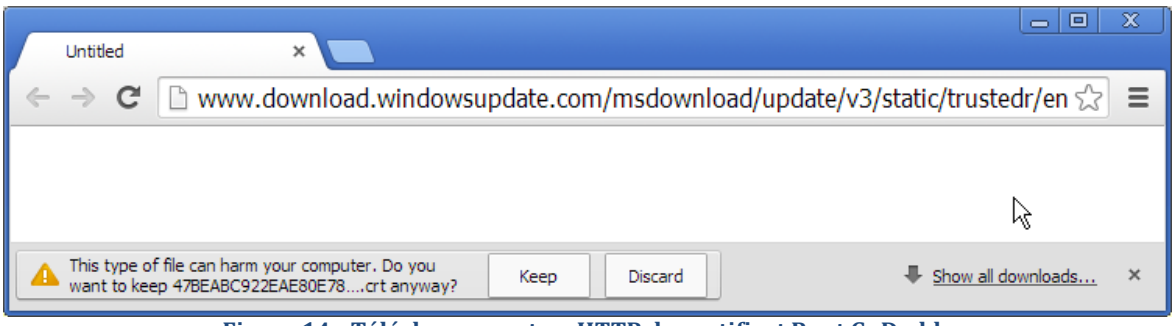


**Figure 14 - Téléchargement en HTTP du certificat Root GoDaddy**

Après quelques recherches, il semble bien que Microsoft utilise cette méthode pour mettre à jour les certificats périmés, supprimés, mais semble également l'utiliser pour enlever et supprimer des certificats **`Root`** révoqués ou qui sont jugés dangereux par Microsoft sur notre ordinateur.

## Désactivation

Si l'on ne désire pas, pour des raisons de sécurité, que des certificats **Root** sur notre ordinateur soient manipulés à notre insu. Par exemple dans le secteur bancaire, ou seul certains sites sensibles (souvent même internes) sont accessibles ou si simplement nous décidons de ne pas accorder notre confiance au gouvernement chinois (CNNIC Root Certificate) ou américain (Government Root Certification Authority). Il est possible de modifier ce comportement dans les GPO de Windows (Figure 15, 16 et 17).

```
Menu : Démarrer
Executer : gpedit.msc
Chemin : /Computer Configuration/Administrative Template
         /System/Internet Communication Management/
Dossier : Internet Communication settings
GPO : Mettre Turn off Automatic Root Certificates Update à Enabled
```

Figure 15 - Désactiver la mise à jour de certificats

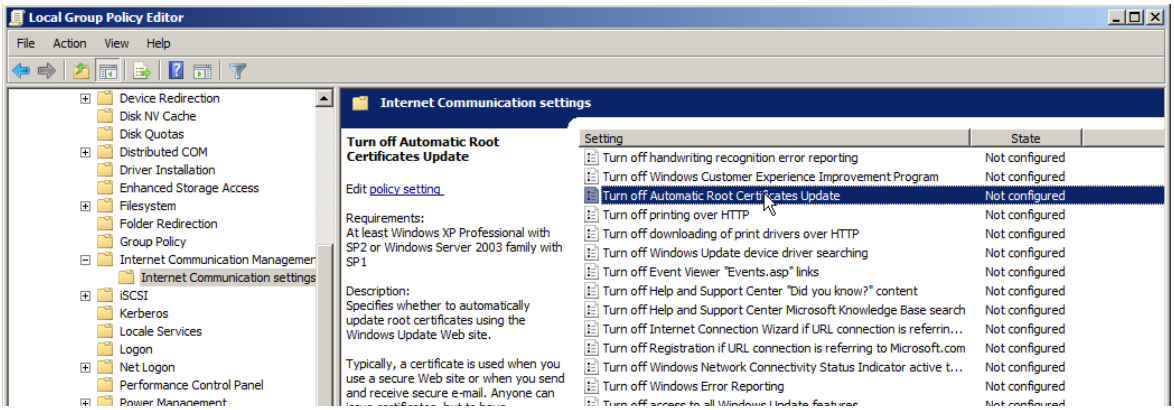


Figure 16 - GpEdit.MSC

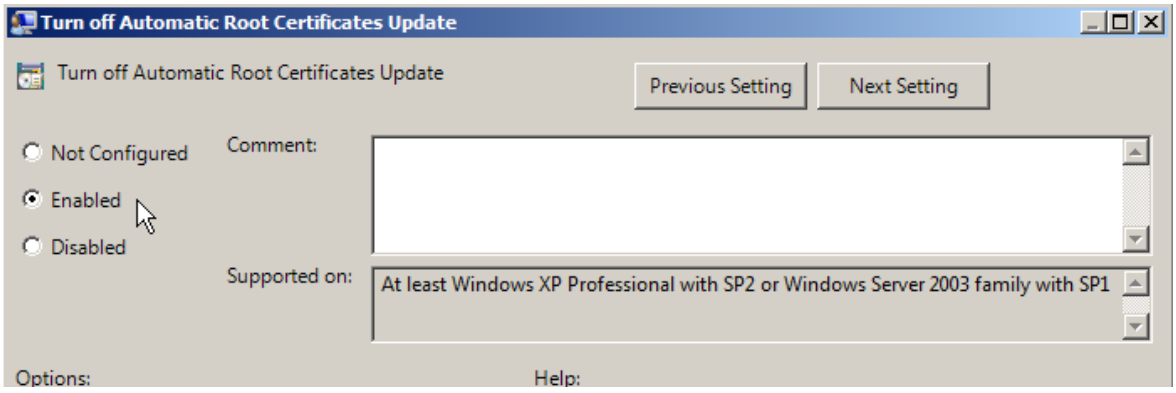


Figure 17 - Désactiver la mise à jour automatique des certificats

Aucun redémarrage de l'ordinateur n'est nécessaire, une fois cette modification effectuée, il suffit de vider le cache SSL du navigateur, supprimer les certificats Root du gestionnaire de certificats Windows et de rafraichir la page de Bank of America pour constater que le certificat n'est pas valable (Figure 18). En effet, aucun certificat Root n'est disponible pour ce domaine, la relation de confiance n'a donc pas lieu d'exister.

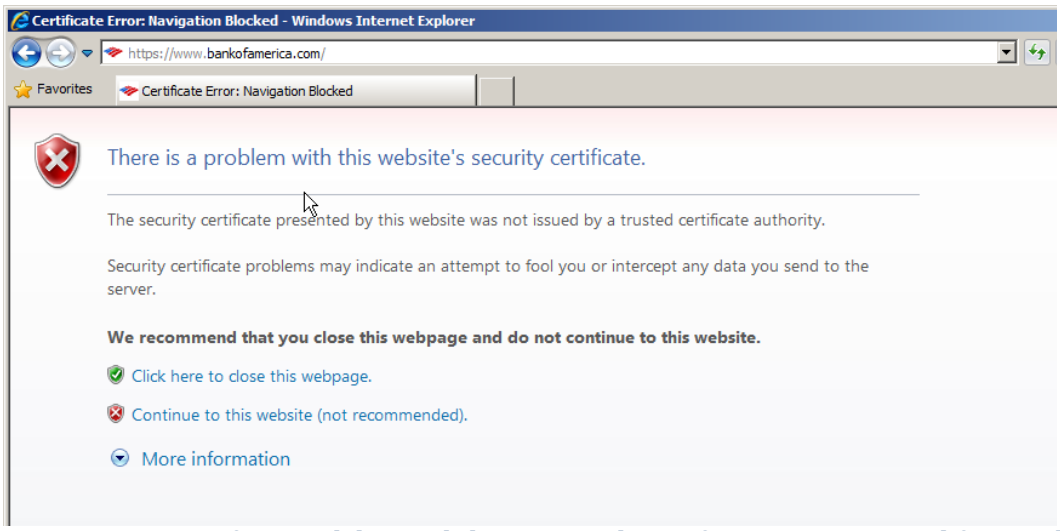


**Figure 18 - Certificat invalide pour la banque sans le certificat Root et avec modification du GPO adéquat**

A noter que la modification de cette règle GPO dans Windows 7 a pour effet d'ajouter un certificat Root de Microsoft dans le gestionnaire de certificats Windows (Figure 19). La raison n'est pas connue.

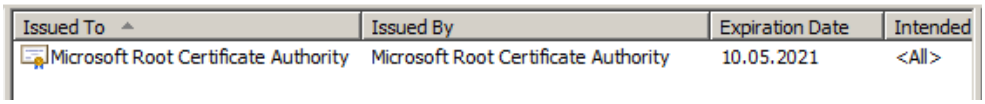


**Figure 19 - Certificat Root Microsoft**

A noter également que chrome utilise le même gestionnaire de certificats, à savoir celui de l'OS. Cette modification affectera donc également chrome, qui, de la même manière affichera un message d'erreur mentionnant qu'aucune confiance n'est attribuée à ce domaine. Firefox à l'inverse, utilise son propre gestionnaire de certificats et n'est pas conséquent pas affecté par cette manipulation. Il convient néanmoins de vérifier dans son gestionnaire de certificats en quel CA l'on place sa confiance.

## Conclusion

Nous constatons que cette fonctionnalité de mise à jour de certificats Root par Microsoft sur Windows 7 n'est absolument pas documentée ni expliquée. Le choix par défaut du GPO n'est également pas justifié par Microsoft.

On peut évidemment le comprendre pour des versions comme Home de Windows 7 où l'utilisateur ignorant du fonctionnement des Autorités de certification ne veut pas qu'on le dérange avec des messages incompréhensibles pour lui. Il donne donc toute sa confiance à la société Microsoft qui lui a vendu une licence d'utilisation de son OS.
Inversement ce choix se justifie difficilement pour des versions Professionnelles de Windows 7 utilisées en entreprise, ou la sécurité informatique est un point vital (exemple : une banque, un état) et où l'on peut se demander de la pertinence de la présence d'un certificat Root pour le gouvernement chinois et surtout sa réapparition après suppression. La simplification de l'utilisation se fait ici au détriment de la sécurité, ce qui n'est du gout de l'auteur pas tolérable.

Après un test le 19 juin, J'ai constaté que la version serveur Windows Server 2012 R2, sortit en octobre dernier est également impacté.

Après un deuxième test effectué ce même jour, l'utilisation de Google Chrome comme navigateur impacte également la machine. Chrome utilisant également le gestionnaire de certificat Windows. Je pense que c'est peut-être cet élément de Windows qui effectue les mises à jours (A vérifier).

## Développement ultérieur du sujet

Le temps à disposition pour ce travail n'étant que de dix heures, certains points n'ont pas pu être développés ici.

Il est néanmoins possible avec plus de temps, dans le cadre un travail d'approfondissement d'utiliser les points proposés ici comme direction :

- Mettre en place un proxy pour faire une attaque de type Man-in-the-Middle et remplacer le certificat téléchargé en HTTP par un autre.
- Expliquer pourquoi lorsque le CA est VeriSign, la procédure ne passe pas par Windows Update, mais télécharge directement le certificat sur le site de VeriSign.
- Ce système permettrait également la suppression de certificats si ce dernier n'est pas ou plus proposé par Microsoft.