

Aide sur l'authentification par certificat

Cette page contient des informations sur l'usage de certificats électroniques pour vous authentifier sur certaines applications du SPF Finances.



Veuillez noter qu'il n'est pas autorisé d'utiliser votre carte d'identité électronique (eID) avec cette méthode d'authentification. Pour vous authentifier avec votre carte d'identité électronique, veuillez utiliser plutôt l'authentification par eID.

Cette page comporte les sections suivantes :

1. [Exigences techniques](#)
2. [Obtention d'un certificat numérique](#)
3. [Utilisation avec Internet Explorer](#)
4. [Utilisation avec Firefox](#)
5. [Problèmes courants](#)

Pour les problème liés à la signature électronique, veuillez suivre [ce lien](#).

1. Exigences techniques

L'authentification par certificat demande la signature électronique d'un token d'identification. La création d'une signature électronique demande un navigateur récent et des bibliothèques de chiffrement de données. Tous les navigateurs ne sont pas capables de produire ces signatures. Les navigateurs suivants sont supportés (d'autres navigateurs peuvent fonctionner également, mais ne sont pas officiellement supportés) :

1. Internet Explorer >= 5.5
2. Firefox >= 3.0



Isabel Office Sign ne supporte pas le navigateur Firefox. Il n'est donc pas possible d'effectuer une signature électronique avec votre certificat Isabel avec Firefox. Veuillez utiliser Internet Explorer.

Les composants indispensables pour effectuer une signature numérique sont les suivants :

- Un certificat de signature.
- Pour Internet Explorer :
La **librairie CAPICOM**. Il s'agit d'une librairie de fonctions cryptographiques, distribuée par Microsoft. Normalement, celle-ci s'installe automatiquement. Voir [section 3](#)).
- Pour Firefox :
 - Aucune librairie supplémentaire (supporté nativement).

2. Obtention d'un certificat numérique

Un certificat électronique est nécessaire pour vous authentifier avec le système. Les seuls certificats acceptés actuellement par le SPF Finances sont les suivants :

- [GlobalSign](#) PersonalSign Pro3 Certificate
- [Certipost](#) Qualified Certificate
- [Isabel](#) Certificate

Pour des instructions détaillées sur la manière d'obtenir un certificat, veuillez consulter le site de ces institutions.



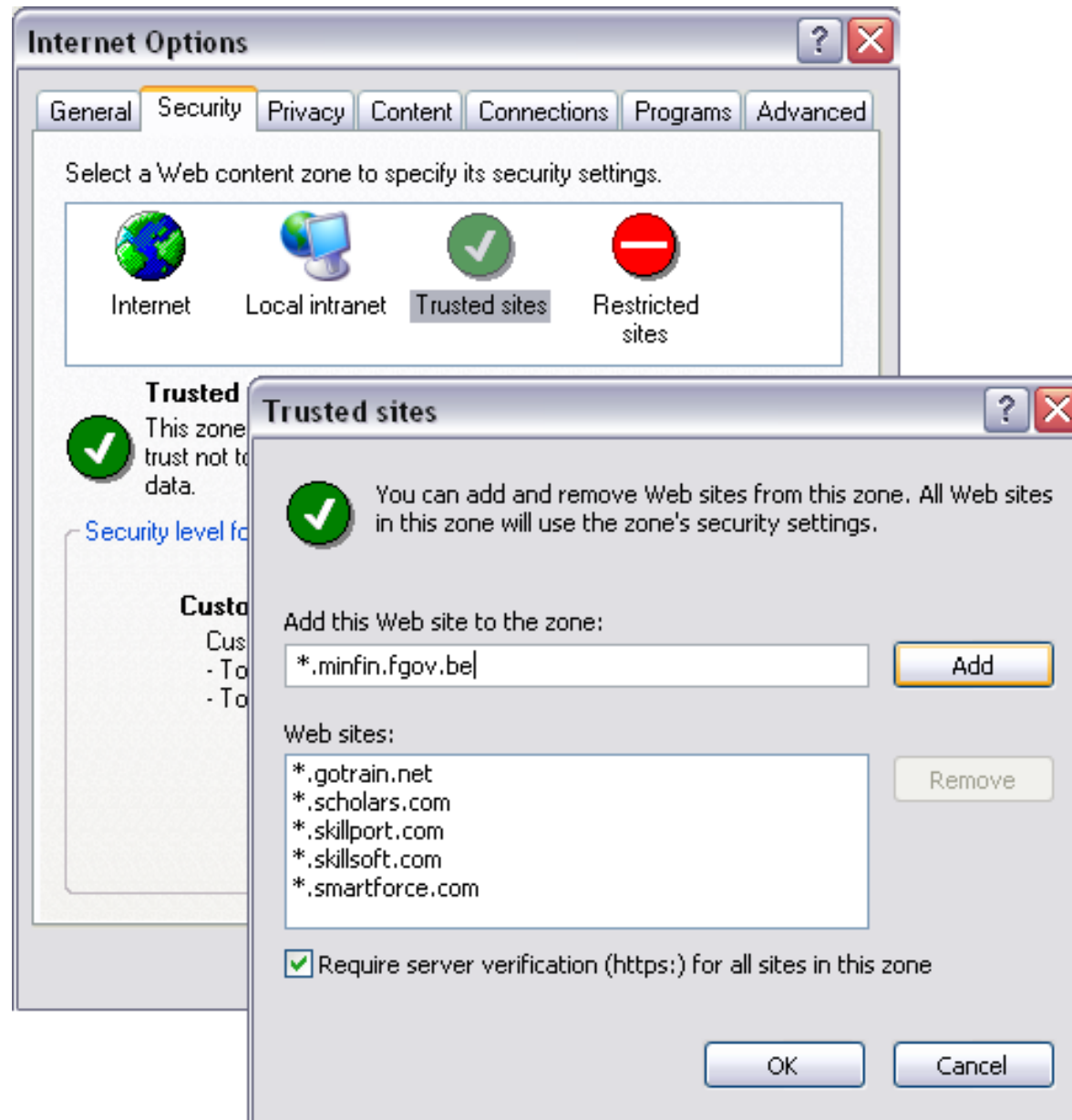
Seuls les certificats de classe 3 sont acceptés.

3. Utilisation avec Internet Explorer



Pour éviter tout problème, nous recommandons fortement l'insertion du site du SPF Finances dans la liste des sites de confiance :

1. Allez dans le menu "Tools > Internet Options...", onglet "Security"
2. Cliquez sur "Trusted Sites", bouton "Sites..."
3. Entrez dans la boîte de texte "*.minfin.fgov.be", et cliquez sur "Add" pour ajouter le site à la liste des sites de confiance. Voir capture d'écran ci-dessous.
4. Cliquez sur "OK", et ensuite sur "Ok".





Si vous faites ceci, vous pouvez passer directement à la [section 3.2](#).

3.1 Installation de la librairie CAPICOM

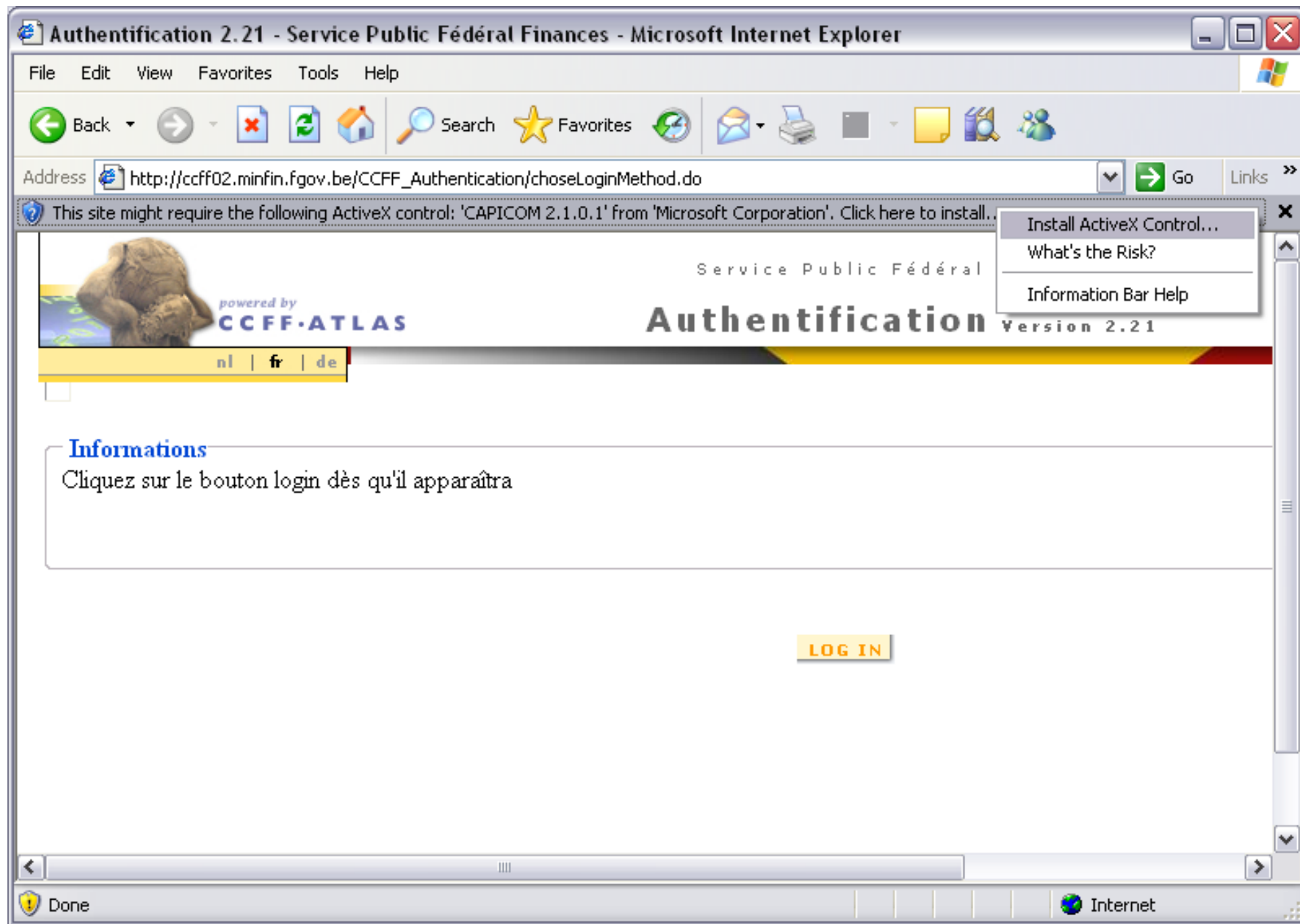
Cette librairie est notamment utilisée pour signer numériquement des données, vérifier des signatures numériques et chiffrer/déchiffrer des données. Si cette librairie n'est pas présente sur votre ordinateur, celle-ci est automatiquement installée (sous forme d'un plugin ActiveX), lorsque c'est possible. L'installation dépend du niveau de sécurité configuré pour votre Internet Explorer :

Niveau de sécurité faible, ou site minfin.fgov.be appartenant aux sites de confiance

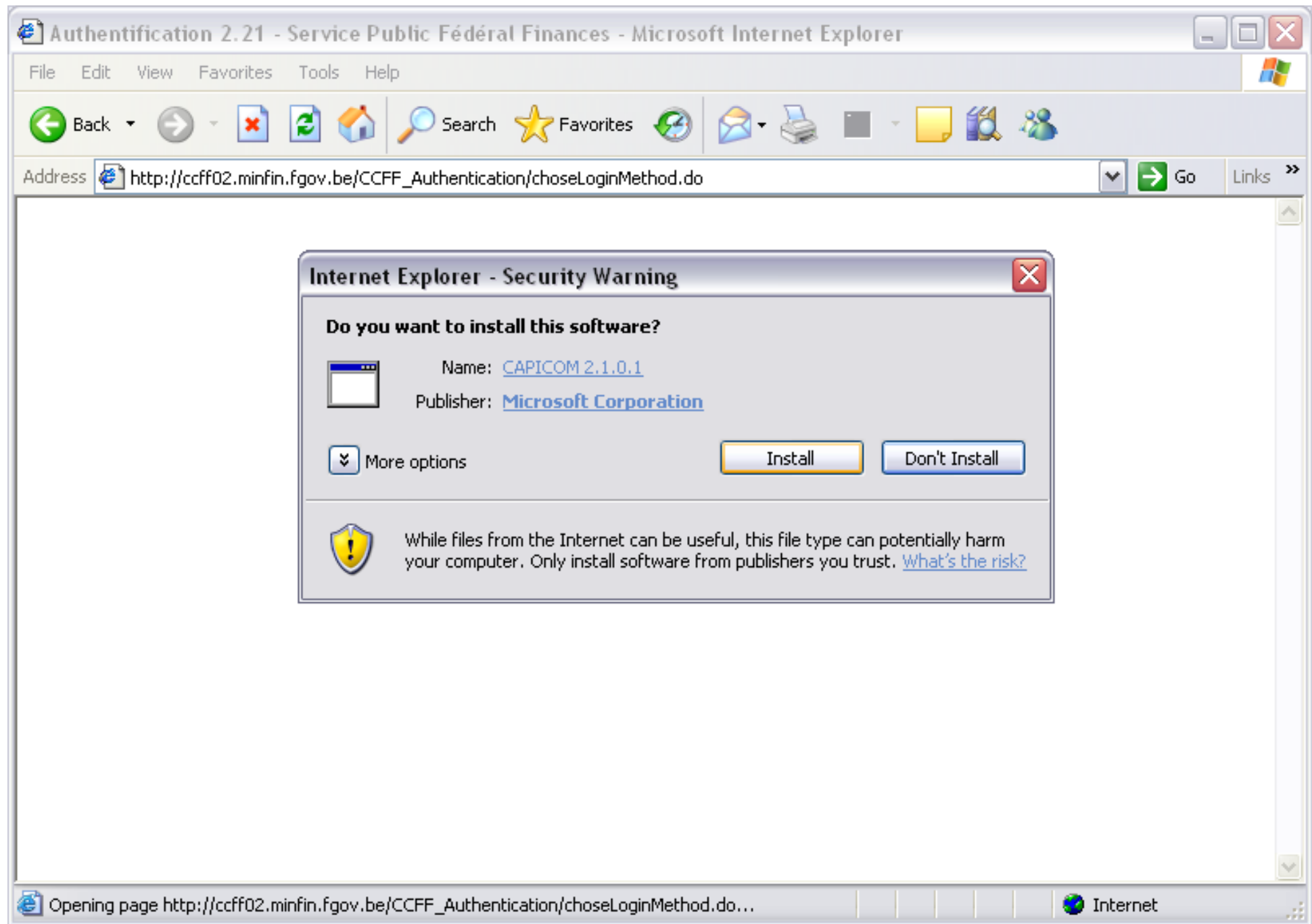
Avec cette configuration, la librairie CAPICOM est **automatiquement installée**. Vous pouvez passer à la [section 3.2](#). Des instructions pour ajouter le site du SPF Finances à la liste des sites de confiance sont données [ici](#).

Niveau de sécurité moyen, site minfin.fgov.be n'appartenant pas aux sites de confiance

Avec cette configuration, Internet Explorer vous demande d'abord si les contrôles ActiveX peuvent être activés. Cliquez sur la barre située en haut de l'écran, et cliquez sur "Install ActiveX Control...".



Internet Explorer vous demande ensuite l'autorisation d'installer la librairie CAPICOM. Vous pouvez installer ce composant. Cliquez sur "Install".





Niveau de sécurité élevé, ou installation manuelle de CAPICOM

Si vous devez installer manuellement la librairie CAPICOM, une version pour Internet Explorer 6.0 SP1 et supérieur peut être téléchargée et installée manuellement depuis le [site web de Microsoft](#).

Une copie de la librairie CAPICOM est aussi disponible [ici](#). Voici les étapes pour enregistrer cette librairie dans Windows:

1. Téléchargez [capicom.cab](#)
2. Décompressez le fichier
3. Copiez la librairie capicom.dll vers le répertoire système de Windows, typiquement: C:\Windows\System32
4. Ouvrez un terminal de commande en tant qu'Administrateur :
Start > Programs > Accessories > click droit sur Command Prompt > Run as... > Administrator
5. Allez dans le répertoire système : cd \Windows\System32
6. Enregistrez la librairie : regsvr32 capicom.dll
7. Redémarrez le navigateur

3.2 Installation d'un certificat numérique dans Internet Explorer

Le certificat numérique doit être enregistré dans votre navigateur. Dans le cas d'un certificat software (Certipost, GlobalSign ou Isabel), l'institution émettrice donne généralement des instructions et/ou des outils pour enregistrer le certificat. Si le certificat est seulement fourni sous la forme d'un fichier, veuillez suivre les instructions suivantes pour enregistrer ce certificat dans Internet Explorer :

1. "Menu Tools" > "Internet Options..."
2. Cliquez sur l'onglet "Content", ensuite sur le bouton "Certificates...". Une liste apparaît avec tous vos certificats installés.
3. Cliquez sur "Import...". Ceci ouvre un assistant. Cliquez sur "Next".
4. Sur la boîte de dialogue qui apparaît, entrez le chemin complet vers le fichier certificat, puis cliquez sur "Next".
5. Entrez le mot de passe que vous avez reçu de l'institution émettrice. Vous pouvez également indiquer ici que la clé privée peut être exportée, afin de pouvoir installer ce certificat sur d'autres machines. Cliquez sur "Next".
6. Sélectionnez "Automatically select the certificate store..." et cliquez sur "Next".
7. Vous recevez ensuite un message indiquant si l'importation a réussi ou non. Cliquez sur "Finish".
8. Le nouveau certificat importé devrait maintenant apparaître dans l'onglet "Personal" de la boîte de dialogue "Certificates". Vous pouvez vérifier la validité du certificat en double-cliquant sur celui-ci. Vous devriez voir la mention "You have a private key that corresponds to this certificate".

Configuration d'Internet Explorer

Certaines options doivent être activées pour vous permettre d'effectuer une signature numérique :

1. Allez dans le menu "Tools" > "Internet Options...".
2. Cliquez sur l'onglet "Security", "Custom Level".
3. Vérifier que "Microsoft VM > Disable Java" n'est **PAS** coché.
4. Vérifier que "Scripting > Active scripting" est **Enabled**.
5. Vérifier que "Scripting > Scripting of Java applets" est **Enabled**.
6. Vérifier que "ActiveX controls and plug-ins > Download signed ActiveX controls" est **Prompt** ou **Enabled**.
7. Vérifier que "ActiveX controls and plug-ins > Run ActiveX controls and plug-ins" est **Enable**.
8. Vérifier que "ActiveX controls and plug-ins > Script ActiveX controls marked safe for scripting" est **Enable**.
9. Cliquez sur "OK", puis sur "Apply".

4. Utilisation avec Firefox

Firefox peut nativement créer des signatures électronique, sans recours à des librairies supplémentaires. Cependant, votre certificat doit être importé avec soin dans Firefox. L'import d'un certificat dans Firefox devrait être décrit par votre Autorité de Certification (Certification Authority ou CA).



Isabel Office Sign ne supporte pas le navigateur Firefox. Il n'est donc pas possible d'effectuer une signature électronique avec votre certificat Isabel avec Firefox. Veuillez utiliser Internet Explorer.

4.1 Installation d'un certificat numérique dans Firefox

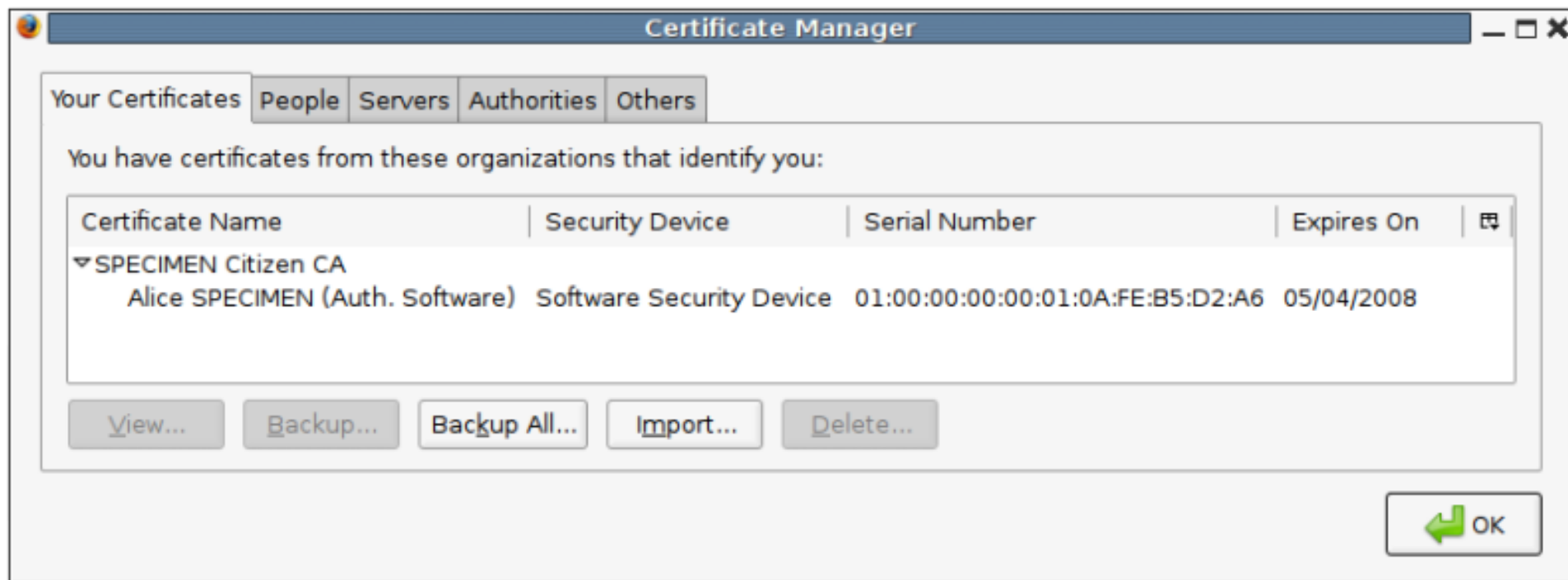
Lorsque le certificat est fourni sous forme de fichier, le certificat doit être en format PKCS12 (extension : .p12). S'il ne l'est pas (l'installation échoue), le certificat peut être importé puis exporté vers ce format PKCS12 en utilisant Internet Explorer, ou en utilisant [openssl](#). Contactez votre fournisseur de certificat pour plus de renseignements sur ces questions. Les étapes suivantes sont nécessaires pour l'enregistrer dans votre navigateur Firefox :

1. Allez dans le menu "Tools > Options... > Advanced" (ou "Edit > Preferences > Advanced" dans les anciennes versions).
2. Cliquez sur l'onglet "Security", "Show certificates", et ensuite sur "Import".
3. Sélectionnez le fichier contenant votre certificat, and cliquez sur "Open".
4. Selon votre configuration, le navigateur vous demandera d'entrer le mot de passe protégeant l'accès à vos certificats.

5. Ensuite, entrez le mot de passe que vous avez reçu de l'institution émettrice de votre certificat, et cliquez sur OK.
6. Votre certificat devrait maintenant apparaître dans l'onglet "Your certificates".

4.1.1 Ouvrez le Certificate Manager de Firefox

1. Allez dans le menu "Tools > Options... > Advanced" ou "Edit > Preferences > Advanced" en fonction de la version de Firefox.
2. Cliquez sur l'onglet "Security" ou "Encryption" en fonction de la version de Firefox.
3. Cliquez sur "Show certificates" ou "View certificates". Ceci ouvre le Certificate Manager



4.1.2 Vérifiez que le certificat de votre fournisseur de certificat est dans la liste des autorités de confiance de Firefox

Firefox ne fera pas confiance à votre certificat si votre autorité de certification n'est pas dans cette liste des autorités de confiance. Voici comment vérifier que votre fournisseur de certificat (par exemple GlobalSign ou Certipost) est dans cette liste :

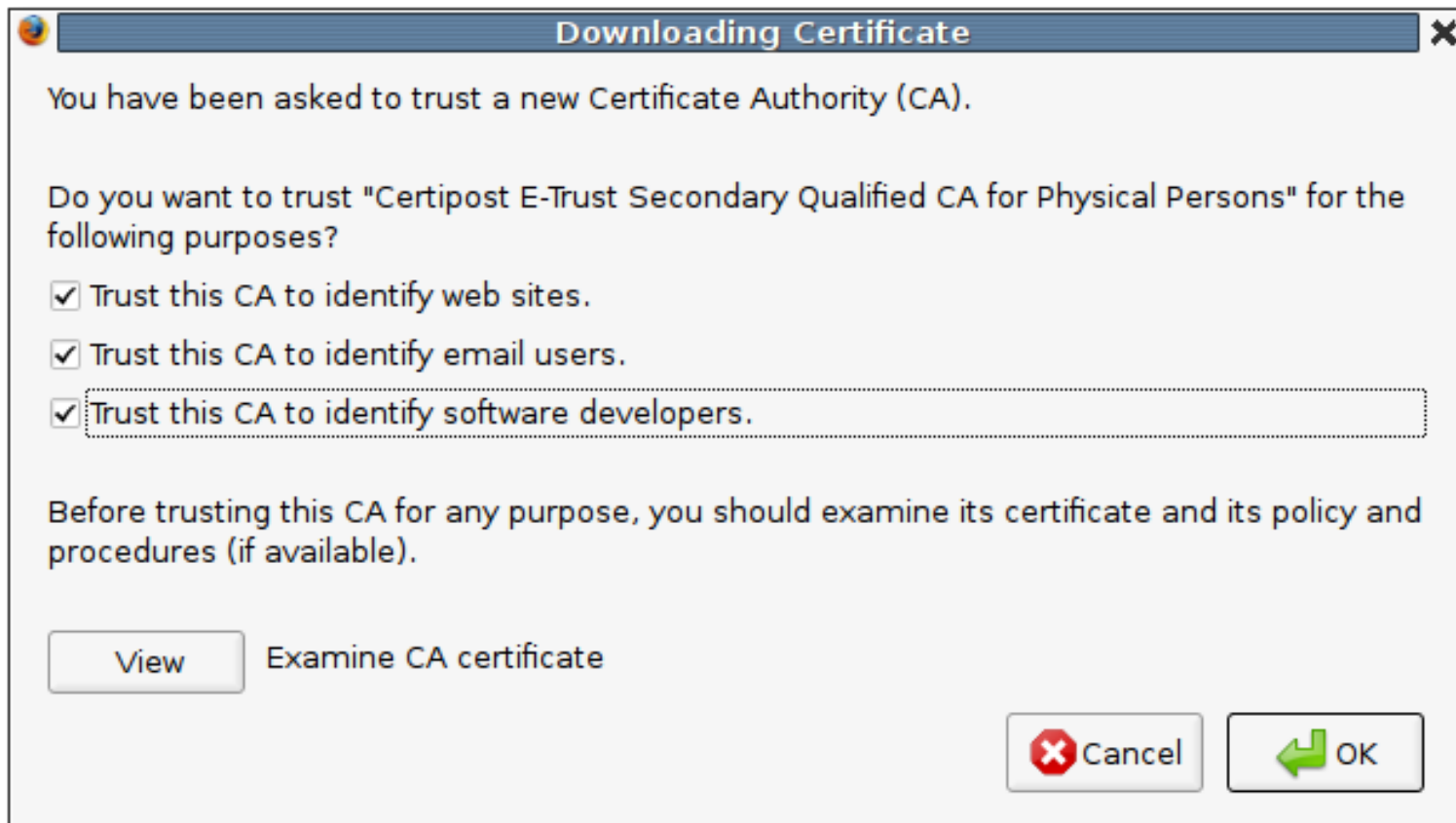
1. Dans le Certificate Manager de Firefox, sélectionnez l'onglet "Authorities".

2. Pour les certificats **GlobalSign** : vérifiez que le certificat "GlobalSign PersonalSign Class 3 CA" est présent.
3. Pour les certificats **Certipost** : vérifiez que les certificats suivants sont présents (en fonction du type de votre certificat) :
"Certipost E-Trust Primary CA for Qualified certificates", "Certipost E-Trust Secondary Qualified CA for Physical Persons", "Certipost E-Trust Secondary Qualified CA for Legal Persons", "Certipost E-Trust Secondary Qualified CA for Communities".

Vous pouvez savoir quel certificat doit être importé en regardant le nom de l'autorité de confiance qui a émis votre certificat. Ce nom peut être connu sous Windows en ouvrant le certificat.

Si le certificat de votre fournisseur manque dans la liste, vous devez l'importer. Voici comment faire :

1. Importez le certificat de l'autorité de confiance. Pour cela :
 - soit cliquez simplement sur le ou les certificat(s) de votre fournisseur :
 - [GlobalSign Root CA](#) (pour les certificats GlobalSign, normalement déjà connus par Firefox)
 - [GlobalSign Primary Class 3 CA](#) (pour les certificats GlobalSign)
 - [GlobalSign PersonalSign Class 3 CA](#) (pour les certificats GlobalSign)
 - [Certipost E-Trust Primary CA for Qualified certificates](#) (pour les vieux certificats Certipost)
 - [Certipost E-Trust Primary Qualified CA](#) (pour les nouveaux certificats Certipost)
 - [Certipost E-Trust Secondary Qualified CA for Physical Persons](#) (pour les nouveaux certificats Certipost)
 - [Certipost E-Trust Secondary Qualified CA for Legal Persons](#) (pour les nouveaux certificats Certipost)
 - [Certipost E-Trust Secondary Qualified CA for Communities](#) (pour les nouveaux certificats Certipost)
 - soit (plus compliqué mais plus sûr) :
 1. téléchargez le certificat de votre fournisseur depuis son site web (cfr <http://www.certipost.be/> or <http://www.globalsign.com/>). Contactez votre fournisseur pour question à ce propos.
 2. Ouvrez le Certificate Manager de Firefox (cfr [section 4.1.1](#)).
 3. Sélectionnez l'onglet "Authorities", et cliquez sur "Import".
 4. Sélectionnez le certificat du fournisseur.
2. Dans chaque fenêtre popup qui apparaît, cochez toutes les cases et cliquez sur "OK". Voir figure ci-dessous.



4.1.3 Importez votre certificat

1. Dans le Certificate Manager de Firefox, sélectionnez l'onglet "Your Certificates".
2. Cliquez sur "Import".
3. Sélectionnez le fichier contenant votre certificat, et cliquez sur "Open".
4. En fonction de votre configuration, il vous sera demandé d'entrer le mot de passe pour accéder à votre magasin de certificats.
5. Entrez le mot de passe reçu de votre fournisseur, et cliquez sur "OK".
6. Votre certificat devrait maintenant apparaître dans l'onglet "Your certificates".

4.1.4 Vérifiez que votre certificat est correctement installé

1. Dans le Certificate Manager de Firefox, sélectionnez l'onglet "Your Certificates".

2. Sélectionnez votre certificat et cliquez sur "View".
3. Vérifiez que Firefox reconnaît correctement les usages du certificat (voir figure ci-dessous).



4.2 Configuration de Firefox

Certaines options doivent être activées pour vous permettre de faire une signature numérique :

1. Allez dans le menu "Tools > Options... > Web Features" (ou "Edit > Preferences > Web Features" dans les anciennes versions).
2. Vérifier que les options "Enable Javascript" et "Enable Java" sont cochées.
3. Vérifier également que votre navigateur ne bloque pas les les fenêtres popup venant du site du SPF Finances.

4.3 Utilisation de votre certificat pour l'authentification

Cette section décrit comment utiliser votre certificat pour vous authentifier sur une application du SPF Finances.

1. Si plusieurs mode d'authentification sont proposés, sélectionner "Authentification par certificats" :



powered by
CCFF-ATLAS

Service Public Fédéral Finances

A A A

08/05/2008, 16:35

Authentication

Version 2.20.1.4

nl | fr | de | en

> **PLEASE CHOOSE AN AUTHENTICATION METHOD :**



[Certificate authentication \(Isabel, GlobalSign ou Certipost\)](#)



[Electronic ID card authentication \(eID\)](#)

2. Un nouvel écran apparaît, et une fenêtre pop-up qui ressemble à ceci s'ouvre :

 **Text Signing Request** 

The site '193.191.216.17' has requested that you sign the following text message:

Identification token #f48fbfcccc983440

Signing Certificate

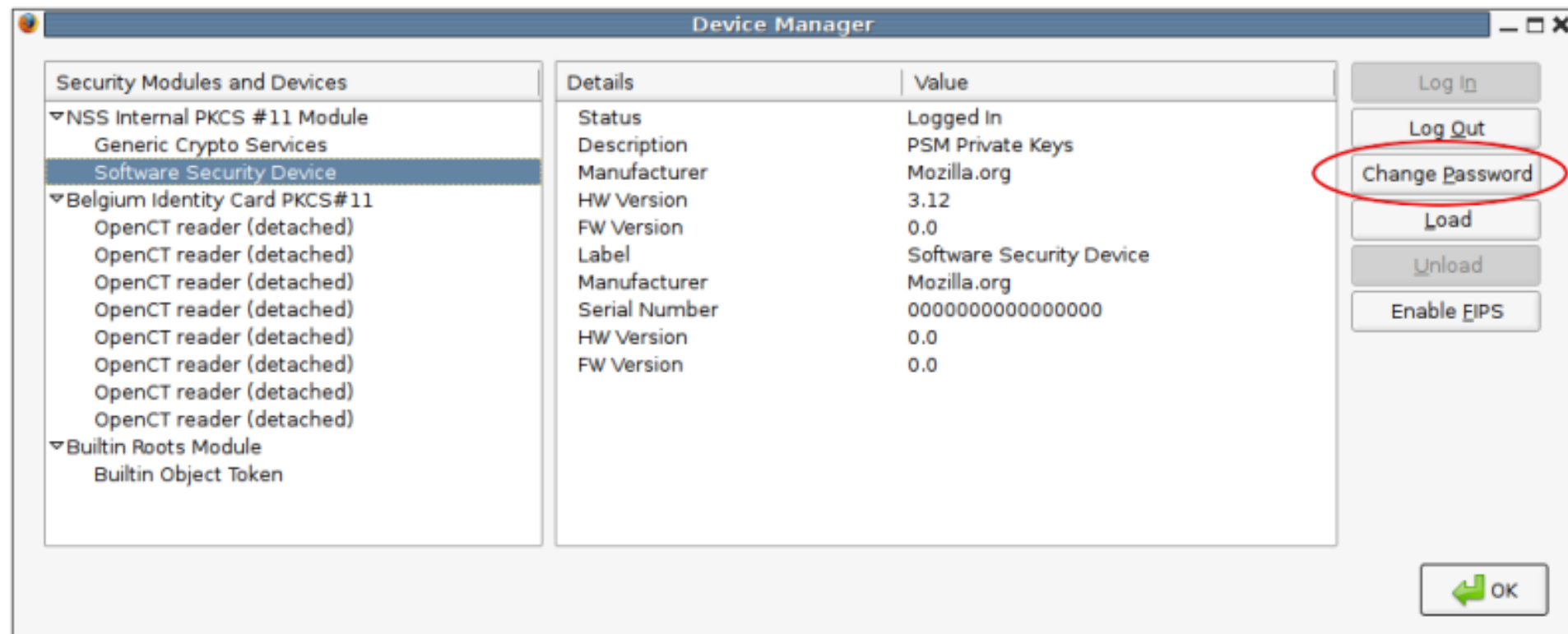
Test SPF Finances - FOD Financien - Federal Public S... 

Issued to: ST=Brussels,L=Brussels,OU=Belgian Federal
Serial Number: 00:89:31:00:BD:8C:1B:4F:35
Valid from 05/06/2008 10:07:20 to 05/07/2018 10:07:20
Purposes: Client,Sign,Encrypt,Object Signer
Certificate Key Usage: Signing,Non-repudiation,Key Enc
Issued by: ST=Brussels,L=Brussels,OU=Belgian Federal
Standing Software Security Device

To confirm you agree to sign this text message using your selected certificate, please confirm by entering the master password:

 Cancel  OK

3. Sélectionnez votre certificat et, si nécessaire, tapez le mot de passe qui protège l'accès à tous vos certificats. Par défaut, **ce mot de passe n'est pas défini dans Firefox**. Dans ce cas, laissez simplement ce champ vide and cliquez sur "OK". Notez qu'il **ne s'agit pas du mot de passe fourni par votre fournisseur et qui protégeait votre certificat**. Il s'agit du mot de passe que vous pouvez définir ici dans Firefox : Menu Edit > Preferences > Advanced > Encryption > Security Devices, sélectionnez Software Security Device et cliquez sur "Change Password". Il est vivement recommandé de définir un tel mot de passe afin de protéger l'accès à vos certificats.



5. Troubleshooting

Erreur 101 : Aucune donnée à signer.

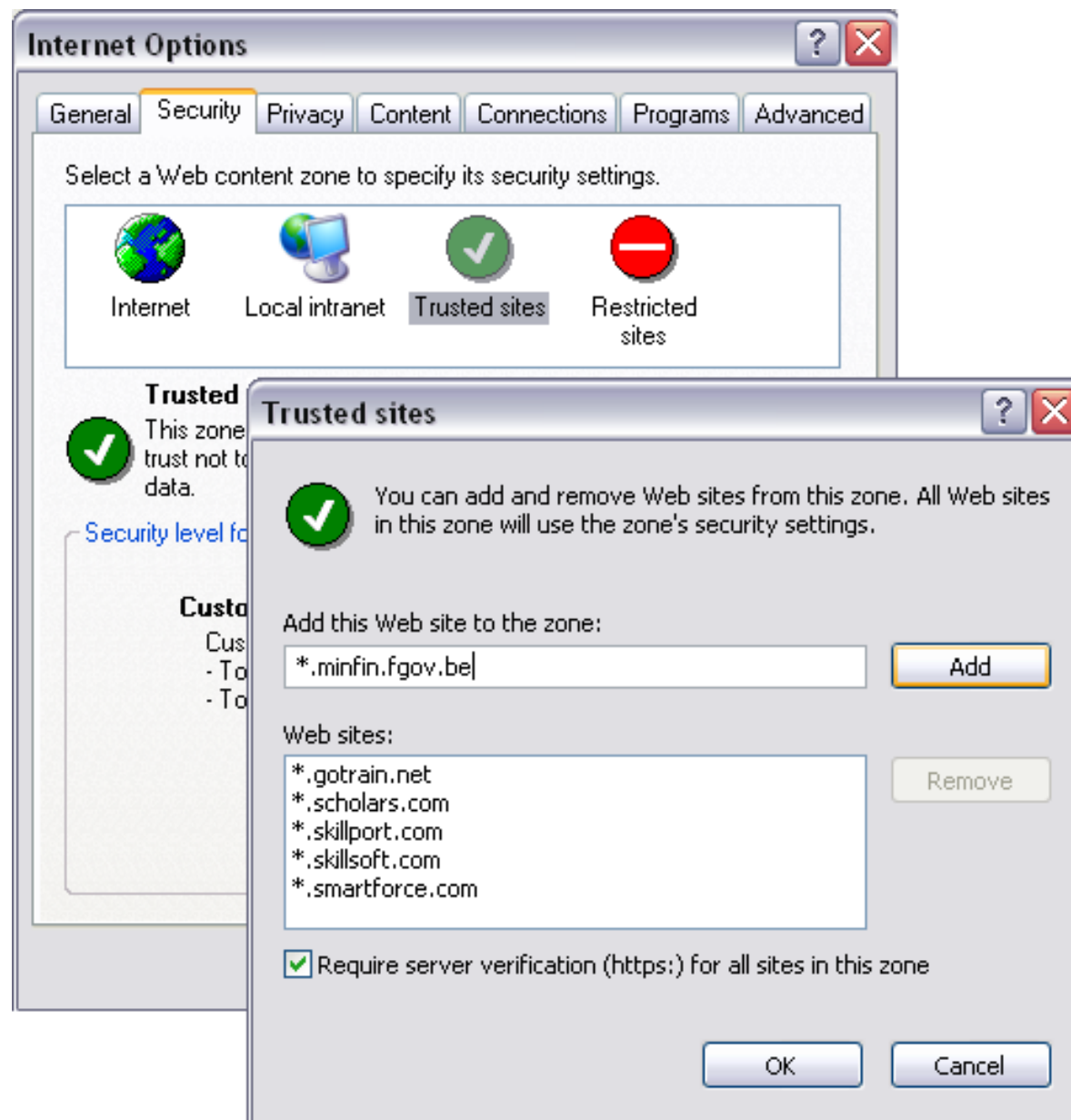
Il n'y a pas de données pouvant être signée. Ce problème apparaît généralement lorsque vous utilisez le bouton "back" du navigateur, en combinaison ou non avec une erreur survenant dans l'application. Dans une telle situation, il arrive que l'application "perde" le document ou les données qui doivent être signées. Ce problème se résout normalement en évitant d'utiliser le bouton "back", en retournant à l'écran précédant, et en recommençant le processus de signature.

Erreur 501 : La librairie CAPICOM n'est pas correctement installée. (IE uniquement)

La librairie CAPICOM n'a pas été trouvée. Vérifiez qu'un fichier nommé capicom.dll est présent dans le répertoire système de Windows (typiquement C:\Windows\System32\ ou C:\Winnt\System32). Cette librairie est automatiquement installée, à condition que en ayez autorisé l'installation, voir [section 3.1](#).

Pour activer l'installation automatique, vous pouvez insérer le site du SPF Finances dans la liste des sites de confiance :

1. Allez dans le menu "Tools > Internet Options...", onglet "Security"
2. Cliquez sur "Trusted Sites", bouton "Sites..."
3. Entrez dans la boîte de texte "*.minfin.fgov.be", et cliquez sur "Add" pour ajouter le site à la liste des sites de confiance. Voir capture d'écran ci-dessous.
4. Cliquez sur "OK", et ensuite sur "Ok".



Erreur 502 : Aucun certificat trouvé. (IE uniquement)

Vous n'avez aucun certificat installé dans votre navigateur, ou aucun certificat n'est adéquat pour signer un document. Vérifiez que vous

avez bien importé votre certificat numérique dans le navigateur.

Erreur 503 : Problème d'accès aux clés du certificat sélectionné. La permission a probablement été refusée. (IE uniquement)

Il s'agit d'un problème de permission d'accès. L'utilisateur actuel n'a pas les permissions nécessaires pour accéder aux clés de vos certificats. Ces clés sont maintenues dans des "conteneurs de clés", auxquels vous devez avoir accès. Les étapes nécessaires pour résoudre ce problème dépendent de la version de Windows que vous utilisez :

Windows NT :

Les permissions du conteneur de clés sont définies dans la base de registre. Pour changer ces permissions, ouvrez regedt32 (pas regedit!), ouvrez la branche HKEY_LOCAL_MACHINE et allez sur la clé HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MachineKeys\<container name>. Sélectionnez Security/Permissions à partir du menu et vérifiez que tout le monde (Everyone) a un accès complet (Full Control) sur cette clé.

Windows 2000 and Windows XP :

Dans Windows Explorer, localisez le répertoire C:\Documents and settings\<username>\Application Data\Microsoft\Crypto\RSA\. Changez les droits d'accès sur ce répertoire et sur tous les fichiers qu'il contient en suivant les étapes ci-dessous :

1. Clic droit sur le répertoire C:\Documents and settings\<username>\Application Data\Microsoft\Crypto\RSA\.
2. Allez sur "Propriété"s
3. Cliquez sur l'onglet "Security".
4. Vérifiez que Vous, Administrator et System avez un accès complet ("full control") sur ce répertoire (vérifiez que toutes les cases "Allow" sont cochées).
5. Cliquez "Advanced".
6. Cochez les deux cases ("Inherit..." et "Replace...") sur le bas pour activer la propagation de ces droits d'accès à tous les sous-répertoires et fichiers.
7. Cliquez sur Apply, ensuite Yes, et OK.
8. Cliquez sur OK.

Vous devrez peut-être reproduire ces étapes pour le répertoire C:\Documents and settings\All Users\Application Data\Microsoft\Crypto\RSA\.

Note : ces fichiers sont des fichiers cachés. Afin de voir ces fichiers cachés, vous devez activer l'option "Display hidden files and folders"

dans Windows, en suivant les étapes ci-dessous :

1. Cliquez sur "Start", allez dans "Settings", et cliquez sur "Control Panel".
2. Si vous êtes dans "Category View" : cliquez sur "Appearance and Themes"
3. Cliquez sur "Folder Options".
4. Sur l'onglet "View", en-dessous de "Hidden files and folders", cliquez sur "Show hidden files and folders".

Erreur 504 : Echec de l'accès aux clés du certificat sélectionné. La permission a probablement été refusée. (IE uniquement)

Voir [Erreur 503](#).

Erreur 505 : Echec de l'accès aux clés du certificat sélectionné. Conflit probable entre vos certificats. (IE uniquement)

Ce problème réside probablement dans un conflit entre les certificats enregistrés dans Windows. Il s'agit d'un problème lié à Windows, pas à l'application du SPF Finances. Ce problème peut être résolu en supprimant manuellement les certificats.

Pour supprimer un certificat sur Windows 2000 et Windows XP:

1. Dans le menu **Démarrer** de Windows, cliquez sur **Exécuter (Start > Run)**.
2. Tapez *mmc* et appuyez sur ENTREE (ENTER).
3. Dans la barre de menu, cliquez sur **Fichier**, sélectionnez **Ajouter / Supprimer un composant logiciel enfichable...**
4. Cliquez **Ajouter...**
5. Double-cliquez sur **Certificats**.
6. Sélectionnez **Mon compte d'utilisateur**.
7. Cliquez sur **Terminer**.
8. Cliquez sur **Fermer** et après sur **OK**.
9. Double-cliquez sur **Certificats - utilisateur actuel**.
10. Double-cliquez sur **Personnel** et après sur **Certificats**.
11. Cliquez sur le certificat à supprimer.
12. Appuyez sur SUPPRIMER et cliquez **Oui**.
13. Fermez la fenêtre **Console1**.

Si vous avez un certificat software, vous devrez le réenregistrer dans le navigateur.

Error 509 : Certificat non trouvé. Le navigateur ne trouve pas le certificat sélectionné. (IE uniquement)

Cette erreur apparaît lorsque Internet Explorer ne trouve pas le certificat sélectionné. Cette erreur apparaît en général avec les certificats Isabel. Cette erreur provient d'une mise à jour incorrecte par Isabel Office Sign des certificats Isabel. Une solution à ce problème est documentée sur le site de support en ligne d'Isabel (www.isabel.be), section "Isabel Web Support", sous le numéro d'identification **48700** (effectuez une recherche avec cet identifiant). Si ceci ne résout pas le problème, contactez le support Isabel.

Erreur 510 : An error occurred during the signature process. (IE uniquement)

La librairie CAPICOM n'a pas pu créer la signature numérique, pour une raison indéterminée. Une ou plusieurs des actions ci-dessous peut aider à résoudre ce problème :

- Réinstallez la librairie CAPICOM. Vous pouvez simplement supprimer le fichier capicom.dll de votre répertoire système Windows (typiquement C:\Windows\System32), et ensuite effectuer la procédure d'installation décrite en [section 3](#).
- Réimportez votre certificat, il pourrait être corrompu.
- Essayez avec Mozilla Firefox.
- Essayez avec une autre machine et/ou une autre version de Windows.

Erreur 601 : Votre navigateur n'a pas réussi à produire la signature (Firefox uniquement)

Votre certificat n'est pas correctement installé dans Firefox et/ou Firefox ne lui fait pas confiance.

Vérifiez que Firefox fait confiance à votre certificat. Pour cela, ouvrez le Certificate Manager de Firefox (cfr [section 4.1.1](#)) et vérifiez que Firefox fait confiance à votre certificat (cfr [section 4.1.4](#)).

Pour tout problème, veuillez parcourir la [section 4.1](#) et vérifier que :

- votre certificat n'a pas expiré
- le certificat de votre fournisseur est dans la liste des autorités de confiance de Firefox (cfr [section 4.1.2](#))

Si vous avez d'autres problèmes liés à l'utilisation de votre certificat avec Firefox, veuillez contacter votre fournisseur de certificat (GlobalSign, Certipost or Isabel).

Erreur 602 : Aucun certificat trouvé. (Firefox uniquement)

Firefox n'a pas pu trouver un certificat valable. Vérifiez que votre certificat est toujours valide, et suivez les indications données dans la [section 4.1](#).

Lorsque je clique sur "OK", la fenêtre de sélection de certificat dans Firefox réapparaît à nouveau. (Firefox uniquement)

Le mot de passe que vous avez tapé n'est pas correct. Attention : il ne s'agit pas du mot de passe de votre certificat (le mot de passe donné par le fournisseur de votre certificat), mais bien du mot de passe défini pour votre "conteneur de certificats". Ce mot de passe n'étant pas défini par défaut dans Firefox, **laissez le champ vide et cliquez sur OK**. Veuillez lire la section [section 4.3](#).