如何使用 **HSM** 來保護 **IIS** 網站伺服器的私鑰**(Private Key)**

How to protect your IIS private key using an HSM

Duncan Jones, 19/09/07

Ideally, you would want to regenerate a certificate using our CSP if you've just bought an HSM to use with IIS, however here are the steps to take in order to protect the existing private key in a new HSM.

Step 1: Export the certificate

- On the *Directory Security* tab, click on *View Certificate....* Go to the *Details* tab and select *Copy to File...* at the bottom this will open the Certificate Export Wizard.
- Hit next and confirm you wish to export the private key.
- Choose the PKCS#12 file type (it's probably your only option) and make sure *Delete the private key if the export is successful* is selected.
- Enter a password to protect this file (and remember it), then choose a save location and you're done.

Step 2: Extract the private key and the certificate

I did these steps on Linux...

- Run the following command on the certificate you exported in step 1:

```
openssl pkcs12 -des3 -in exported_cert .pfx -out exported_cert .pem.
```

You will need to enter the password you specified in step 1, and then choose a new password to protect the PEM file (although you may as well use the same password).

- Run

```
openssl rsa -text -in exported_cert .pem
```

(you will need to enter the password you chose to protect the PEM file). This should output a bunch of info about the key, including (at the bottom) the RSA private key. Cut and paste this key (including the ----BEGIN RSA PRIVATE KEY----- and -----END RSA PRIVATE KEY-----) and place into a new file called privatekey.pem.

- Check this RSA key is sound by running

```
openssl rsa -check -in privatekey.pem.
```

It should say something like RSA Key ok.

- Next, open the exported_cert .pem file in a text editor (or cat it to the terminal) and extract the bottom chunk of the output, which contains the certificate. Copy and paste the text, including the BEGIN CERTIFICATE and END CERTIFICATE lines and save in a new file: mycert .cer.

Step 3: Install the certificate into the IIS server

- In Windows explorer, double click on your new mycert .cer file and choose *Install Certificate...*. Hit next twice, leaving all settings on their default, and then hit finish. It should tell you that you've imported the certificate successfully.
- Next, return to MMC and the properties of your default web site. On the *Directory Security* tab, select *Server Certificate...* and a dialog box should pop up. Hit next, and then choose *Remove the current certificate*. Hit next a couple of times and then hit finish. This should remove the certificate.
- Now, click on *Server Certificate...* again, hit next and this time choose *Assign an existing certificate*. This should display a list of installed certificates to you select the one that corresponds to the one we just installed. Hit next until you can hit finish, closing the dialog box. The certificate is installed.

○ I had some problems identifying which certificate I had just installed. IIS only gives you the option to identify certificates using the "friendly name". Unfortunately, I had many certificates that somehow shared the same "friendly name".

○ To solve this crisis, I added the "Certificates" snapin to MMC, and then located the certificate I had installed within the *Personal* > *Certificates* folder. The only way I could determine which certificate was mine was to compare the thumbprints of mycert .cer and the thumbprints of each of the installed certificates. To view the thumbprint, double click on your mycert .cer file, choose the Details tab, and scroll to the bottom you should see a thumbprint entry. Next, double click on each of the certificates in the snapin folder and compare the thumbprint value.

○ Once you've found the certificate that matches, you can choose *Edit Properties...* on the installed certificate and change the friendly name to something you will definitely identify.

Step 4: Import the private key into the HSM

- Run

C:\nfast\bin\generatekey.exe --import simp le.

Choose a protection type, then choose RSA, then enter the full path to the privatekey.pem file. Specify a ident and a plainname, and the key should be imported.

- Run

C:\nfast\bin\keytst.exe –c -m myca to create a MSCAPI container called myca.

Run

C:\nfast\bin\csputils.exe –m -U ALL, which should list your newly created myca container. The first column of output should list the File ID, which we'll need next.

- Now run C:\nfast\bin\cspimport .exe --import –k XXXX –appname simple YYYY exchange, where XXXX is the ident you chose for your imported key and YYYY is the File ID as returned by csputils.exe. You will be prompted to enter "yes" in order to import.

Step 5: Reassociate the IIS certificate with the HSM key

- Stop the IIS server. To do this, click on Default Web Site in MMC and click the stop button in the toolbar.
- Now run

certutil –f –csp "nCipher Enhanced SChannel Cryptographic Provider" –repairstore my "48 05 d7 6e b2 5f 0e ba 46 6f f2 c4 be 4e a3 11",

replacing the long hex string with the thumbprint of your installed certificate.

- Provided that command completes successfully, we are done! You can now restart the IIS server by pressing the start button in the MMC toolbar.