Setting up ThreeDSecure MPI demos to work with Product Integration Testing (PIT)

These demos demonstrate how to accomplish Product Integration Testing (PIT) with Visa. Although our ThreeDSecure MPI is certified and has gone through Interoperability testing with Visa, every merchant that signs up for 3D Secure, whether they develop the application themselves, use a certified component, or buy an off the shelf solution, are ***required*** to complete PIT testing.

USING THE DEMOS: To begin using these demos, you must first sign up for Product Integration Testing (PIT).

1. Begin this process by filling out the enrollment form at https://dropit.3dsecure.net/PIT/UI?action=enroll.
2. On the enrollment page, it is not necessary that you input your actual Bank Id Number for processing credit card transactions into the BIN field. We recommend using an obviously fake number, such as "999999". It is only necessary that the BIN in your PIT profile matches the MerchantBankId property in the ThreeDSecure control.
3. In addition to the BIN field, you must select the "MPI" checkbox, and then fill out the Merchant ID and Password boxes. These values must match the MerchantNumber and MerchantPassword properties of the ThreeDSecure control, but can otherwise be any value.
4. Leave the "ACS Verify Enrollment URL" box blank.
5. If any of the values in your profile do not match the values set in the ThreeDSecure PIT testing demo, your transactions will not show up on the PIT's "Review Test Activity" page, so double-check that everything is accurate between the demo code and your PIT profile.

PART ONE: The PIT requires client-side authentication for all transactions, so the next step is to generate a certificate request and submit it to the PIT's automated certificate generator.

1. First, copy all the demo files to C:\Inetput\wwwroot\pit
2. Now, select Start->Run and type "mmc" in the box.
3. Click the File menu, and select "Add/Remove snap-in".
4. Click the Add button, and select "Internet Information Services"
5. Open the "**Internet Information Services\local computer\Web Sites\Default Web Site**" directory tree.
6. Right-click on "Default Web Site" and select "Properties"
7. Click on the "Directory Security" tab, and then on "Server Certificate"
8. Select the "Create New Certificate" radio button and press Next.
9. Select a name for your cert request. Something like "PIT Client Cert". Bit length should be 1024, and none of the other radio buttons should be checked. Press Next.
10. Organization and Organizational Unit can be anything.
11. The Common name MUST be the IP Address of your server.
12. Country, State, and City can be any data.
13. Save the request as c:\certreq.txt
14. Now log into the PIT online interface (https://dropit.3dsecure.net/PIT) and click the "Request Certificate" link.
15. Open the c:\certreq.txt file with Notepad, copy the contents, and paste it into the "Cert Request (PEM)" field on the "Request Certificate" page.
16. Once you receive the emailed response, save the **MPIclient_certificate.der** and **MPIclient_certificate_chain.p7** to your desktop.
17. Go back to the Directory Security tab and click "Server Certificate" again.
18. Select the "Process the pending request and install the certificate" radio button and press Next.
19. Browse to the MPIclient_certificate.der file.
20. Click Finish and you are done with part one.

PART TWO: If you view the certificate now, you will note that it is not yet valid. This is because we have not yet installed the root certificate or the intermediate CA certificate. Download the der-formatted PIT Root Certificate from the "User's Test Guide" off of the main PIT home page. The direct link is https://dropit.3dsecure.net/PIT/pit_root.der.

1. Double-click on this DER file, and then click the "Install Certificate" button.
2. On the next screen, select "Place all certificates in the following store".
3. Click "Browse", and click the "Show Physical Stores" checkbox.
4. Put the certificate in "**Trusted Root Certification Authorities\Local Computer**"
5. Click Finish and you're done with part two.

PART THREE: It is now time to install the intermediate certificate, located in the .p7 chain.

1. Open Internet Exporer and select the Tools menu. Then click on "Internet Options".
2. Click the "Content" tab, and then click the "Certificates" button.
3. Press the "Import" button. You will be asked for a file name. Browse to the **MPIclient_certificate_chain.p7** on your desktop and press "Next".
4. Select the "Place all certificates in the following store" radio button, and then press the "Browse" button.
5. Make sure the "Show Physical Stores" checkbox is checked, and place the certificate in "**Intermediate Certification Authorities\Local Computer**". Press Next and then Finish.
6. Your server certificate is now installed correctly on your webserver.

PART FOUR: Because ASP applications running in your webserver do not have access to the local machine's certificate stores, you will need to export all three of these certificates in order for the 3D Secure component to communicate with the PIT's directory server.

1. First, we will export the client-side authentication certificate.
2. Go back to MMC, open the Properties menu for the Default Web Site, click on the Directory Security tab, and view the certificate you installed in Part 1.
3. Select the "Details" tab, and then press the "Copy to File" button.
4. When asked to export the private key, select "Yes, export the private key."
5. On the next screen, the "Personal Information Exchange - PKCS #12 (.PFX)" radio button will be selected, and all the other formats will be grayed out.
6. Under this selection, make sure "Include all certificates in the certificateion path if possible" is checked, and both "Enable strong protection" and "Delete the private key" are **NOT** checked. Now press Next.
7. Choose a password for this certificate. Use something you'll remember. For this example we are using "pitpass"
8. Choose a filename for this certificate. We are using "c:\pitclient.pfx"

To use this certificate in ThreeDSecure component, set the SSLCertStore an SSLCertSubject property like this:

```
obj3DS.SSLCertStoreType     = 2 ' sstPFXFile - because ASP cannot access machine stores
obj3DS.SSLCertStore         = "C:\pitclient.pfx" ' location of pfx file
obj3DS.SSLCertStorePassword = "pitpass" ' password for the pfx file
obj3DS.SSLCertSubject       = "255.255.255.255" ' IP address from part 1
```

9. The ThreeDSecure component can now freely communicate with the PIT server.

PART FIVE: In addition to the certificate used for client-side authentication, all PARes packets are signed, and their signatures must be verified by the ThreeDSecure control. Therefore, both the Root certificate and the Intermediate Signing Certificate must be exported and added to the RootCertificate property.

1. To export these to certificates, you need to install a certificate browser. Go back to mmc, select the File menu and then Add/Remove Snap-in again.
2. Add "Certificates", and when asked what certificates to manage, select the "Computer Account" radio button.
3. Open the "**Certificates\Trusted Root Certificateion Authorities\Certificates**" tree.
4. Double-click the certificate named "pit_root". Select the "Details" tab and press the "Copy to File" button just as before.
5. Select the "Base-64 encoded X.509 (.CER)" radio button and press Next. You will be asked for a file name. We suggest "C:\pit_root.cer".
6. Now open "Certificates/Intermediate Certificate Authorities/Certificates" and export the pit_ca certificate the same way. Use the file name "c:\pit_ca.cer".
7. To add the certificates to the ThreeDSecure component, open the pit_root.cer file and paste the contents into the RootCertificate property. To add the CA cert, open the pit_ca.cer file and paste the contents into the Root Certificate property with a preceding '+'.

For example:

```
obj3DS.RootCertificate = "MIICHzCCAYigAwIBAgIUBJvEyXm..."  ' contents of pit_root.cer
obj3DS.RootCertificate = "+" & "MIICHjCCAYegAwIBAgIVAJysplt..."  ' contents of pit_ca.cer
```

Using the plus (+) sign at the beginning of the second certificate indicates that it is an additional certificate used to verify the signature of a PARes. You can add any number of certificates in this manner.

After this step, the pit_root.cer and pit_ca.cer files on your hard drive are no longer necessary and can be deleted.

8. You are now finished setting up the certificates needed for the ThreeDSecure component to communicate with the PIT servers.

PART SIX: *Note: This step is only needed for the ASP edition, because IIS permissions issues do not allow access to the physical machine certificate stores.*

1. Double-click on the pitclient.pfx file from Part Four. The Certificate Import Wizard will pop up. Click Next, and on the next page, input the password (pitpass) and check the box "Mark this key as exportable." Then press Next. On the next click the radio button "Place all certificates in the following store". Chose the "Personal" store. Click Next, and then Finish.
2. Now use IE and go to the directory server for the PIT. (https://dropit.3dsecure.net:7443/PIT/DS). You will be asked which certificate to use. There should only be one listed, but if there are more, make sure to select the one with your IP address. Then click OK.
3. You should now see "DSServlet running." This means you have connection to the directory server with your client certificate. Double-click on the little lock icon on the bottom bar in IE. A Certificate window should pop up. This is the server certificate that you will need to accept with the SSLAcceptServerCert property. Click the "Details" tab and then press the "Copy to File" button. Choose the "Base-64 encoded X.509" radio button and press Next. Specify a filename to export the certificate to. I will use "c:\servercert.cer". Click Next, and then Finish. Copy the contents of this file, excluding the BEGIN CERTIFICATE and END CERTIFICATE lines, into the SSLAcceptServerCert property.
4. You are now finished setting up the certificates needed for the ThreeDSecure component to communicate with the PIT servers.