Configuring PDF Sign&Seal to use IdenTrust Certs

In order to use the advanced features of IdenTrust Certificates the following configuration changes are required to a default configuration of PDF Sign&Seal:

All PDF Sign&Seal configurations are defined in a PDF Sign&Seal configurations file. However not all the settings can be changed via the product GUI and some need to be edited manually in the configuration file by a system administrator before roll-out to end-users.

Administrator Configuration Steps

The OCSP server address for the IdenTrust bank system needs to be configured and so do the list of acceptable certificate policies. Navigate to this folder:

C:\Documents and Settings\{your username}\Application Data\Ascertia\PDF Sign&Seal\Configurations

Right click on the file called "PSSPreferences.XML" and select "open with" and select Notepad or Wordpad. Use the editor to find and change this block of text so that all the highlighted elements are modified as shown here:

```
<OCSP>
<Nonce>true</Nonce>  {note this is optional}
<CheckResponderRevocation>true</CheckResponderRevocation>
<CheckResponderAuthority>false</CheckResponderAuthority>
<OcspResponseTolerance>
   <ThisUpdate>120</ThisUpdate>
   <NextUpdate>120</NextUpdate>
   <ProducedAt>120</ProducedAt>
</OcspResponseTolerance>
<HardwiredAddresses>{enter your bank OCSP responder address here http://......}
      </HardwiredAddresses>
<SignOCSPRequest Enabled="true">
</SignOCSPRequest>
<OCSPCacheSettings />
</OCSP>
```

Further down the file changes these settings (do check for the latest OIDs with your cert issuer):

```
<PolicyChecking Enable="true">
   <PolicyOids>1.2.840.114021.1.4.2</PolicyOids>          for business hardware signing
   <PolicyOids>1.2.840.114021.1.7.2</PolicyOids>          for business software signing
   <PolicyOids>1.2.840.114021.1.13.2</PolicyOids>          for consumer hardware signing
   <PolicyOids>1.2.840.114021.1.19.2</PolicyOids>          for consumer software signing
   <CheckSubCABasicConstraintSet>false</CheckSubCABasicConstraintSet>
   <CheckSubCAKeyUsageSetforCertandCRL>false</CheckSubCAKeyUsageSetforCertandCRL>
   <CheckEEKeyUsageSetforSigning>0</CheckEEKeyUsageSetforSigning>
</PolicyChecking>
```

Now save these changes, test them and then replace the Preferences.XML file in the existing PDF Sign&Seal set-up with this new file, so it gets distributed to all new users.

End-User Configuration Steps

Start PDF Sign&Seal and Click on the preferences tool in the quick access bar or under the tools tab:
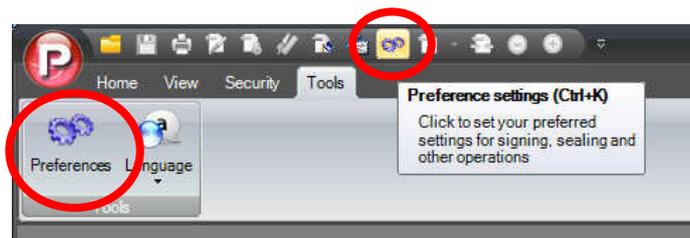
Configuring PDF Sign&Seal

Now click on the Verification tab of the screen that is shown and click the check boxes as shown:
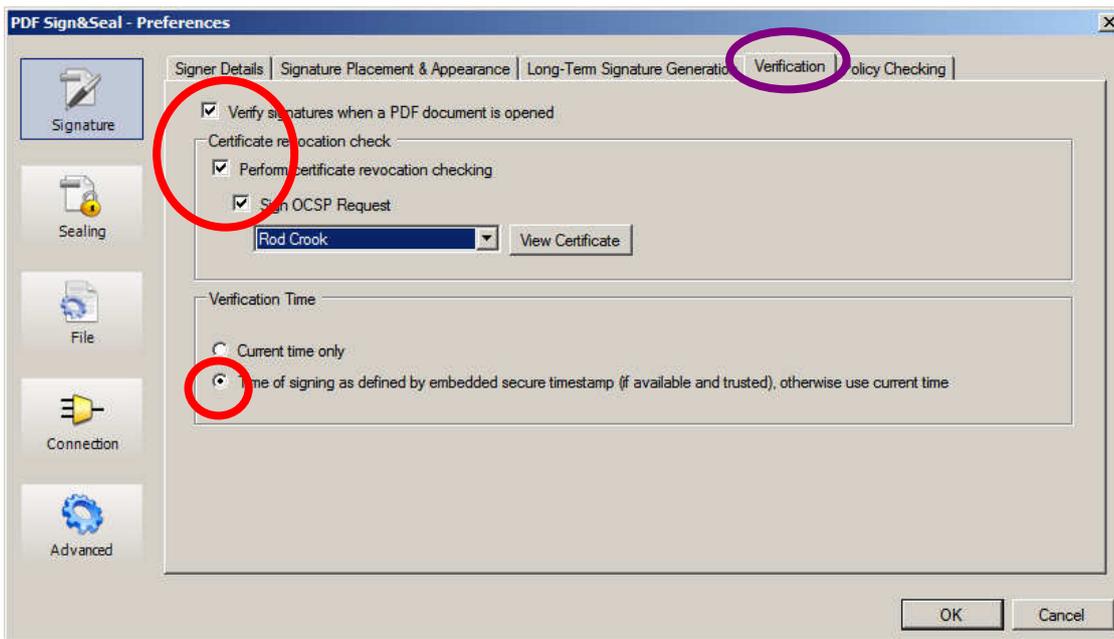
Select the correct certificate in the highlighted drop down list to sign OCSP requests with – typically this will be your IdenTrust utility certificate, however certain banks may request the Identity certificate to be used – check with your issuer.

Click on Policy Checking tab and you will see the acceptable OIDs that were entered in the configuration file.
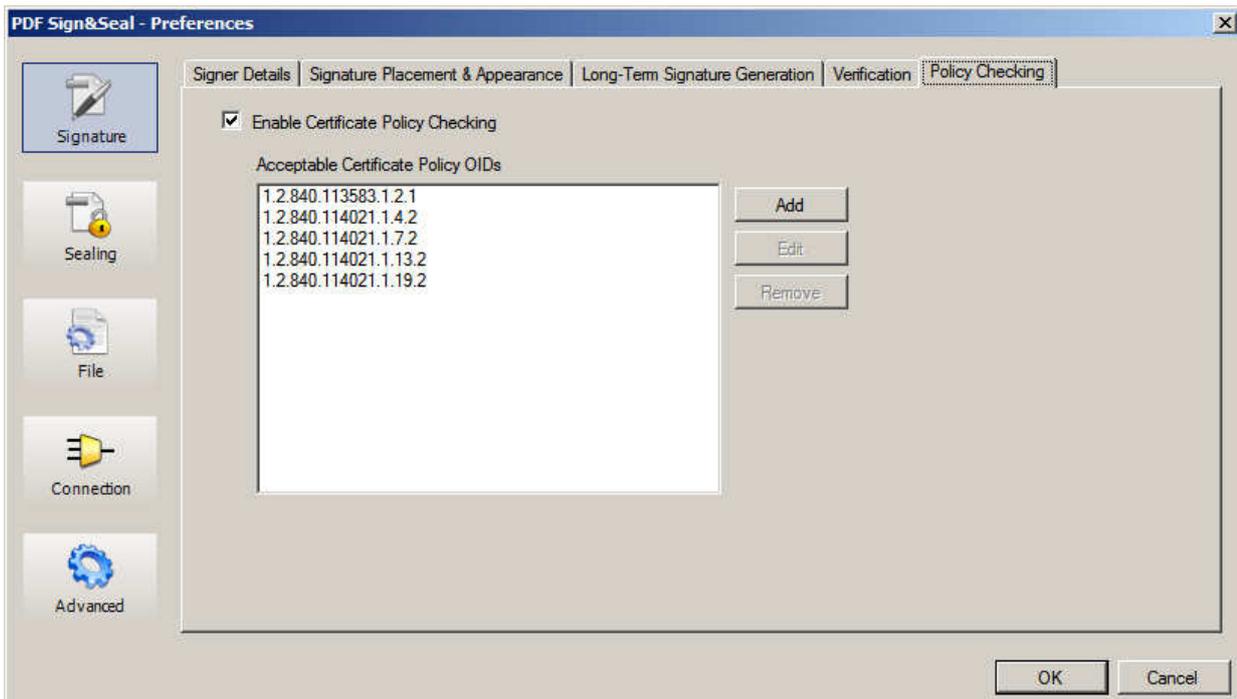
When this tick box is enabled PDF Sign&Seal will ONLY show the certificates that comply with one of these policies. If you do not see any certificates shown under the Signer Details tabs it means that no suitable certificates can be found.

Assuming you have an IdenTrust issued signing certificate installed, then you are ready to sign!

Note: PDF Sign&Seal is still at the pre-compliant stage of the IdenTrust testing process.

Identity Proven, Trust Delivered

ascertia