Using PDF Sign&Seal v4.2 with Adobe CDS Certificates

PDF Sign&Seal v4.2 offer advanced signing features to make it easy for busy managers to sign and approval important documents. This action adds legal weight trust to documents and when used with CDS certificates long-term trust is created with can be checked anywhere in the world.

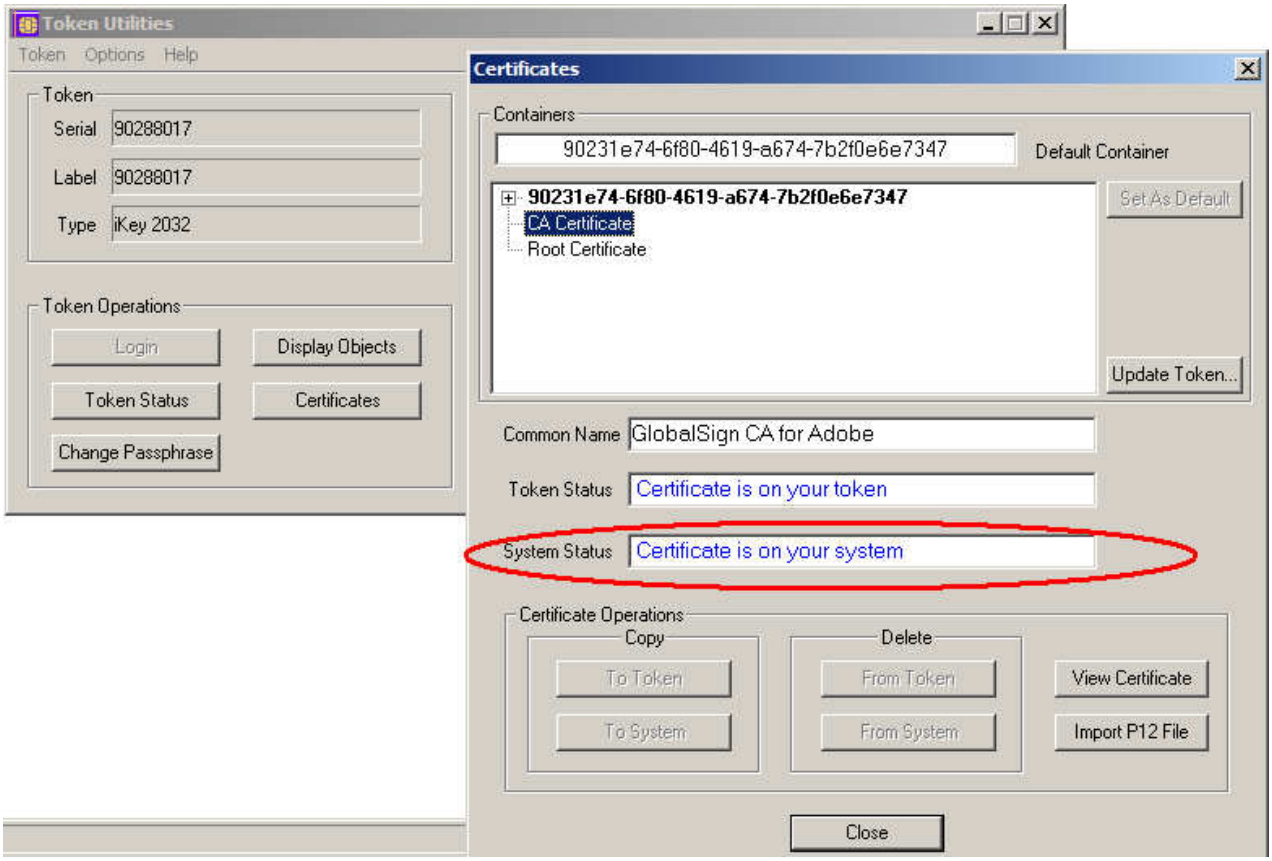
From PDF Sign&Seal v4.2 onwards the use of Adobe Rooted CDS Certificates is automatically recognised and appropriate policies are used which override the defined behaviour. This approach ensures the user experience is optimised and that manual intervention to apply detailed policy settings is no longer required. As an example the address of the Time Stamp Authority no longer needs to be entered in the preferences "long-term signature generation" tab. The URL for TSA was long and complicated and now PDF Sign&Seal simply extracts this from the certificate and uses it.

PDF Sign&Seal also automatically embeds CRL and/or OCSP data for the certificate chain. The user need do nothing.

Note that if the TSA or OCSP VA or CRL data is not available, e.g. perhaps PDF Sign&Seal is being used on an offline laptop, the signature creation process will fail. This is a protection mechanism to ensure that the user is aware that long-term signatures cannot be created.

Before using PDF Sign&Seal you must ensure that the certificate chain is loaded into the Windows CAPI store. Run the SafeNet Token Utilities program found on the Start > All programs menu…

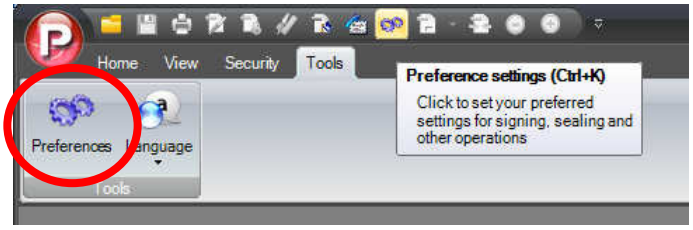
Now click on Certificates and check that the all certificates exist on both the token and the system.

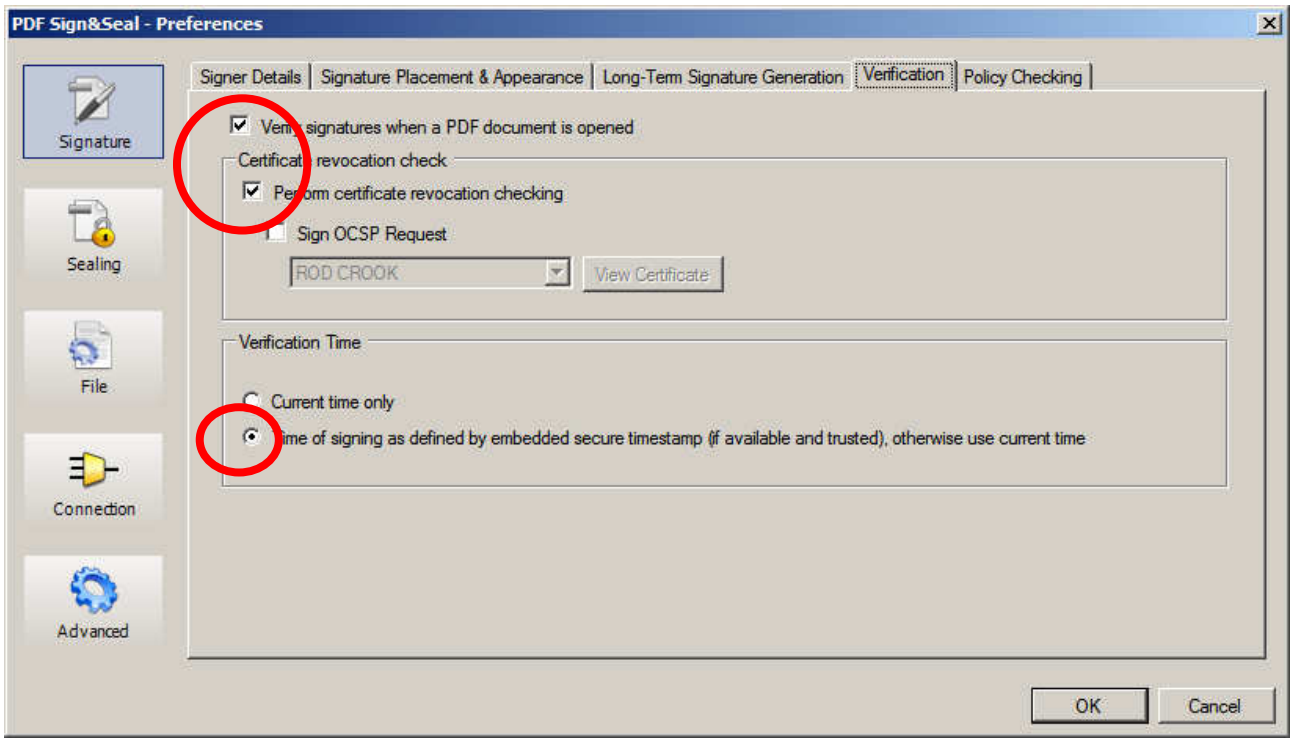


The screenshot above shows the intermediate Issuer CA being reviewed. If the target certificate is not shown as existing on the system then click on the "copy to system" button. Repeat this check for all three certificates, copying to the system as required.

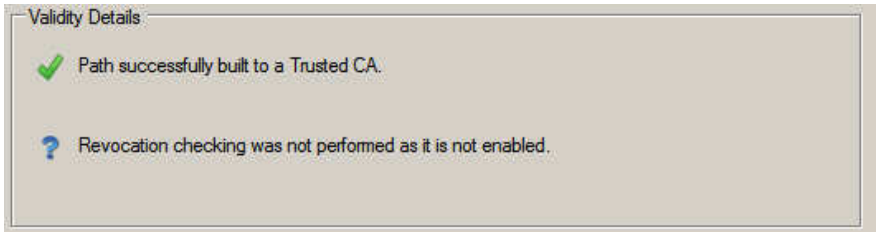
Using PDF Sign&Seal v4.2 with Adobe CDS certificates

If PDF Sign&Seal is required to check the digital signatures within a document then its verify setting should be doubled checked. Within “preferences” and its verification tab ensure that the “Verify signatures when a PDF document is opened” option and the “Perform certificate revocation checking” option are both selected. The following screen shots show how this setting is made:





Without these options a blue question mark will be shown on the signature detail screens indicating that PDF Sign&Seal cannot check to say that the signatures are indeed trusted.



Further Information

Separate datasheets describe the functionality of PDF Sign&Seal. All Ascertia datasheets and solution sheets are signed with a GlobalSign CDS certificate using long-term certifying signatures.

Ascertia software can be downloaded from the main website www.ascertia.com - ask Ascertia or our partners for further details of how our products easily be easily added to your existing documents and workflow systems - ***info@ascertia.com***

For Technical support issues liaise with our technical experts at ***support@ascertia.com***