Enabling Adobe Reader to show a Green Tick for Trusted Certificates from other CAs

Trust is essential in today's e-business environment to meet legislative, regulatory and internal compliance requirements. Ascertia's products respond to these needs by providing advanced digital signature trust services to confirm sign-off and approval within business documents and workflows, and delivering traceability, accountability, integrity, audit as well as secure archiving.

The PDF specifications are open and used by many different vendors to provide useful e-business solutions. With any unprotected PDF document, end-users are generally unable to determine if the document is fraudulent or genuine, who the originator was, whether the document is official, authorised or approved and has it been modified in any way. Many organisations would like to resolve such trust issues, have their PDF documents to be accepted with confidence and to promote their brand image as secure and trustworthy.

Ascertia is a world leader in providing products that can sign and verify PDF and PDF/A documents. However the default configuration of the ubiquitous Adobe® Reader® product means that any signatures that do not chain to the Adobe Root CA are shown with a status of "unknown". This document describes how other CA certificates can be added very simply as a new trust point within Adobe Reader. Now when end-users check the trust status of signed business documents they can find the correct answer.

The Trust Symbols

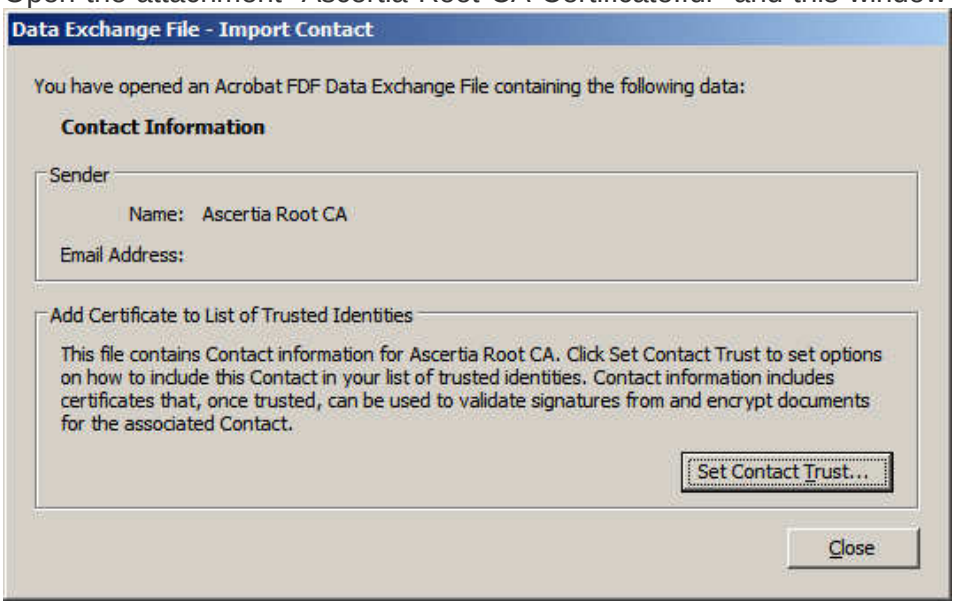
When a document is signed by a trustworthy certificate issued by a Certificate Authority not chained to the Adobe Root CA, most end-users will not see a green 'trusted' tick, instead they see a blue question mark indicating the trust status is 'unknown'. The reason for this is that a certificate chain could not be built to a Trusted Identity. One of the easiest ways of getting your end-users to be able to trust your documents is to create a document like this that can present your Root CA certificate to Reader – now a green tick will be seen if the certificate is trusted. If the certificate is untrusted or if changes have been made to the document (invalidating the signature) then of course a red cross is shown.

How to embed your Root Certificate

This PDF is an example of the type of document that can be created to simply add a new trust point to Reader. To the right is a digital signature signed by Rod Crook of Ascertia under the Ascertia Root CA. It is expected that everyone will see a blue question mark indicating that the signature has an unknown status. Follow these seven steps to get a tick:

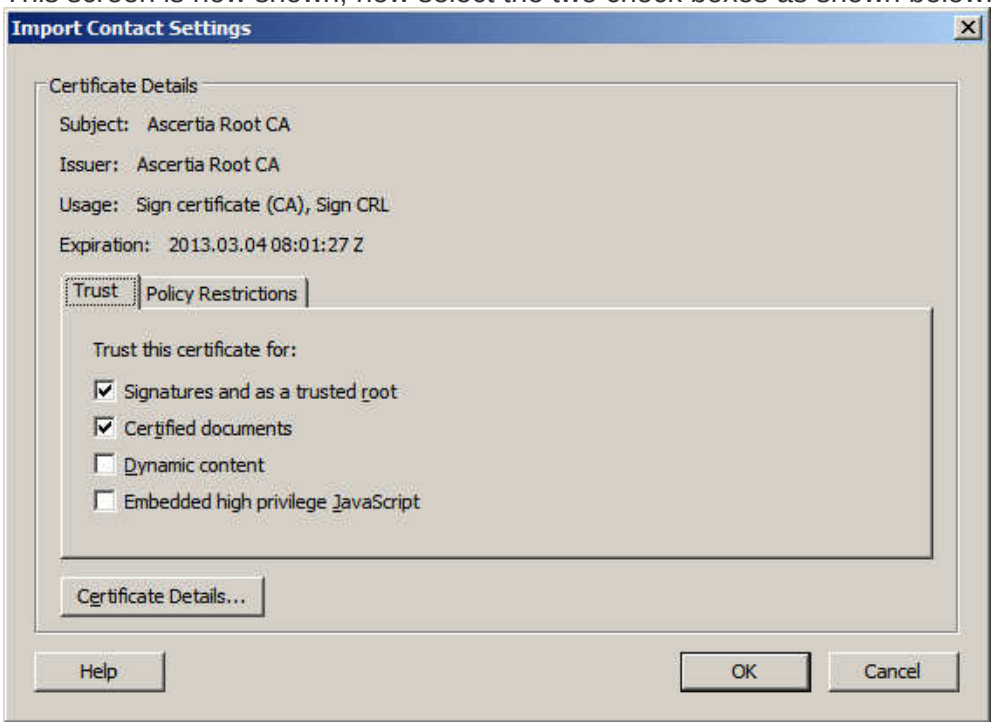
Signed By: Rod Crook
Reason: I approve this document
11/03/2010 22:10:28 GMT +00:00

1) Click on the attachments tab on the left of the screen (it's a paperclip icon as shown):
2) Open the attachment "Ascertia Root CA Certificate.fdf" and this window is shown:

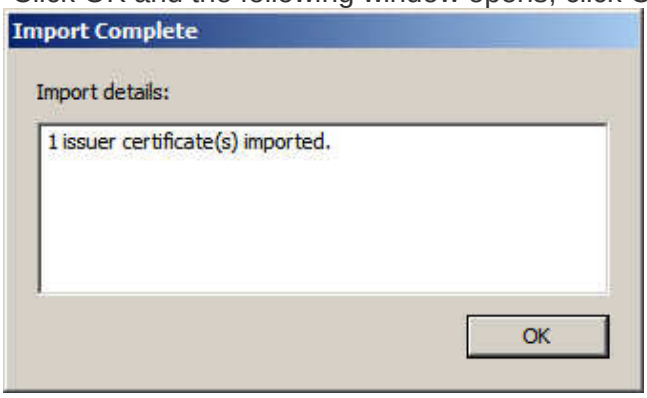


3) Click on the “Set Contact Trust “ button

4) This screen is now shown, now select the two check boxes as shown below:



5) Click OK and the following window opens, click OK again



6) Now click the close button and the update to the Trusted Identities list is complete.

7) Now go back and click on the signature block shown on page 1 to re-validate it - you should see the blue question mark change to a green tick.

If you need further help in understanding the trust aspects discussed here then do contact Ascertia as shown below. The FDF files described can be easily created using Adobe® Acrobat®. The Ascertia products that can be used to sign and verify PDFs include ADSS Server (also called PDF Signer Server), PDF Sign&Seal, Secure Email Server and in future the Trusted Archive Server. The Ascertia web-site www.ascertia.com provides details of these.

For Sales Support: **Email sales@ascertia.com**

For Product Support: **Email support@ascertia.com**