



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 standard is 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 for the PDF documents that they issue.

Ascertia is one of the world's leading vendors of products that can sign and verify PDF and PDF/A documents. However the default configuration of the ubiquitous Adobe® Reader® product means that any certificate that does not chain to the Adobe Root CA is shown as unknown. This document details how other CA certificates can be added very simply as a new trust point within desktop copies of Adobe Reader. After this simple step is completed once end-users can check the correct trust status of the certificates being used to sign your documents.

The Trust Symbols

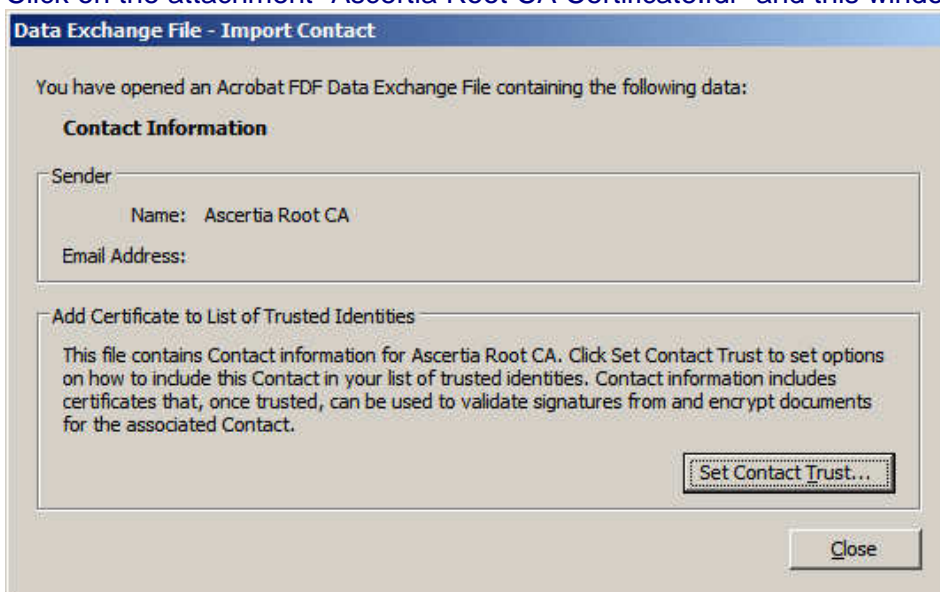
When a document is signed by a trustworthy certificate issued by a CA not chained to the Adobe Root CA most end-users will not see a green 'trusted' tick, instead they see a blue question mark indicating the certificate status is 'unknown'. The reason for this is that a certificate chain cannot be built to a Trusted Identity. If the end-user knows your organisation then one of the easiest ways of getting them 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.



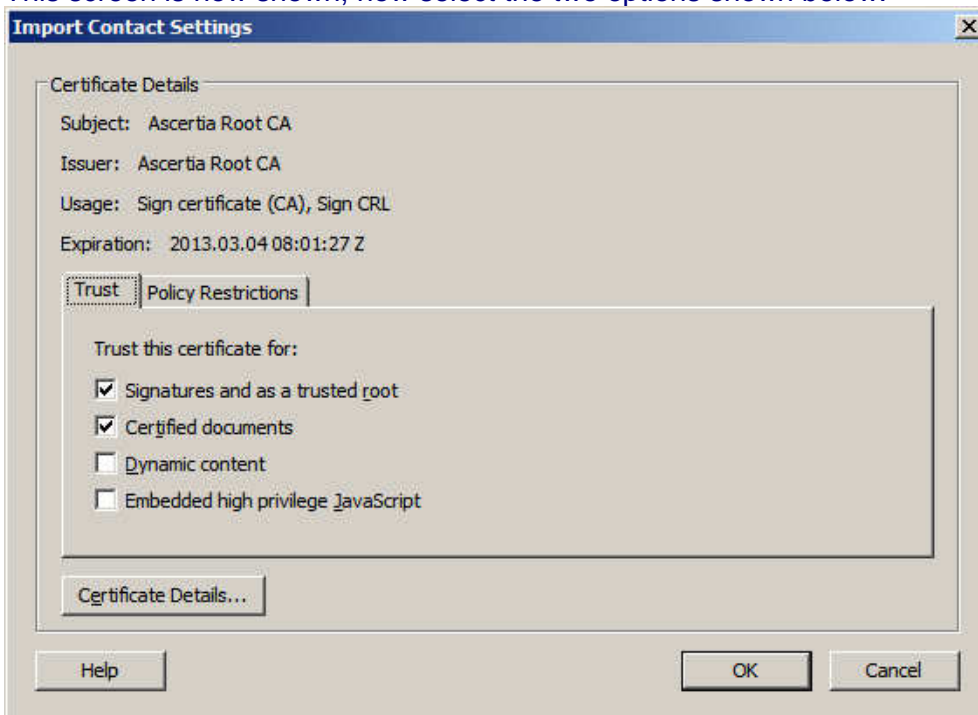
How to embed your Root Certificate

This document is an example of a 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 steps to get a tick:

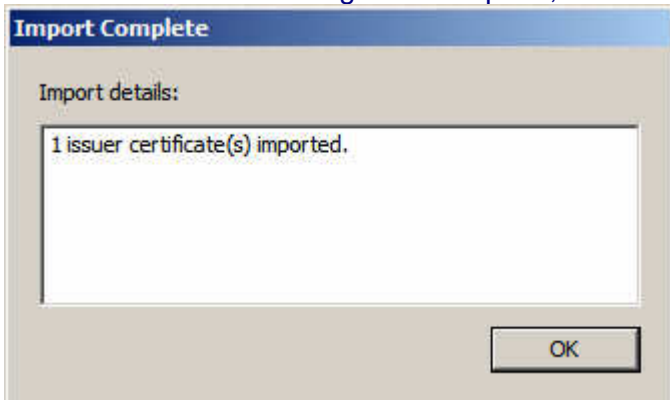
- 1) Click on the attachments icon on the left of the screen (it's a paperclip icon).
- 2) Click on the attachment "Ascertia Root CA Certificate.fdf" and this window opens...



- 3) Click on the “Set Contact Trust “ button
- 4) This screen is now shown, now select the two options 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 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 Ascertia products that can be sued 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 provides details of these.

Contact Details

For Sales Support:

Email sales@ascertia.com

For Product Support:

Email support@ascertia.com

All trademarks are the property of their respective owners.



Identity Proven, Trust Delivered