

Digital Security of Electronic Certificates (eCerts)

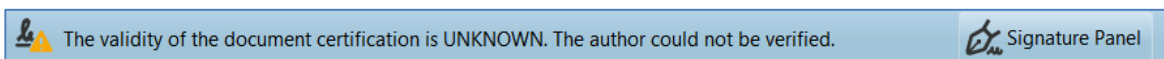
One of the security features AWTA uses to protect the authenticity of Electronic Certificates (eCerts) is a digital signature. It secures both the file and its content against unauthorised changes as any alterations will automatically void the document and display this status to the viewer. A digital signature is present on every eCert we distribute making it integral to the verification of their authenticity.

Enhancements to Certificate security

AWTA is implementing a new and improved digital signature system to secure our eCerts. The “self-signed” signature provides enhanced security features and will be introduced on the 1st July 2015. As a self-signed certificate is not automatically trusted, customers must add it to the list of trusted certificates before it can be used to verify an eCert. This should be done on every computer where our eCerts are viewed.

Trusting our Certificates

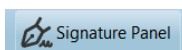
If the new signature is not updated, then our eCerts remain “untrusted” and the following banner will show that their validity is “unknown”.



Once you accept our new digital signature, this message will disappear and all AWTA eCerts will be authenticated automatically. This one-off change is simple to implement, just follow these steps.

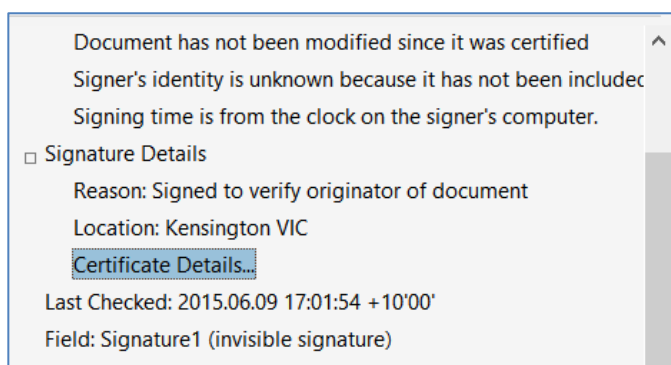
1. Open an eCert that you know came from AWTA.

Click on the “Signature Panel” button at the top right hand corner.

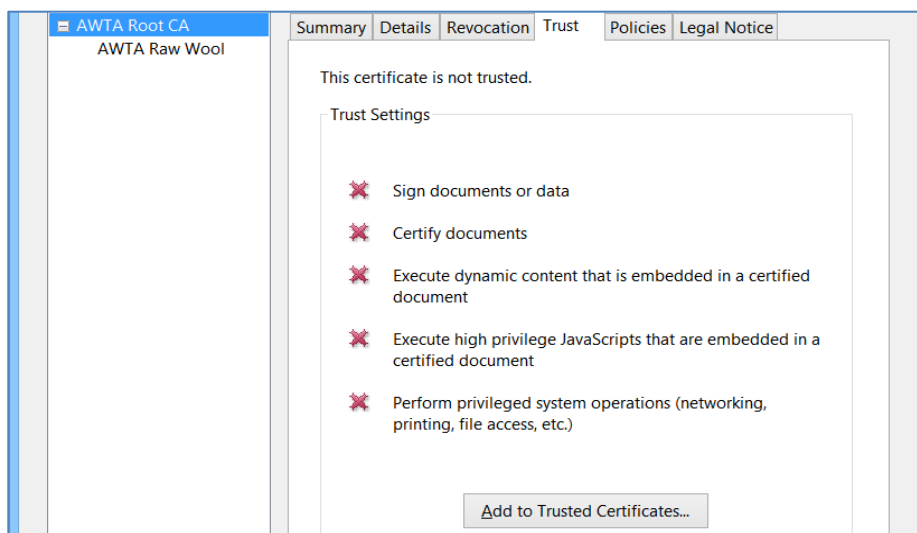


2. The status will show that the signer’s identity is unknown.

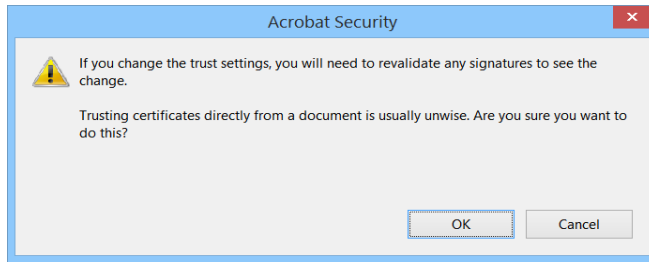
Click on “Signature Details” followed by “Certificate Details”.



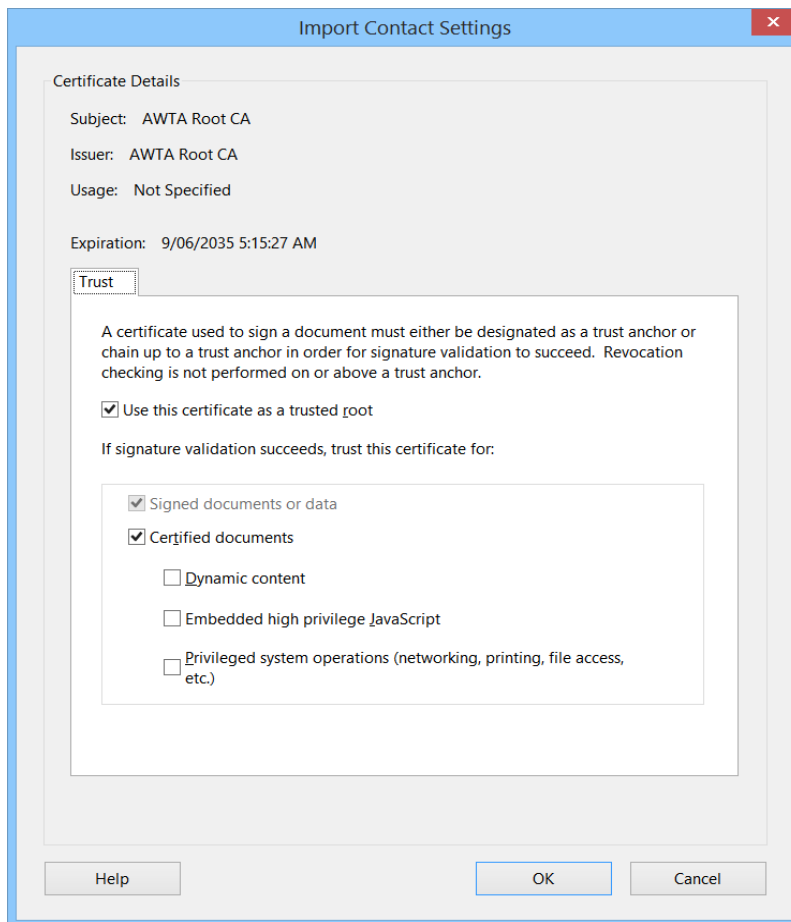
3. The Trust tab shows “This certificate is not trusted”. Select “AWTA Root CA” then click on “Add to Trusted Certificates...”.



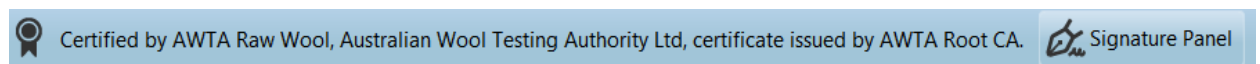
4. Adobe Reader warns the user that trusting certificates directly from a document is not wise. Click [OK].



5. The “Import Contact Settings” display should look like this where “Use this certificate as a trusted root”, “Signed documents or data” and “Certified documents” should all be ticked.



6. Click [OK] then close Adobe Reader.
7. All AWT eCerts will now have valid signatures that appear as shown below.



Certificate Verification facility

Customers who receive eCerts with unknown digital signatures or who suspect certificates they possess are not genuine, can obtain another copy via the Certificate Verification service on our website at the link below:

<http://www.awtaooltesting.com.au/index.php/en/services/certificate-verification>

FURTHER INFORMATION

John Billing
Data Processing Manager Raw Wool

Phone: (03) 9371 2134
Fax: (03) 9371 2190

Email: john.billing@awta.com.au

Ian Ashman
General Manager Raw Wool

Phone: (03) 9371 2101
Fax: (03) 9371 2190

Email: ian.ashman@awta.com.au