Change to Austraclear Website certificates for Internet/ANNI

Attached are the details of the Root CA which needs to be present on systems accessing Austraclear services via Internet or ANNI:

This should have no impact to machines running windows 7 or higher as the Root CA is installed on demand if it has not been required previously.

Certificate Thumbprint:

a8 98 5d 3a 65 e5 e5 c4 b2 d7 d6 6d 40 c6 dd 2f b1 9c 54 36

Field	Value
Public key parameters	05 00
Subject Key Identifier	03 de 50 35 56 d1 4c bb 66 f0 …
Authority Key Identifier	KeyID=03 de 50 35 56 d1 4c b…
Key Usage	Digital Signature, Certificate Si…
Basic Constraints	Subject Type=CA, Path Lengt…
Thumbprint algorithm	sha1
Thumbprint	a8 98 5d 3a 65 e5 e5 c4 b2 d7…

a8 98 5d 3a 65 e5 e5 c4 b2 d7 d6 6d 40 c6 dd
2f b1 9c 54 36

Certificate Information:

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data to be signed with the current time

Issued to: DigiCert Global Root CA

Issued by: DigiCert Global Root CA

Valid from 10/11/2006 **to** 10/11/2031

A check can be performed on Windows in a few ways. These are:

1) **Via Powershell on the machine connecting to Austraclear:**

```
Get-ChildItem Cert:\LocalMachine\AuthRoot\ | sls A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436
```

Expected output should be:

```
[Subject]
```

CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US

[Issuer]

  CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US

[Serial Number]

  083BE056904246B1A1756AC95991C74A

[Not Before]

  10/11/2006 11:00:00 AM

[Not After]

  10/11/2031 11:00:00 AM

[Thumbprint]

  A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436

2) Via MMC (as administrator):

Start > run > mmc
File > Add/Remove Snap-in
Select Certificates from the left, Click Add, Select Computer Account > next > Local Computer >
Finish > OK
Expand Certificates, Trusted Root Certification Authorities, Certificates
Look for "DigiCert Global Root CA".

Double Click the certificate and select the Details tab. Scroll down to Thumbprint and confirm it
matches the thumbprint at the start of the document. That is,

```
a8 98 5d 3a 65 e5 e5 c4 b2 d7 d6 6d 40 c6 dd 2f b1 9c 54 36
```


3) Digicert online checker (for internet connected computers)

Browse to https://global-root-ca.chain-demos.digicert.com/ . If the page loads successfully with no SSL
chaining errors, the appropriate Root CA is installed.

A download link is also available for the DigiCert Global Root CA:

https://www.digicert.com/CACerts/DigiCertGlobalRootCA.crt

Installation of the root CA can be performed by your administrator. Steps can be found below:
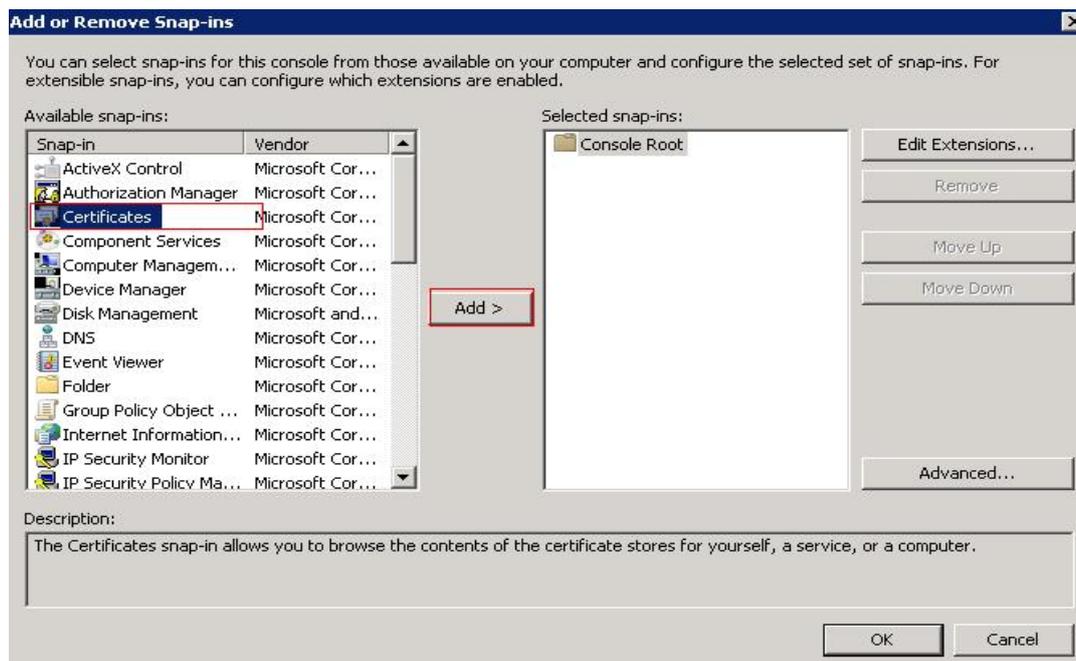
Click Start -> Run -> Enter 'MMC' and click 'OK'
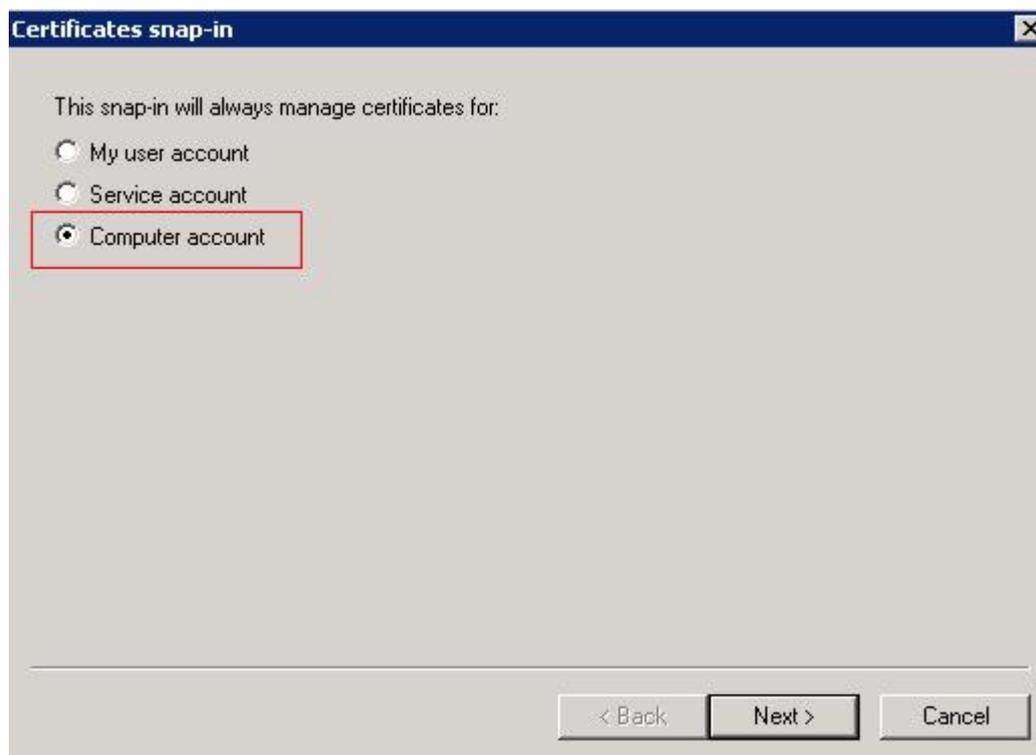
2. Click File -> Add/Remove Snap-In…
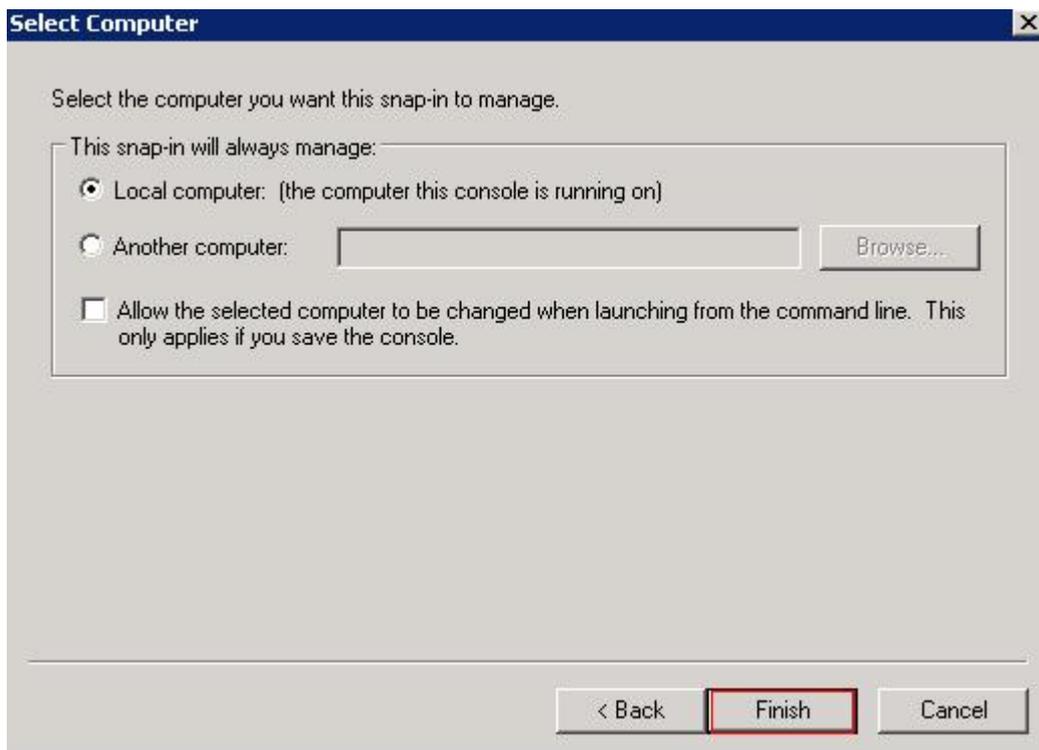
3. Add Certificate

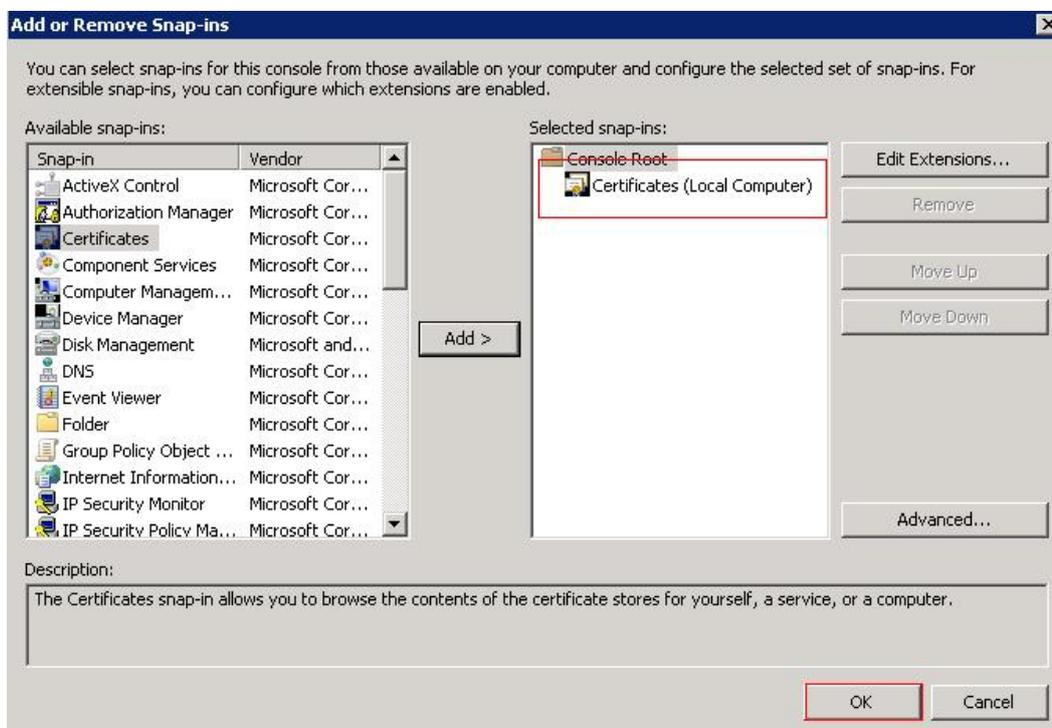Select 'Certificates' in left panel and click 'Add' to move to right panel , Then Click 'OK'

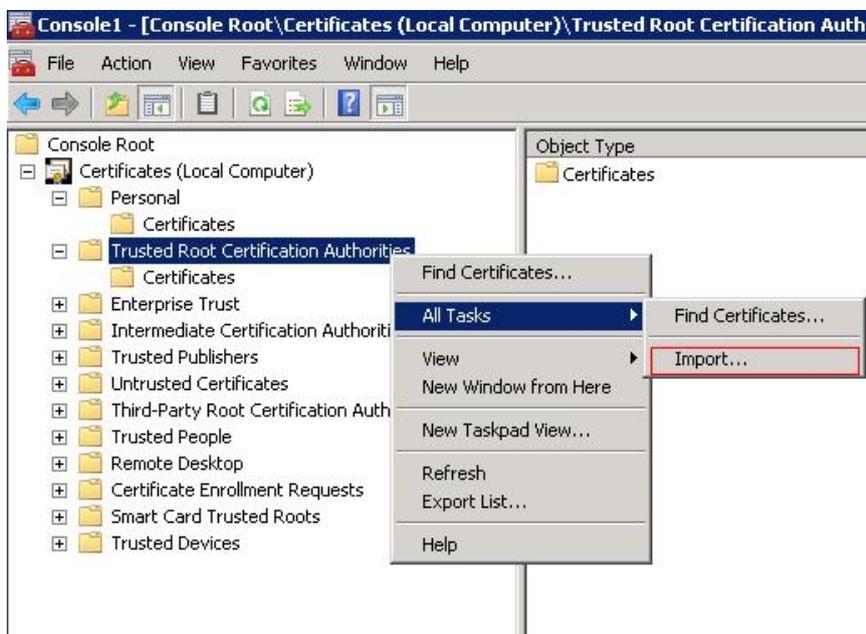4. Select 'Computer Account' option and click 'Next'

5. Click 'Finish'

6. Click 'OK'

7. Start to import Trusted Root Certificate

A. Expand Certificates Node;

B. Right click Trusted Root Certificates -> All Tasks -> Import.
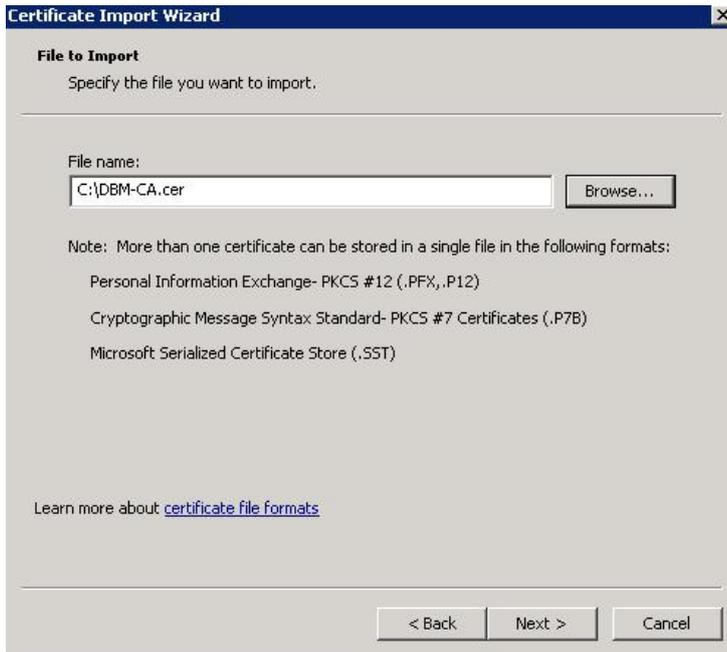

8. Click Next
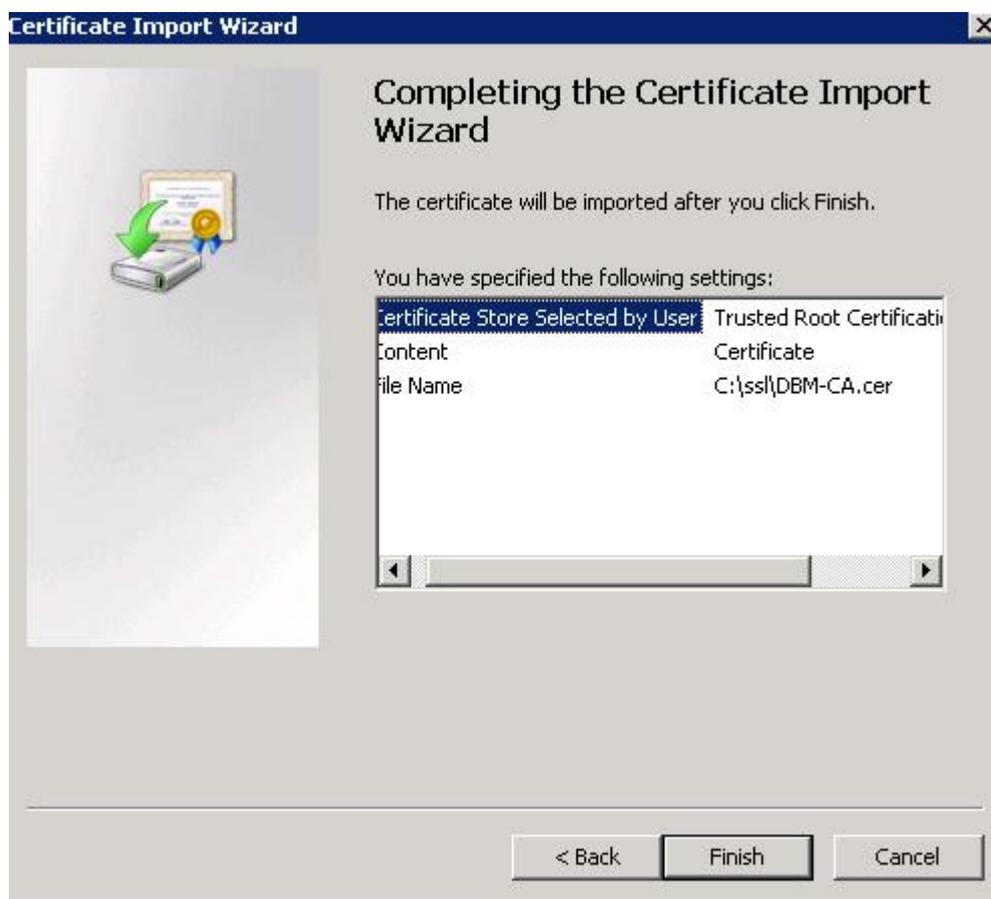

9. select downloaded Certificate file

Click 'Browse' to select correct Certificate file and click Next

10. Click Next

11. Click Finish

12. Done