Few troubleshooting scenarios and steps to troubleshoot

1. Not able to start CA service
2. Make sure the root CA certificate is in the trusted root store
3. The Root CA certificate is valid and not expired.
4. The CA is able to validate its own certificate  
    export the root CA certificate in .cer format.  
    Execute the command certutil –verify –urlfetch <cert.

IF  
Error: The system cannot find the file specified. 0x2 (WIN32: 2)". The policy module for a CA is missing or incorrectly registered. To view or change policy module settings, rigth-click on the CA, click Properties, and then click policy module tab.  
Then compare the number of certificate for the CA with the registry key "CACertHash"  
under HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\CA

IF

Failing in revocation check, fix the revocation errors.

1. Check the permissions on the Machinekeys folder

Give Administrators and System full control, or the service account that is trying to access

the MachineKeys.

1. Check if the CA certificate private key is on the HSM and the HSM is connected.

Try to verify the key set, execute certutil –verifykeys

1. If still the issue persists then enable debug logging of the CA service.  
   To enable logging execute the command certutil.exe -f -setreg ca\**debug** 0xffffffff Collect the following logs

|  |  |
| --- | --- |
| • | %Systemroot%\certsrv.log (Certsrv.exe) Certificate Services |
| • | %SystemRoot%\certutil.log (Certutil.exe) |
| • | %SystemRoot%\certreq.log (Certreq.exe) |
| • | %SystemRoot%\certmmc.log (Certmmc.dll) Certificate Services MMC snap-in |
| • | %SystemRoot%\certocm.log (Certocm.dll) Certificate Services Setup |

1. Not able to request certificates.
2. Make sure the root CA certificate is in the trusted root store
3. The Template is published on the CA.
4. The user / system have permissions to request certificate from the CA.
5. The user / system have permissions on the template.
6. The client is able to validate the CA certificate and the chain.  
   Export the issuing CA certificate in .cer format.  
   Execute the command certutil –verify –urlfetch <cert.

If failed for revocation check, fix it.

1. The CA appears in the Enrollment Services in Active Directory.  
   CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,DC=contoso,DC=com
2. Verify that the CERTSVC\_DCOM\_ACCESS group has the appropriate DCOM Access   
   permissions and DCOM Launch and Activation permissions on the computer that hosts   
   the certification authority.   
   1. Click Start, point to Program, point to Administrative Tools, and then click   
   Component Services.   
   2. Expand the Component Services node.   
   3. Expand the Computers node.   
   4. Right-click the My Computer node, and then click Properties.   
   5. Click the COM Security tab.   
   6. Under Access Permission, click Edit Limits.   
   7. Verify that the CERTSVC\_DCOM\_ACCESS group has Allow Local Access and Allow   
    Remote Access permissions, and then click Cancel.   
   8. Under Launch and Activation Permissions, click Edit Limits.   
   9. Verify that the CERTSVC\_DCOM\_ACCESS group has Allow Local Activation and

Allow Remote Activation permissions, and then click Cancel.   
10. Click Cancel, and then close the Component Services console.

1. Check if the CA and the clients are in the same domain.
2. No firewalls between them
3. Check the event logs for any errors.
4. Take a network trace.
5. Not able to see computer based templates on web enrollment page.
6. Make sure on the template under subject name “Supply in request “is checked.
7. The user has permission to view the template.
8. The Template is published on the CA.
9. In case of 2008 R2, make sure the template is not a V3 template.
10. Try restarting IIS using iisreset.
11. Restart the CA service.
12. LDAP over SSL not working.
13. Make sure the domain controller has a server auth certificate.
14. Make sure the root CA certificate is in the trusted root store.
15. The domain controller is able to validate its own certificate.   
     Export the domain controller certificate in .cer format.  
     Execute the command certutil –verify –urlfetch <cert>

If any revocation errors, fix them.

1. Verify if the client is able to validate the domain controllers certificate   
   Export the domain controller certificate in .cer format.  
   Execute the command certutil –verify –urlfetch <cert>

If any revocation errors, fix them.

1. On the domain controller the certificate is associated with the private key.

To confirm, copy the Thumb print of the DC certificate.

On the DC execute the command certutil –repairstore MY “<Thumb print>”

1. Check the permissions on the Machinekeys folder

Give Administrators and System full control, or the service account that is trying to access the

MachineKeys.

1. In case of 2003, if the domain controller received a new certificate as the old certificates expired then try rebooting the domain controller.
2. If it’s a 2008 or 2008 R2 domain controller, import the certificate with the private key in the “Active directory domain service” service store.
3. Take a network trace.
4. Auto enrollment failing.
5. Make sure the root CA certificate is in the trusted root store
6. The user / system have permissions on the template to auto enroll.
7. The user account and computer account must have Read, Enroll, and AutoEnroll permissions on the certificate template.
8. The group policy for auto enrollment is enabled and is applied to the user / system.
9. Verify if the client is able to validate the issuing CA certificate   
    Export the issuing CA certificate in .cer format.  
    Execute the command certutil –verify –urlfetch <cert>.

If any revocation error, fix them.

1. The template is published on the CA.
2. Try restarting the CA service.
3. See there is 3rd party Gina installed. If yes remove it and use MSgina.  
   HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
4. Try requesting certificate using MMC.
5. Verify that the CERTSVC\_DCOM\_ACCESS group has the appropriate DCOM Access   
   permissions and DCOM Launch and Activation permissions on the computer that hosts   
   the certification authority.   
   1. Click Start, point to Program, point to Administrative Tools, and then click   
   Component Services.   
   2. Expand the Component Services node.   
   3. Expand the Computers node.   
   4. Right-click the My Computer node, and then click Properties.   
   5. Click the COM Security tab.   
   6. Under Access Permission, click Edit Limits.   
   7. Verify that the CERTSVC\_DCOM\_ACCESS group has Allow Local Access and Allow   
    Remote Access permissions, and then click Cancel.   
   8. Under Launch and Activation Permissions, click Edit Limits.   
   9. Verify that the CERTSVC\_DCOM\_ACCESS group has Allow Local Activation and

Allow Remote Activation permissions, and then click Cancel.   
10. Click Cancel, and then close the Component Services console.

1. Check the event logs for any errors.

If no events like event id 2, 3, 19, 21 then enable event logging.

#### To Enable auto enrollment event logging For user Autoenrollment failures HKEY\_CURRENT\_USER\Software\Microsoft\Cryptography\Autoenrollment: Create a new DWORD value named AEEventLogLevel"; set value to 0.

#### Machine Autoenrollment HKEY\_LOCAL\_MACHINE\Software\Microsoft\Cryptography\Autoenrollment: Create a new DWORD value named "AEEventLogLevel", set value to 0.

1. Not able to decrypt files.
2. Compare the thumb print of the user certificate with the thumb print on the file, Properties of the file > Advance > Details.
3. Check the NTFS permissions.
4. See if the data recovery agent is able to decrypt the file.
5. Copy the thumb print of the user certificate and execute the command certutil –repairstore MY “<Thumb print>”
6. Check the type of profile the user has, roaming or local.
7. Is the encrypted file on the file server, if yes the private key associated with be in the profile created on the file server and not the users workstation.
8. Try exporting the certificate with the private key and then importing it again. While importing make sure you do not select the option “Enable strong private Key protection”.
9. Generate Request to send it to 3rd party CA.

Use the article <http://support.microsoft.com/kb/931351> to generate the inf file.  
 Execute the command certreq -new request.inf request.req  
 Submit the request to the CA and issue a certificate.  
 Once you get the certificate from the CA certreq -accept certnew.cer  
   
 If you use MMC to import the certificate the private key will not be associated to the   
 certificate.  
 In that case copy the thumb print of the certificate.  
 In command prompt execute the command certutil –repairstore MY <thumbprint>

1. Moving certificate authority.

If the destination server is 2003 then the hostname needs to be the same.  
You can follow the article <http://support.microsoft.com/kb/298138>

From 2003 to 2008, inplace upgrade.  
<http://technet.microsoft.com/en-us/library/cc755153(WS.10).aspx>  
  
From 2003 to 2008 R2, inplace upgrace or backup and restore.  
<http://technet.microsoft.com/en-us/library/ee126170(WS.10).aspx>

Few other links on migration  
 <http://technet.microsoft.com/en-us/library/ee126140(WS.10).aspx#BKMK_JoinDom>   
 <http://technet.microsoft.com/en-us/library/cc742388(WS.10).aspx>   
 <http://technet.microsoft.com/en-us/library/ee126102(WS.10).aspx>

1. Few errors when you execute certutil –verify –urlfetch <cert.cer>

Example 1:

A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file. 0x800b0101 (-2146762495)

------------------------------------

Expired certificate

Example 2

The certificate is revoked. 0x80092010 (-2146885616)

------------------------------------

Certificate is REVOKED

Leaf certificate is REVOKED (Reason=6)

Example 3

A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider. 0x800b0109 (-2146762487)

------------------------------------

Verifies against UNTRUSTED root

Example 4

An internal certificate chaining error has occurred. 0x800b010a (-2146762486)

------------------------------------

419.3000.0: 0x800b010a (-2146762486)

Incomplete certificate chain

Cannot find certificate:

CN= Contoso Issuing CA, DC=Contoso, DC=Com

Example 5

The revocation function was unable to check revocation for the certificate. 0x80092012 (-2146885614)

------------------------------------

Revocation check skipped -- no revocation information available

Certificate is valid