Troubleshooting Errors When Using DSC

When you try to register a Digital Signature Certificate (DSC) or upload a form with signature on it, you may face errors such as,

- "*Your* Certifying Authority (*CA) is not trusted. Please use a trusted CA*".
- "User Id against this Digital Certificate already exists."
- "*Your certificate has been revoked.*"

Let us look at the steps to fix the mentioned errors.

## Steps to Troubleshoot Error –"*Your CA is not trusted. Please use a trusted CA* "

There are three steps that you need to follow to troubleshoot the error.

Steps 1

To use a trusted Certifying Authority (CA), follow the steps mentioned below.

1. Open the Internet Explorer.
2. In the Internet Explorer, select the **Tools > Internet Options** command.
3. The Options dialogue box is displayed. Click the **Content** tab.
4. Under the Certificates section, click the **Certificates** button.
5. The Certificates dialogue box is displayed. The dialogue box displays a list of certificates that are installed on the computer. **Select the correct certificate** and click the **View** button to open the certificate.

6. Under the Certificate Information section, check the **Issued by** and **Valid from and to** details. The DSC must be issued by a trusted CA and the dates must be as per DSC validation.
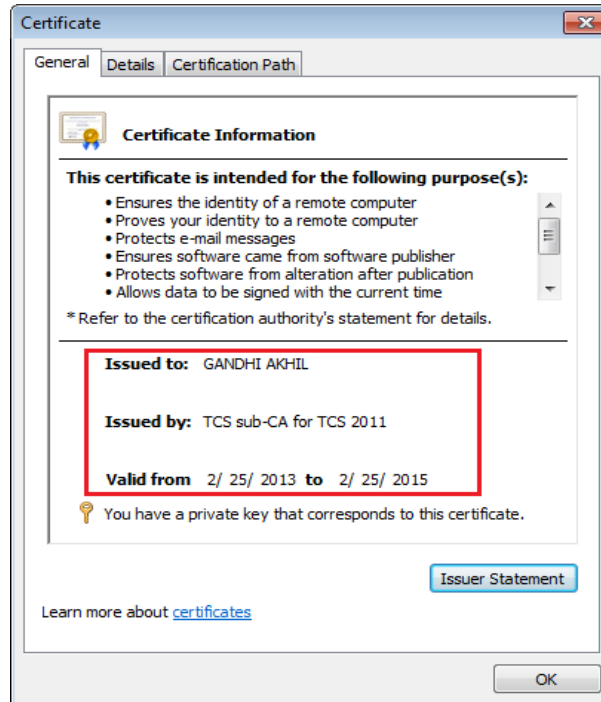
Note: Following trusted CAs can issue a DSC that is recognized by MCA.

- Tata Consultancy Services (TCS)
- National Informatics Center (NIC)
- IDRBT Certifying Authority
- SafeScrypt CA Services, Sify Communications Ltd.
- (n) Code Solutions CA
- MTNL Trust Line
- *Customs & Central Excise
- E-MUDHRA

*Does not issue DSCs to person other than those from the Department

7. If the current DSC is not issued by a trusted CA, then get a new DSC from CA.

Step 2

If the certificate was issued by a trusted CA and still you receive an error for not using a trusted CA, follow the steps:

1. Click the **Certification Path** tab in the Certificates dialogue box.
2. Check the details in the **Certificate path** and **Certificate status** section.
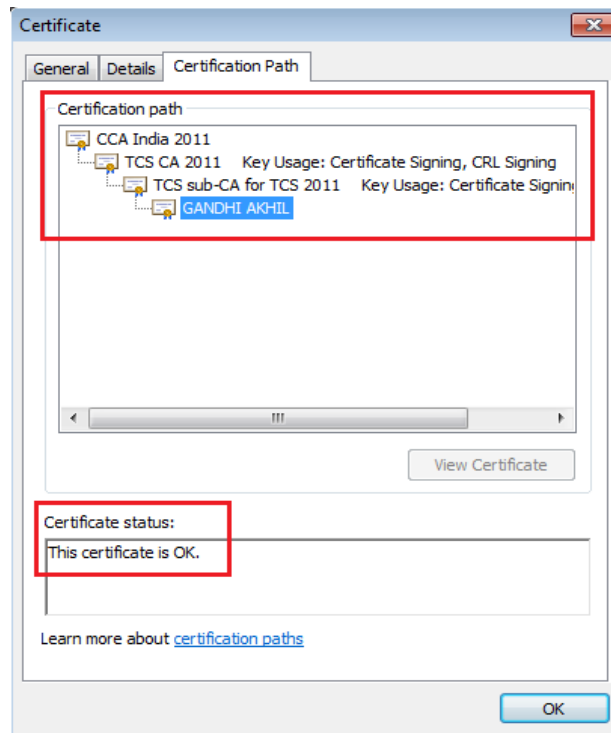
3. In case the trust chain is missing under the Certification Path section, check with CA for the trust chain. If there is a trust chain, follow steps given below:

Note: The subject key identifier of parent and the Authority Key Identifier of immediate child should be same in the certificate.

   a. In the Certification path section, select the parent (CCA India 2011) and click on the **View Certificate button**.
   b. Click the **Details** tab and click on Subject Key identifier as shown below.
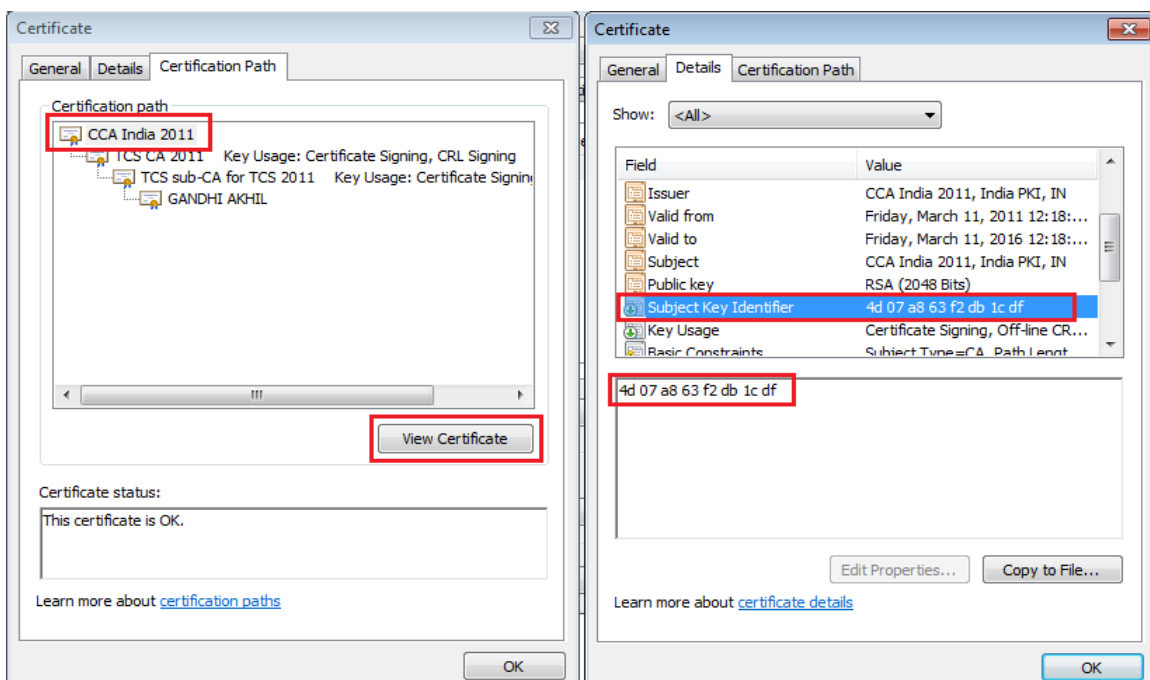
c. Select the immediate Child (TCS CA 2011) and click the **View Certificate** button.

d. Click the **Details** tab and select the Subject Key identifier.
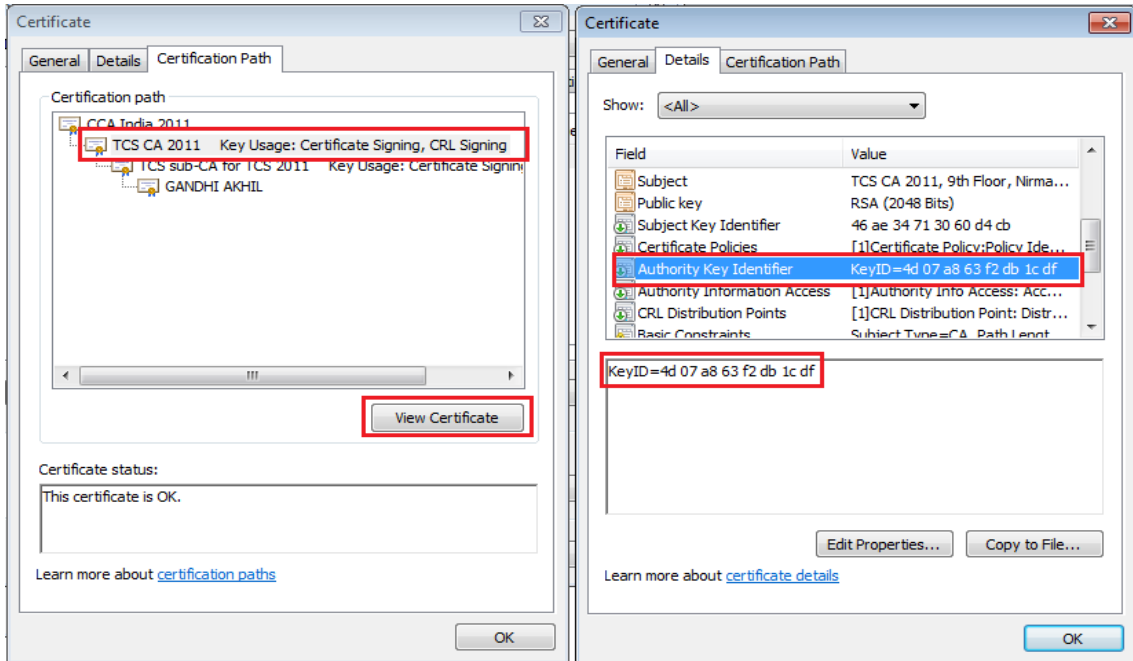
Repeat step 3 for all nodes in .CER. If the values do not match, Get in touch with your CA as the DSC that you are using is having some problem with trust chain.

Step 3

If the parent and child CAs match and still you face the same error of not using a trusted CA, check, whether the sub CA or parent CA has changed its root certificate or not. If the Root certificate has changed for the CA then that root certificate has to be installed in MCA server.

Note: If after following all three steps you still face a problem, raise a complaint at http://www.mca.gov.in/MCA21/ and click on the **User Complaints & Grievances link.** When raising a ticket, provide the .Cer file and the screen shot of the error message that you are facing.

Steps to Troubleshoot Error –"DSC Already Registered "

When you are trying to register your DCS with the MCA21 application and you face error message , "DSC Already Registered ", then follow the steps :

1. Open the Internet Explorer.
2. In the Internet Explorer, select the **Tools >** Internet Options command.
3. The Options dialogue box is displayed. Click the **Content** tab.
4. Under the Certificates section, click the **Certificates** button.
5. The Certificate dialogue box is displayed. Click the **Details** tab and check the **Serial number** and **Issuer** details.
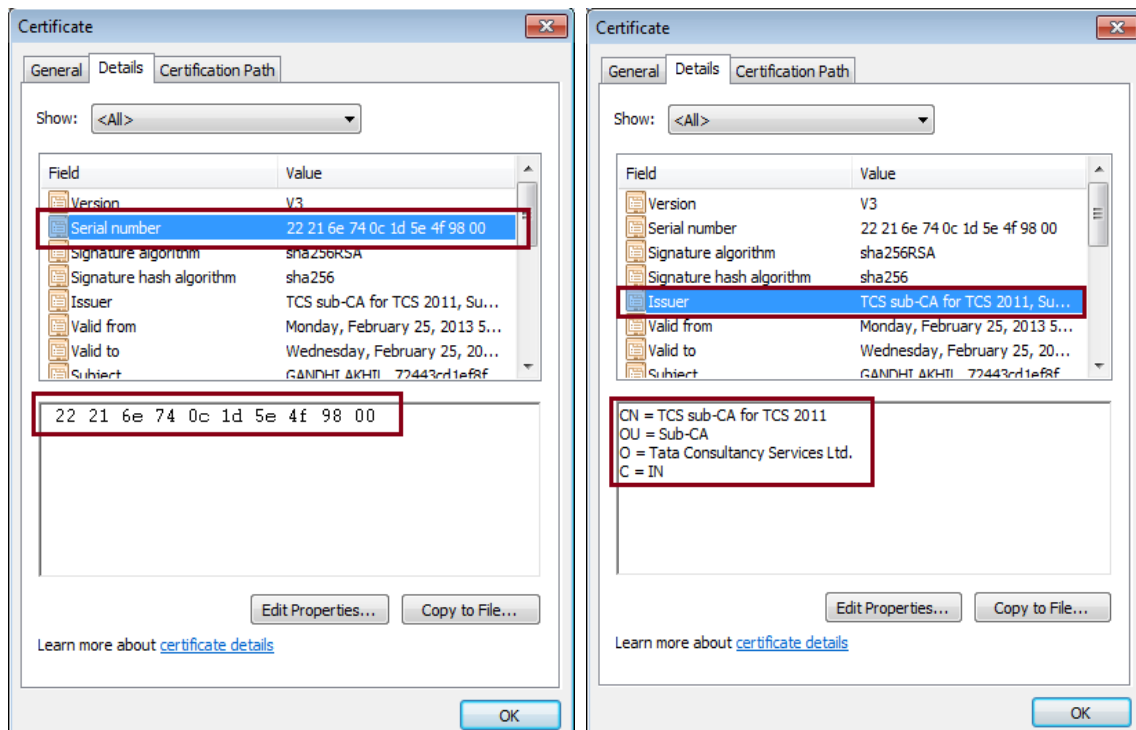

6. Open the http://www.mca.gov.in/MCA21/ Web site and click the **User Complaints & Grievances** link. Raise a ticket and file a complaint providing the serial number, issuer of the certificate along with the screen shot of the error message.

Steps to Troubleshoot Error – "DSC Revoke"

When using a DSC, if you face error message, "DSC Revoked ", then follow the steps to remove the error message:

1. Open the Internet Explorer.
2. In the Internet Explorer, select the **Tools >** Internet Options command.
3. The Options dialogue box is displayed. Click the **Content** tab.
4. Under the Certificates section, click the **Certificates** button.
5. Under the **Certificate Information** section, check the **Issued by** and **Valid from and to** details. The DSC must be issued by a trusted CA and the dates must be as per DSC validation as shown in the screenshot below.
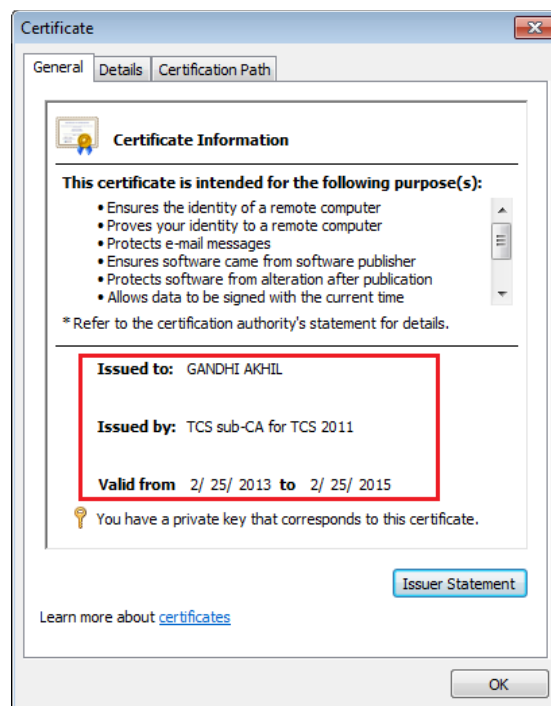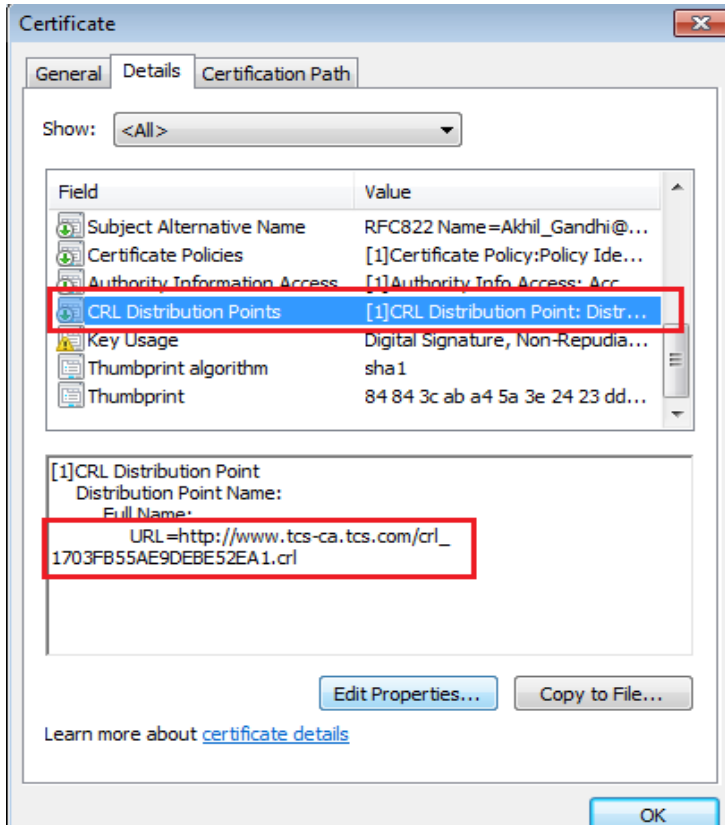
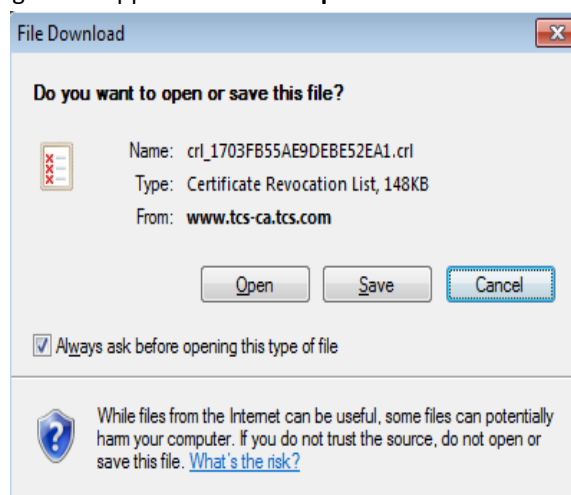6. Click the **Details** tab and check the details such as, **Serial number** and **Issuer.**
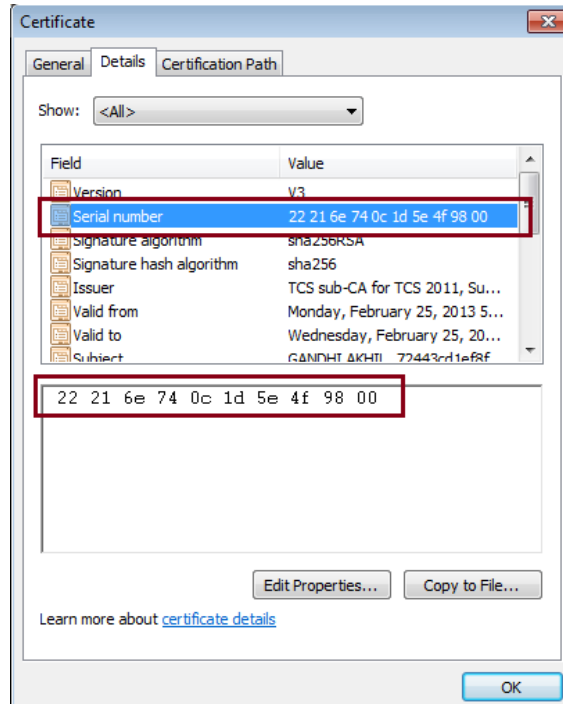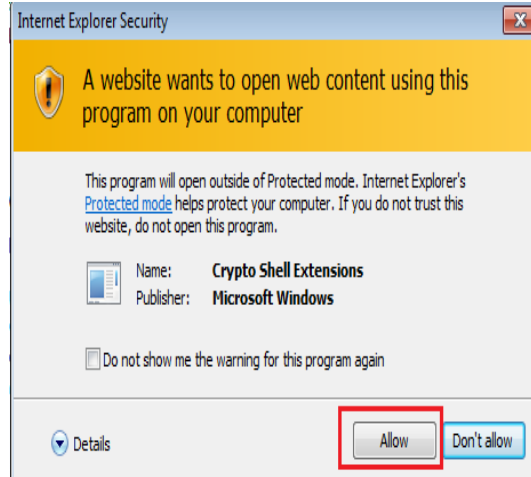
7. In the Details tab, **select CRL (Certificate Revocation List) Distribution points**.

8. Copy the URL of CRL and paste it in Internet Explorer to open the file.
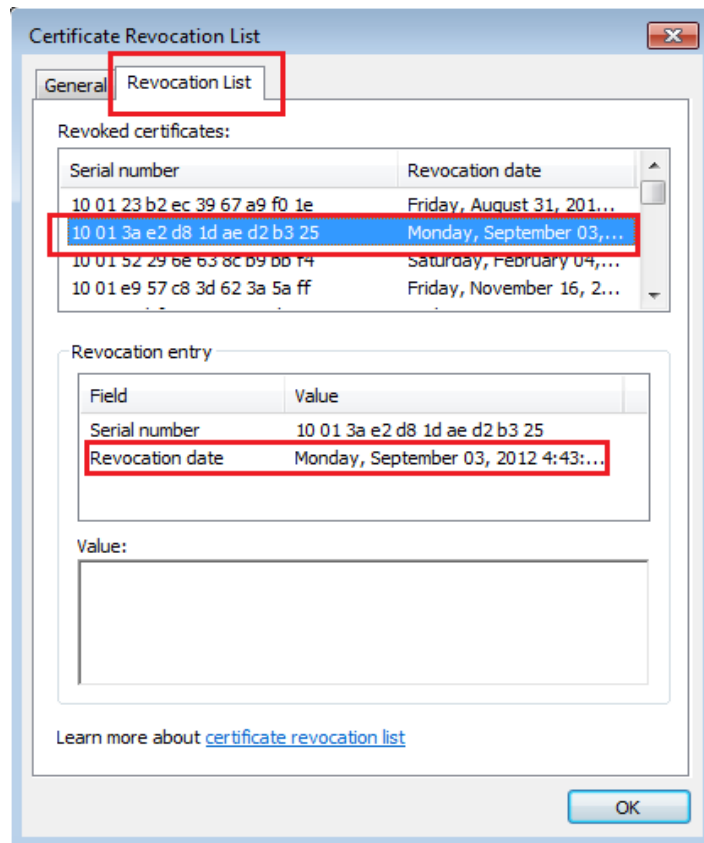9. The File Download dialogue box appears. Click the **Open** button.

10. The Internet Explorer Security dialogue box is displayed. Click the **Allow** button.

11. In the Web page displayed, check whether the certificate Serial Number is present or not.
12. Go to the **Revocation List** tab and check whether the serial number present in the certificate exists.

13. If the serial number exists in the revocation list then, the certificate that you are using has been revoked by CA. Contact CA to maintain the serial number for your use. If the serial number is not listed in the revocation list, log a ticket.

14. To log a ticket, open the http://www.mca.gov.in/MCA21/ and click **User Complaints & Grievances.** When raising a ticket, provide the .Cer file and the screen shot of the error message that you are facing.

SAG