



## **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- "Your certificate has been revoked."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.

Certificate
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
<ul> <li>Ensures the identity of a remote computer</li> <li>Proves your identity to a remote computer</li> <li>Protects e-mail messages</li> <li>Ensures software came from software publisher</li> <li>Protects software from alteration after publication</li> <li>Allows data to be signed with the current time</li> </ul>
* Refer to the certification authority's statement for details.
Issued to: GANDHI AKHIL
Issued by: TCS sub-CA for TCS 2011
Valid from 2/ 25/ 2013 to 2/ 25/ 2015
You have a private key that corresponds to this certificate.
Issuer Statement
Learn more about <u>certificates</u>
ОК

**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.

Certificate
General Details Certification Path
Certification path CCA India 2011 TCS CA 2011 Key Usage: Certificate Signing, CRL Signing TCS sub-CA for TCS 2011 Key Usage: Certificate Signin GANDHI AKHIL
View Certificate
Certificate status: This certificate is OK.
Learn more about <u>certification paths</u>
ОК





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.

Certificate E		Certificate			<b>-</b> ×-
General Details Certification Path	- ₿.	General Details Co	Certification Path		
Certification path	-	Show: <all></all>		•	
TCS CA 2011 Key Usage: Certificate Signing, CRL Signing		Field		Value	*
		Issuer		CCA India 2011, India PKI, IN Friday, March 11, 2011 12:18	l 3:
		Valid to		Friday, March 11, 2016 12:18	3: =
		Subject		CCA India 2011, India PKI, IN	ı 🗐
		Public key		RSA (2048 Bits)	
		Key Lisage	lentmer	4d 07 as 63 t2 db 1c dt Certificate Signing, Off-line C	
		Basic Constrain	nte	Subject Type=C4_Path Leng	+
< □ III View Certificate		4d 07 a8 63 f2 db 1	1c df		
Certificate status:					
This certificate is OK.					
Learn more about <u>certification paths</u>	-	Learn more about <u>ce</u>	Ed ertificate details	lit Properties Copy to	File
ОК					OK





- 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.

Certificate	Certificate
General Details Certification Path	General Details Certification Path
Certification path	Show: <all></all>
TCS CA 2011 Key Usage: Certificate Signing, CRL Signing	Field Value ^
GANDHI AKHIL	Subject     TCS CA 2011, 9th Floor, Nirma       Public key     RSA (2048 Bits)       Subject Key Identifier     46 ae 34 71 30 60 d4 cb       Certificate Policies     Litertificate Policies Policies
	Authority Key Identifier KeyID=4d 07 a8 63 f2 db 1c df
	Authority Information Access       [1]Authority Info Access: Acc         CRL Distribution Points       [1]CRL Distribution Point: Distr         Rasic Constraints       Subject Type=CA Path Lendt
View Certificate	KeyID=4d 07 a8 63 f2 db 1c df
Certificate status: This certificate is OK.	
Learn more about <u>certification paths</u>	Edit Properties Copy to File
ОК	ОК

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 <a href="http://www.mca.gov.in/MCA21/">http://www.mca.gov.in/MCA21/</a> 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.

Certificate 💌	Certificate
General Details Certification Path	General Details Certification Path
Show: <all></all>	Show: <all></all>
Field Value	Field Value
V3         Serial number       22 21 6e 74 0c 1d 5e 4f 98 00         Signature aigonom       sha256         Signature hash algorithm       sha256         Issuer       TCS sub-CA for TCS 2011, Su         Valid from       Monday, February 25, 2013 5         Valid to       Wednesday, February 25, 20         Subject       GANDHT AKHTL 72443cd1ef8f         22 21 6e 74 0c 1d 5e 4f 98 00	Version       V3         Serial number       22 21 6e 74 0c 1d 5e 4f 98 00         Signature algorithm       sha256RSA         Signature hash algorithm       sha256         Issuer       TCS sub-CA for TCS 2011, Su         Valid from       Monday, February 25, 2013 5         Valid to       Wednesday, February 25, 20         Subject       GANINHT AKHTI         CN = TCS sub-CA for TCS 2011       OU         OU = Tata Consultancy Services Ltd.       C = IN
Edit Properties Copy to File Learn more about <u>certificate details</u>	Edit Properties Copy to File Learn more about <u>certificate details</u> OK

6. Open the <a href="http://www.mca.gov.in/MCA21/">http://www.mca.gov.in/MCA21/</a> 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**.

Certificate	×
General Details Certification Path	
Show: <ali></ali>	•
Field	Value
Version	V3
📕 Serial number	22 21 6e 74 0c 1d 5e 4f 98 00
Signature algorithm Signature hash algorithm Issuer Valid from Valid to Subject 22 21 6e 74 0c 1d 5e	sha256KSA sha256 TCS sub-CA for TCS 2011, Su Monday, February 25, 2013 5 Wednesday, February 25, 20 GANDHT AKHTI 72443cd1ef8f
Ed Learn more about <u>certificate details</u>	it Properties Copy to File
	ОК





7. In the Details tab, select CRL (Certificate Revocation List) Distribution points.

Certificate	<b>—</b> ×
General Details Certification Path	]
Show: <all></all>	•
Einld	Value
Relation Alternative Name	Value
Certificate Policies	[1]Certificate Policy:Policy Ide
Authority Information Access	[1]Authority Info Access: Acc
CRL Distribution Points	[1]CRL Distribution Point: Distr
Key Usage	Digital Signature, Non-Repudia
	sna 1 84 84 3c ab a4 5a 3e 24 23 dd
	••••••••••••••••
[1]CRL Distribution Point Distribution Point Name: Full Name: URL =http://www.tcs-ca.t 1703FB55AE9DEBE52EA1.crl	cs.com/crl_
Ec Learn more about <u>certificate details</u>	lit Properties Copy to File
L	ОК

- 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.

File Dow	nload 🔀
<b>Do yo</b>	u want to open or save this file?
x-	Name: crl_1703FB55AE9DEBE52EA1.crl
<u>×</u>	Type: Certificate Revocation List, 148KB
	From: www.tcs-ca.tcs.com
	Open Save Cancel
☑ Al <u>w</u> a	ays ask before opening this type of file
2	While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. <u>What's the risk?</u>





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.

Revoked certificates:			
Serial number		Revocation date	
10 01 23 b2 ec 39 67 a9 f0	) 1e	Friday, August 31, 201	
10 01 3a e2 d8 1d ae d2 b	3 25	Monday, September 03,	
10 01 52 29 66 63 8C D9 D	D T4	Saturday, February 04,	
10 01 e9 57 c8 3d 62 3a 5	a ff	Friday, November 16, 2	-
Serial number Revocation date	10 01 3a e2 Monday, Ser	d8 1d ae d2 b3 25 ntember 03, 2012 4:43:	
Value:			
Learn more about <u>certificate</u>	e revocation lis	<u>st</u>	
		0	ĸ





- 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 <u>http://www.mca.gov.in/MCA21/</u> 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.