

## STEP BY STEP PROCEDURE FOR CLAIMING CLASS 3 INDIVIDUAL DSC

**Note: Check your browser compatibility before claiming the certificate**

Go to <http://mtnltrustline.com>

1. Click *IE Browser Compatibility Check* and follow the instructions in the webpage.
2. Click *Class 3 Individual* link for claiming DSC after completing step 1.

The screenshot shows the mtnltrustline.com website in Microsoft Internet Explorer. The browser's address bar displays <http://www.mtnltrustline.com>. The website has a blue header with the MTNL TRUSTLINE logo and navigation links: Home, Contact us, Sitemap. Below the header is a secondary navigation menu with links: Home, Repository, Services, Support, Resources, Commercial, About us. The main content area is titled "Our certificates are accepted for IFFCO, Northern Railway, MCA 21, E-filing, E -ten" and is divided into four columns:

- Getting started:** IT Act 2000, About Us, Repositories, How to apply, User Guide, Claiming of FREE digital certificate to broadband customers, Become partner of MTNL (LRA), List of partners.
- Services:** Class 1 Individual, Class 2 Individual, Class 2 - ipsec, Get Class 2 Individual DSC online, **Class 3 Individual** (circled in orange), Class 3 Server, LRA LOGIN, **IE Browser Compatibility Check** (circled in orange).
- Test Certificate:** Precautions while downloading Certificate, Revocation Conditions, Test Certificate, Help, Help for downloading and searching certificates and CRLs.
- Ask Questions:** FAQ, Contact us, Feedback, MTNL CA Certificate Hierarchy, The Institute of Company Secretaries of India, Reference for USB crypto token.

### 3. Click *Claiming Certificate* link against **Individual**.

Mahanagar Telephone Nigam Ltd., Delhi - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://mtnltrustline.com/products/individual2.htm>

The validation procedures for Class 3 Certificates issued to individuals are based on the personal (physical) presence of the Subscriber before a MTNLTRUSTLINE authorized person that confirms the identity of the Subscriber using a well-recognized form of government issued identification and one other identification credential.

The validation procedures for Class 3 Certificates issued to Organizations are based on a confirmation that the Subscriber Organization does in fact exist, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so.

Class 3 Individual Certificates are appropriate for Digital Signatures, encryption, and access control in transactions requiring a high assurance about the Subscriber's identity.

Class 3 Server Certificates are appropriate for server authentication; message, software, and content integrity; and confidentiality encryption.

Please give your pop3 e-mail id while registering your request. Otherwise you won't be able to send the mail. As the signed mail is supported by POP3 mail clients like Outlook express etc. as of now.

Individual Certificate [Claiming Certificate](#) [Revocation](#)

Please install the complete hierarchy in your system before use of certificate so that certificate taken by you will be shown valid. For installing the certificate.

[click here](#)

Copyright © 2003, Mahanagar Telephone Nigam Limited. All Rights Reserved.

Privacy statement

[MTNL Portal](#) | [MTNL Corporate site](#) | [MTNL Delhi Home](#) | [MTNL Mumbai Home](#) | [Delhi Directory](#)  
[Customer care portal](#) | [E-receipt system](#) | [Bill payment through credit card](#) | [Bill view system](#)  
[Internet Telephony](#) | [Email over telephone](#) | [Bill Alert](#) | [Payment Portal](#) | [Web to mobile service](#)  
[Internet User Service](#) | [Services](#) | [Tariff](#) | [Download Form](#) | [Tenders](#) | [Disclaimer](#)

Done Internet

4. Enter *SUBSCRIBER ID*, *REFERENCE ID*, *PASSWORD* and click *Submit*.

Certificate Claim - Microsoft Internet Explorer

Mahanagar Telephone Nigam Ltd

mtnlTrustLine  
Certification Services from MTNL

**MTNLTrustLine Certificate Claiming**

SUBSCRIBER ID:

REFERENCE ID:

PASSWORD:

**Please Note :**

- 1.Before claiming certificate,key generation check should be done on the system where certificate is claimed.To test key generation click [Test Key generation](#).
- 2.After successful installation of certificate,export the same with private key to a safe location.
- 3.Before importing certificate to crypto-USB token,complete step 2.
- 4.For any help refer our user guide.To download userguide click [mtnlTrustline User Guide](#)

**Note: Check Name and E-Mail Address before proceeding as this appears as it is in the certificate.**

5. Read the notes given in the page. Drop down the *CSP* List. Select the required *CSP* and click *Generate Keys*.

The screenshot shows a web browser window titled "Order - Microsoft Internet Explorer". The page header includes the mtnTrustLine logo and "Mahanagar Telephone Nigam Ltd". The main content area is titled "Class 3 Individual Subscriber Certificate" and "Certificate Details". It contains three input fields: "Name" with the value "SANAWWAR KHAN", "Reference Id" with "00091028", and "E-Mail Address" with "khan\_san1974@rediffmail.com". Below these fields is a dropdown menu for "CSP" set to "Microsoft Enhanced Cryptographic Provider v1.0". A "Generate Keys" button is highlighted with a red oval and an arrow. An "Important:" section follows with three instructions in red text. The browser's taskbar at the bottom shows the Start button, several open tabs, and the system clock at 13:57.

Order - Microsoft Internet Explorer

**mtnTrustLine**  
Certification Services from MTNL

**Mahanagar Telephone Nigam Ltd**

**Class 3 Individual Subscriber Certificate**

Certificate Details

Name: SANAWWAR KHAN

Reference Id: 00091028

E-Mail Address: khan\_san1974@rediffmail.com

Select a CSP(Crypto Graphic Service Provider) and Click "Generate Keys" Button for key pair generation

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Generate Keys

**Important:**

1. Select Microsoft Enhanced Cryptographic Provider if the certificate is to be installed in IE browser else select CSP as per requirement.
2. When "Generate Keys" button is clicked, pop-up windows appear, click 'Yes' and 'OK' to proceed.
3. Certificate Installation may take few minutes. Do not click in between the process.

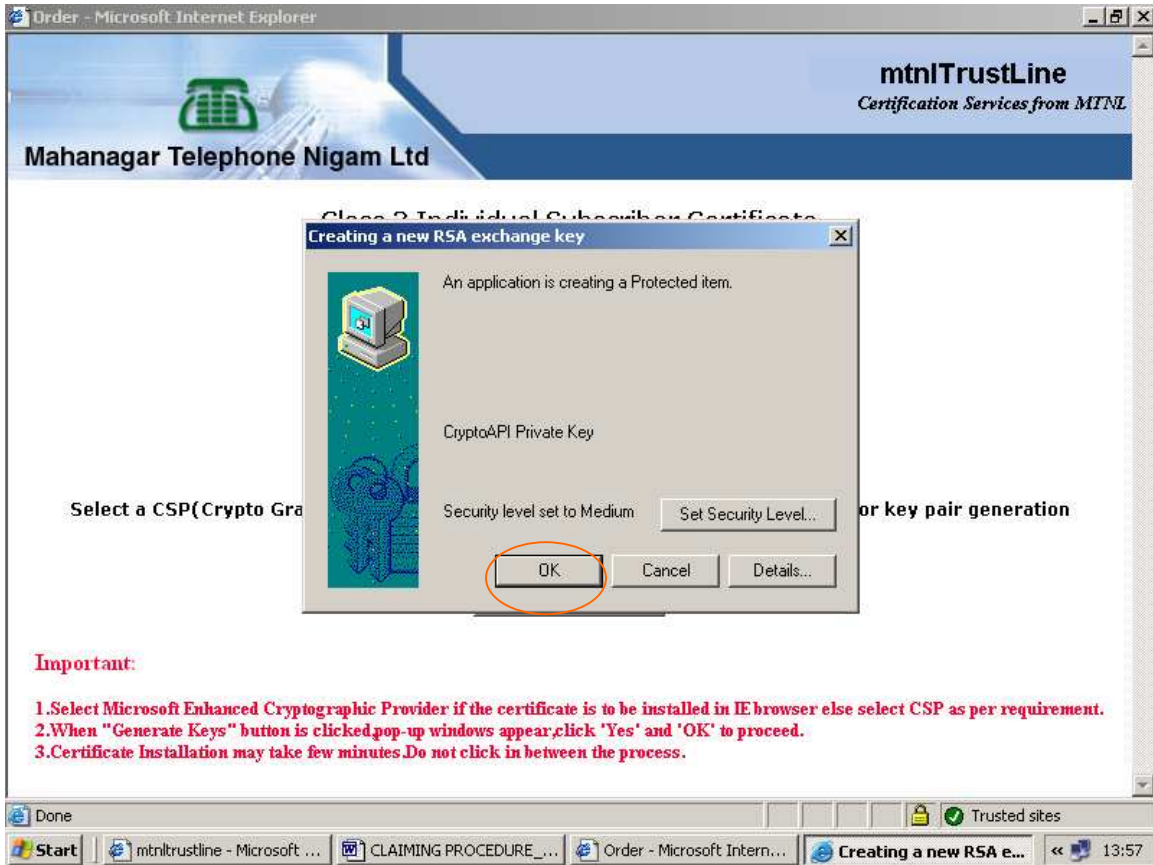
Done Trusted sites

Start mtntrustline - Microsoft I... CLAIMING PROCEDURE... Order - Microsoft Inte... 13:57

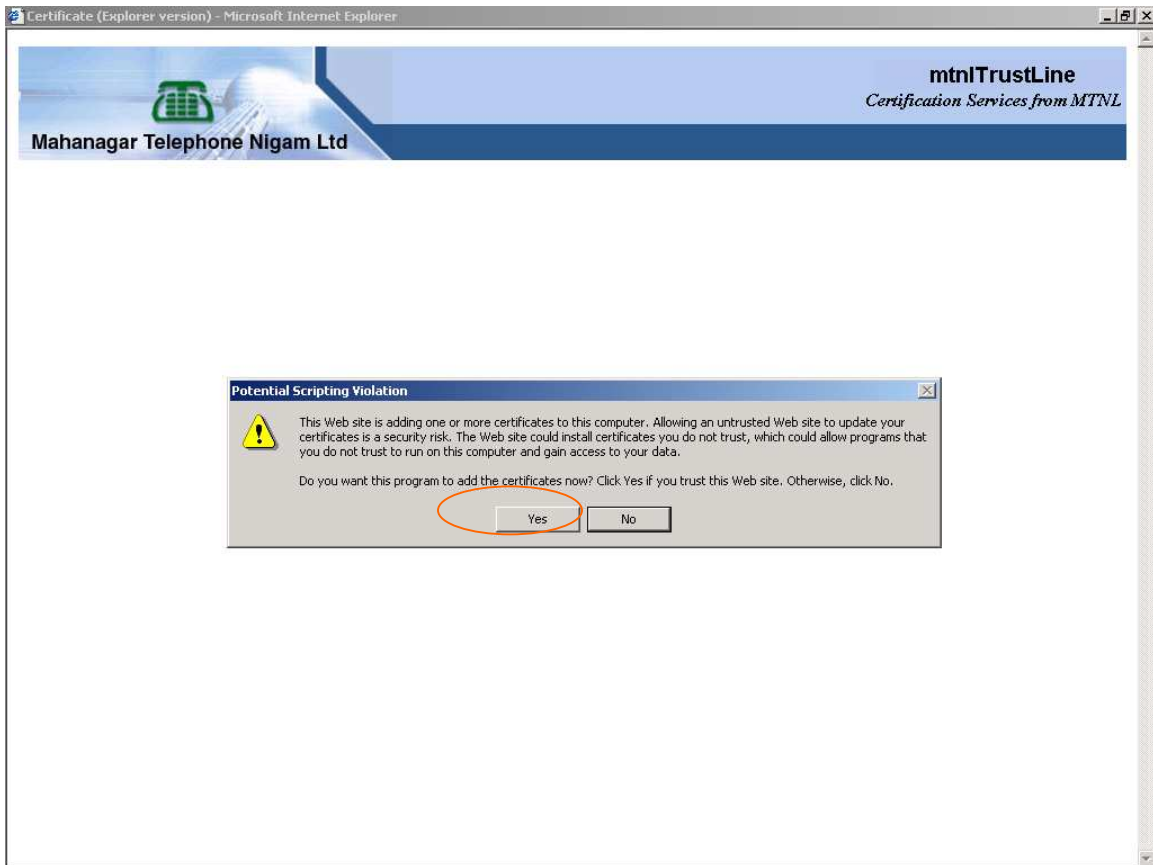
6. Click *Yes* in the Potential Scripting Violation pop up.

The screenshot shows a Microsoft Internet Explorer window titled "Order - Microsoft Internet Explorer". The page header includes the logo for Mahanagar Telephone Nigam Ltd and the text "mtnlTrustLine Certification Services from MTNL". The main content area is titled "Class 3 Individual Subscriber Certificate" and "Certificate Details". A form field for "Name" contains the text "SANAAWWAR KHAN". A "Potential Scripting Violation" dialog box is overlaid on the page, displaying a warning icon and the text: "This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?". The "Yes" button in the dialog is circled in red. Below the dialog, a "CSP:" dropdown menu is set to "Microsoft Enhanced Cryptographic Provider v1.0", and a "Generate Keys" button is visible. To the left of the dialog, the text "Select a CSP(Cryp" is partially visible, and to the right, "pair generation" is visible. At the bottom of the page, there is a red "Important:" section with three numbered instructions: "1. Select Microsoft Enhanced Cryptographic Provider if the certificate is to be installed in IE browser else select CSP as per requirement.", "2. When 'Generate Keys' button is clicked, pop-up windows appear, click 'Yes' and 'OK' to proceed.", and "3. Certificate Installation may take few minutes. Do not click in between the process." The browser's taskbar at the bottom shows the Start button, several open windows including "mtnltrustline - Microsoft...", "CLAIMING PROCEDURE...", "Order - Microsoft Intern...", and "Potential Scripting Vi...", and a system clock showing "13:57".

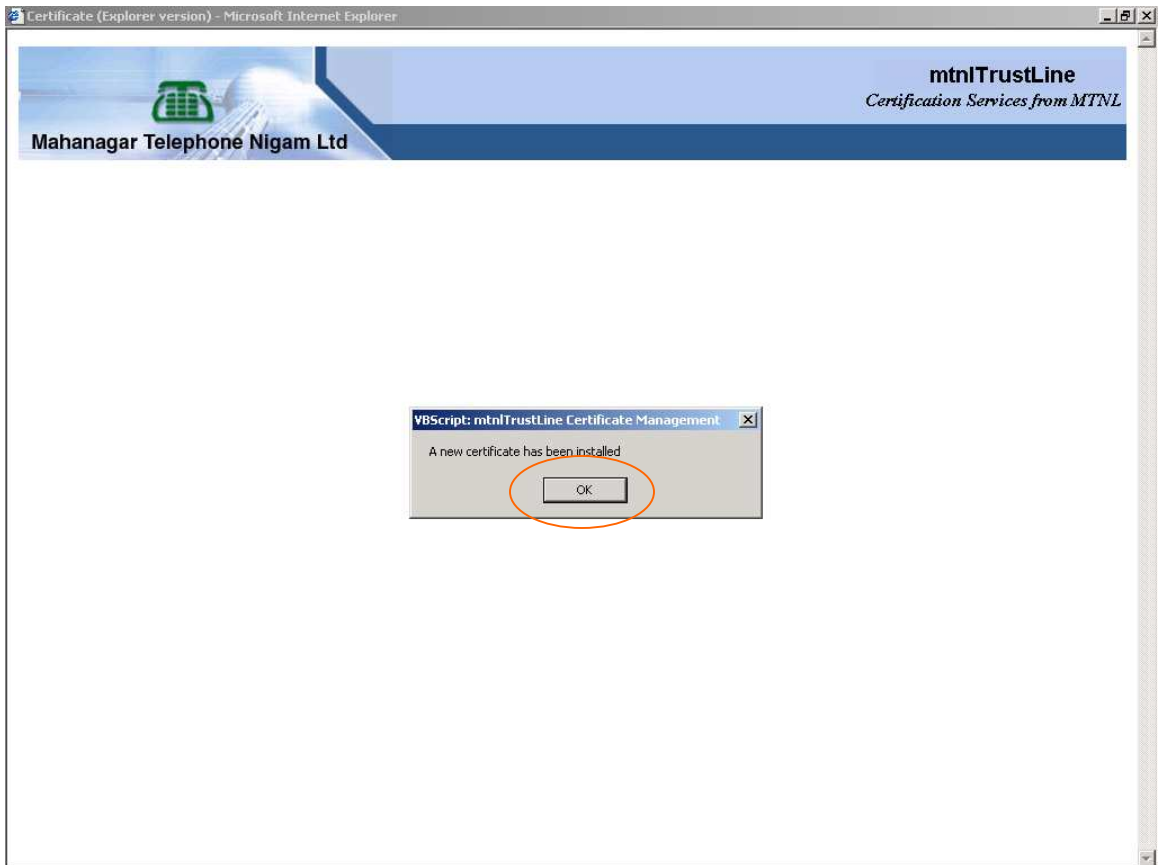
7. Click *OK* in the Creating a new RSA exchange key pop up.



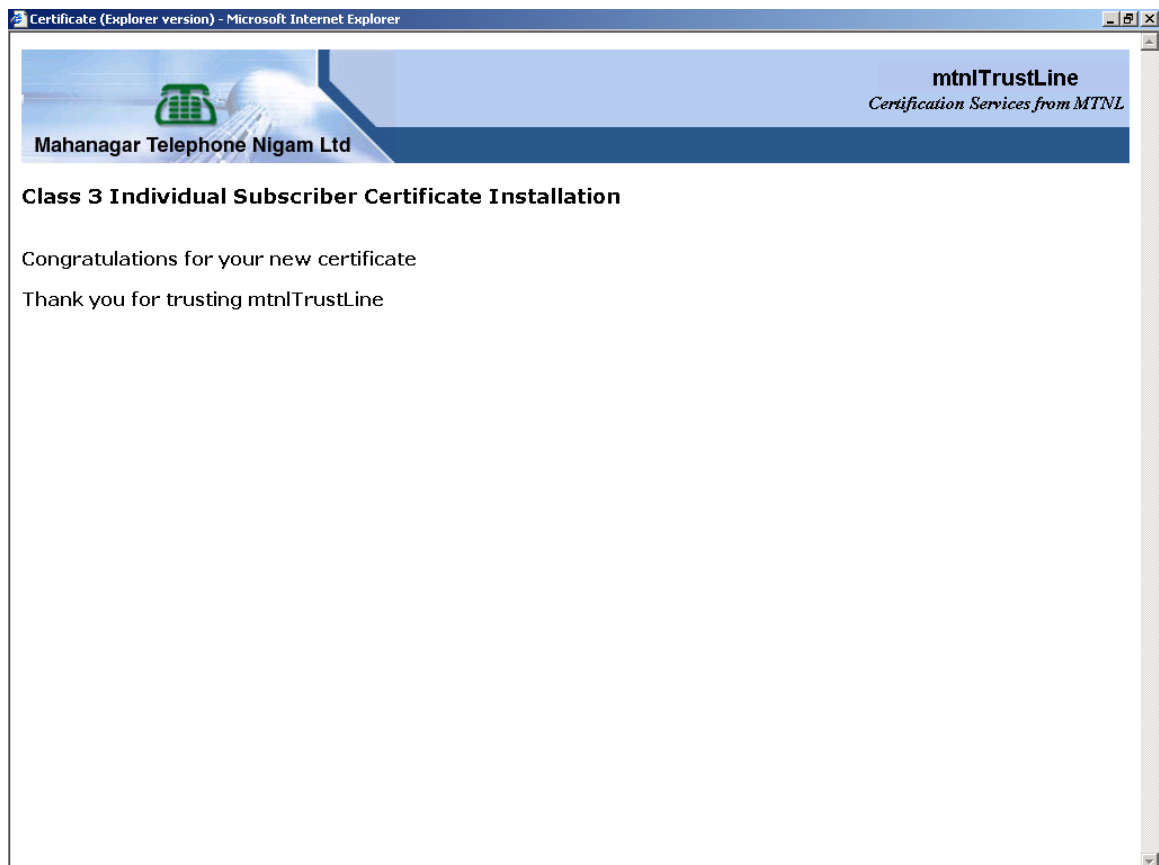
8. Click *Yes* in the Potential Scripting Violation pop up.



9. Click *OK*.



10. The certificate is successfully installed.



**Follow the steps below for completing the claiming process :**

1. To see the certificate (if installed in internet explorer browser) follow the steps below:

*Open internet explorer click Tools → Internet Options → Content → Certificates.*

2. Install mtntrustline CA hierarchy from the following page

<http://mtntrustline.com/hierarchy.htm>

3. Keep a copy of the certificate by exporting it with private key (if certificate installed in browser). Refer user guide for help

(<http://mtntrustline.com/UserGuide.doc> ).

4. For other help refer User Guide.