

Guide for Bidders of e-auction

The Office of Controller of Certifying Authorities (CCA), has enlisted Certifying Authorities (CA) for issuing Digital Signatures. CA issue Digital Signature Certificate to the end-user. You can approach any one of the CAs for getting Digital Signature Certificate. The website addresses are given below.

www.safescrypt.com

www.nic.in

www.idrbtca.org.in

www.tcs-ca.tcs.co.in

www.ncodesolutions.com

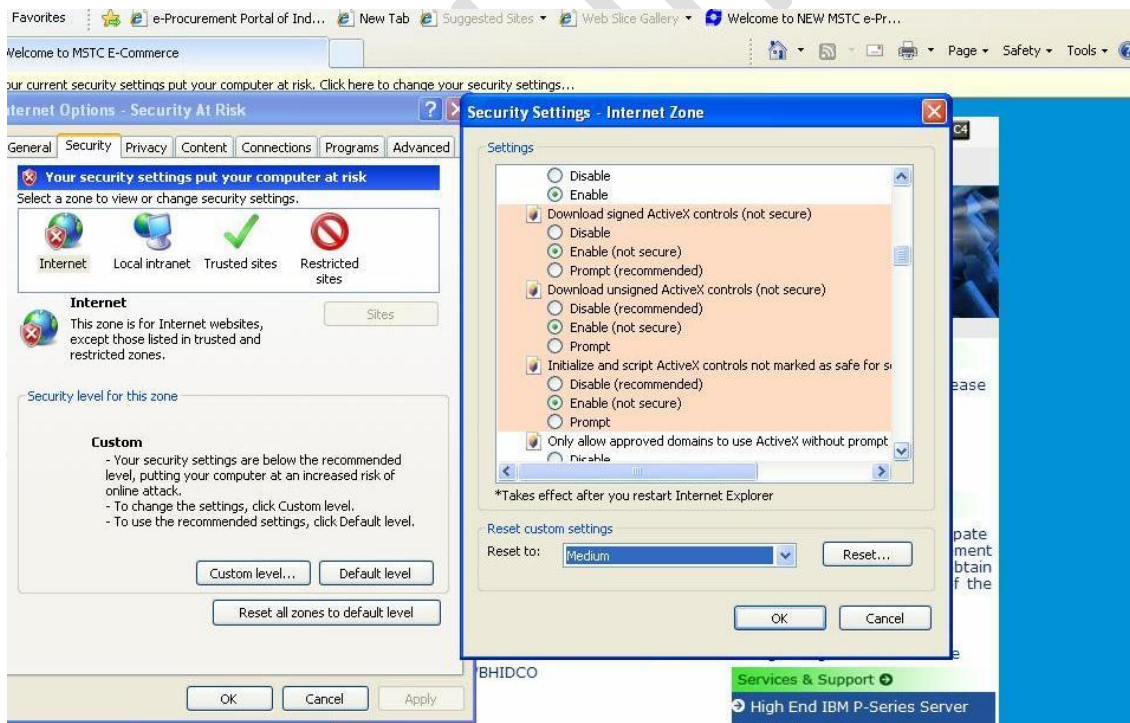
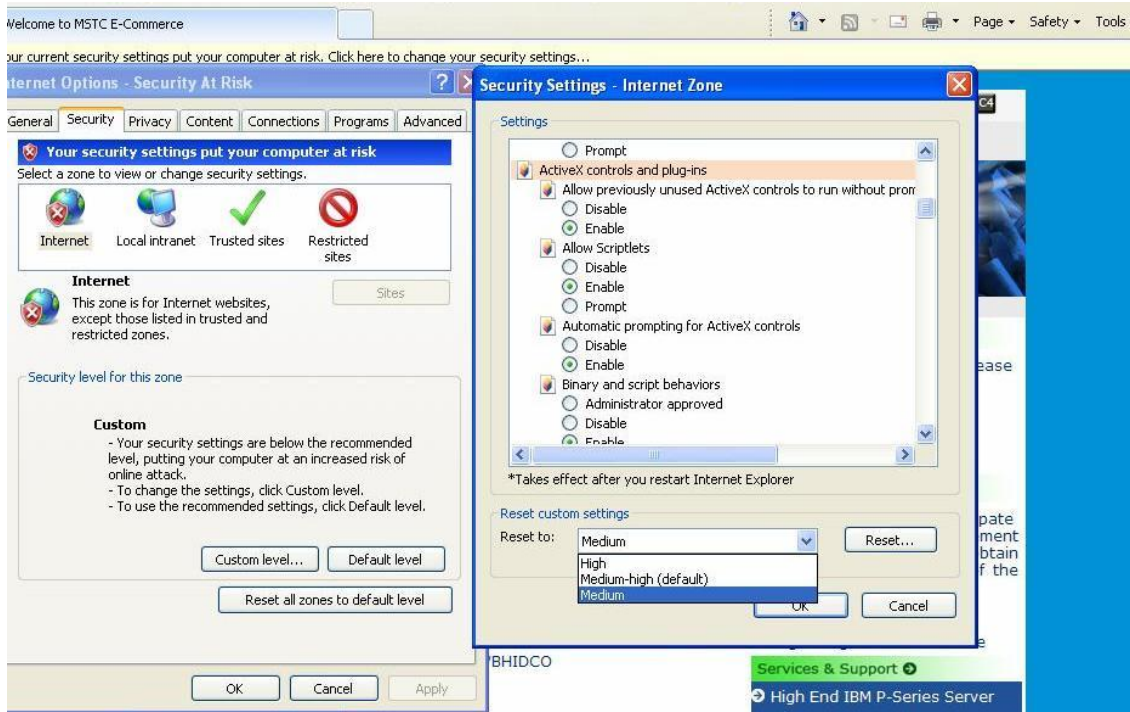
www.e-Mudhra.com

(The following section is meant only to provide guidance to bidders about the suggested browser configuration for the website of MSTC. These guidelines are subject to change from time to time depending on the development of the portal. Bidders are advised to keep checking the latest guidelines from the website to keep themselves updated. They may also contact the offices of MSTC to seek clarification on any point. MSTC shall not be responsible for any mistake committed by any bidder or for any consequent loss to the bidder due to misunderstanding anything written hereunder.)

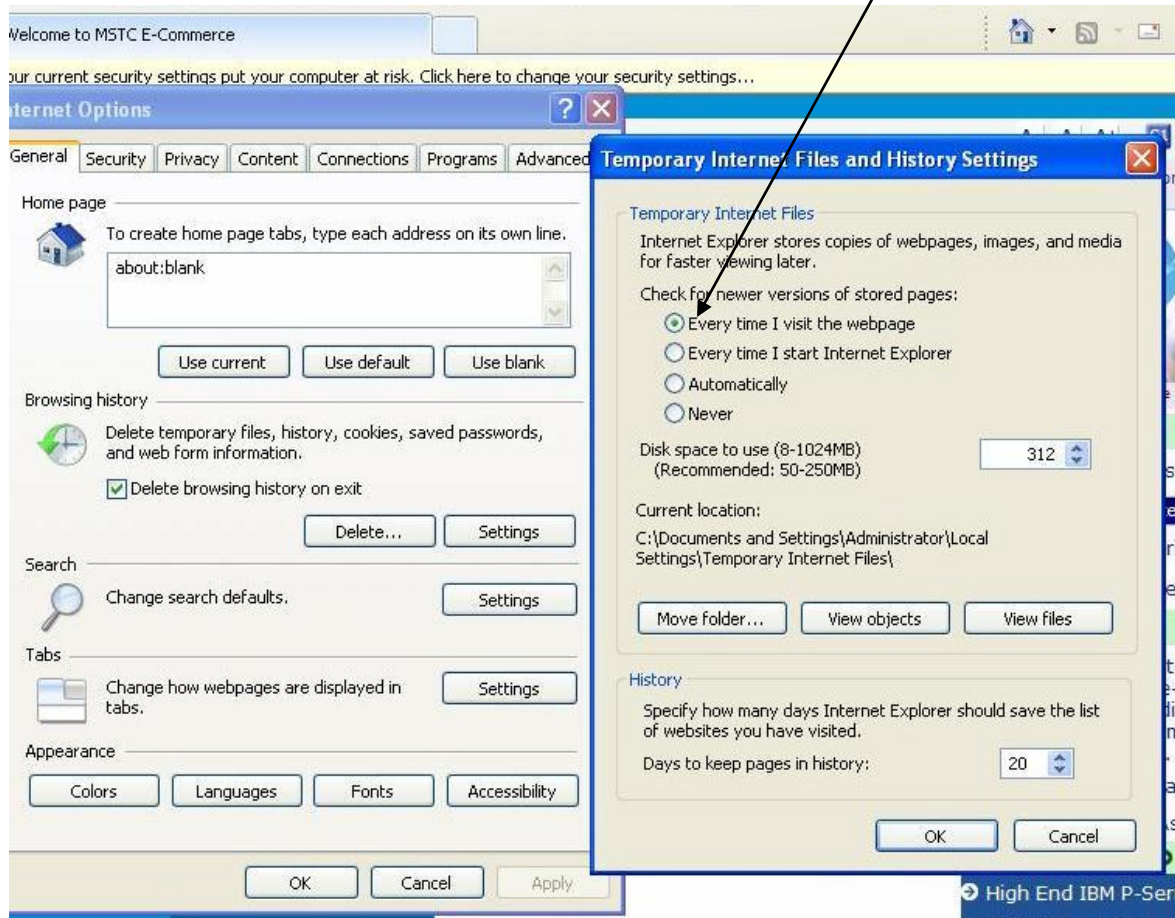
System Requirement

- 1) The following requirements need to be fulfilled for optimum use of the features available on the website of MSTC.
- 2) A computer connected to internet through an ISP.
- 3) The computer should have adequate RAM depending on version of Windows.
- 4) The computer (Desktop / Laptop) should have Windows XP SP3 or above as the Operating System.
- 5) The website is best viewed in Internet Explorer version 7 or above.
- 6) All the ActiveX controls of the Internet Explorer should be set in **Enable** mode. As described below.

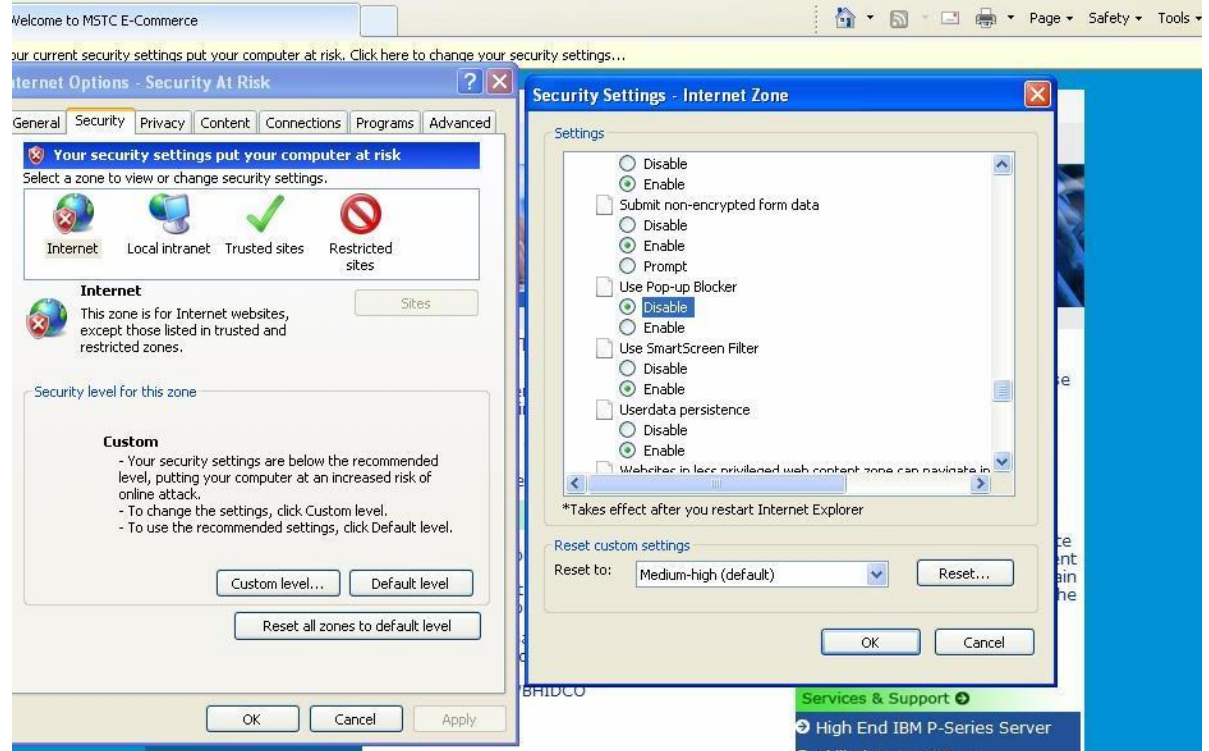
Tools> Internet Options > Security > Custom level > Enable **ALL** Active-X Controls and Plug-ins



- 7) The settings under Browsing History (Under Tools → Internet Options → General) for Check for newer versions of web pages should be kept at **Every time I visit the webpage** as shown below.



8) All Pop-Blockers should be kept in **Disable** or turn off mode.

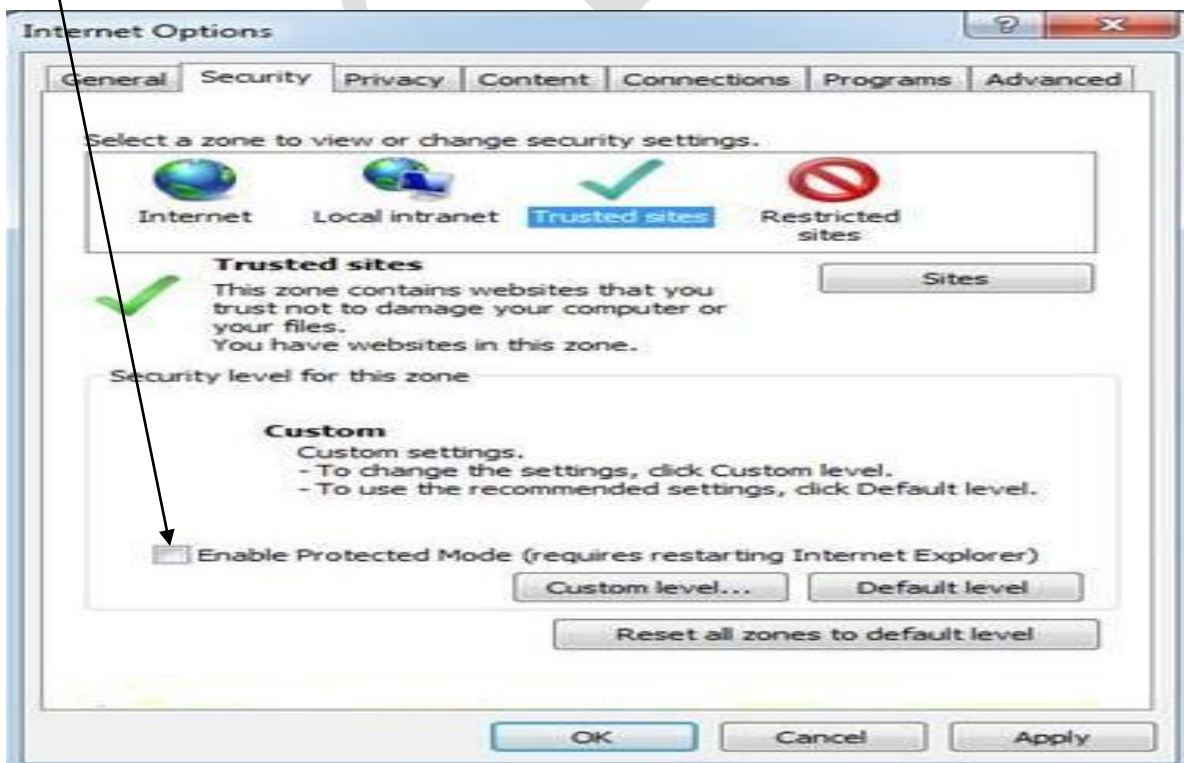


9) Scripting should be in **Enable** mode under Tools -> Internet Options -> Security -> Custom Level.

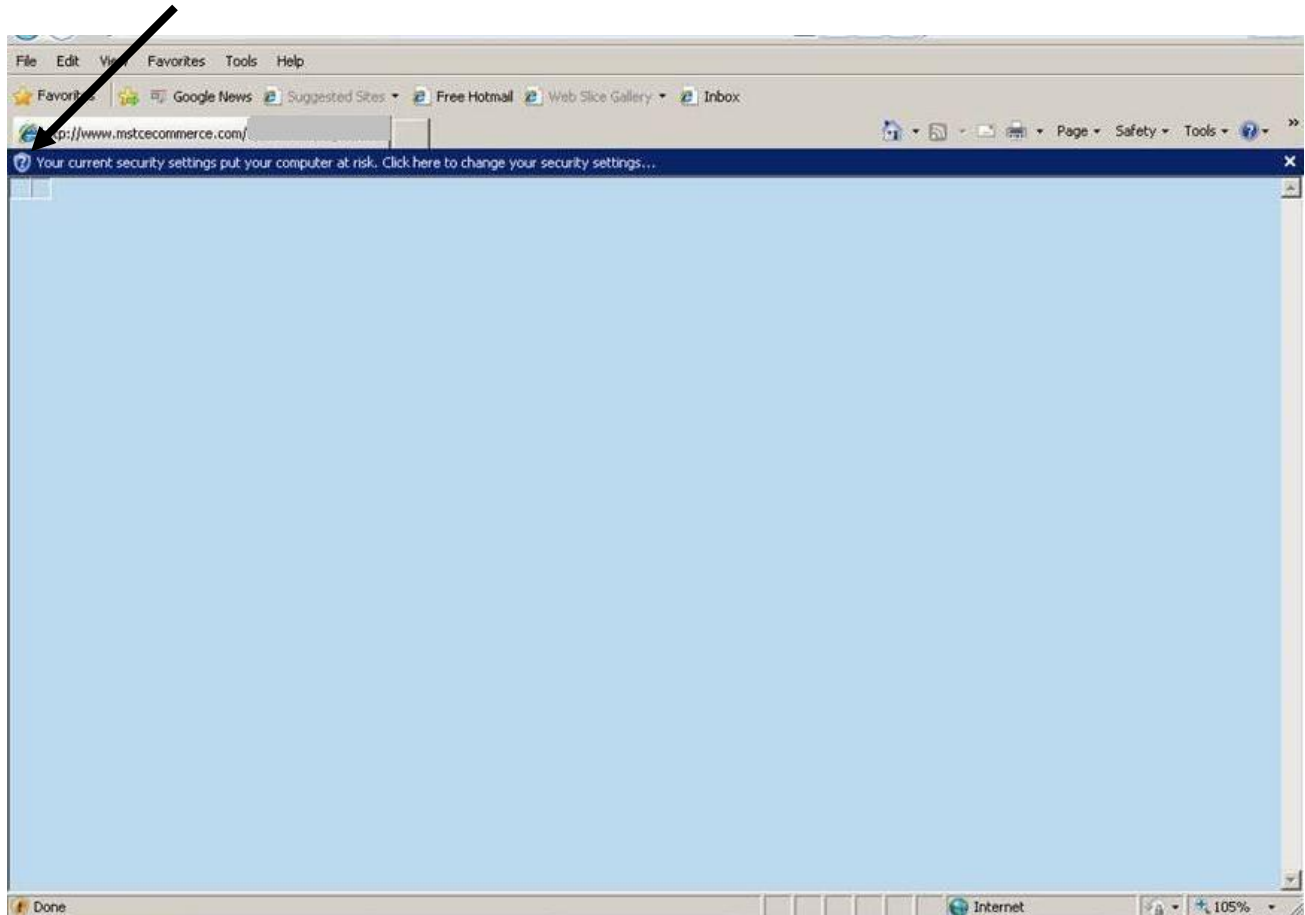
10) The protected mode of the computer should be turned off for higher version of Windows where available.



Under Tools> Internet Options > Security > There is a check box **“ENABLE PROTECTED MODE”**. To enable the Digital Signature Certificate appear in the Signer the box should be unchecked as shown below.

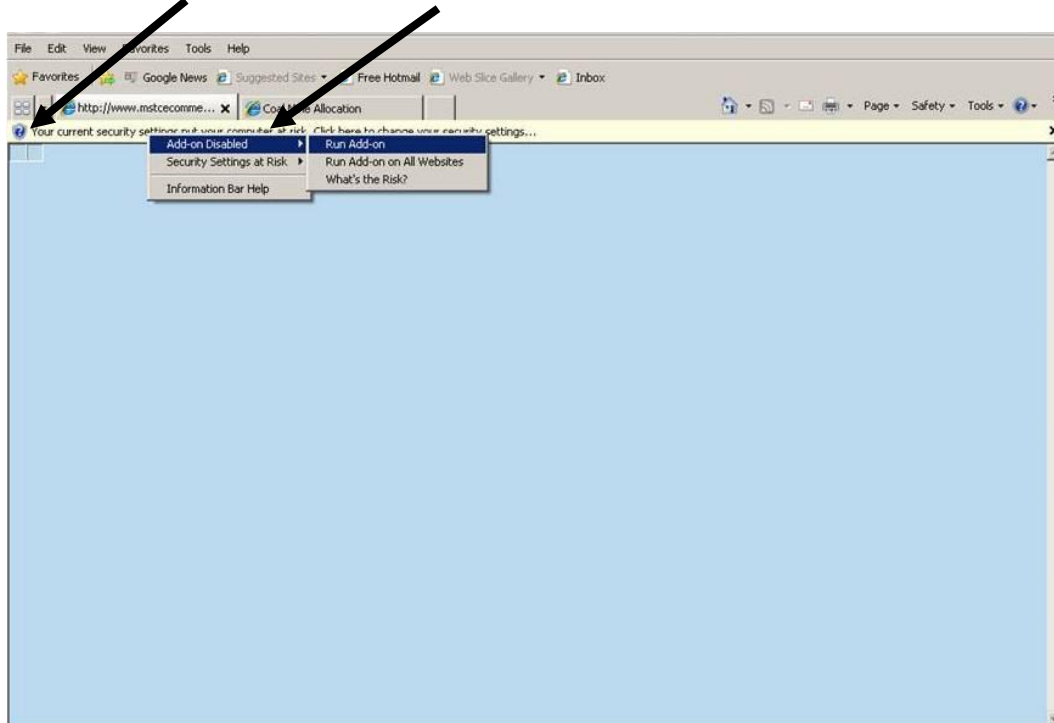


After changing the settings the message might appear on your screen “**Your current security settings put your computer at risk. Click here to change your security settings**” as shown in subsequent screenshots. This should not be fixed unless it appears with a blue question mark as shown below.

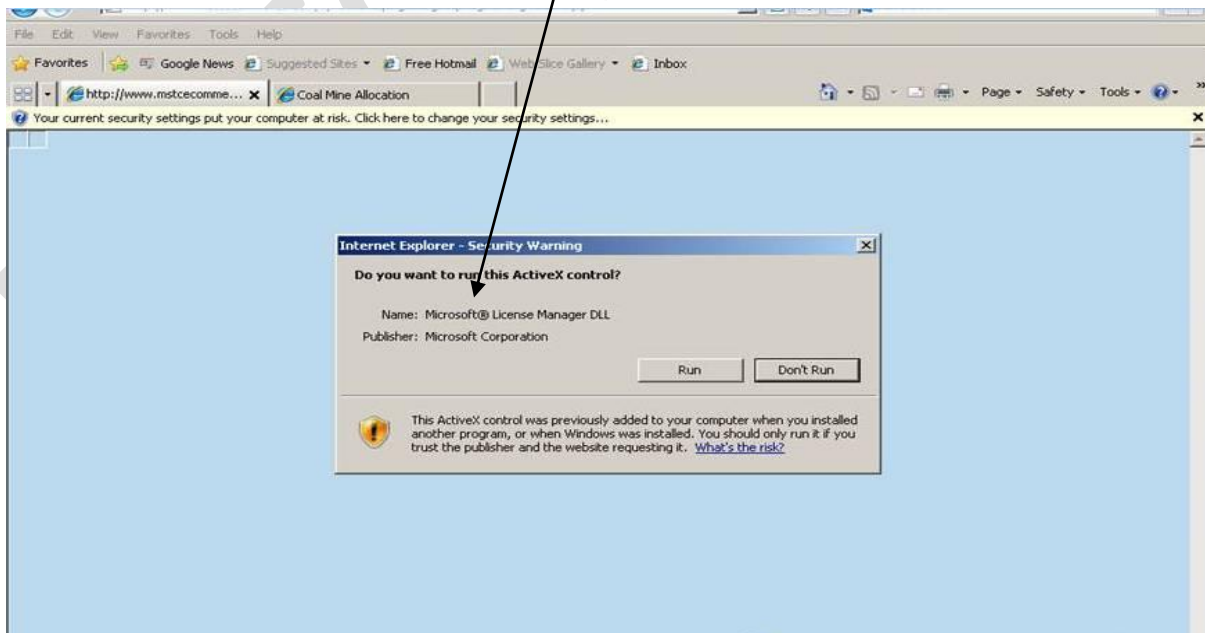


In the above case, the **blue question mark** sign indicates that add-on/s want to run. That should be done by right clicking on the icon and running the add-ons as shown in subsequent screenshots.

Right Click on the message and run the add-on/s as they appear.



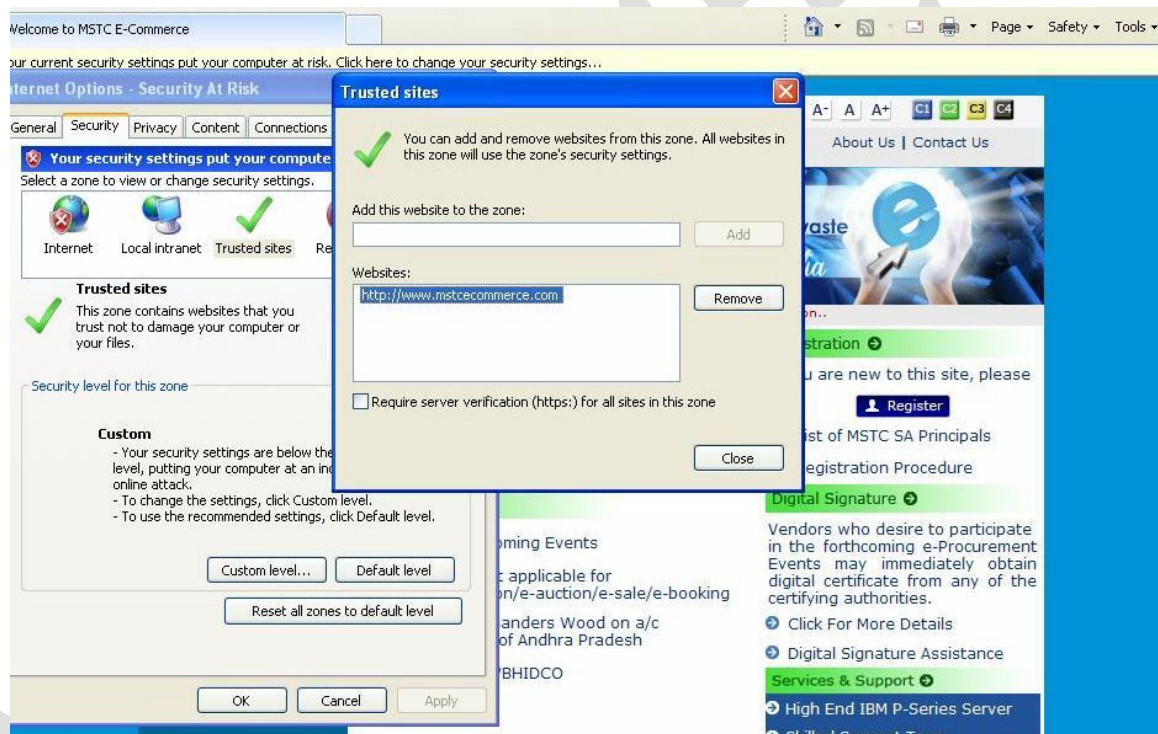
A sample add-on is shown below when the add-on wants to run. Click on run to allow that add-on.



Another add-on “TCS Signer” (cab file) also needs to run similarly to allow DSC’s to sign digitally.

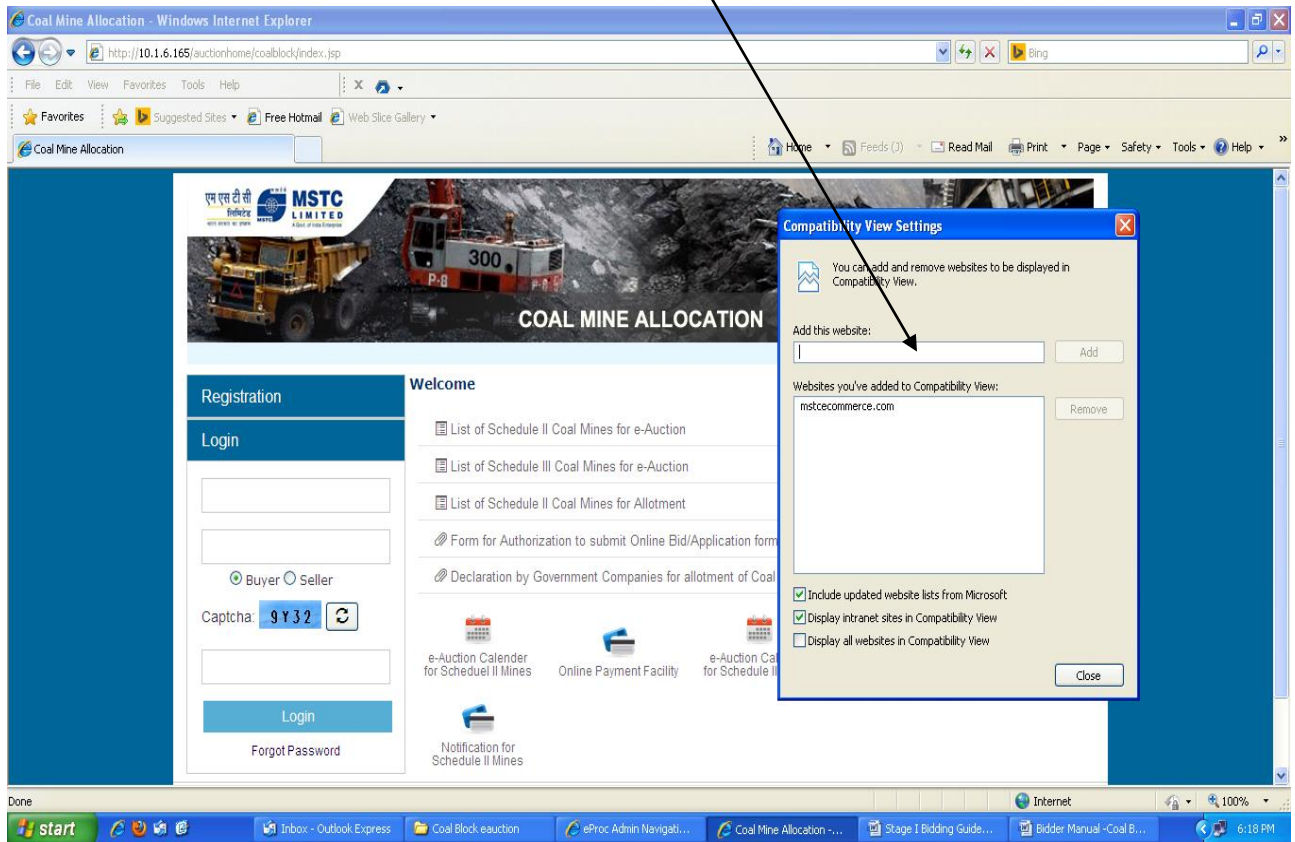
11) Latest Drivers for your Digital Signature Certificate should be installed properly in the computer.

12) The website <https://www.mstcecommerce.com> should be added to the list of Trusted Sites.



- 13) The website <https://www.mstcecommerce.com> should be added to the list of Compatibility View Settings under Tools.

Tools > Compatibility View Settings > Add our website



- 14) The computer should have Java Runtime Environment version 7 update 9 or above installed in it.
- 15) Windows user should have administrative privilege to install packages on being prompted on screen like TCS signer certificate needs to be installed for DSC operation, java applet needs to be loaded etc.