



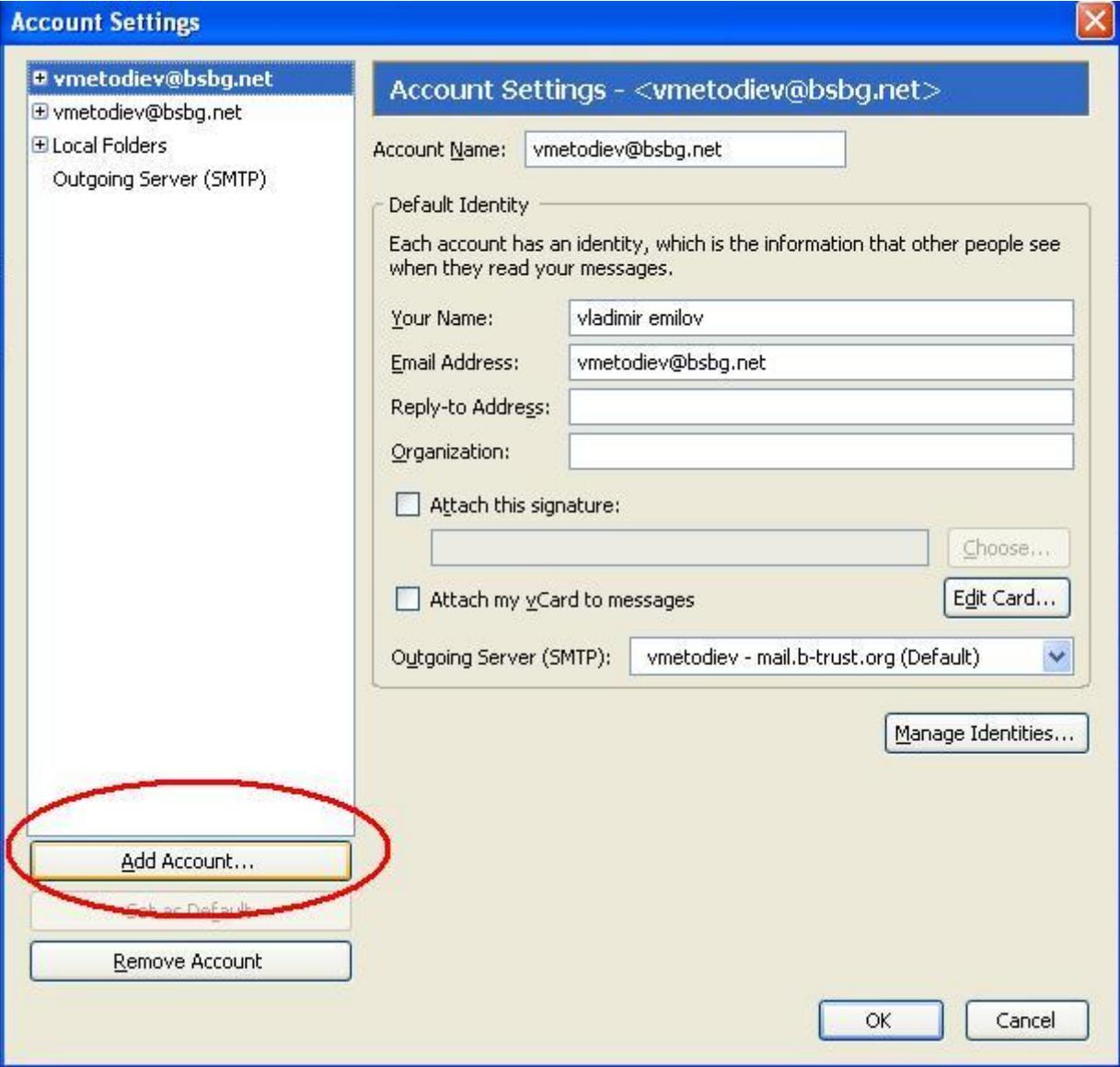
## Configure B-Trust e-mail in Mozilla Thunderbird

Using of electronic signature authorization for signing and/or encrypting email in **Mozilla Thunderbird** requires e-mail account in **POP3/SMTP** server.

1. Start **Mozilla Thunderbird**.
2. From **Tools** menu choose **Account Settings...**



3. Choose **Add Account...** and make the configuration from the following picture.





4. Fill in the fields as follows:

- **Your Name** type your name;
- **E-mail Address** type the e-mail address from your digital signature;
- mark **POP**;
- **Incoming mail server** type **mail.b-trust.org**;
- **Incoming User Name** type the e-mail address from the **E-mail Address** field;

- **Account Name** въведете имейл адреса от полето **E-mail Address**;

**Account Wizard**

**Identity**

Each account has an identity, which is the information that identifies you to others when they receive your messages.

Enter the name you would like to appear in the "From" field of your outgoing messages (for example, "John Smith").

Your Name:

Enter your email address. This is the address others will use to send email to you (for example, "user@example.net").

Email Address:

< Back **Next >** Cancel

**Account Wizard**

**Server Information**

Select the type of incoming server you are using.

POP  IMAP

Enter the name of your incoming server (for example, "mail.example.net").

Incoming Server:

Uncheck this checkbox to store mail for this account in its own directory. That will make this account appear as a top-level account. Otherwise, it will be part of the Local Folders: Global Inbox account.

Use Global Inbox (store mail in Local Folders)

Your existing outgoing server (SMTP), "mail.b-trust.org", will be used. You can modify outgoing server settings by choosing Account Settings from the Tools menu.

< Back **Next >** Cancel

**Account Wizard**

**User Names**

Enter the incoming user name given to you by your email provider (for example, "jsmith").

Incoming User Name:

Your existing outgoing (SMTP) username, "inetudiev", will be used. You can modify outgoing server settings by choosing Account Settings from the Tools menu.

< Back **Next >** Cancel

**Account Wizard**

**Account Name**

Enter the name by which you would like to refer to this account (for example, "Work Account", "Home Account" or "News Account").

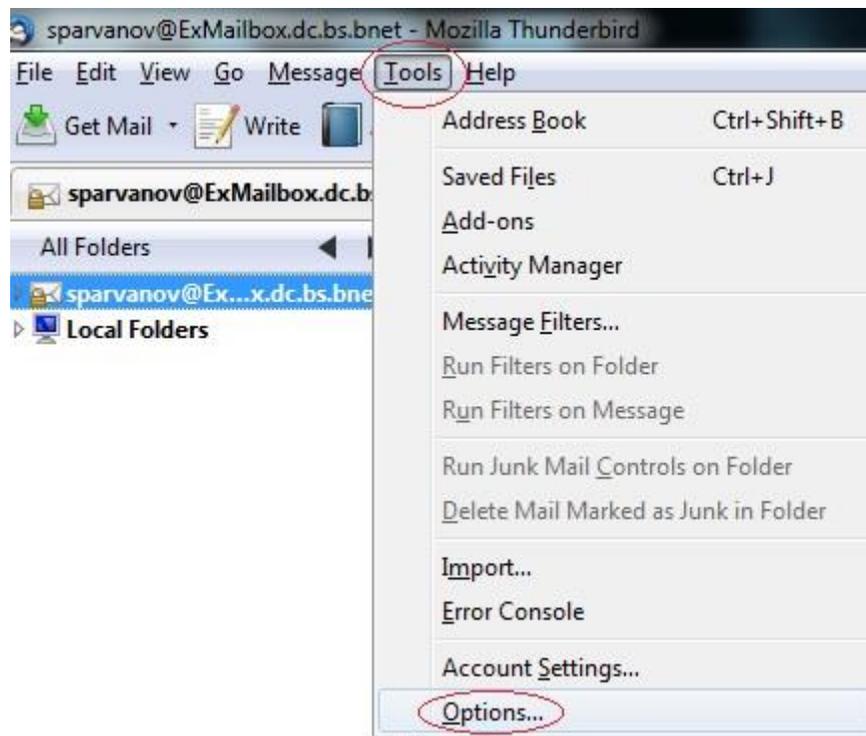
Account Name:

< Back **Next >** Cancel

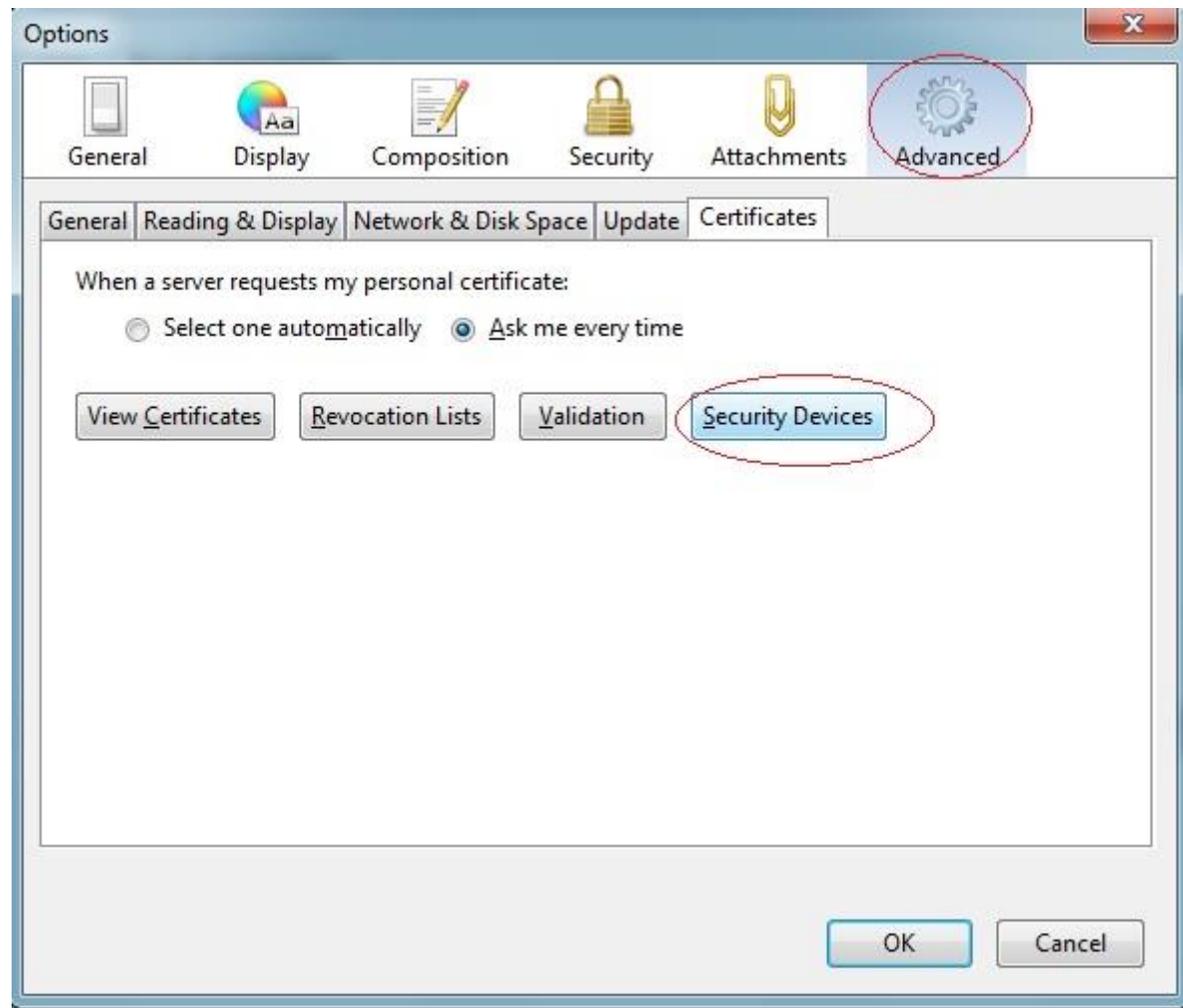
5. Check the configuration and confirm with **Finish**



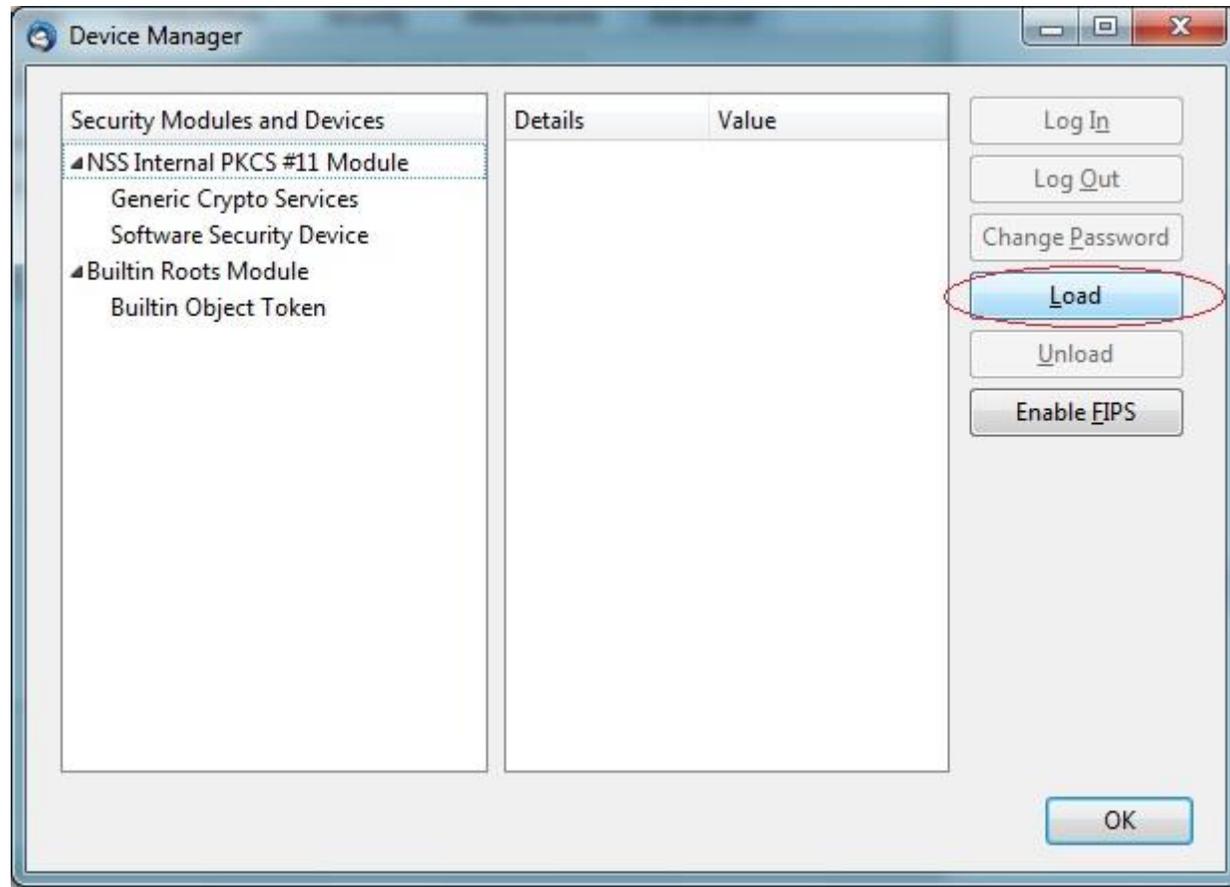
6. From **Tools** menu choose **Options...**



7. In **Privacy** tab choose **Security Devices**.

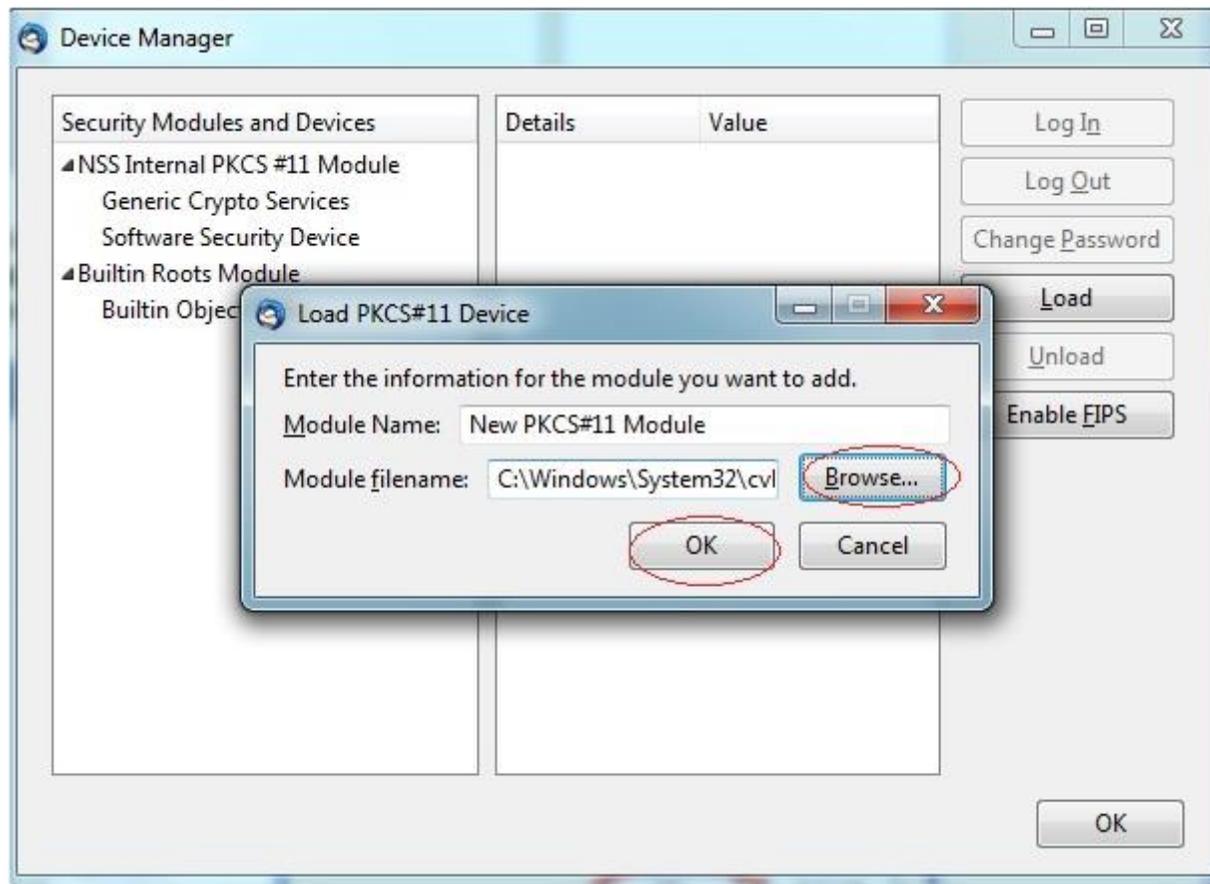


8. Click **Load**.



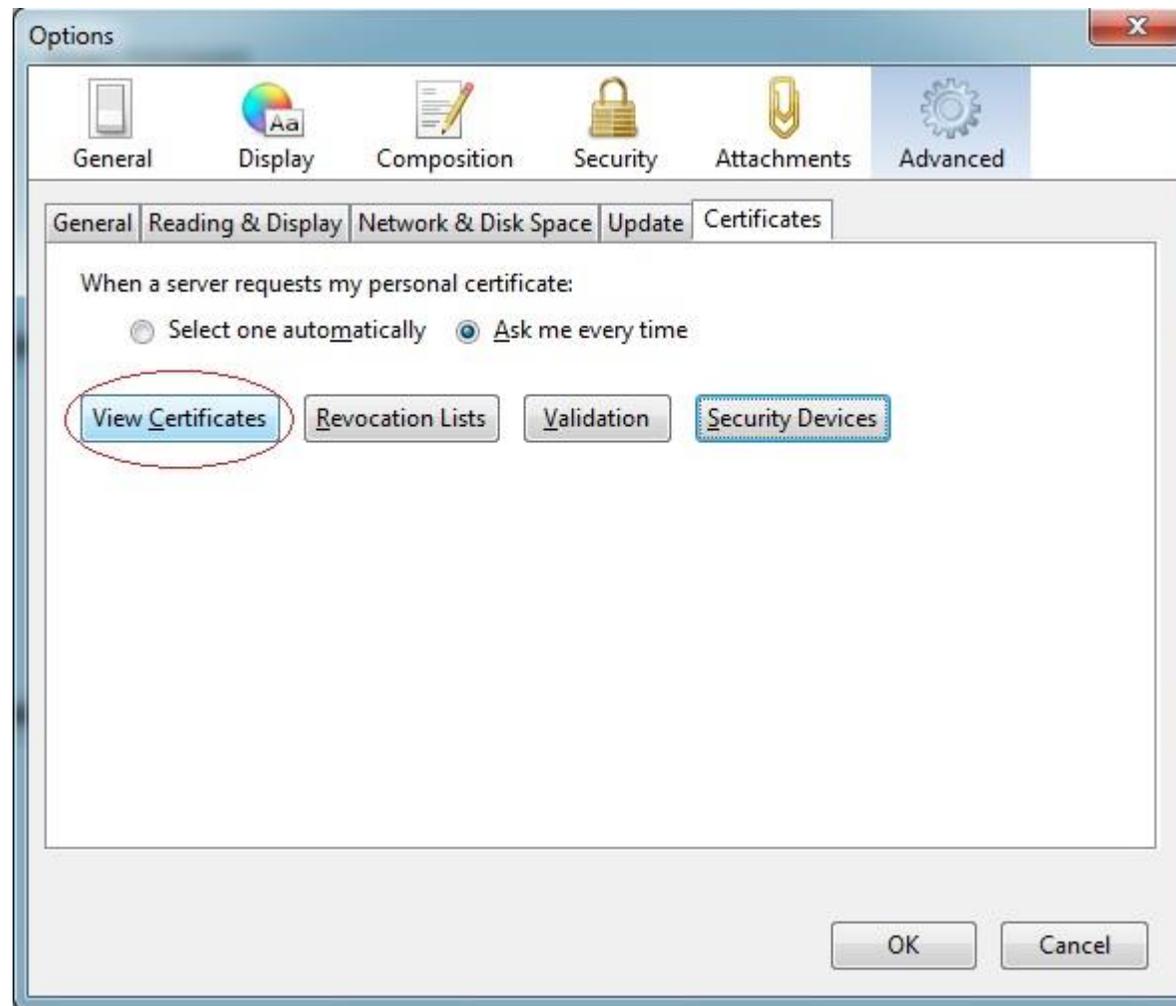
9. In the **Module Name** field type **cryptovision**. Click **Browse...** and choose the file:

- **cvP11.dll** for Windows, located in the Windows system directory (**C:\Windows\system32** or **C:\Windows\SysWOW64**);
- **cvP11.so** for Linux, located in **/usr/local/lib**;
- **cvP11.dylib** for Mac OS X, located in **/Library/cv cryptovision**.



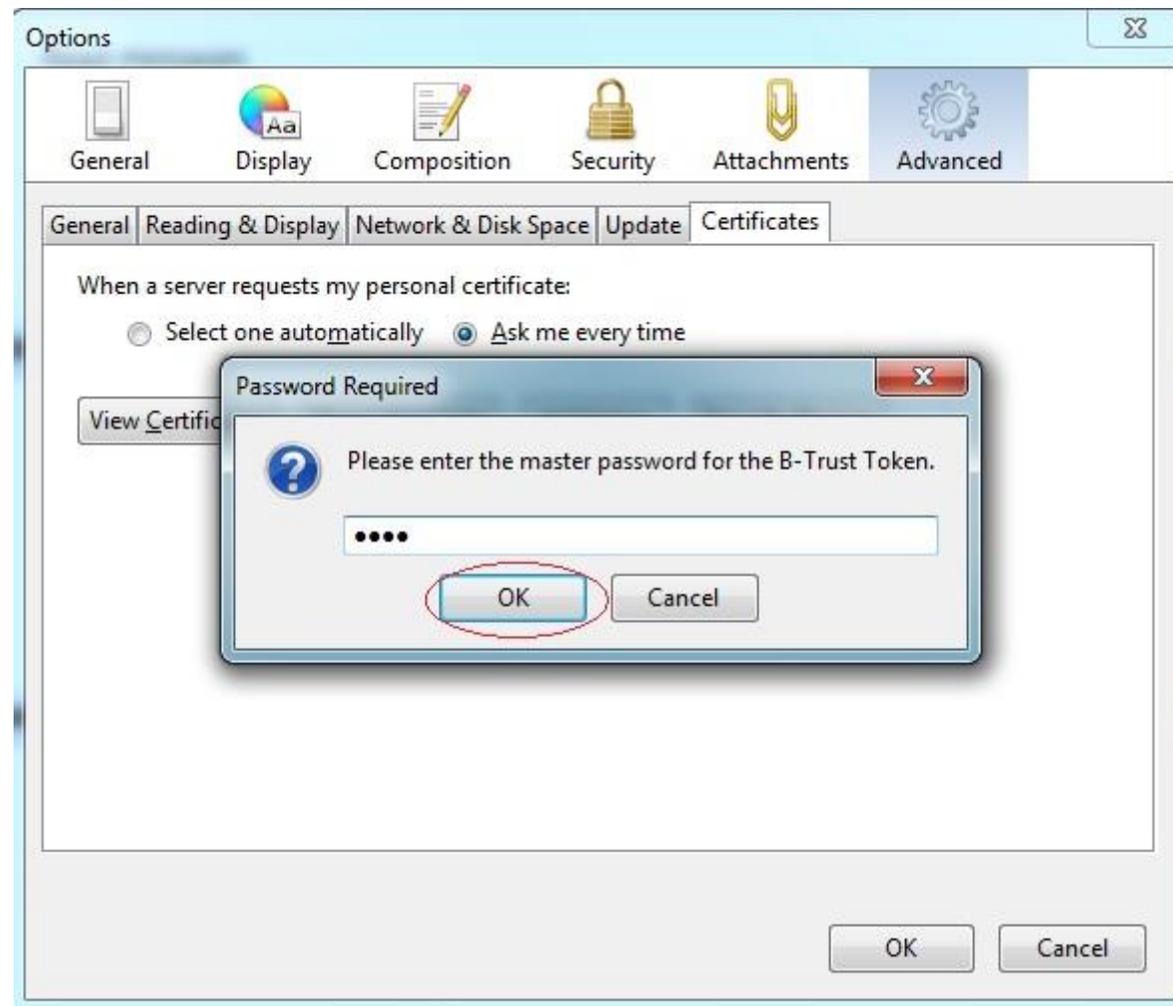
Confirm with **OK** until you reach **Privacy**..

10. Click **View Certificates**. If the module is successfully loaded and your digital signature is plugged in, you will see a window where you must type the PIN code to see the **Certificate Manager** window.

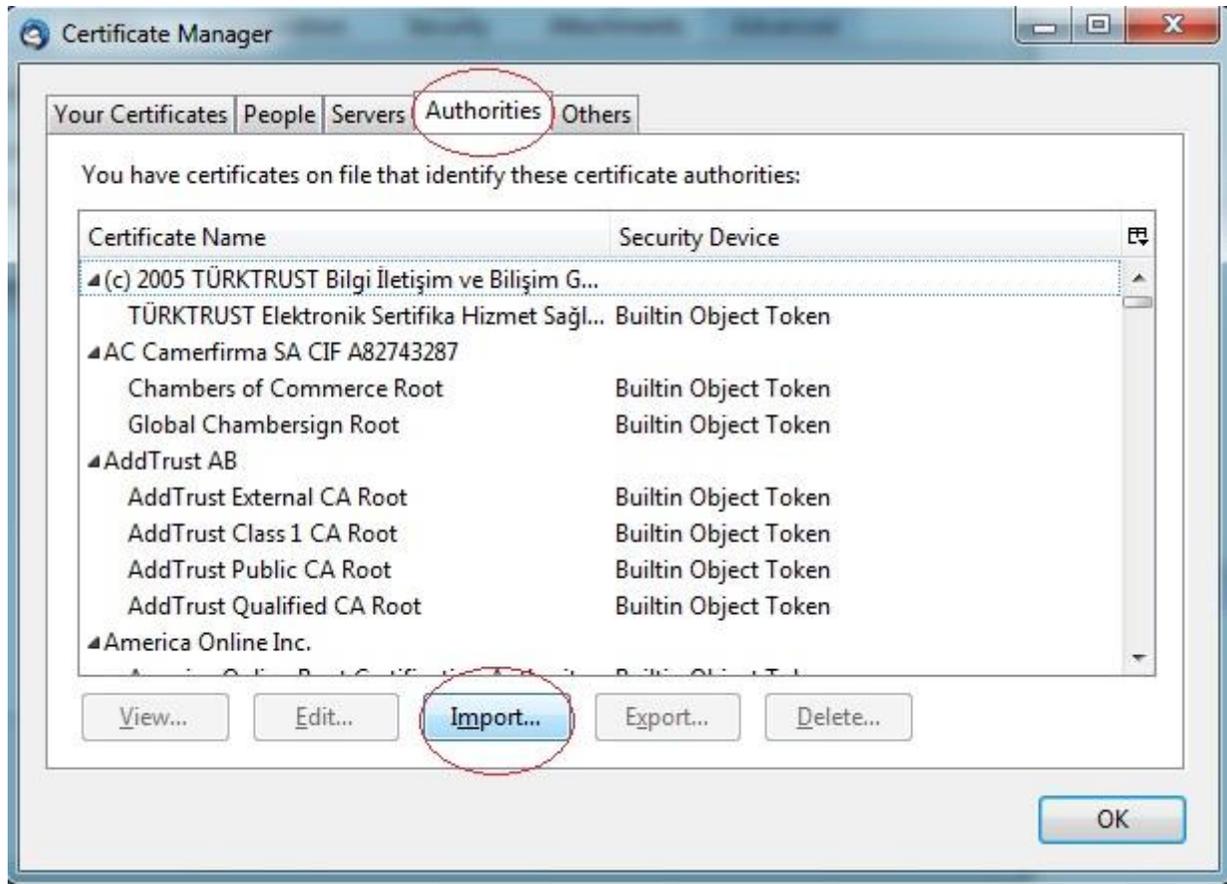


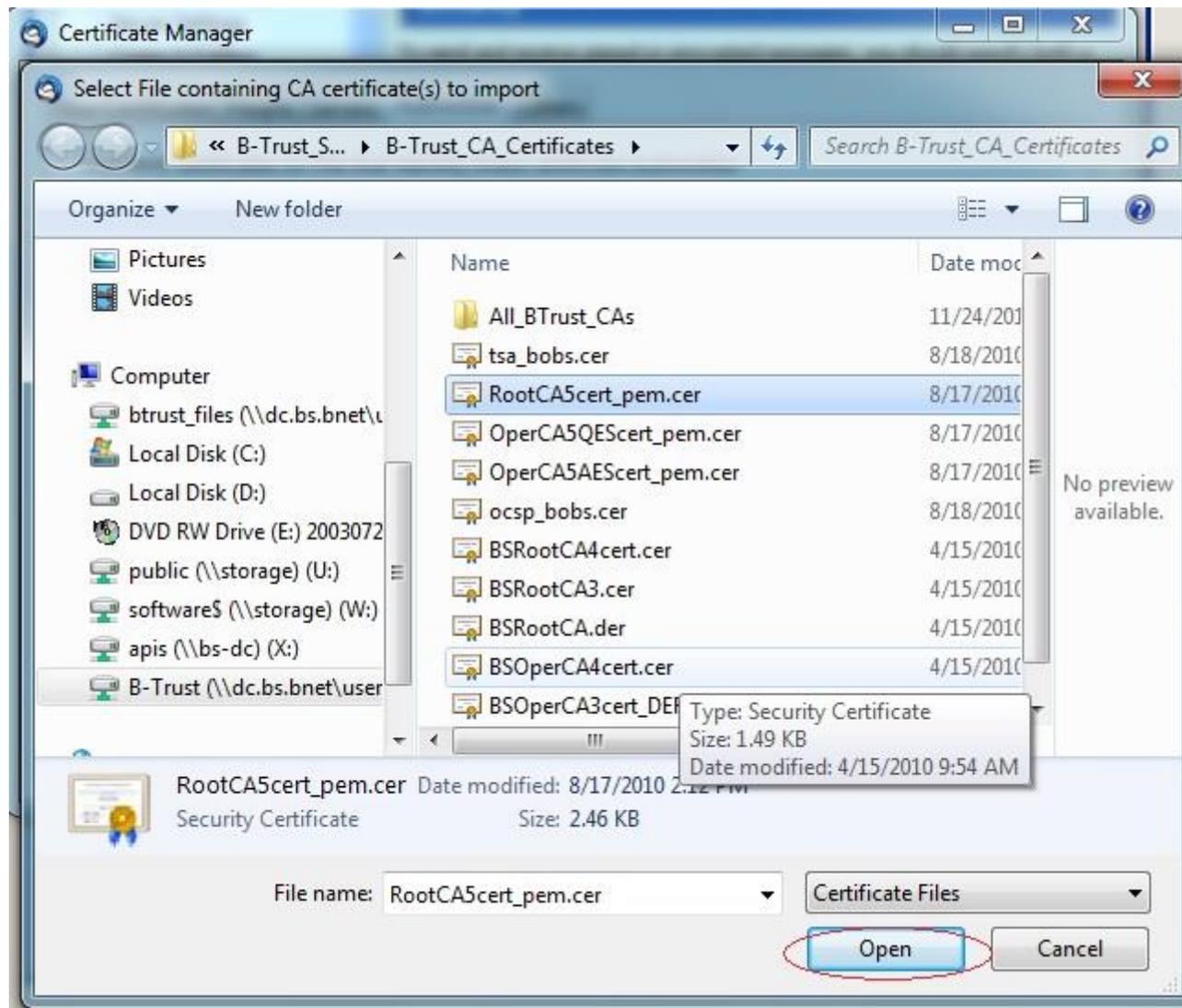
**IMPORTANT:** All of the operations in **Certificate Manager** window are executed directly into the smart card - for example the **Delete** button permanently deletes your digital signature from the smart card.

11. Choose **Authorities** tab.

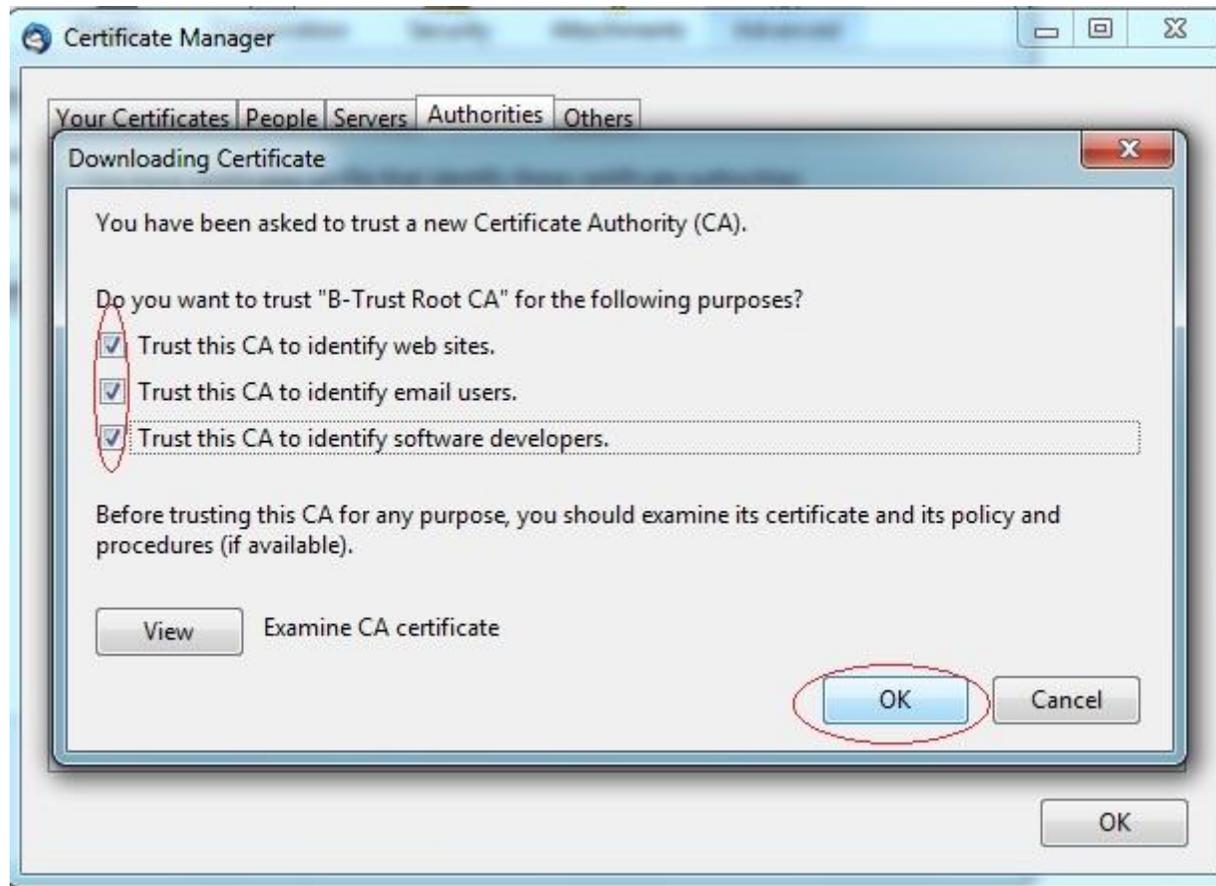


12. Click **Import...** and choose the first file from the **B- Trust CA\_Certificates** directory, located in your B-Trust install disk, and click **Open**.





13. Mark the three checkboxes and click **OK**



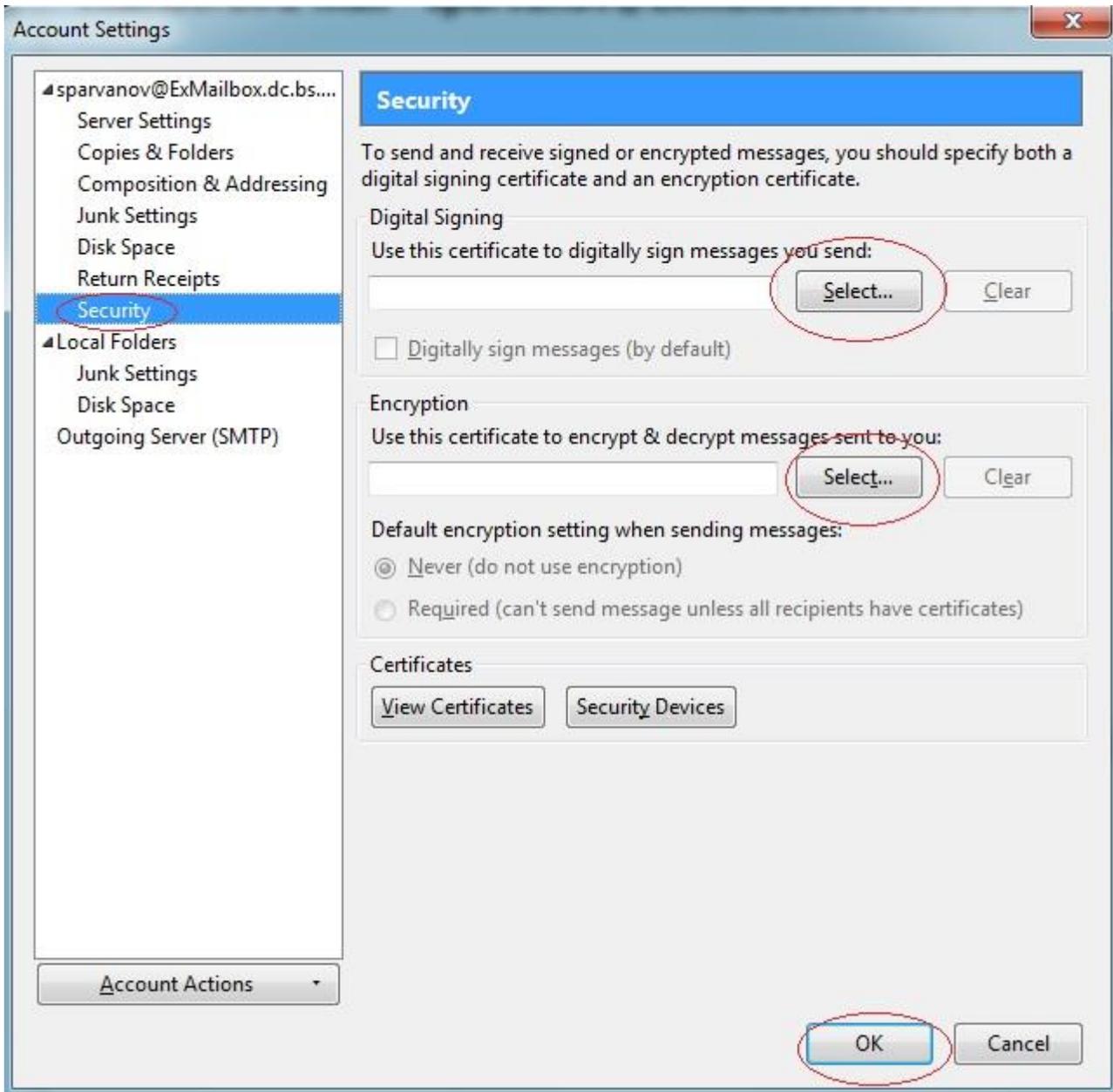
Repeat points 7 and 8 for all files with **.cer** extension from the specified directory.

14. Return to **Advanced** and click **View Certificates** . If configuration is successful, you will see the data for your digital certificate.

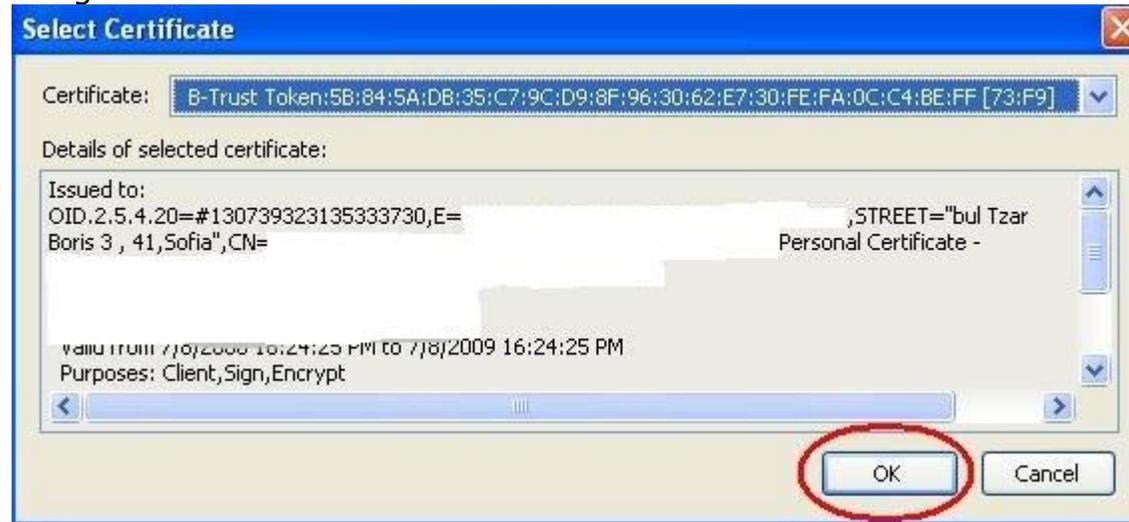
**IMPORTANT:** All of the operations in **Certificate Manager** window are executed directly into the smart card - for example the **Delete** button permanently deletes your digital signature from the smart card.

15. Go to the main windows.

16. From **Tools** menu choose **Account Settings -> Security -> Select...**

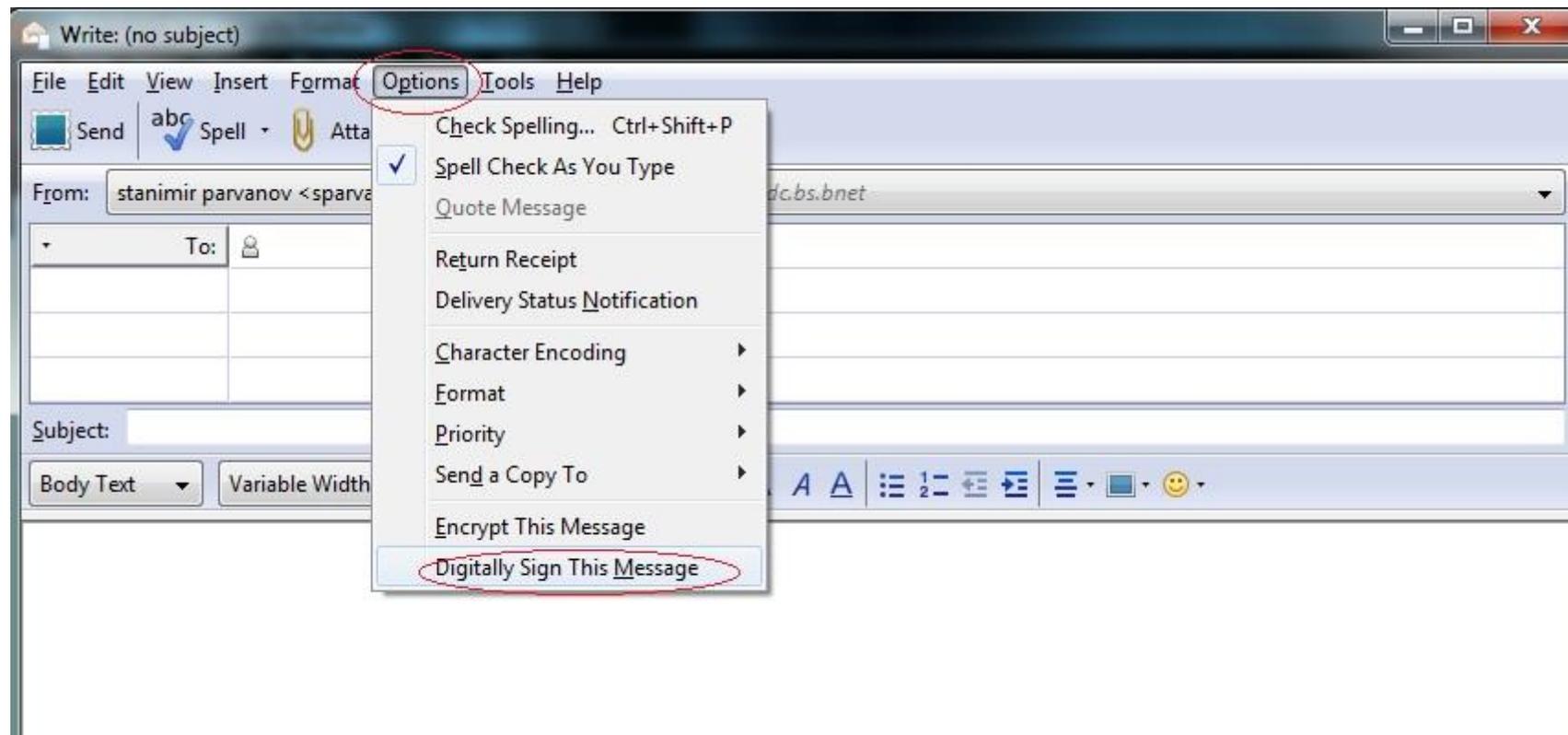


17. Select your digital signature and confirm with **OK**.



18. Confirm all windows with **OK**.

19. Create new e-mail and choose the options for sign and/or encrypt. From the standard toolbar click **Options...** , in the **Security** mark the checkbox **Digitally sign this message** -and/or **Encrypt this message**.



20. Click **Send**. After you type the **PIN** code the signed and/or encrypted message will be send.