

Some things you should know about Certificate Private Key passwords in Microsoft Internet Explorer.

First: Although you are using Internet Explorer to interface with your certificates, be aware that your certificates are actually stored in the Microsoft Certificate Store. The Microsoft Certificate Store is integrated into the Microsoft Operating System. Internet Explorer, Outlook, and other Microsoft applications can see and use your certificates, but the certificates are not stored in those applications.

Second: Your Certificate is an electronic personal identity document. YOU are the only person who is ever allowed to use your certificate. You are the only person who is ever allowed to have control of your certificate's Private Key. Every certificate has a Private Key and a Public Key. The Private Key is the heart of the certificate; if you have the Private Key you can make full use of your certificate. If you don't have the Private Key (or if you do not have control of the Private Key), then your computer will not allow you to use the certificate for anything. Setting a password on your certificate prevents other people from copying your certificate Private Key. This prevents other people from stealing your certificate; it also prevents other people from 'accidentally' using your certificate. You are REQUIRED by the Department of Defense (which has complete authority over the ECA certificate program) to protect your certificate Private Key with a password.

Third: Microsoft protects each certificate Private Key with its own password. So if you have an Identity Certificate and an Encryption Certificate, they will each have their own password. You **SHOULD** use the same set of characters for each password, but it is also possible to use a different set of characters as the password on each Private Key. Think of it as having two different combination locks where YOU set the combination. You are able and allowed to use the same combination on both; but they are not set like that unless YOU set them that way.

Fourth: The process of setting a password is not automatic, nor is it intuitive, when using Microsoft Internet Explorer. (Actually, this is true of most versions of the commonly available web browsers.) But you are still REQUIRED by the Department of Defense to protect your certificate Private Key with a password.

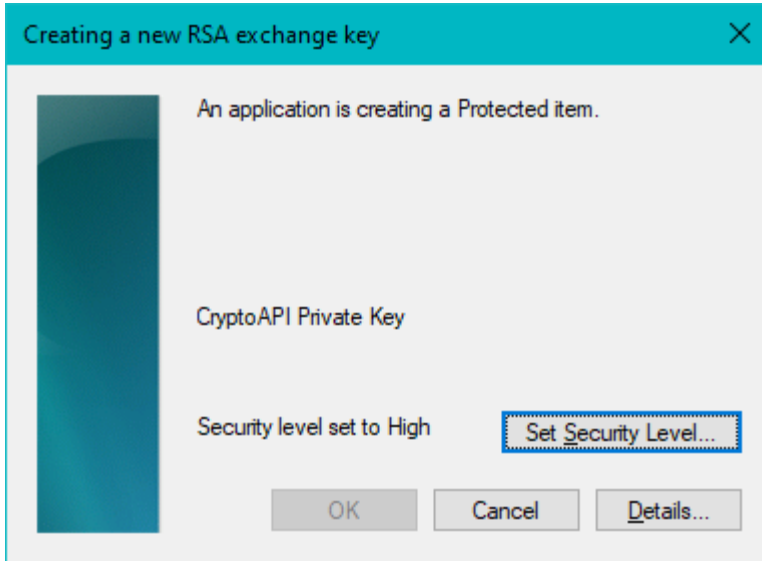
Fifth: The certificate Private Key password can only be set at time of Key Generation or at Private Key Importation. Key Generation occurs when you make the online certificate request; your computer creates the Private and Public Keys for your certificate. Private Key Importation occurs when you import (or restore, or install, etc.) your certificate from a backup (or export) file copy of your certificate. (NOTE: This does NOT happen when you import your issued certificate from the Certificate Server; what you import there is your Public Key.

Sixth: Your certificate Private Key is created on and by YOUR computer when you make the online request. (We know that you were communicating with our web site, but Key Generation happened entirely at your end.) WidePoint did not, has not, and will never have the Private Key to your certificate at any time. That means that we also did not ever have the password that you assigned to that Private Key. Therefore, WidePoint cannot reset the password, nor tell you what that password is. (If we had this information or an ability to reset the password for you, we would. We want you to be successful, but we don't have the ability to alter the password on your certificate Private Key. However, we do have some ideas that might help you at the bottom of this page.) So if you find that Microsoft demands a password from you to use the certificate, and you cannot find the password that Microsoft wants, the only solution is to get a new certificate. (And, yes, you will have to pay for it.)

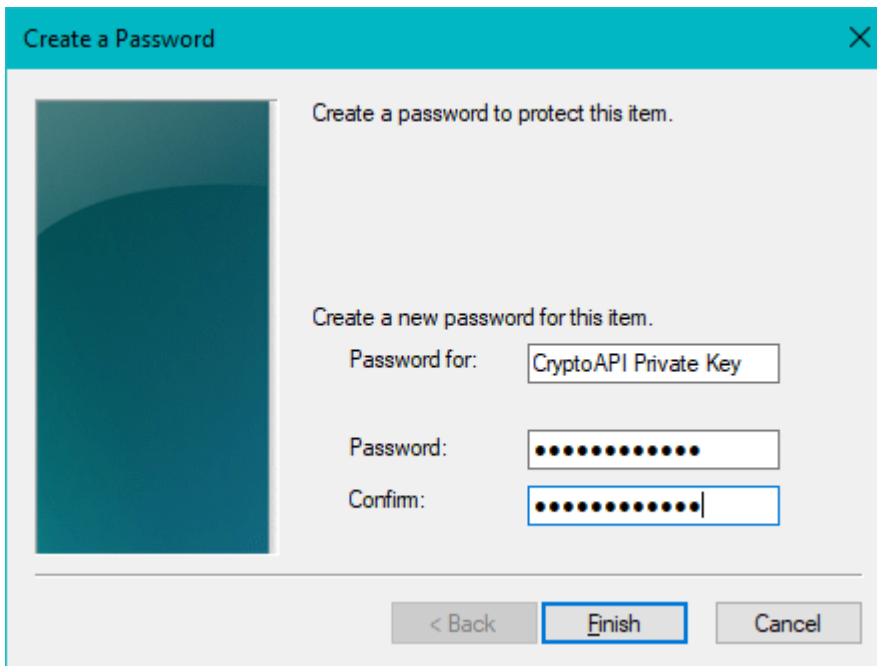
Setting a Password at Key Generation

When you make an online request, you should see a dialogue box as shown below. This is your first opportunity to set a password on the certificate Private Key.

1. In the Creating a new RSA exchange key dialogue box, click the **Set Security Level...** button



2. **Enter** and **confirm** a password then click **Finish**. NOTE: **Your certificate Private Key is created on and by YOUR computer when you make the online request. (We know that you were communicating with our web site, but Key Generation happened entirely at your end.) WidePoint did not, has not, and will never have the Private Key to your certificate at any time. That means that we also did not ever have the password that you assigned to that Private Key. Therefore, WidePoint cannot reset the password, nor tell you what that password is.**



3. You may now click the OK button.

