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 it's own password. So if you have an Identity Certificate and an Encryption Certificate, they will each have their own password. You MAY 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: If you missed your opportunity to set a password on your certificate Private Key when you made your online certificate request (Key Generation), or if you want to change your certificate Private Key password, you will need to re-import your certificate from a backup (or export) file. Unfortunately, there are no buttons to "Set Password," "Change Password," or anything like that. You just import the certificate (again) and assign whatever new password you want.

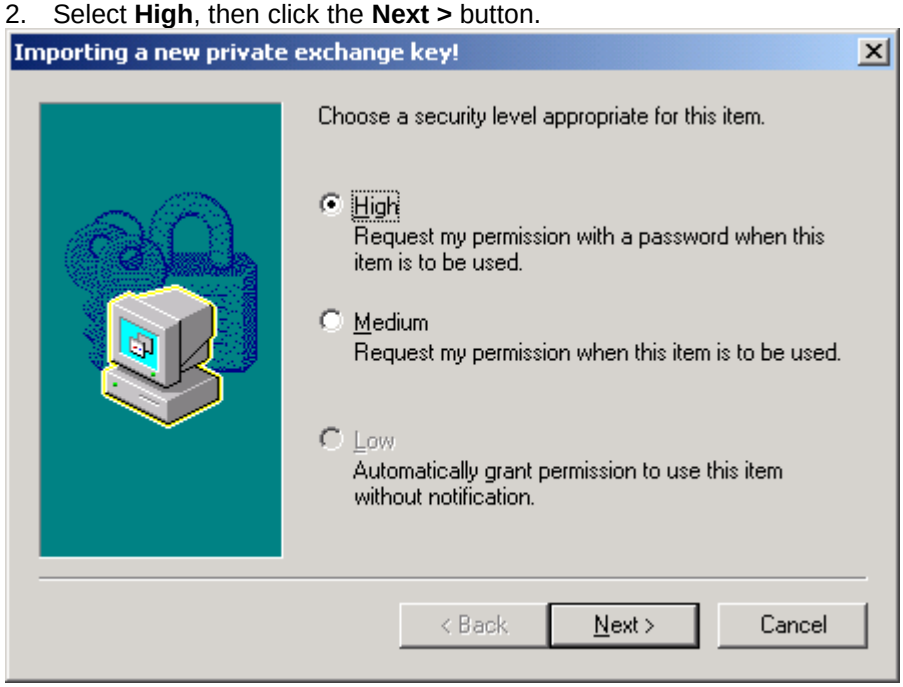
Seventh: Your certificate Private Key is created on and by YOUR computer when you make the online request. (We know that you were communicating with our web site, but Key Generation happened entirely at your end.) ORC did not, has not, and will never have the Private Key to your certificate at any time. That means that we also did not ever have the password that you assigned to that Private Key. Therefore, ORC 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.)

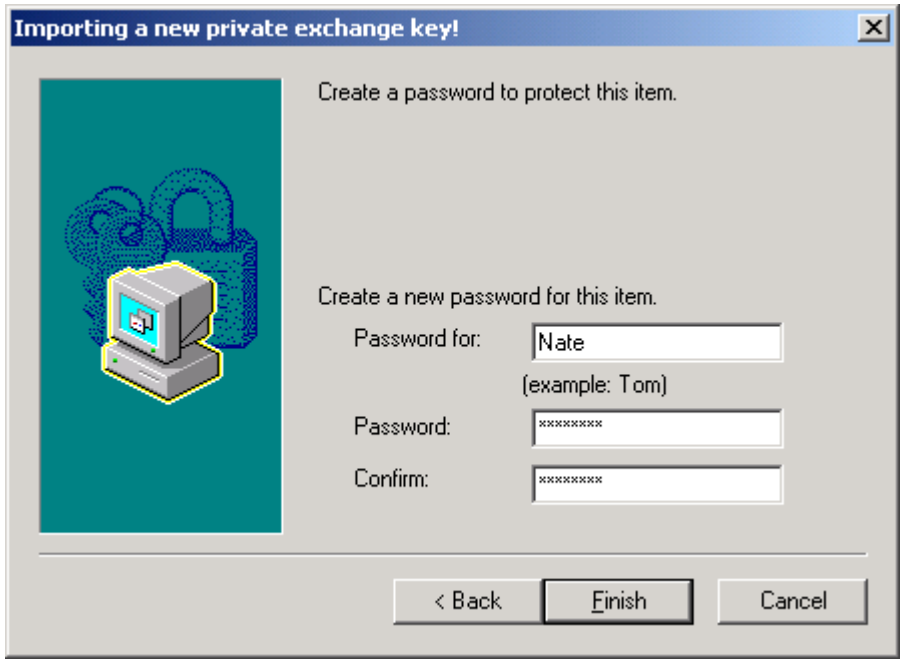
Setting a Password at Key Generation
When you make an online request, you should see a dialogue box as shown below. This is your first opportunity to set a password on the certificate Private Key.

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

2. Select **High**, then click the **Next >** button.



3. Enter and confirm a password.
   Note: Windows XP users will not be able to enter any data in the **Password for:** text box (they may not even see it). All other Windows users must enter some text into this text box. In the example we entered the person's name and certificate type.
   Click the **Finish** button.



4. Click the **OK** button.

If you have not set a password on your Certificate Private Key or if you wish to change the password on your Certificate Private Key...

Wait until you certificate has been issued and you have imported the certificate from the certificate server and then perform the following steps... 1. Make a backup (or Export) copy of your certificate.

2. Import your certificate back into Internet Explorer; you will have the opportunity to assign a password at the end of this process.

"My certificate won't take my password." OR "I forgot my certificate password"

Many Subscribers contact us with this problem. Some of them will state, bluntly, that they have forgotten the password (or that they have forgotten which password) that they assigned to their certificate Private Key. Many more are certain that they know the password that they assigned to their certificate Private Key (some even have it written down in front of them - *not recommended*).

Whichever is the case, if you and Internet Explorer (or any other Microsoft application) disagree about the password assigned to your certificate Private Key, Microsoft is going to win that argument every time. To the best of our knowledge, Microsoft does NOT change the password once it has been assigned. So we need to find the password that Microsoft wants.

The good news is that many of the people who contact us with this problem DO find the password that Microsoft wants. ALL of these people have discovered that the password that was actually assigned was NOT what the person was sure about (even those who had something written down). You should be able to try (and fail) over and over. Microsoft does not 'lock you out' of your certificate. *(CAUTION: If you are using a SmartCard, then you CAN 'permanently' lock the SmartCard; but that will not be Microsoft, it will be the middleware that runs that card reader.)*

Ultimately, if you cannot find the password, then all ORC can do is to sell you a new certificate.

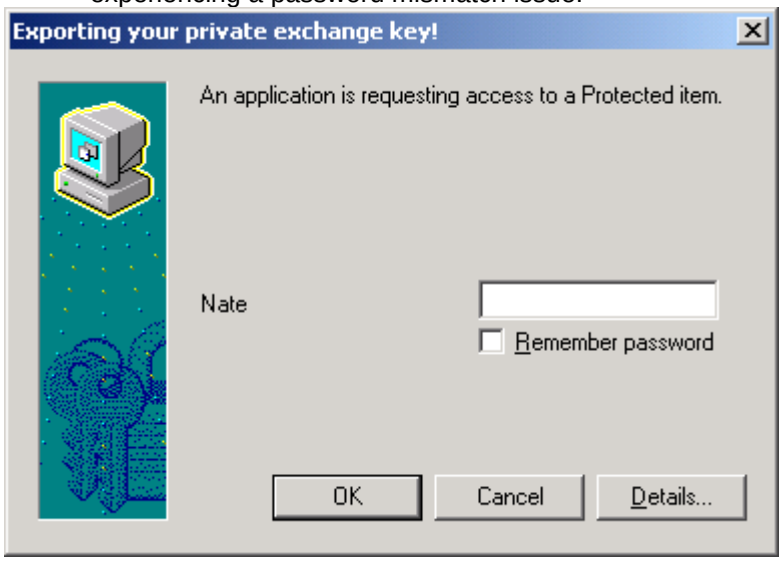
Potential work-around: If you already have a backup file of your certificate, you can re-import (or re-install) your certificate from the backup file. You can then assign the password that you want as part of that process. Bear in mind that when you made the backup file you were forced to assign a password to protect the file. You will need to know the password that you assigned to the certificate backup file.
(CAUTION: Do NOT remove or delete the current certificate; the import process will NOT create multiple instances of the same certificate. It will simply 'overwrite' the certificate already there. Some Subscribers hurt themselves by removing or deleting the wrong certificate.)

You can confirm that you are having a password issue (and not some other problem) by following the steps below.

Run through the process of making a backup (or Export) copy of your certificate. Since you are doing this for test purposes, save the file on your 'Desktop.'

A. If you can successfully complete the process (i.e. - you get an 'export was successful' result and you produce a file of *filename*.pfx) then you DO know your certificate password. Whatever problem you are having is NOT password related.

B. If you get through the Certificate Export Wizard and it fails on the very last step (i.e. you see the dialogue box below, but the process still fails), then you are experiencing a password mismatch issue.

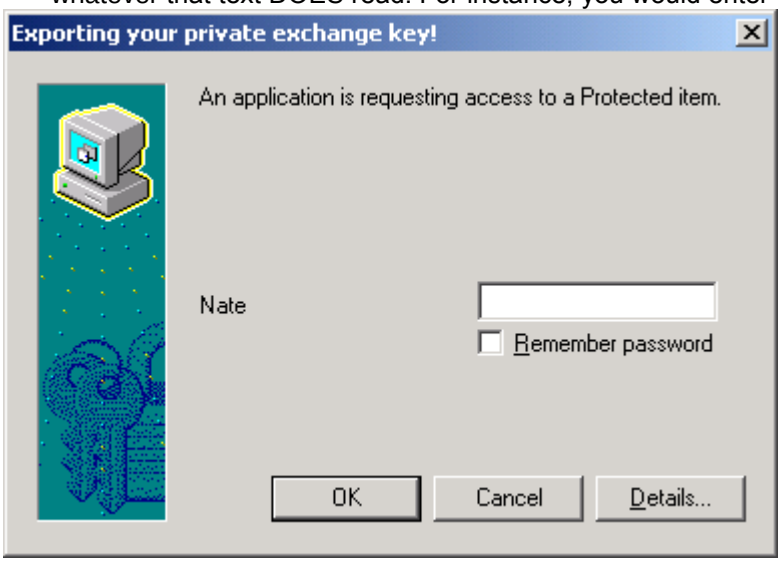


C. If you cannot get to the end of the procedure EXACTLY AS IT IS SHOWN, then you are experiencing a bigger problem then a password mismatch issue. Your certificate Private Key may have been 'marked' as non-exportable (and possibly 'marked' as non-functional. This can happen in a variety of ways; you should contact the ECA Help Desk if you have not already done so.

Listed below are some of the ideas or techniques that we tell people to try when they are searching for the correct password.

1. Try leaving the password field blank and click the **OK** button. *It is possible to assign a password that is blank. We've seen it happen to a few subscribers and we have been able to do this in testing.*
2. Try typing your password with CAPS LOCK 'On' *Note: CAPS LOCK 'On' is NOT the same thing as "ALL CAPS"*

3. Try using your network (or computer) log-on password. If your company makes you change this password often (most do), then try your previous log-on password (and maybe the one before that).
4. If you have several passwords that you use for different functions, try them all. (You might want to try them all with the CAPS LOCK trick.)
5. If, in the dialogue box where you must enter the password, the text to the left of the password field does NOT read "CryptoAPI Private Key"; then enter whatever that text DOES read. For instance, you would enter “Nate”.



NOTE: if your computer runs the Windows XP operating system, this will not help you. All Private Keys are called "CryptoAPI Private Key" in Windows XP.