

How to get your very own Digital Certificate

Purpose:

This will guide you through the process of getting a digital certificate, installing it, exporting it, importing it, and using it to sign and encrypt email messages using Internet Explorer and Microsoft Outlook. Instructions for other programs are available on the verisign website at: <http://www.verisign.com/client/guide/index.html>

The verisign website is fairly good about giving client-specific information as you proceed, but the process is complex and this guide should fill in some blanks.

Obtain the certificate in Internet Explorer:

1. Open an Internet Explorer browser and go to <http://www.verisign.com/client/enrollment/index.html>. (This page is buried several layers deep if you try to navigate to it from the verisign homepage). Click on the “Enroll Now” button when you are ready to start the application.
2. Fill in the blanks on the information page as follows:
 - a. “contents of your digital id” fields:
 - i. Firstname: enter your first name or your nick name. (eg: jdorn)
 - ii. Lastname: enter your last name. (eg: Dornback)
 - iii. Email: enter in the email address you will be using with this certificate. (this must be accurate – verisign will send you a confirmation email later on). (eg: jdorn@cren.net)
 - b. “Challenge Phrase” field:
 - i. Enter in a phrase you can remember (somewhat like a password) in case you need to revoke your certificate later on. Do not use punctuation.
 - c. Choose the “60 day free trial” option.
 - d. Do not enter any billing information (you are getting a free trial version)
 - e. “Select cryptographic Service” – leave this option as default.
 - f. Check the box to allow additional security. This will allow you to specify the amount of security your key has in Internet Explorer in a later step.
 - i. Low: no extra security. Private key is only protected by computer logon.
 - ii. Medium: you will be prompted if you want to use your key when it is being accessed.
 - iii. High: you must enter a password when the private key is being accessed.
 - g. Accept the agreement by clicking the Agree button.
3. A window will pop up confirming that an application is creating a protected item. You can change the security level here by clicking on the “Set Security Level” button. Click the OK button to continue. The page will then display “Step 2 of 4.”
4. Check your email for a message from Verisign. You should receive a message “within the hour.” When you get the email, copy the link from the message into Internet Explorer. Do not use Netscape or other browsers – the information is specific to IE. When the page comes up, copy and paste the PIN (the 32 character long combination of letters and numbers) into the field on the Verisign page. Click the Submit button.
5. Step 4 of 4 will be displayed with information about your certificate. Click on the Install button to install the certificate in to Internet Explorer.
6. The certificate is now installed in Internet Explorer. Disregard the instructions on the page on how to install the certificate in Outlook as they are incomplete.

How to get your very own Digital Certificate

Export the Certificate from Internet Explorer:

1. Export the certificate from IE. This saves the certificate as a file on your hard drive so that you can import it into other applications, or save a backup copy, etc.
 - a. In Internet Explorer, click the “Tools” menu, and select “Internet Options.” Click the “Content” tab. (it is not on the security tab)
 - b. Click the “Certificates” button (about the middle of the window). Click the Personal tab – your certificate should be listed here.
 - i. Select your certificate, and click the “Export” button. A wizard will come up.
 - ii. Click the next button (accepting defaults) until you are prompted for a password. This password protects the certificate file while it is on your computer, and you will be asked for it again when you try to import the certificate into another application. Enter a password and click Next.
 - iii. Select the location and file name for the certificate. Click next. Click Finish. A window may come up asking you for permission to export the key. Click OK. An alert will come up saying that the export was successful.
 - iv. Click the “Trusted Root Certification Authorities” tab – this is where we want CREN to be listed automatically so that we are a respected CA.
 - v. Close the certificates option menu, and then click OK on the Internet Options menu.

Install the Certificate in Outlook:

1. Open Microsoft Outlook. From the “Tools” menu, select Options, then go to the “Security” tab.
2. Click the “Settings” button. Under the Certificates and Algorithms area, click the “choose” button and choose your certificate for signing certificate and encryption certificate. Click OK in the “Change security settings” window.
3. If you want to sign every message you send, click the check boxes at the top of the Security tab. If you only want to sign certain messages, leave the options unchecked. Close the options menu.

Send a Signed and Encrypted Email:

1. Compose a new email in Outlook as you normally would. Before you send the message, click the options button in the new message window. (Alternately, select Options from the View menu in the new message window).
2. Click the check boxes for the options you want (either Sign, Encrypt, or both).
3. Send the message. The message will show up in Outlook with small icons denoting that it has been signed or encrypted.

Decrypting Email from other people:

1. To decrypt email from other people, you must have a copy of their certificate. To get this, have them send you a signed email. In outlook, open the email and then right click on the person’s email address, and select the option to add them to your contact list. Their key will be automatically added to the list of people you can decrypt from.
2. When the other person sends you an encrypted email, you will not be able to read it in the preview pane of Outlook. To view the message, open the message, and outlook will automatically decrypt it for you.