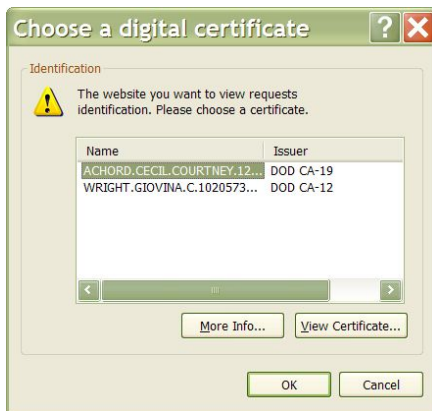


Using your Common Access Card(CAC)

What's on a CAC?

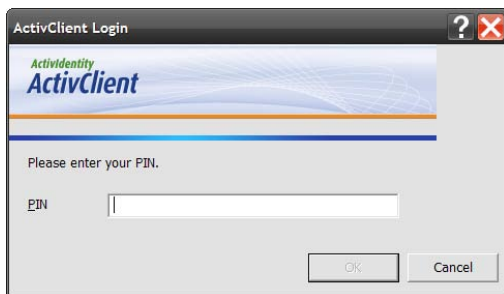
There are three PKI certificates(or keys) on your CAC. An ID certificate, a Signature certificate, and an Encryption certificate. The ID Certificate gets you onto PKI secured web sites, the Signature certificate lets you digitally sign e-mail, and the Encryption certificate works in combination with someone else's Signature certificate to allow you to send encrypted e-mail. (PKI stands for Public Key Infrastructure, but I won't go into any of that here.)

These certificates are copied to your computer the first time you insert your CAC card, but cannot be used unless your CAC is in the reader and the correct PIN code is entered. I say this because in some boxes that come up on your computer (i.e. when going to access a secure web site), there may be certificates left over from past CAC cards, and other people's CAC cards who have used your computer.



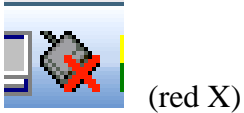
PIN Code/E-mail

The PIN code you set when you were issued your CAC card is asked for whenever the computer needs to use a Certificate, not upon insertion. It is important you remember this number, because enter it in three times wrong and you will have to get it reset at the pass office. There is no one you can call to tell you it if you forget it, so in this case as well, you will have to go get it reset at the pass office. You also need to make sure the e-mail address you gave the pass office as they were making your card is the correct one.

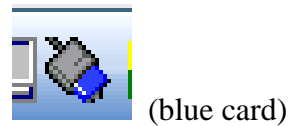


Inserting your CAC card into the reader:

When you insert your CAC card into the reader, this little icon(or similar) in your systray (by the clock) should go from this:



to this

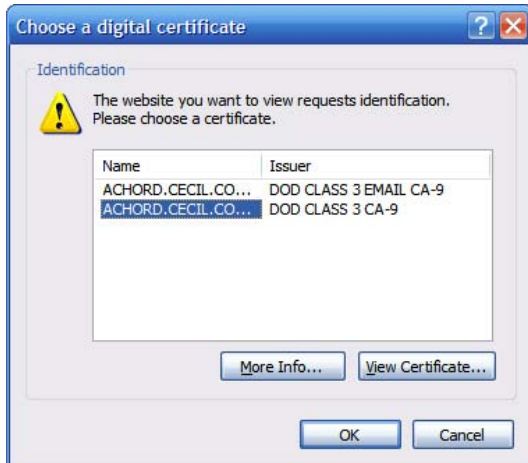


(after blinking back and forth from blue to red for a couple of seconds)

Using your CAC card on a PKI secured web site(Works in Internet Explorer only)

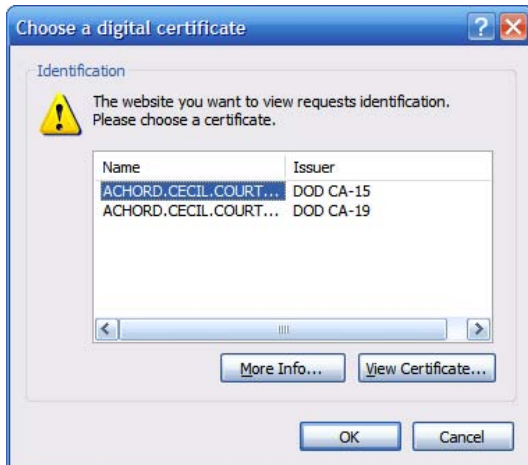
When going to a PKI secure site, like say the one we use in the installation section to grab the DoD root certificates <https://infosec.navy.mil>, you will be prompted with the following box asking you to choose a digital certificate:

What to choose?

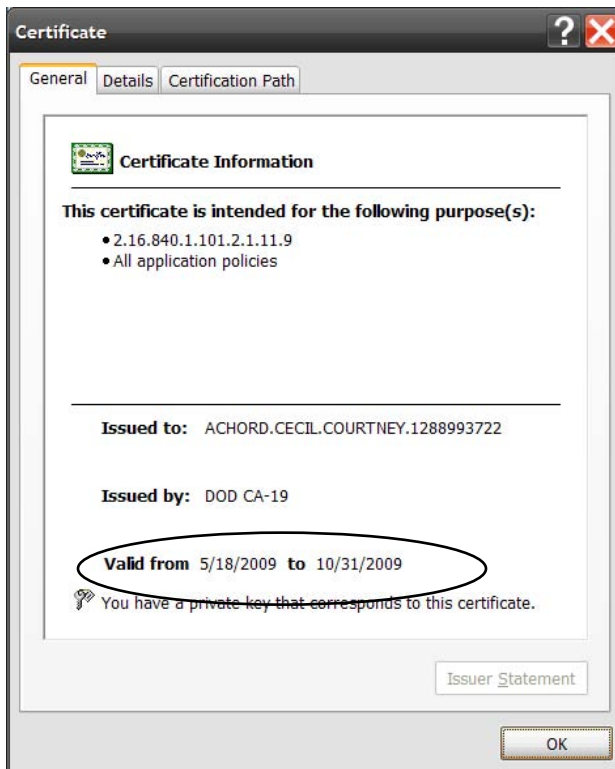


In this box, it shows two kinds, because the web site designer did not hide my e-mail certificate as not-applicable. Because we are going to a web site, we should choose the one that does not have the word e-mail somewhere in the Issuer field.

What about this one?

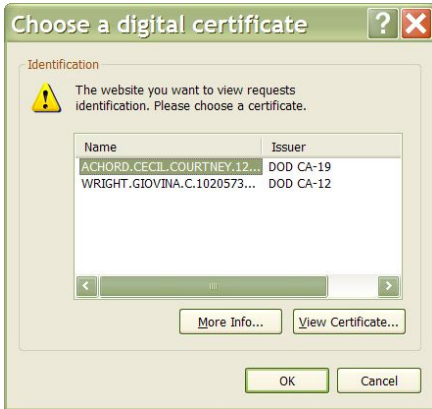


In this box, the web site designer did filter my e-mail cert like he should, but I've got two regular ones here. This means I have a leftover from a previous CAC card of mine. How do I know which one to pick? CA-19 has to be the newer one right? Well, this time it is, but this is almost never the case. To find out which one you should pick, click one and then click "View Certificate"



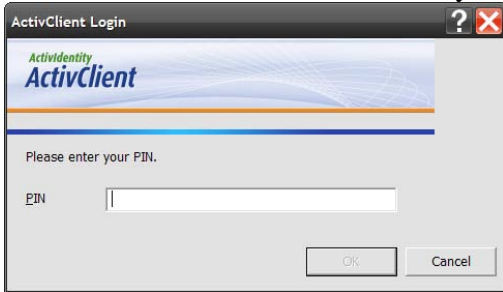
See the "Valid From", this matches the valid dates of my current CAC card, so that's the one I should choose.

How about this one?



Well, obviously I'm going to choose mine, but why is Gina's there, and can I use that one? It's there because she used her CAC card on this computer before, and no, you can't use it as you don't have her CAC and her PIN. (see "What's on a CAC" paragraph two)

Once you choose the correct certificate, you will be prompted for your PIN, enter it and click OK, and the PKI secured site you had originally wanted to go to should load.



Note: You will only be asked for your PIN one time after inserting your CAC during attempted access to secure e-mail or a secure website. If you restart your computer, remove and re-insert your CAC, or after a period of inactivity, the next time you try a secure e-mail or secure website, it will ask for your PIN again.

Using your CAC card for secure e-mail

Secure e-mail is another main function of your CAC card. You can Digitally Sign an e-mail (this guarantees the reader this e-mail is from you) and/or encrypt e-mail so that the other person cannot read a message you sent without their CAC card and PIN.

Digital Signature

When you digitally sign an e-mail (with your signature certificate) and send it to anyone, they can read it regardless of who they are, people who have CAC cards or not.* It is for identification purposes, but is also necessary in setting up the conditions needed for encrypted e-mail.

*However, only the people with the DoD root Certificates installed/updated will Outlook be able to properly verify that "Certificate Chain". Without the DoD root certificates installed or updated, a person receiving a message signed by a CAC card, may have their Outlook freeze or lockup until it gives up on the chain verification, and shows you the message. This means it is important to repeat Step 3 of the Installation section periodically.

Encrypted e-mail

When you encrypt an e-mail(with your encryption certificate), only the intended receiver can view it, and they must use their CAC card to do so.

To send encrypted e-mail to someone you need your encryption certificate and the intended receiver's signature certificate. Conversely, the other person needs their encryption certificate and your signature certificate to send you one. That's how the math works.

OK, so how do I do that?

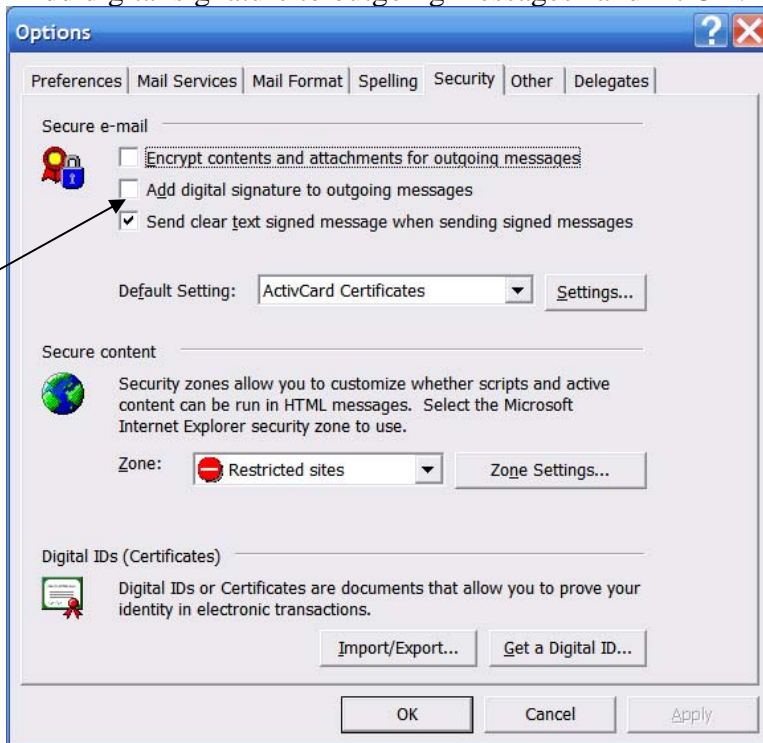
Basically it means that someone must send you a digitally signed e-mail first. Then you use that e-mail to add them to your contacts. Once their contact with attached digital signature is in your contacts, you can make an e-mail, selecting that contact to send to, then with your CAC card inserted, click the encrypt button on that e-mail before hitting send.

Step by step in the next section.

Using Outlook with CAC

Preparation

First off, ActivCard/ActivClient when first installed sets a default that is sort of annoying. What you may notice is that Outlook will now try to digitally sign EVERY E-MAIL sent, and cannot do so without your CAC inserted, so no e-mail will go out. TO FIX THIS GO HERE: In Outlook's main window, go to Tools>Options in the Security Tab, Uncheck "Add digital signature to outgoing messages" and hit OK.



---The fix

Sending Digitally Signed e-mail

To send a digitally signed e-mail do the following:

Create a new message, forward a message, or reply to a message

Within this new message you should see two icons somewhere in the toolbar that look like this(or similar):



Click the one with the red ribbon to digitally sign this e-mail.

You will be asked for your PIN code at some point if needed(most likely when you go to send).

Note: You will notice that if you get a digitally signed e-mail from someone and reply to it or forward it, Outlook will assume you want to yourself digitally sign the reply or forward. If you don't have your CAC card in this will make Outlook lock up for a while until it fails on the message. You can unclick the button with the red ribbon before sending to avoid this to not digitally sign the reply or forward, or actually insert your CAC card and try again if you indeed want to keep it digitally signed.

Sending Encrypted E-mail

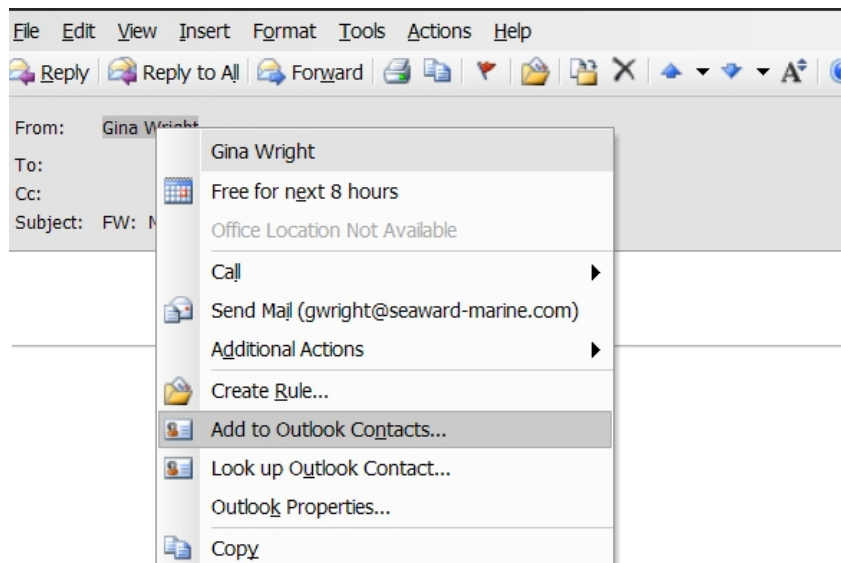
In order to be able to send and receive encrypted e-mail from someone you must do the following once for a particular person, and again if either party is issued a new CAC card:

Have your CAC card inserted. Enter your PIN code if/when prompted.

Send the person you want to communicate with a digitally signed e-mail asking them to send you a digitally signed one back.

They must add you to their contacts from within the digitally signed e-mail you sent them.

You must add them to your contacts from within the digitally signed e-mail they sent you back.



It may ask you if you would like to update an existing contact that you have already for that person, this is fine.

Now you can send them an encrypted e-mail.

To send an encrypted e-mail do the following:

Create a message, forward a message, or reply to a message

Anyone you add to the “to” or “cc” field you must do by clicking the “To” or “Cc” buttons and selecting them from your contacts, using the contact or contacts previously set up by the digitally signed e-mail back and forth.

Again we look at these two icons in the toolbar:

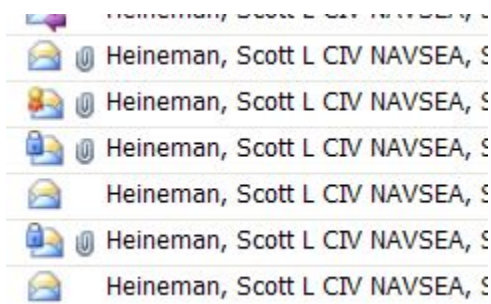


This time you click the one with the blue lock. You can also digitally sign as well, so just click both for good measure.

You will be asked for your PIN code at some point if needed(most likely when you go to send).

Identifying Digitally Signed and Encrypted E-mail

In your main view in outlook messages will appear with the blue lock(encrypted) or red ribbon(digitally signed)



Also, with a particular e-mail open you can see in the lower right corner of the “header” a blue lock or a red ribbon.

What happens to all my encrypted e-mail I have saved when I get a new CAC card?

You can't read them anymore.

...

Relax, there is a convoluted, but quick method of changing those encrypted e-mails over to your new CAC.

Info on that here:

<https://infosec.navy.mil/PKI/keyrecovery.html#mailcrypt>

I will have my own walkthrough for ya'll to simplify the process.