



CAC/PKI TRAINING GUIDE

***Common Access Card/
Public Key Infrastructure***

Phone: 703.769.4500

Fax: 703.769.7605

<http://setdweb.belvoir.army.mil>



Table of Contents

1	GENERAL	4
2	INTRODUCTION	4
3	WHAT IS PUBLIC KEY INFRASTRUCTURE?	6
3.1	WHAT IS A CERTIFICATE AUTHORITY?	7
3.2	WHAT ARE CERTIFICATES?	8
3.3	WHAT IS THE COMMON ACCESS CARD?	9
4	EXPLAINING DEERS AND RAPIDS	10
5	DOD PUBLIC KEY INFRASTRUCTURE ROLES	11
5.1	RESPONSIBILITIES OF THE VO/LRA	11
5.2	RESPONSIBILITIES OF THE DOIM	12
5.3	RESPONSIBILITIES OF THE IMO	13
5.4	RESPONSIBILITIES OF THE CARD RECIPIENT	13
6	INSTALLATION TRAINING SCENARIOS	14
6.1	SYSTEM REQUIREMENTS	14
6.1.1	Operating Systems	14
6.1.2	Applications	14
6.2	INSTALLING ACTIVCARD GOLD 2.0.1 MIDDLEWARE	15
6.3	INSTALLING CARD READER AND DRIVERS	28
6.3.1	SCM SCR111 Serial SmartCard Reader	28
6.3.2	ActivCard Serial SmartCard Reader	40
6.3.3	Schlumberger Reflex 72 Serial Smart Card Reader	49
6.3.4	Schlumberger Reflex USB Card Reader	57
6.3.5	Schlumberger Reflex PCMCIA Card Reader	64
6.4	CHECKING CARD READER INSTALLATION WITH DEVICE MANAGER	70
6.5	OBTAINING AND INSTALLING ROOT CERTIFICATES	74
6.5.1	Obtaining and Installing Test CAC Root Certificates	74
6.5.2	Obtaining Root Certificates	88
6.5.3	Installing Root Certificates	94
6.6	REGISTERING CAC PKI CERTIFICATES	99
6.7	CONFIGURE OUTLOOK 98/2000 CLIENT SECURITY PROFILE	108
7	FUNCTIONAL TRAINING SCENARIOS	123
7.1	SENDING AND RECEIVING DIGITALLY SIGNED AND ENCRYPTED EMAIL	123
7.1.1	Sending Email	123
7.1.2	Receiving Email	128
7.2	RETRIEVING OTHER USERS CERTIFICATES	134
7.3.1	From a Signed Message	134
7.3.2	Retrieval from DOD PKI Directory	137
7.3	NETWORK LOGIN	148
7.3.1	Windows NT & 2000 Network Login	148
7.3.2	Windows 98 Network Login	149
7.4	LOGIN TO A PK-ENABLED WEBSITE	150
8	TROUBLESHOOTING GUIDE	154



**Product Manager
Secure Electronic Transactions – Devices**

8.1	FREQUENTLY ASKED QUESTIONS.....	154
8.2	WHERE DO I GO FOR HELP?.....	161
APPENDIX A – ACRONYMS		162
APPENDIX B – DEFINITIONS.....		163



1 General

The Army Common Access Card (CAC)/Public Key Infrastructure (PKI) program implements Department of Defense (DoD) policy to adopt smart card technology department-wide. Smart card technology implementation has been led through guidance and direction of the Deputy Secretary of Defense and Public Law 106-65, National Defense Authorization Act for FY 2000. In response to these directives, the U.S. Army has aggressively pursued the programmatic steps required to ensure a seamless integration of this emerging technology at the operational level. The CAC will be implemented to provide the following functionality: personnel identification, building access, network access utilizing Public Key Infrastructure (PKI) certificates and eventually sending and receiving digitally signed and encrypted email. The CAC will replace the current Teslin military identification card (ID) and serve as the official ID card for civilians and eligible contractors. The CAC will also be used for physical access to facilities and serve as a token to enable logical access to networks and systems.

The CAC will be issued using the existing Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System (DEERS/RAPIDS) infrastructure. Approximately 1.4 million CACs will be issued to all Army active duty military, National Guard members, select Reservists, DoD civilians and eligible contractors in FYs 01 to 02.

2 Introduction

On 6 May 1999, the Deputy Secretary of Defense issued a memorandum that encouraged widespread use of public key-enabled applications and provided specific guidelines for applying PKI services throughout the Department. The strategy to achieve the target DoD PKI is intrinsically linked to the overall DoD strategy for achieving information assurance (IA). The 12 August 2000 Deputy Secretary of Defense memorandum further defines these guidelines and supercedes the memorandum of 6 May 1999. On 10 November 1999, the Deputy Secretary of Defense directed that the CAC be used as the DoD's primary platform for the PKI authentication token. The report submitted in compliance with the requirement in Section 374 of FY 2000 Defense Authorization Act (Public Law 106-65) requiring the evaluation of the option of using the smart card as the DoD's authentication token concludes the smart card is the most feasible, cost effective technology for the authentication mechanism to support the DoD PKI and to protect its critical information.

The DoD CAC will employ smart card and PKI technology. The CAC is the size of a credit card and contains an Integrated Circuit Chip (ICC) that is capable of storing a significant amount of data, has both read and write capabilities as well as a Personal Identification Number (PIN) selected by the cardholder. This PIN acts as a security code for the cardholder preventing others from fraudulently using the card. The CAC also contains a magnetic stripe, a Code 39 bar code,



a two-dimensional PDF417 bar code, a color photograph and printed text. As DoD implements applications that use these automated technologies on the CAC, data can be added, modified, or removed from the card as needed. These cards will be used for visual identification, access to buildings and controlled spaces, and access to DoD computer networks and systems. Eventually, users will be able to use their cards to send and receive secure e-mail messages and access secure Web sites. Additional component-specific uses may be added as well.

Through RAPIDS version 6.0, one or more PKI certificates are stored on the CAC. Certificates contain user identity data, the validity period for the certificate, and the public key portion of the public/private key pair used in public key encryption. Managing keys and certificates through a PKI helps an organization establish and maintain a trustworthy network environment.

With a few exceptions, all the members of these target populations will be issued a CAC:

- Active Duty members.
- Selected Reserve and National Guard members. This includes members in these categories who are on Active Duty. There may be some exceptional situations where members in other Reserve categories will receive a CAC, because they require an electronic card to gain physical access to controlled areas or logical access to government computers.
- Civilian DoD employees, including Non-appropriated Fund (NAF) and Foreign National employees. Issuance of cards to foreign military will follow the same rules as those for Foreign National DoD employees.
- Designated DoD contractors who require an electronic card to gain physical access to controlled areas or logical access to government computers.

The following populations will continue to be issued Teslin Uniformed Services identification and privilege cards, unless a CAC is issued for exceptional conditions, as noted in the preceding:

- Reserve members who are in the Standby Reserve, Individual Ready Reserve, or the Inactive National Guard, i.e., components that are not classified as Selected Reserve. These members will receive a DD Form 2 (Reserve).
- Designated DoD contractors who do not require an electronic card to gain physical access to controlled areas or logical access to government computers, but do require an ID card to conduct government business or a privilege card to access authorized DoD benefits. This mostly applies to contractors who are employed overseas or are considered emergency essential because they are likely to be assigned overseas, are serving overseas, or are employed at US installations where benefits are authorized locally. These individuals will receive DD Forms 2750 or 2764.



The following other populations will continue to receive the teslin Uniformed Services identification and privilege cards, as indicated, without exception:

- Reservists not receiving a CAC will receive a DD Form 2 (Reserve).
- Retirees with full retirement benefits receive a DD Form 2 (Retired).
- Reserve retirees receive a DD Form 2 (Reserve Retired) until they reach age 60, at which time they qualify for full retirement benefits.
- Family members of Active Duty, Reserve, and retired (with full retirement benefits) sponsors will receive DD Forms 1173 and 1173-1. While there are some exceptions, children below the age of 10 do not receive any cards.

3 What Is Public Key Infrastructure?

A Public Key Infrastructure (PKI) is a system of Certificate Authorities (CAs), Registration Authorities (RAs), directories, client applications and servers that model trust and allow for secure/encrypted electronic data transfers/transactions. Each person or entity (such as a server or individual) is issued one or more certificates by the CA, which are digital records that contain information, such as the entity's name and public key, and the signer's signature and data. Each CAC will contain a public and a private key specific to the cardholder. These keys can be used for data and e-mail encryption. Each person to receive a CAC will be issued an identity certificate, an e-mail encryption certificate, and a digital signature certificate to be used by applications that are part of the DoD PKI. The CA is a secure server that signs end-user certificates and publishes Certificate Revocation Lists (CRLs) for certificates that are no longer valid. Directories are secured and trusted repositories of information, usually collected during the registration process.

The DoD PKI plans to utilize RAPIDS workstations as Verifying Officer/Local Registration Authorities (VO/LRAs) to:

- Register DoD personnel who will receive the CAC with the CA.
- Create and print the CAC.
- Download certificates to the CAC.

The RAPIDS workstation will also support revoking certificates, resetting a user's CAC PIN and updating information in DEERS. It is envisioned that the CAC will be used for applications, such as computer access, network access, e-mail encryption, web authentication, building access, digital signature, and other functions as PKI applications are developed and deployed by the DoD.



PKI is essential in supporting Public Law 103-355, the Federal Acquisition Streamlining Act of 1994, which requires the broad use of Electronic Commerce and Electronic Data Interchange (EDI) by Federal agencies. In his 1997 Management Reform Memorandum number 16, Deputy Secretary of Defense, Dr. John Hamre, directed the development of a DoD-wide PKI that supports information security. PKI provides the framework and services for the generation, production, distribution, control, and accounting of certificates. Certificates contain the user's identity and public key.

Public key technology is often referred to as asymmetric or a two-key system. Each user has a pair of keys – the keys are not the same but match up in a unique way. One key is kept only by the user and is called the private key. The other key is widely distributed and is called the public key. These electronic key pairs provide users with two important capabilities. The first is the ability to digitally sign a document. The second is the ability to encrypt and decrypt messages. When digitally signing a document, the user's private key is used to sign it and their public key is used to verify the signature. When sending an encrypted message, the recipient's public key is used to encrypt the message. The recipient's private key is used to decrypt the message. Identity and Digital Signature private keys never leave the card. The E-mail Encryption private keys are generated off the card and escrowed by the CA. It is important for both the CAC recipient and the VO to understand the importance of updating RAPIDS with the correct e-mail address. The e-mail address must actually match the address used on the server; otherwise, the certificates cannot be used.

3.1 What is a Certificate Authority?

The DoD CA is a computer server that contains and automates the registration process using PKI technology. A certificate is a computer-generated record that ties a user's identification with the user's public key in a trusted bond. This trust is based on a registration process and is automated by the CA. The Secure Sockets Layer (SSL) session encrypts all communications between DEERS/RAPIDS, and the CA. Public and private keys help ensure that the information transmitted between computers is secure.

Three types of servers support the DoD PKI:

- Multiple Root CA servers authorize issuance of certificates to users in the DoD PKI.
- A CA issues certificates to users.
- A Directory server makes other users' public certificates available to PKI applications.



3.2 What are Certificates?

A certificate is a computer-generated digital record that ties a user's identity with the user's public key in a trusted bond. This trust is based on the individual's/entity's identity being verified then registered by the RA, and the certificates being created, signed, and issued by a trusted server known as the CA. As long as the trusted CA signs a certificate and the trusted CA's signature can be verified, any tampering with the certificate can easily be detected. Three types of servers support the DoD PKI:

- The DoD Root CA server authorizes subordinate CA servers to issue certificates to users in the DoD PKI. The DoD Root CA is the common point of trust for all certificates issued by the DoD PKI.
- A CA creates, signs, and issues public key certificates to individuals/entities at the request of a RA. It posts certificate information to the Directory Server, maintains the CRL, and posts CRLs to the Directory Server.
- A Directory Server stores the certificates containing public keys for all registered individuals/entities and makes these available to other individuals/entities that need to verify a certificate or use a public key for encryption.

Public and private keys help ensure that the information transmitted between computers is secure. Having the keys themselves are of no benefit, the user must have a PK-enabled application to make use of them. This provides:

- Confidentiality or privacy: protecting data from anyone who is not authorized to review it.
- Integrity: protecting data from unauthorized modification during transmission, storage, and processing.
- Identification and authentication: verifies that you are who you say you are.
- Non-repudiation: Because of the authentication, PKI prevents the e-mail sender from denying he or she sent the message. This is also the case when any document is signed with the individual's digital signature certificate. This is known as non-repudiation.

It is, therefore, imperative that each individual keeps their private key and the PIN on the CAC secure. **Do not divulge the PIN to anyone.**

When a card is being terminated, RAPIDS will revoke the certificates associated with the CAC. RAPIDS will automatically terminate the identity and digital signature certificates for reasons such as a lost card or invalid entry. If information on the card changed or the card has a defective chip, the VO will retain that CAC and issue a new one.



3.3 What is the Common Access Card?

The CAC differs from the standard Teslin Uniformed Services ID card in several ways. The CAC employs smart card and PKI technology. The CAC is made of plastic (polyvinyl chloride (PVC)) and contains an ICC with 32 kilobytes (KB) of memory storage. The standard (code 39) and two-dimensional (PDF417) bar codes contain demographic and card management information. Unlike the bar codes, the magnetic stripe and chip have the capability to update (erase and save) stored information. The magnetic stripe has the ability to store building access or financial information. The chip contains identification, demographic, card management, benefits, digital certificates, and other application-specific data. The digital certificates can be used to verify or authenticate the cardholder via a computer system or network, encrypt information, and sign digital documents, such as electronic mail.



Figure 1: Front of CAC

The front of the CAC contains such information as Organization Seal, Branch of Service, Color Photograph, Personnel Category, Name, Rank and Pay Grade, Issue Date, Expiration Date, Card Type, Card Identification Information, Hologram, PDF417 Bar Code which contains DoD Electronic Data Interchange Person Identifier and Social Security Number information, and the ICC.



Unauthorized reproduction, imitation, or likeness of the CAC is punishable under 18 U.S.C. Section 701.

Figure 2: Back of CAC

The back of the CAC contains a Magnetic stripe, Code 39 bar code, Date of Birth, Social Security Number, Geneva Conventions Category, Blood Type, and Organ Donor Status.

If due to multiple personnel categories, a person requires multiple CACs, all CACs are to receive the identity certificates. The e-mail certificate will be requested if the e-mail address is present in the Service Record view. For dual eligibility situations (such as DoD Contractor and Reservist), both eligible CACs will be given identity certificates. E-mail certificates will be added to the CAC if the corresponding personnel category has an e-mail certificate.

4 Explaining DEERS and RAPIDS

DEERS is the database that tracks personnel and medical DoD benefits. The DoD operates one of the largest health care systems in the world. DEERS has rules that determine benefits based on the beneficiary's data and status in DEERS. Tracking and determining personnel and medical DoD benefits help reduce the fraud and abuse of these benefits. Also, it ensures that all beneficiaries receive the benefits to which they are entitled.

RAPIDS is the application software that allows users to communicate with the DEERS database. RAPIDS determines benefits and using the same rules as DEERS, allows users to issue machine-readable automated ID cards and print the DD Form 1172. Additionally, it provides a means to update sponsor and family member information in the DEERS database.

The DEERS and RAPIDS data is protected under the Privacy Act Statement (10 U.S. Code 133; Executive Order 9397, November 22, 1943, (Social Security Number); and Title 5, United States Code Section 301). RAPIDS users can only confirm information on the sponsor or family member. As required by the Privacy Act of 1974, the operator cannot volunteer personal information from the DEERS record.



RAPIDS is designed to automate the following functions:

- Update the DEERS database. RAPIDS workstations communicate with the DEERS database, allowing you to update sponsor and family information in the DEERS database quickly and easily.
- Determine eligibility for benefits. RAPIDS can analyze a beneficiary's data to determine the correct benefits and eligibility period based on the DoD Eligibility Tables.
- Create DD Forms 1172, Application for Uniformed Services Identification Card and DEERS Enrollment and DD Form 1172-2, Application for Department of Defense Common Access Card, DEERS Enrollment. You can use RAPIDS to generate and to print the DD Form 1172.
- Produce ID cards.
- Implement the use of smart card and PKI technology to issue the CAC.

With the 10 November 1999, mandate from the Deputy Secretary of Defense to create a DoD CAC, RAPIDS Version 6.0 was developed to include the hardware, software, communications, and security requirements to issue the CAC.

5 DoD Public Key Infrastructure Roles

The main roles in the DoD PKI Infrastructure are:

- Verifying Officer/Local Registration Authority (VO/LRA).
- Director of Information Management (DOIM).
- Information Management Officer (IMO).
- Card Recipient.

5.1 Responsibilities of the VO/LRA

The VO is in a key position of responsibility. The following are the main responsibilities of the VO with regards to the PKI portion of the CAC and processes expected of the RAPIDS user:

- Use the RAPIDS workstation to issue the CAC, and to request certificates and download them to the CA prior to issuing to the card recipient.



- Assist in the management of the recipients' keys and certificates.
- Verify identity of customers.
- Receive and entering subscriber information, and verifying correctness.
- Securely communicate requests to and responses from the CA.
- Execute revocation requests received from LRA/VOs or other authorized sources.
- Approve server certificates.
- Update the CAC as necessary to reflect any change in the personnel category of the CAC recipient. This automatically issues/revokes certificates as needed.
- Update other data stored on the CAC ICC.
- Ensure that users understand their responsibilities with respect to the CAC and the information, including the PKI keys, certificates and PIN stored on it.

The VO will perform the additional responsibilities of LRA which include:

- Verifying the identity of CAC recipients via official documentation.
- Registering the CAC recipients with the CA.
- Requesting certificates for CAC recipients from the CA.
- Printing CACs.
- Saving applications, certificates, and data to chips on CACs.
- Requesting CAC recipients to enter a PIN for their CAC.
- Terminating end user CACs and along with this function, automatically revoking the associated PKI certificates that are no longer valid.

The RAPIDS workstation serves as the RA to approve and issue VO/LRA certificates on the CAC, and revoke certificates as necessary.

5.2 Responsibilities of the DOIM

The DOIM holds a key position within the DoD PKI structure. The DOIM is the highest level in the Information Systems hierarchy within an installation. The main responsibilities of the DOIM are as follows:

- Distribution of Card Readers and Middleware to Units.
- Instructional classes for IMOs/SAs on:



- Installation of Card Readers and Middleware.
- Setup and configuration of the email client.
- Registering of Certificates.
- Use of PKI Certificates for signing and encrypting email.
- Distribution of Training Materials.
- Troubleshooting Card Reader and Middleware problems, secure email problems and determining next level of support.
- Augmented Infrastructure.

5.3 Responsibilities of the IMO

The IMO is the person that will have the most contact with PKI users. The IMO is also the first resource for PKI users for distribution, installation and troubleshooting for specific aspects of the PKI infrastructure. The main responsibilities of the IMO are as follows:

- Installation of Card Readers and Middleware throughout the IMO's organization.
- Installing and Configuring email clients for signing and encrypting email.
- Installation of Certificates for signing and encrypting email.
- Short Instructional Lessons.
- Troubleshooting and determination of next level of support.

5.4 Responsibilities of the Card Recipient

Following are the responsibilities of the CAC cardholder:

- Use certificates and private keys only for official purposes.
- Protect your private key from unauthorized use. Protect it as you would your bankcard.
- Report any loss or compromise of your private key to the RAPIDS issuing facility.
- Comply with any policies established by the RAPIDS issuing facility.



6 Installation Training Scenarios

6.1 System Requirements

6.1.1 Operating Systems

There are three different Operating System (OS) platforms that have been tested with the DoD PKI infrastructure. A computer's Operating System will provide the basis for all hardware and middleware that will be utilized for the DoD PKI implementation. The OS platforms are typical of those that would be in use at any given fielding site.

The OS platforms are:

- Windows 98.
- Windows NT 4.0 with SP6.
- Windows 2000 Professional.

There may be variations in the setup and installation of specific card readers and middleware depending on the OS in use at a particular site.

Windows 2000 & NT Platform Installation:

An installer must be logged in as an **ADMINISTRATOR** in order to successfully install Card Readers and Middleware on Windows 2000 and NT Platforms.

6.1.2 Applications

Specific applications need to be installed and configured on a workstation to support the interoperability of all aspects of the PKI infrastructure. These will include applications for email services and web browsing.

Email Services:

- Microsoft Outlook 98 2nd Edition or Outlook 2000

Web Browsers:

- Microsoft Internet Explorer 5.0 with 128-bit encryption.
- Netscape Communicator 4.77 with 128-bit encryption.



If the Web Browser installed on your machine does not have 128-bit encryption, download the latest version from the websites listed below:

- For Internet Explorer: www.microsoft.com/downloads
- For Netscape Communicator: www.netscape.com

6.2 Installing ActivCard Gold 2.0.1 Middleware

Before starting the Installation process, close all running Windows Applications.

Insert the ActivCard Gold for CAC Version 2.0.1 CD in the CD-ROM drive.

The InstallShield Wizard should launch automatically.

If not, browse the CD using *My Computer*. Navigate to the **ActivCard Gold 2.0.1** folder.

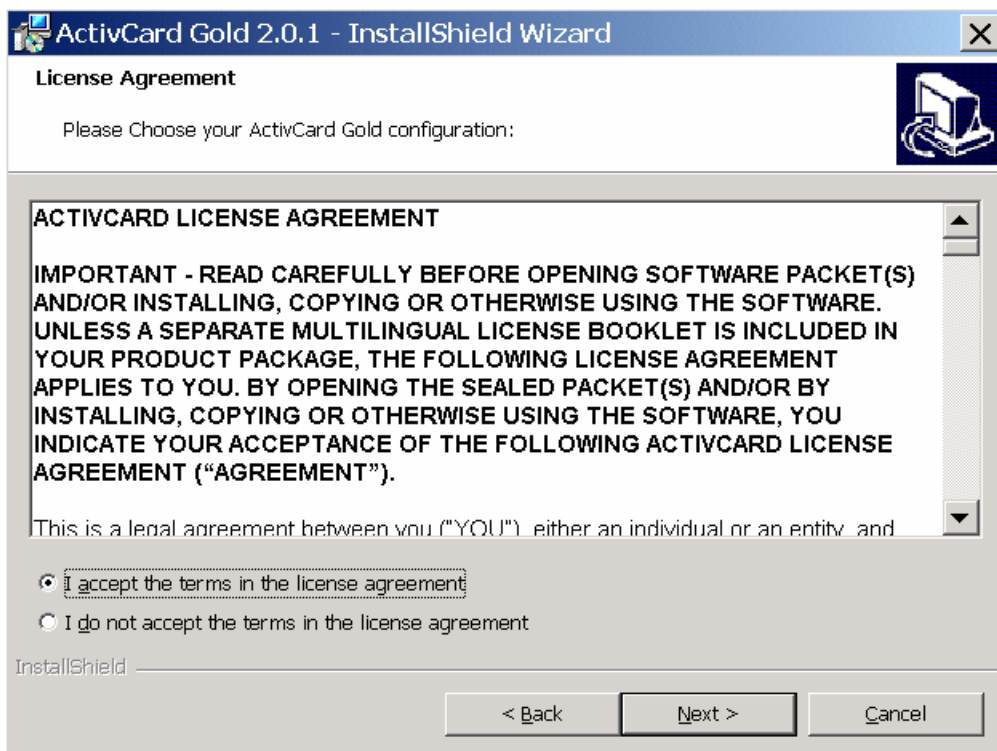
Double-click the *run.exe* icon to begin the installation.



1. Click "***Install Product***" to begin the ActivCard Gold 2.0.1 Installation.



2. When the InstallShield Wizard appears, click the “*Next*” button.



3. Select the “*I accept the terms in the license agreement*” radio button then click “*Next*” to continue.



ActivCard Gold 2.0.1 - InstallShield Wizard

Customer Information

Please enter your information.

User Name:
NBAKER

Organization:
PMSETD

InstallShield

< Back Next > Cancel

4. Enter your name in *User Name* field. Enter Organization name in the *Organization* field. Click “*Next*” to continue.

ActivCard Gold 2.0.1 - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

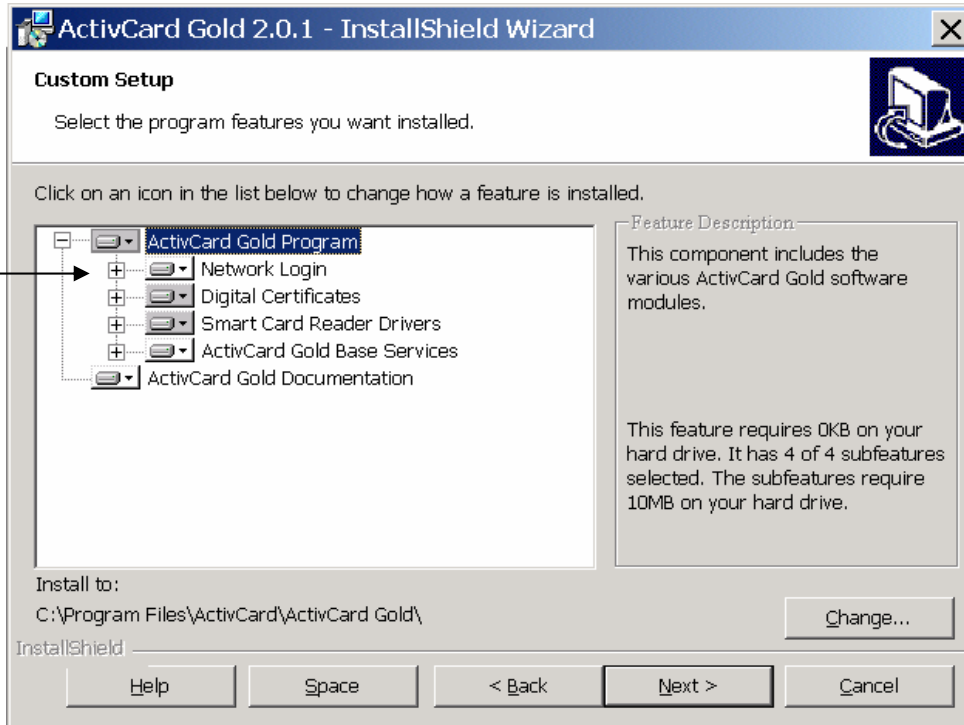
Typical
All program features that can be installed will be. (Requires the most disk space.)

Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.

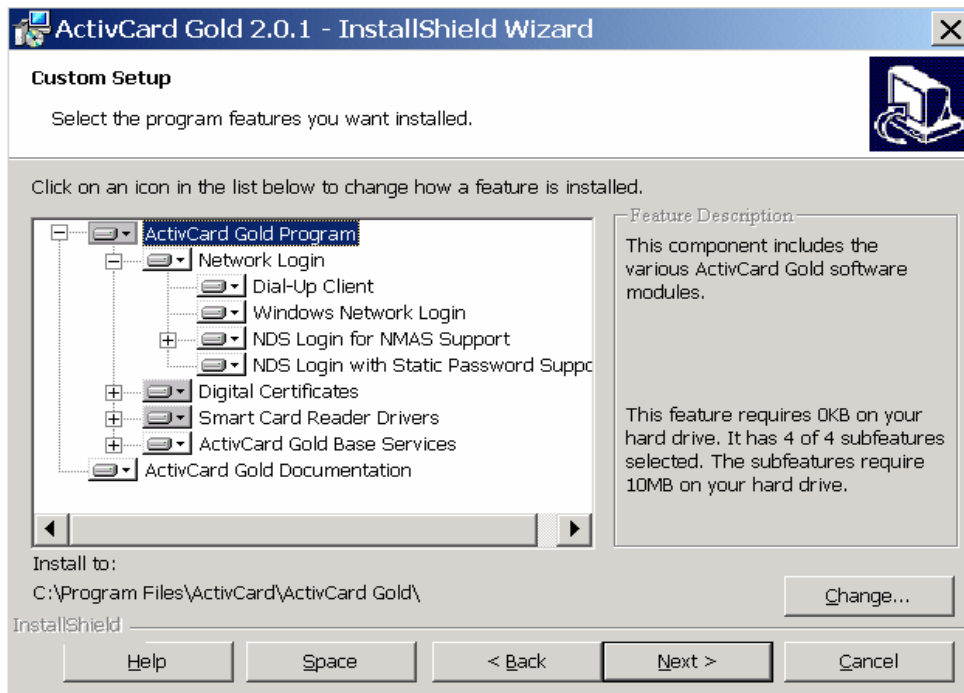
InstallShield

< Back Next > Cancel

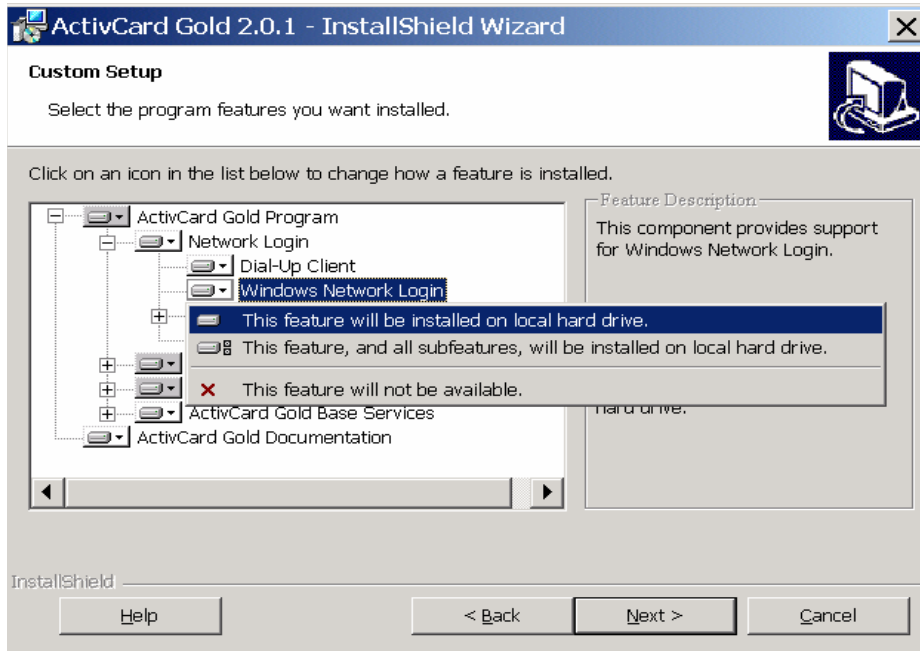
5. Select the “*Custom*” radio button for the Setup type and then click “*Next*”.



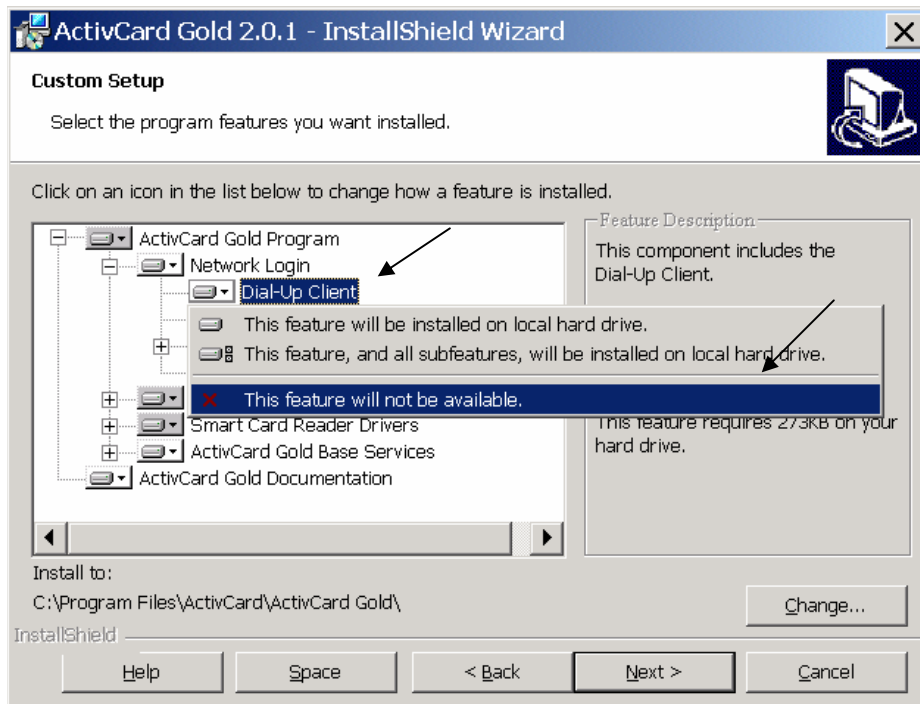
6. The *Custom Setup* screen should look like the one shown above. Click on the “+” icon next to Network Login to expand the menu.



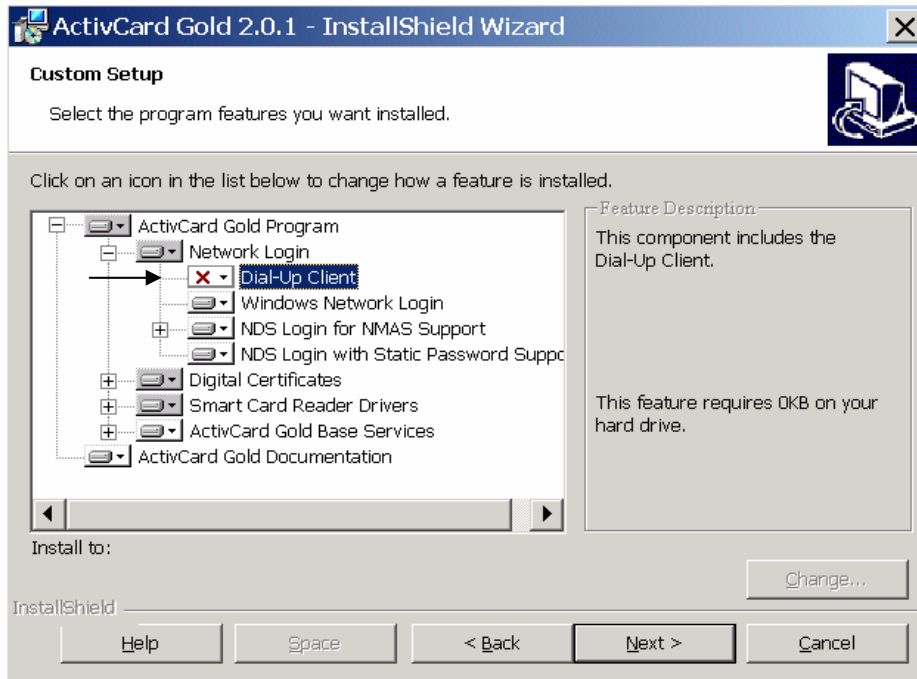
7. Once the menu is expanded the screen should look like the one shown above.



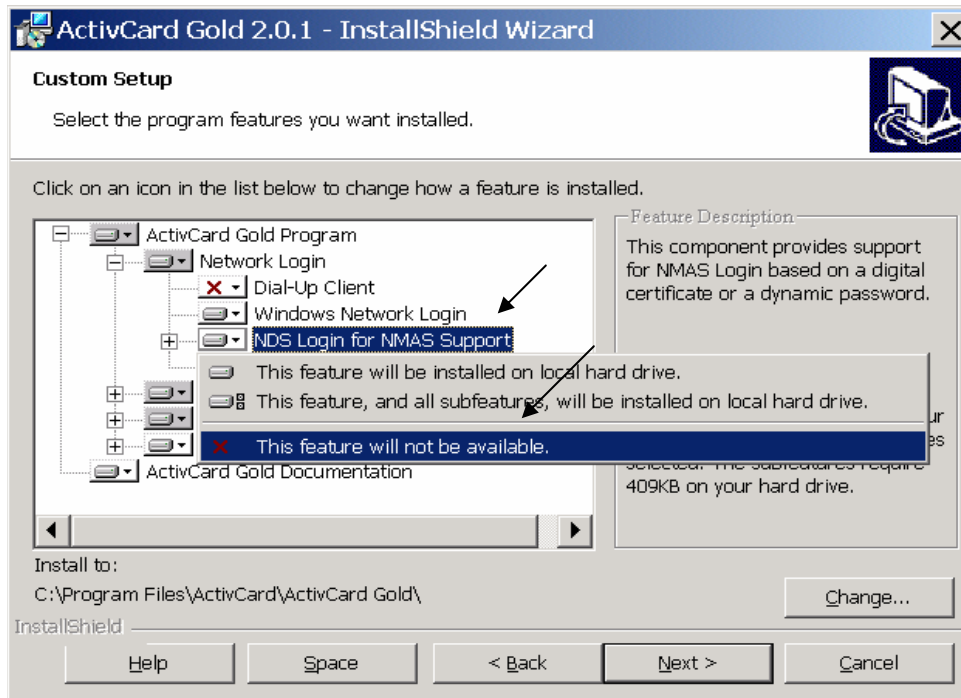
8. Click on the “*Windows Network Login*” icon. Clicking on this icon will open a menu. Choose “*This feature will be installed on local hard drive.*”



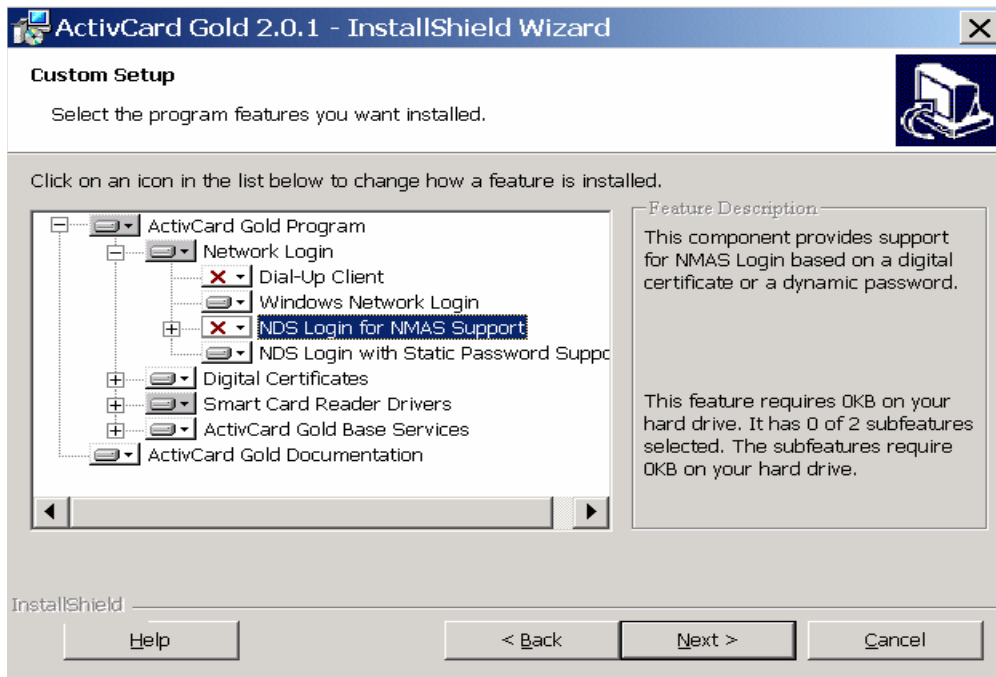
9. Click on the *Dial-Up Client* icon. Choose “*This feature will not be available*” from this menu.



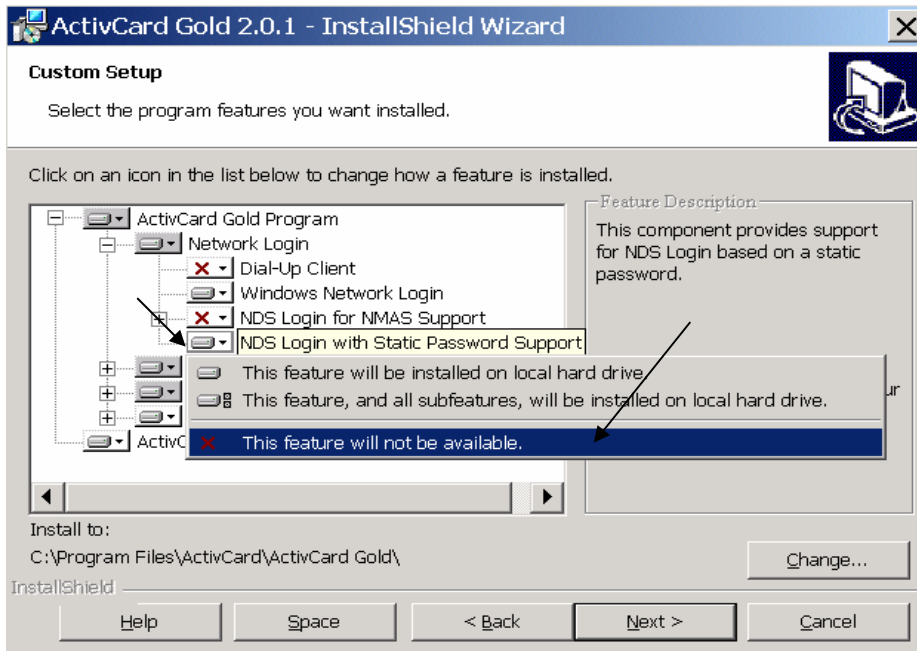
10. A red “X” will appear next to the *Dial-Up Client* icon.



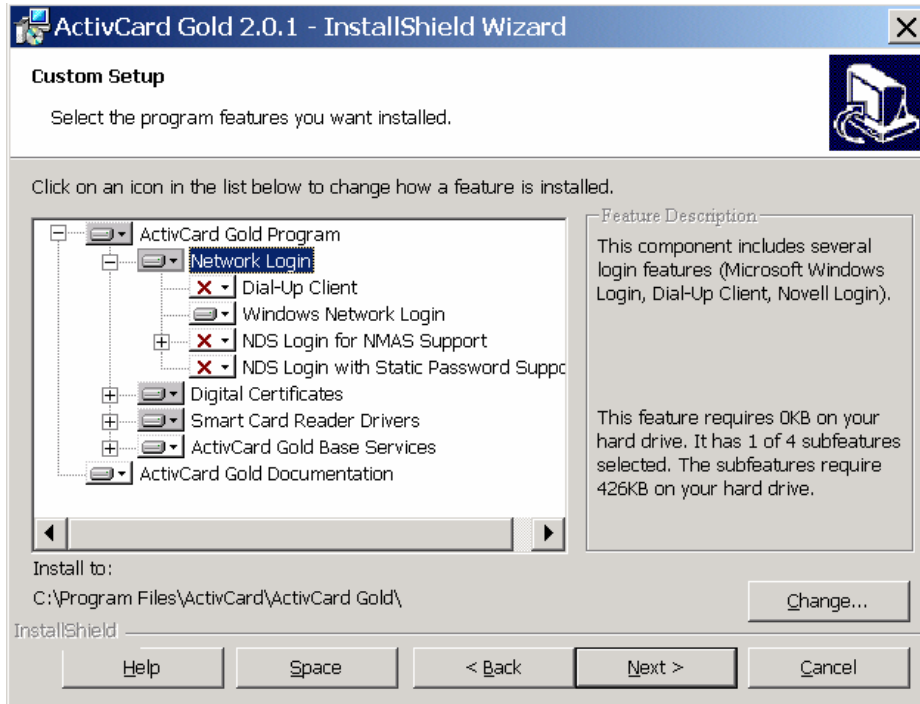
11. Click on *NDS Login for NMAS Support* icon and choose “*This feature will not be available*” from the menu.



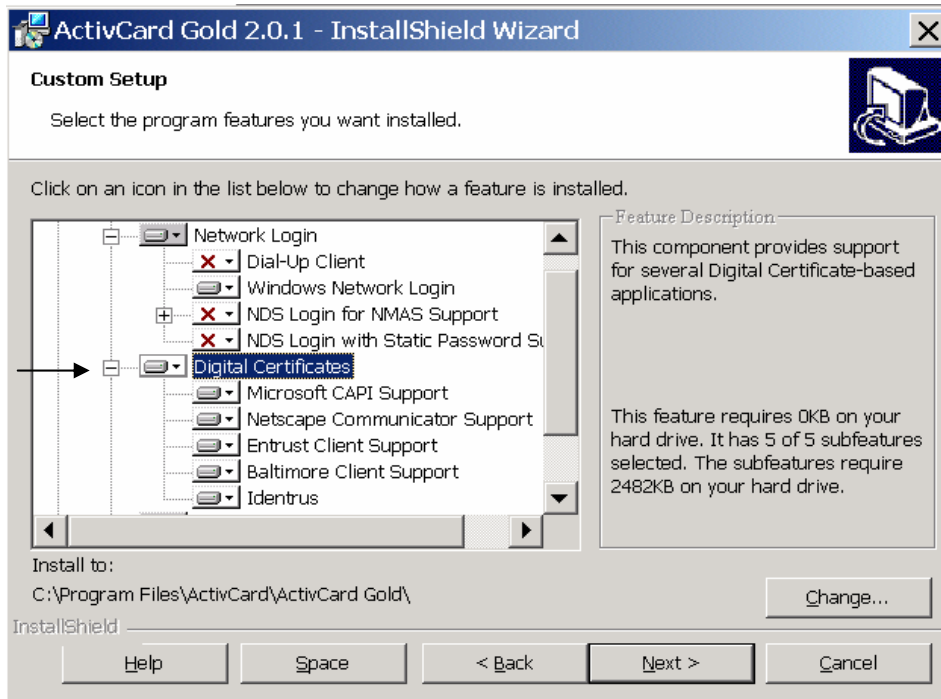
12. A red “X” will appear next to “*NDS Login for NMAS Support*” icon.



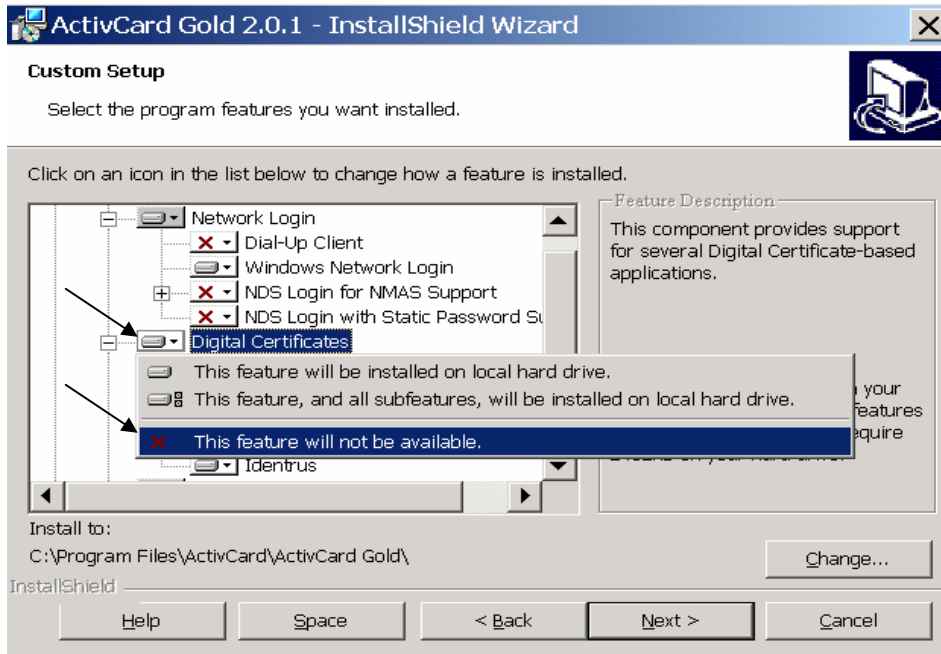
13. Click on *NDS Login with Static Password Support* icon and choose “*This feature will not be available*” from the menu.



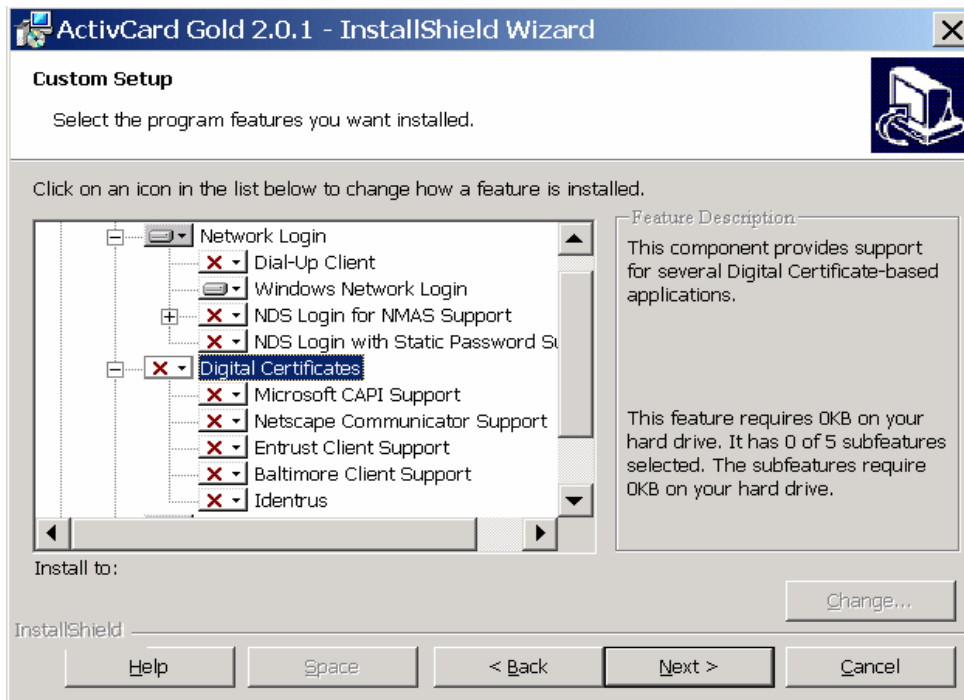
14. A red “X” will appear next to *NDS Login with Static Password Support* icon.



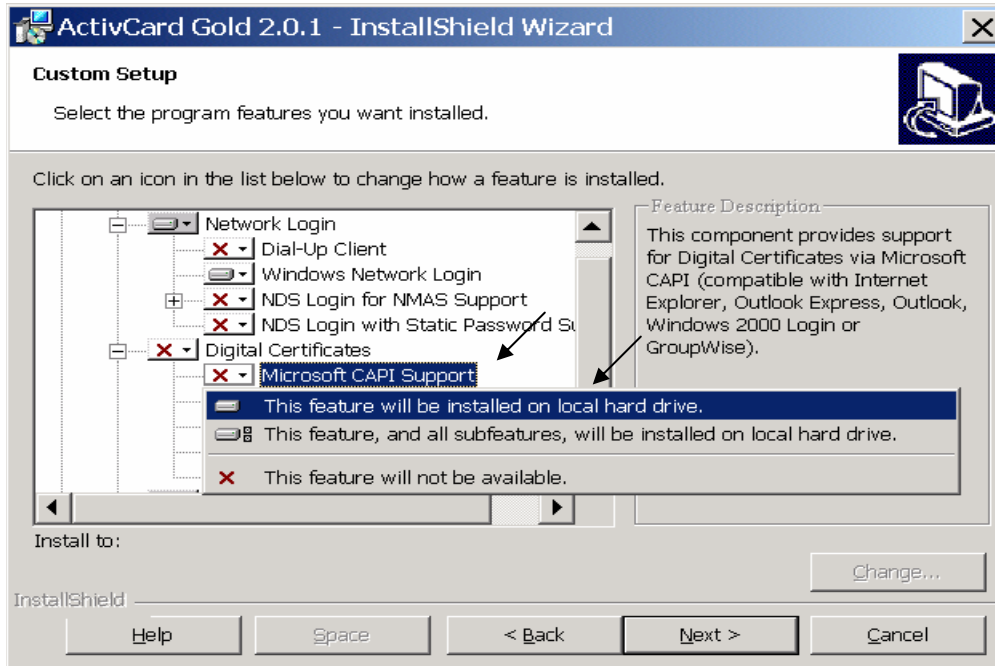
15. Click on the “+” sign next to *Digital Certificates* to expand this menu.



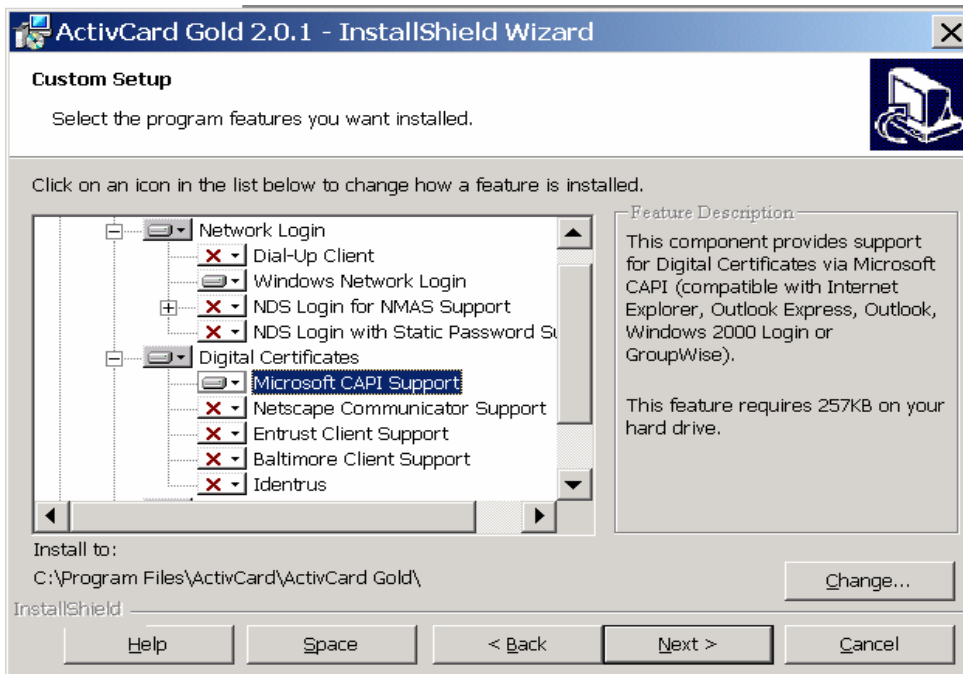
16. Click on the *Digital Certificates* icon and choose “*This feature will not be available*” from the menu.



17. Red X’s should appear in front of all of the options in the *Digital Certificates* menu.



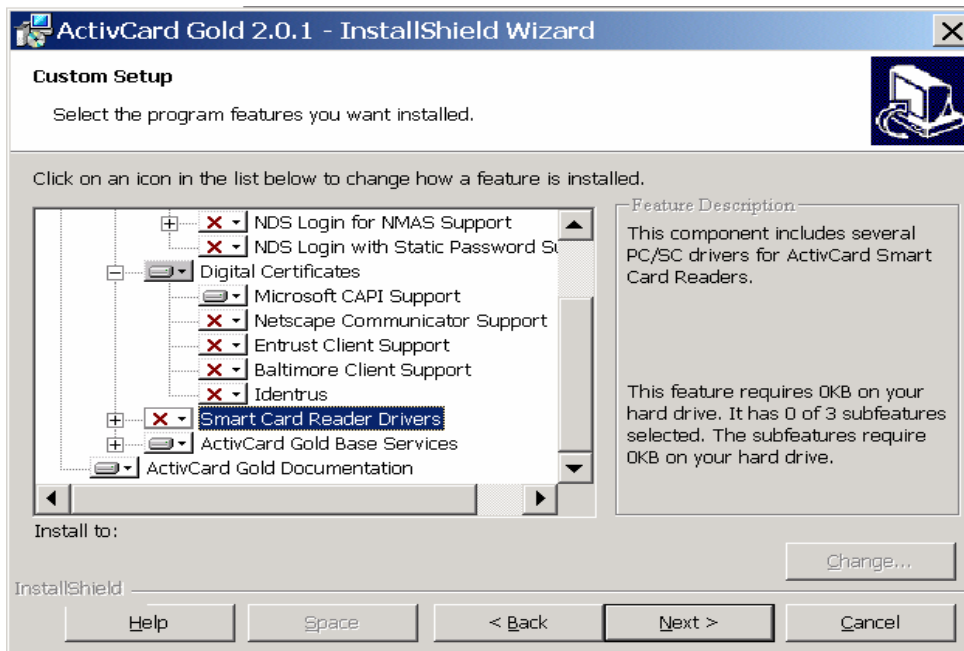
18. Click the *Microsoft CAPI Support* icon and choose “*This feature will be installed on local hard drive*”.



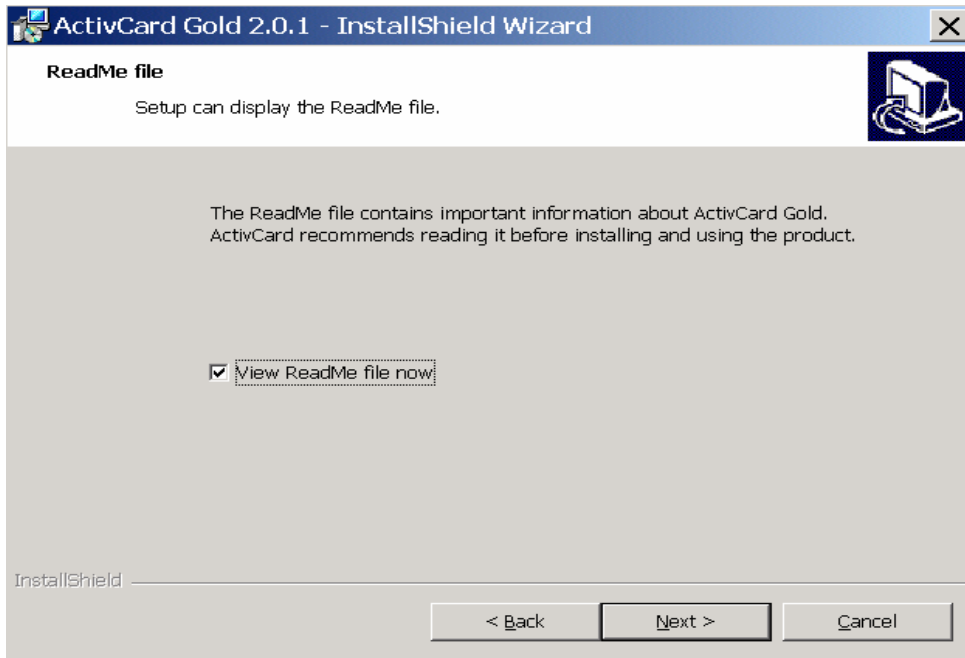
19. The screen should now look like the one shown above.



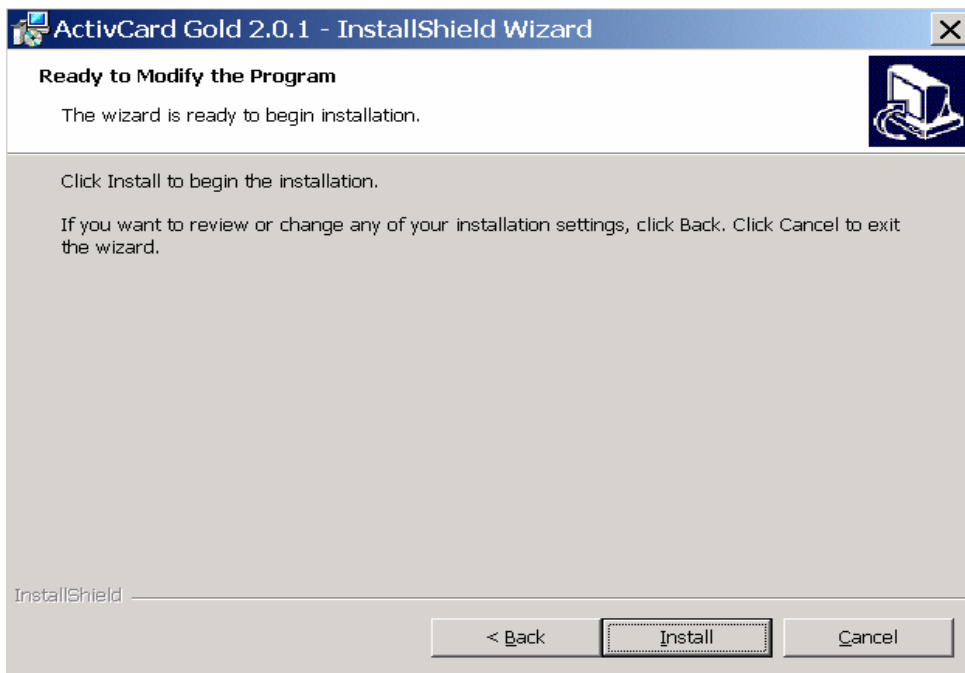
20. Scroll down and click on the *Smart Card Reader Drivers* icon and choose “*This feature will not be available*” from the menu.



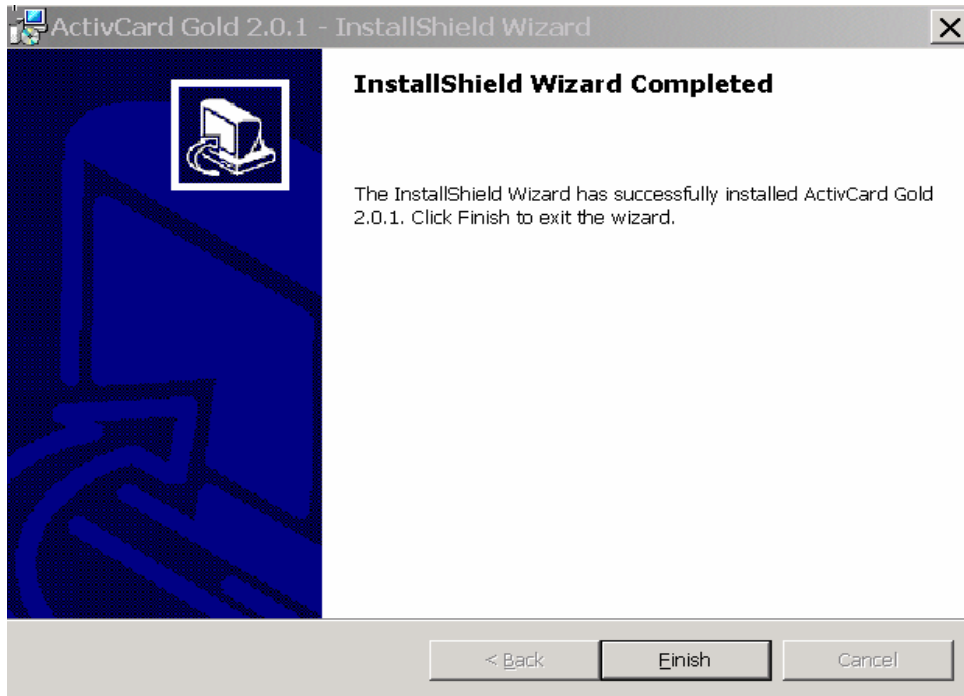
21. A red “X” will appear in front of the *Smart Card Reader Drivers* icon. Click “*Next*” to continue with the Installation.



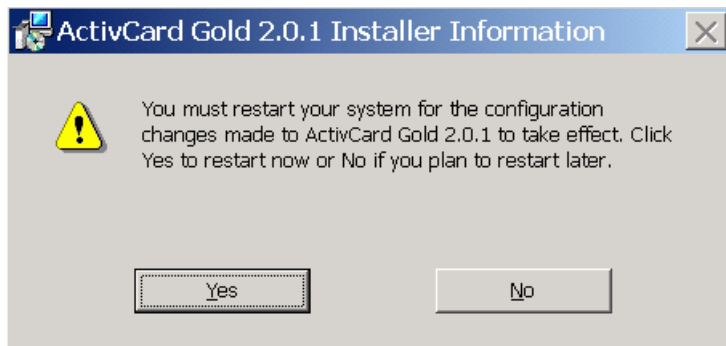
22. Leave the box checked next to “***View ReadMe file now***” if you would like to view the ReadMe file. If you do not want to view this file, uncheck the box. Click “***Next***” to continue.



23. Click “***Install***” to begin the installation.



24. Click “*Finish*” to close the InstallShield Wizard.



25. If you will be installing a Card Reader next, click “No” and manually Shut Down your computer using the *Start* menu, *Shut Down* option. If you will not be installing a Card Reader, click “*Yes*” to restart your system now. After the computer is restarted the installation is complete.



A Smart Card Reader icon will now be visible in the System Tray.



6.3 Installing Card Reader and Drivers

Several different card readers have been tested with the DoD PKI infrastructure. The card readers read the ICC located on the CAC. The ICC stores a significant amount of data and is accessed through the use of a middleware application. Card readers can be attached to the Personal Computer in 3 different ways: Serial connection, USB (Universal Serial Bus) connection and PCMCIA (Personal Computer Memory Card International Association) connection.

Installation will cover 6 different card readers:

- SCM SCR111 Serial SmartCard Reader.
- ActivCard Serial SmartCard Reader.
- Schlumberger Reflex 72 Serial SmartCard Reader.
- Schlumberger Reflex USB SmartCard Reader.
- Schlumberger Reflex PCMCIA SmartCard Reader.

6.3.1 SCM SCR111 Serial SmartCard Reader



Attach the SCM SCR Card Reader to the back of the PC by plugging the serial plug into the serial port. To connect the reader to the PC:

1. Ensure that the PC is turned off.
2. Connect Connector 1 to an available COM port on your PC or laptop.
3. Connect Connector 2 to either the Keyboard or the Mouse PS/2 port.



4. Connect the Keyboard or Mouse to Connector 3 (if necessary).

NOTE: If you are using a laptop, Connector 3 may be left un-connected. However, both Connectors 1 and 2 MUST be used at all times.

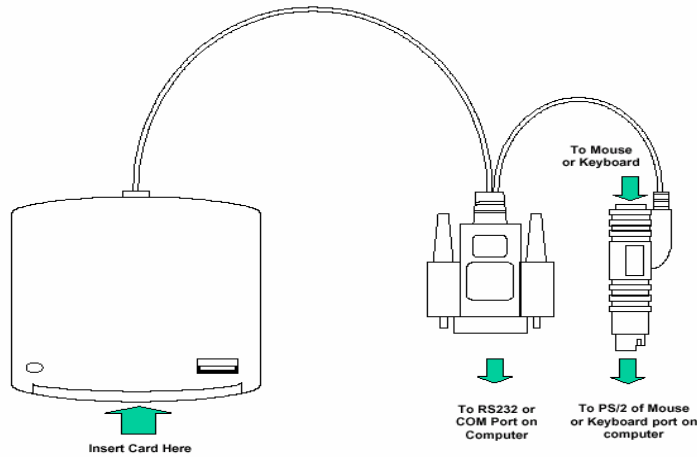
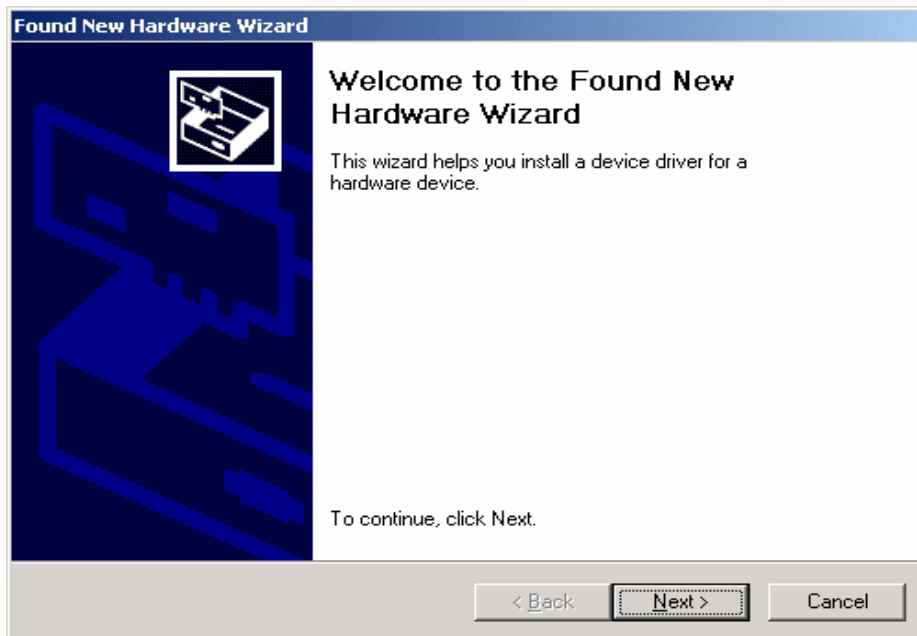


Figure 3: Installation of Serial Card Reader to PC

5. After the card reader is connected, turn your PC on.

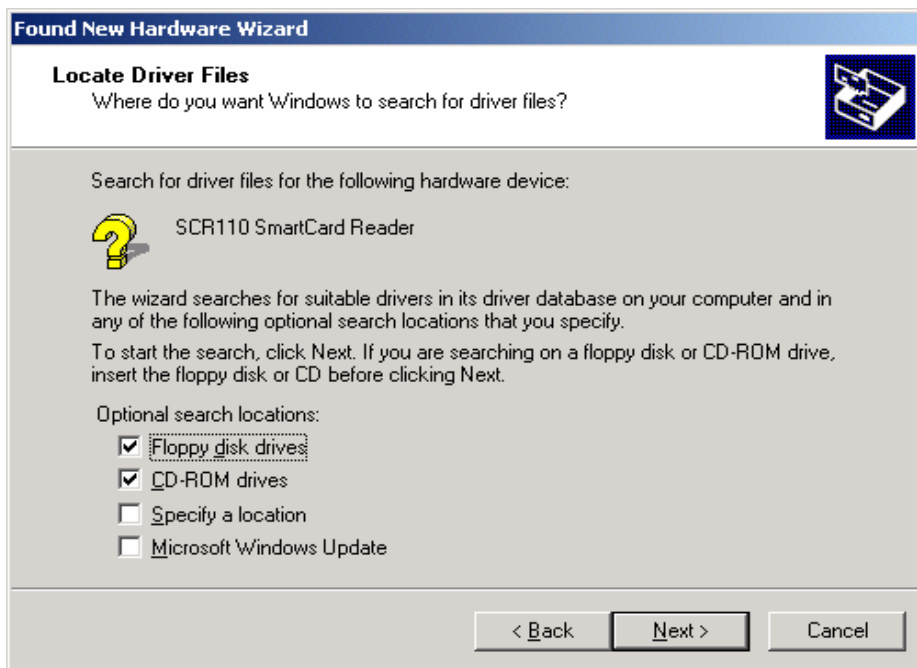
6.3.1.1 Installation on Windows 2000



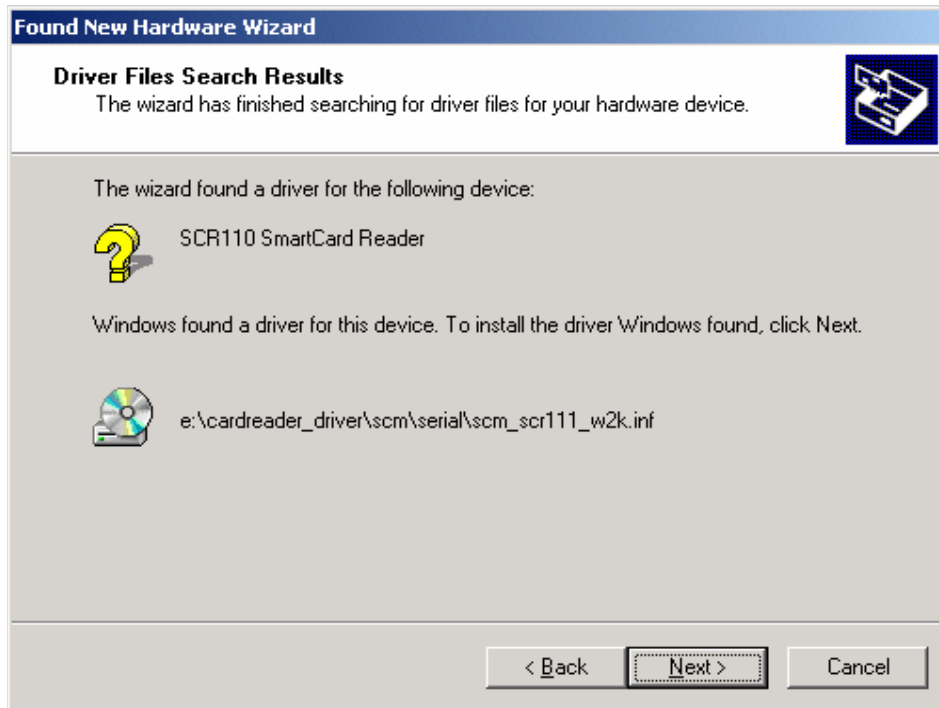
1. The “*Found New Hardware*” Wizard should appear when the PC is turned on. Click “*Next*” to start the installation.



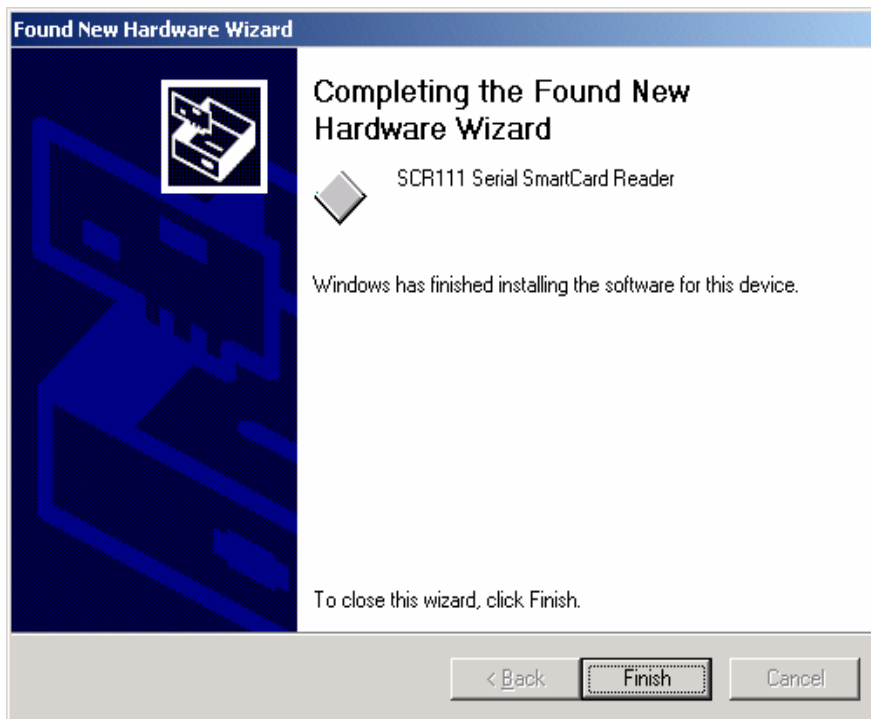
2. Select the radio button next to “*Search for a suitable driver for my device*”. Click “*Next*” to continue.



3. Check the box next to “*CD-ROM drives*” to select this option. Click “*Next*” to continue.



4. The Wizard will find the driver on the CD-ROM. Click “*Next*” to continue.



5. Click “Finish” to complete the Card Reader installation.

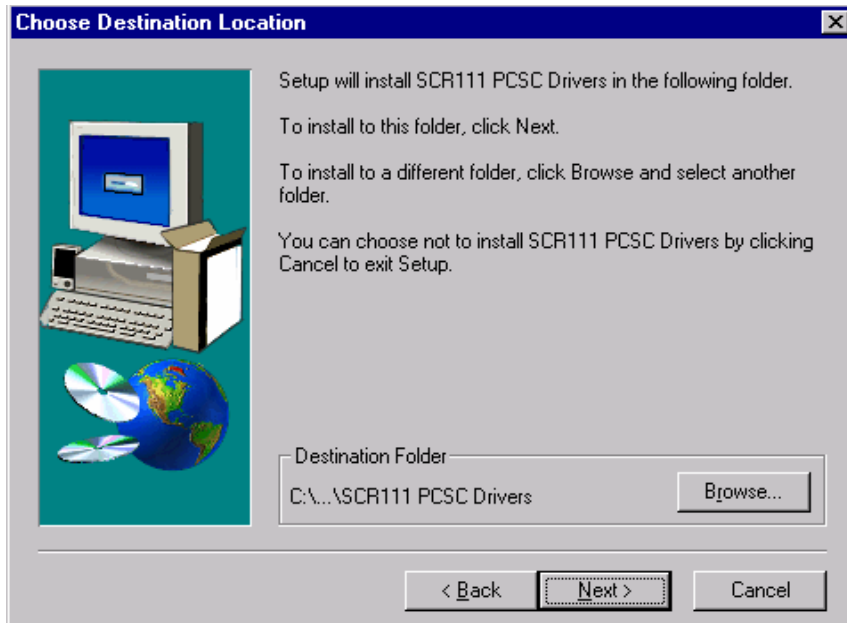


6.3.1.2 Installation on Windows NT Platform

1. Place the CD in the CD-ROM drive. Browse the CD using *My Computer*. Navigate through the following folders: Card Reader Drivers folder, SCM folder, Serial folder. Double-click the *setup.exe* icon in the Serial folder. The Installation Wizard will launch to begin the card reader installation.



2. When the Welcome screen appears, select “*Next*”.



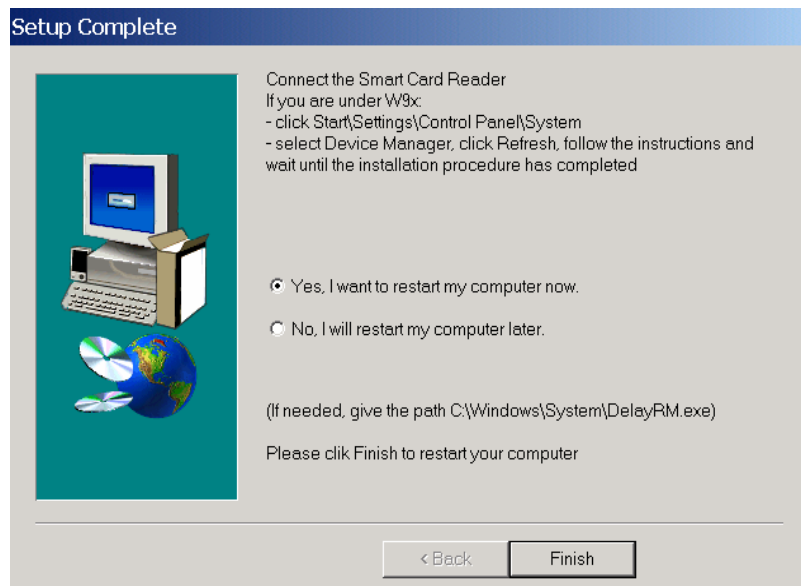
3. Accept the default file folder, click *“Next”*.



4. Accept the default Program folder, click *“Next”*.



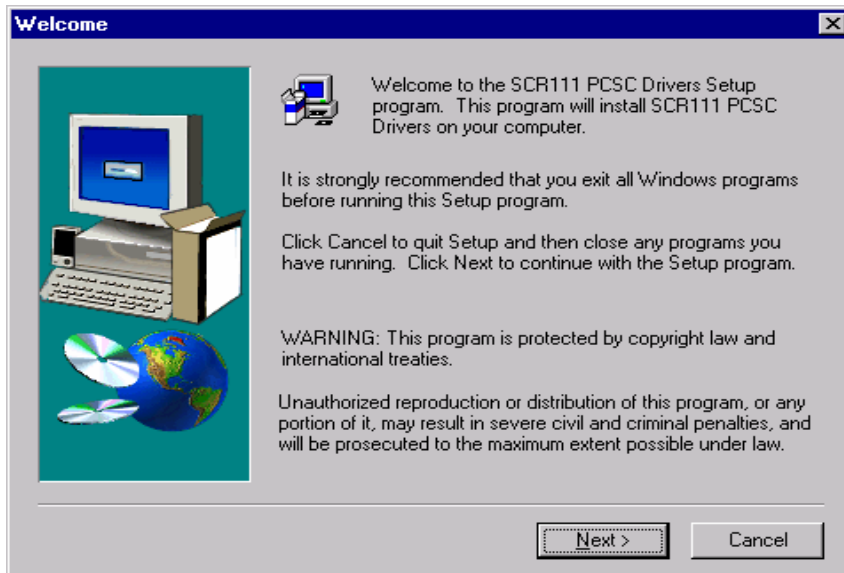
5. This message is valid for SCM SCR 111 Card Readers being installed on Windows 98 machines. Click “**OK**” to continue with Installation.



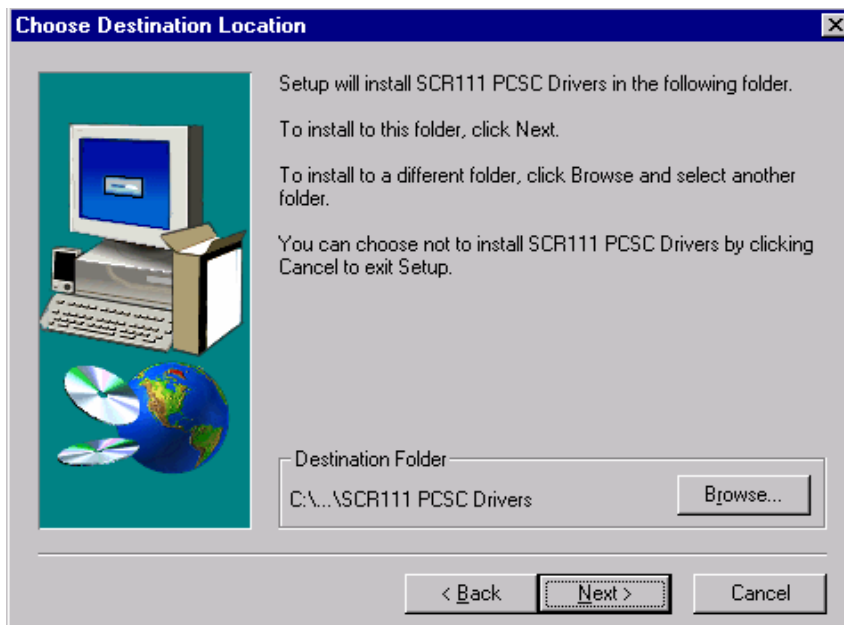
6. If you are installing this card reader on Windows 2000 or NT, Click the “**Yes, I want to restart my computer now.**” radio button then click “**Finish**” to complete the installation.

6.3.1.3 Installation on Windows 98 Platform

1. Place the CD in the CD-ROM drive. Browse the CD using *My Computer*. Navigate through the following folders: Card Reader Drivers folder, SCM folder, Serial folder. Double-click the *setup.exe* icon in the Serial folder. The Installation Wizard will launch to begin the card reader installation.



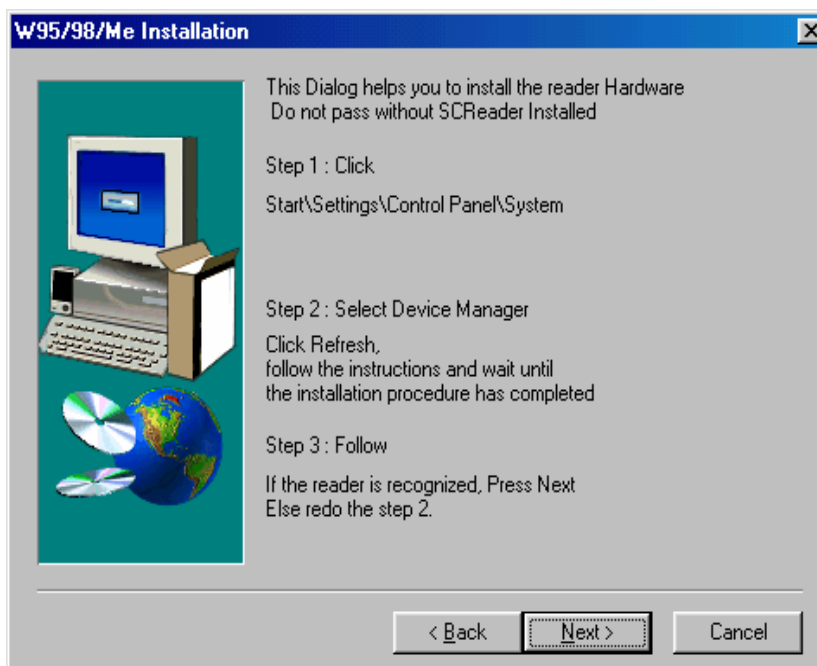
2. When the Welcome screen appears, select “*Next*”.



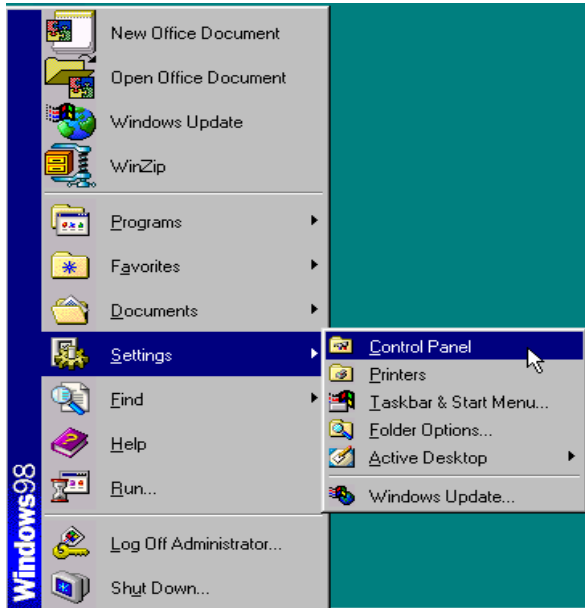
3. Accept the default file folder, click “*Next*”.



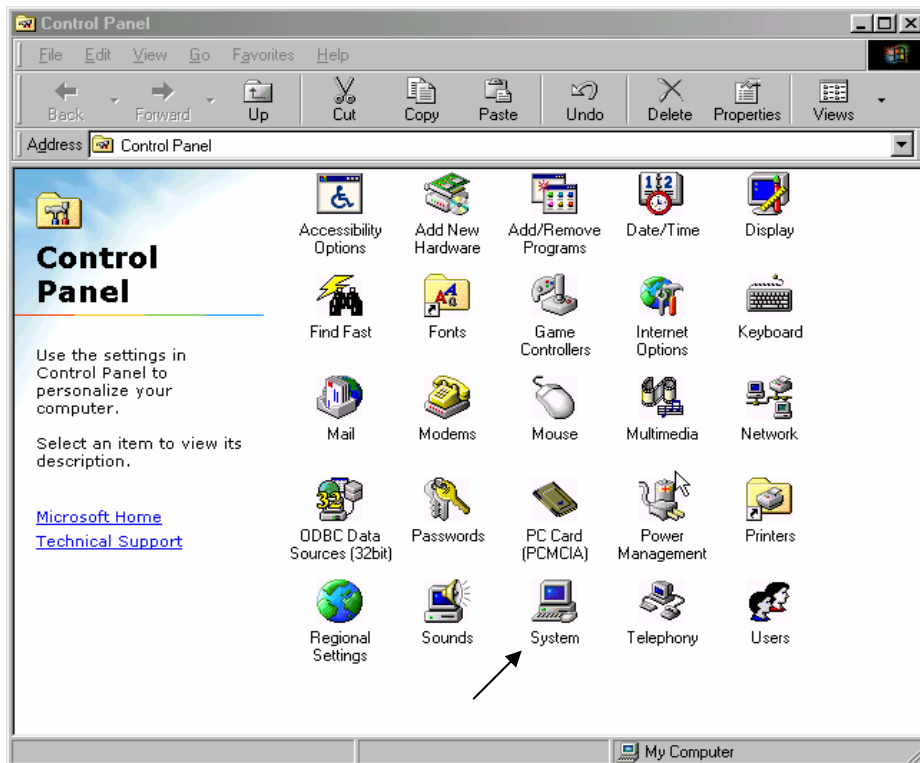
4. Accept the default Program folder, click “*Next*”.



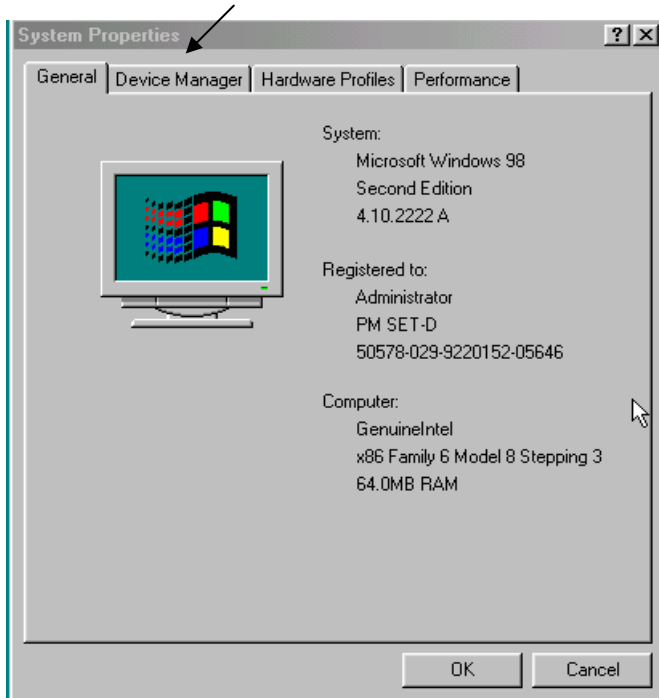
5. Do not click “*Next*” until you complete the steps listed on the screen.



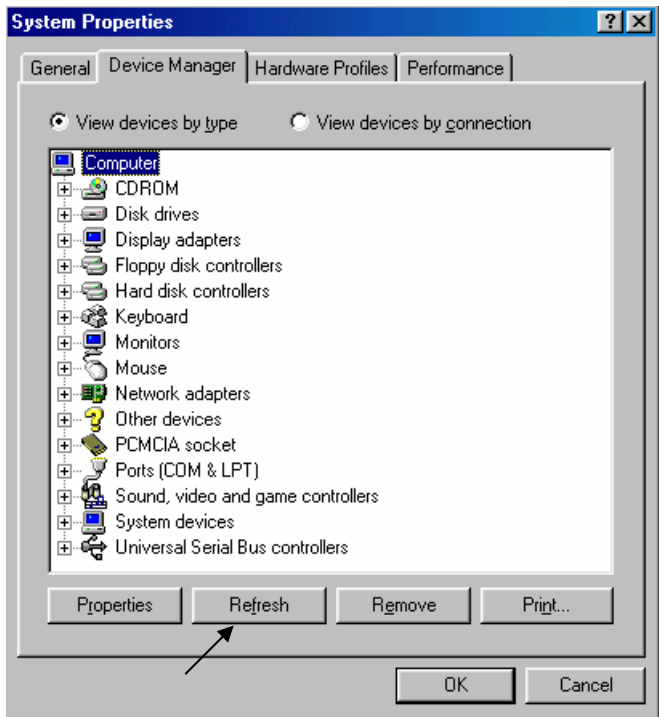
6. Click *Start, Settings, Control Panel*. The Control Panel will open.



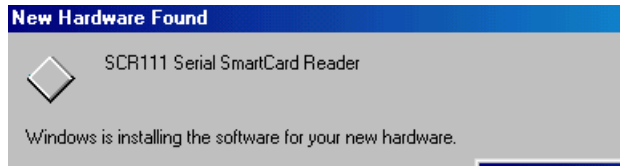
7. Double click the *System* icon.



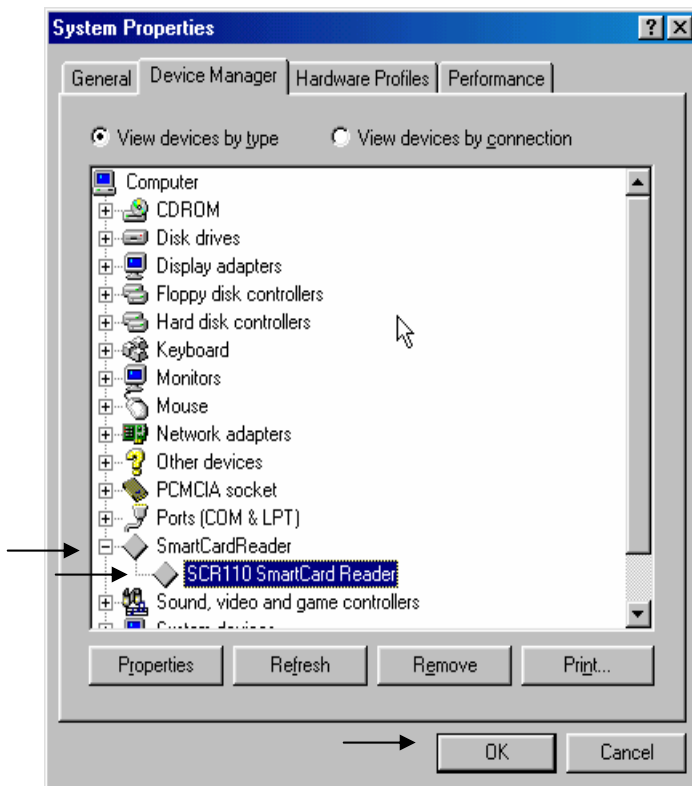
8. The *System Properties* window will open. Click the *Device Manager* tab.



9. Click the “*Refresh*” button at the bottom of the *Device Manager* tab window.

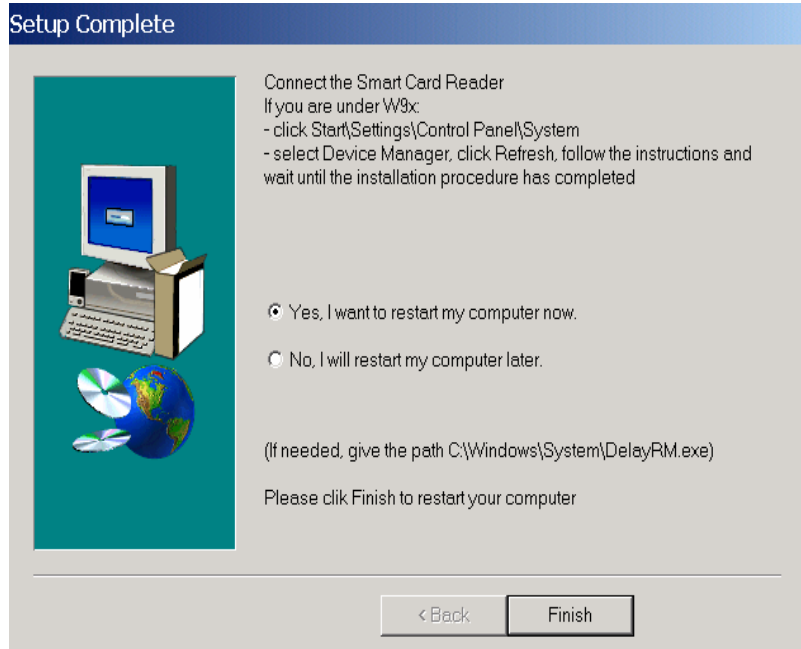


10. The New Hardware Found screen will appear and Windows 98 will automatically install the driver software.



11. Once the driver software is completely installed, you will see the above screen.

The **SmartCardReader** Heading will now appear in the **Device Manager** tab window. Click the “+” sign to expand this menu. The SCM SCR 111 Card Reader will appear in this menu. Click “**OK**” to close the window. Return to the SCM SCR installation screen. This screen will be minimized in your task bar.



12. Click the “*Yes, I want to restart my computer now.*” radio button then Click “*Finish*” to complete the installation.

6.3.2 ActivCard Serial SmartCard Reader



The ActivCard SmartCard Reader must be attached to the PC before installation begins.



The ActivCard Serial SmartCard Reader has 3 connectors:

1. Ensure that the PC is turned off.
2. Connect Connector 1 to an available COM port on your PC or laptop.
3. Connect Connector 2 to either the Keyboard or the Mouse PS/2 port.
4. Connect the Keyboard or Mouse to Connector 3 (if necessary).

NOTE: IF you are using a laptop, Connector 3 may be left un-connected. However, both Connectors 1 and 2 MUST be used at all times.

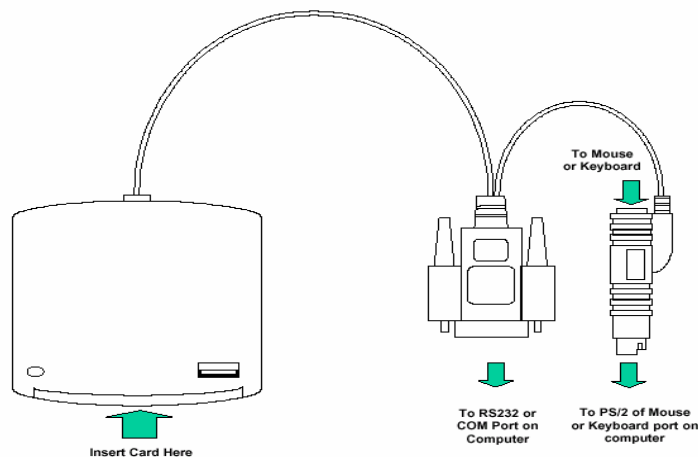


Figure 3: Installation of Serial Card Reader to PC

5. After the card reader is connected, turn your PC on.

6.3.2.1 Installation on Windows 2000 & NT Platforms

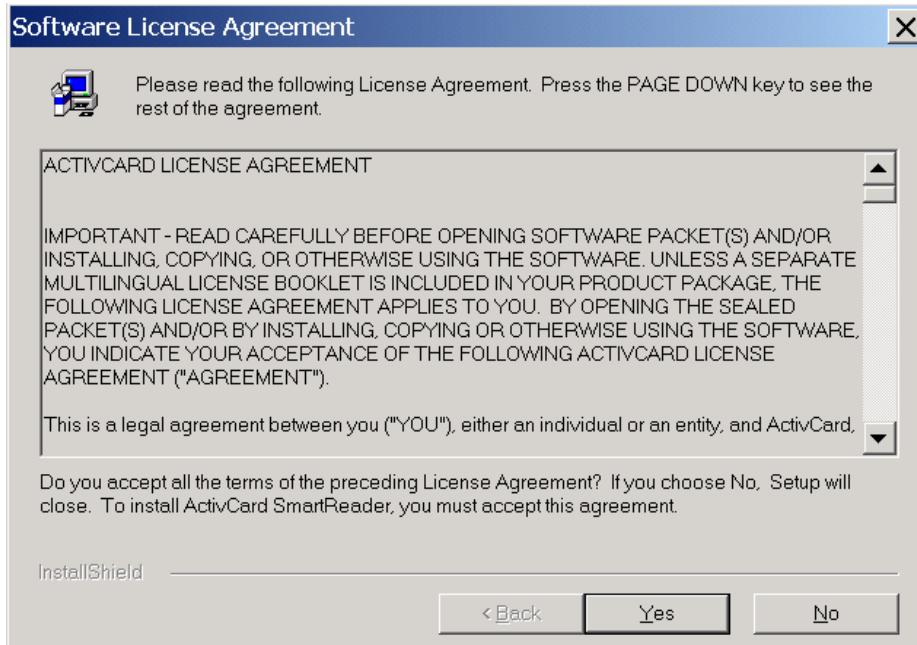
In some instances, on Windows 2000 Platforms, the ActivCard Card Reader will automatically install when the PC is turned on. No installation message will appear. In other instances the “Found New Hardware” wizard will install the card reader. Please use Device Manager to check the installation of the card reader BEFORE following the instructions below.



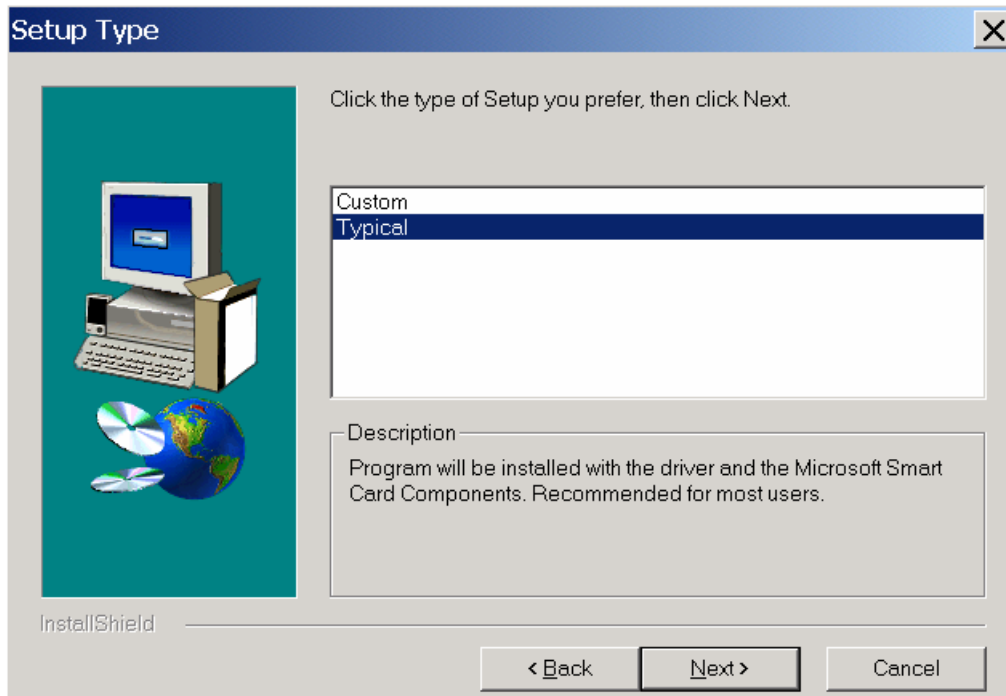
1. Place the CD in the CD-ROM drive. Browse the CD using *My Computer*. Navigate through the following folders: Card Reader Drivers folder, ActivCard folder, Serial folder. Double-click the *SmartReader NT&2000.exe* icon in the Serial folder. The Installation Wizard will launch to begin the card reader installation.



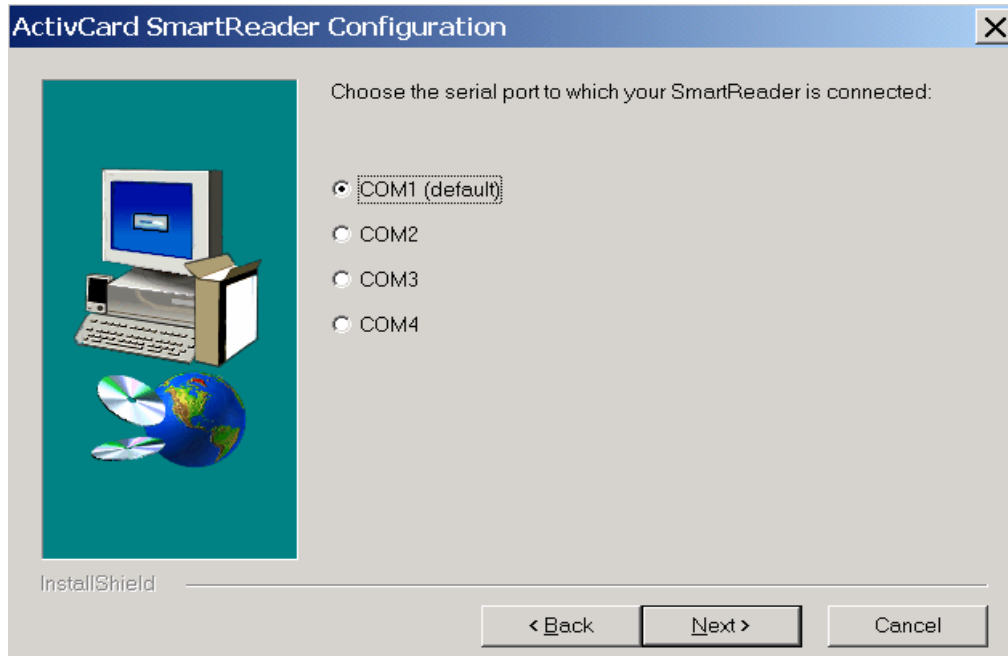
2. When the Welcome screen appears, click “*Next*”.



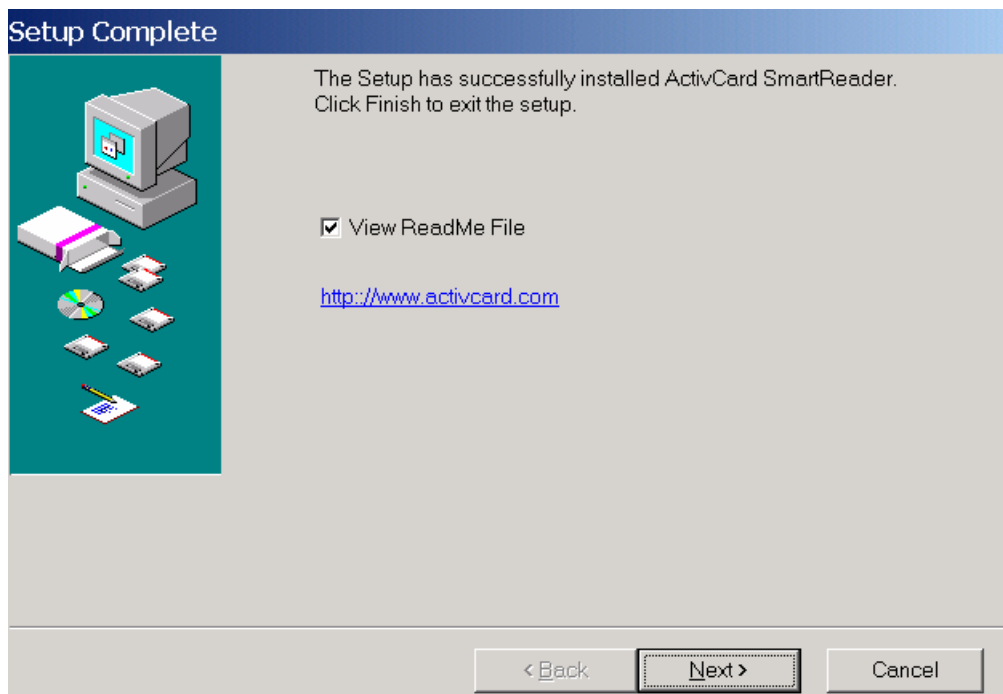
3. Click “*Yes*” to accept the Software License Agreement.



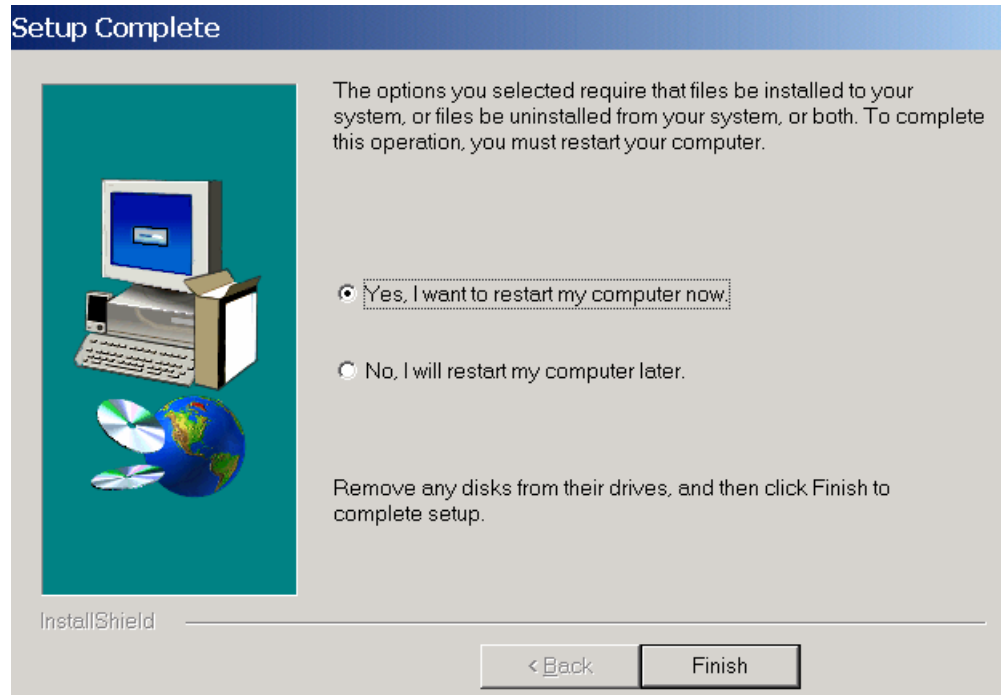
4. Select “*Typical*” for the setup type and then click “*Next*”.



5. Select “*COM1 (default)*” to choose the correct serial port and click “*Next*”.



6. If you would like to view the ReadMe file, leave the “*View ReadMe File*” box checked. If you do not want to view the file, uncheck this box. Click “*Next*” to complete the installation.



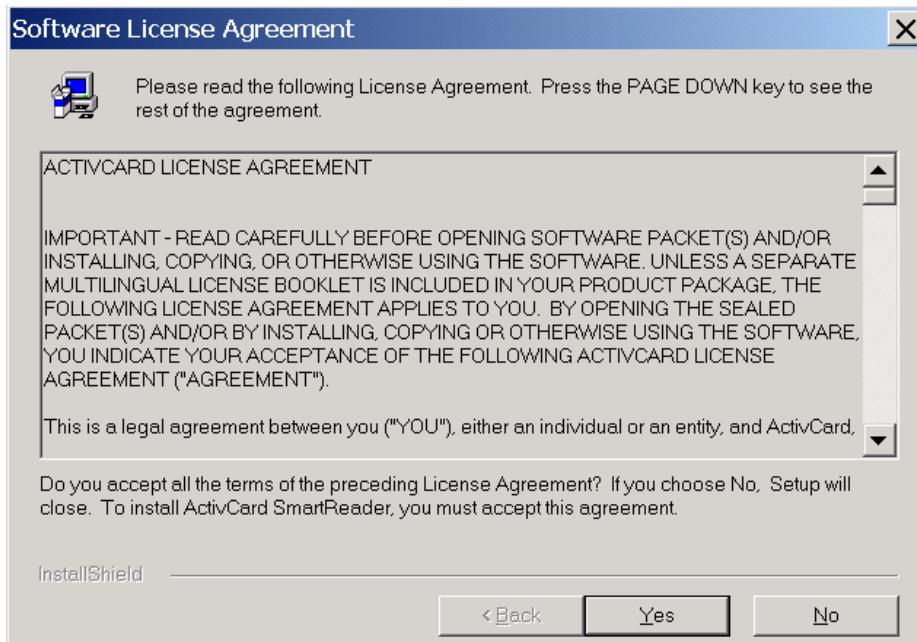
7. Click “*Yes, I want to restart my computer now.*” to complete the Setup.

6.3.2.2 Installation on Windows 98 Platform

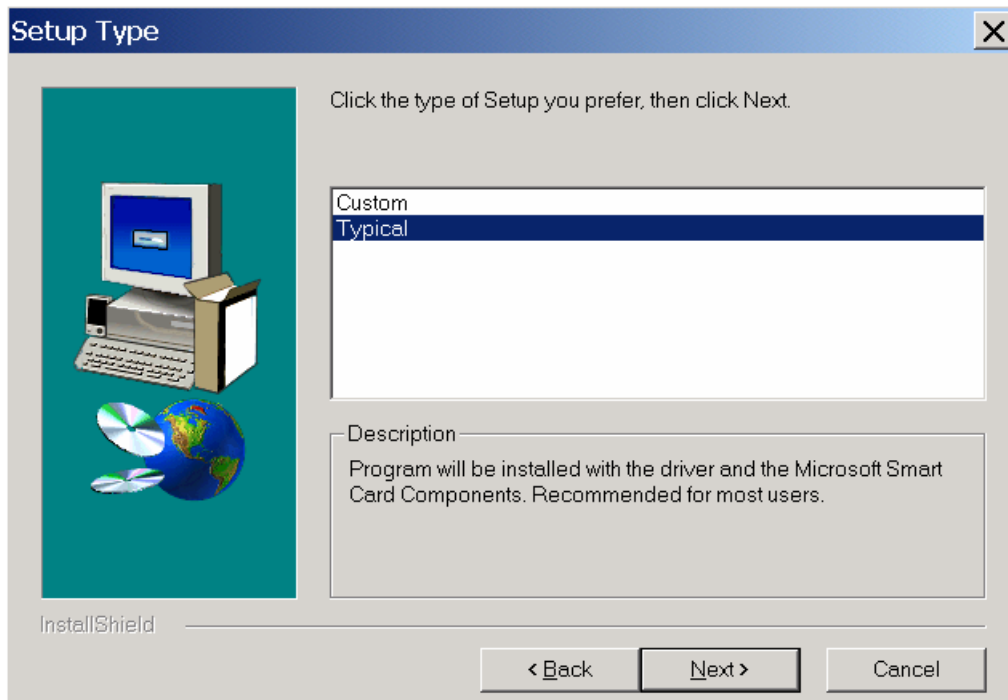
1. Place the CD in the CD-ROM drive. Browse the CD using *My Computer*. Navigate through the following folders: Card Reader Drivers folder, ActivCard folder, Serial folder. Double-click the *SmartReader 98&95.exe* icon in the Serial folder. The Installation Wizard will launch to begin the card reader installation



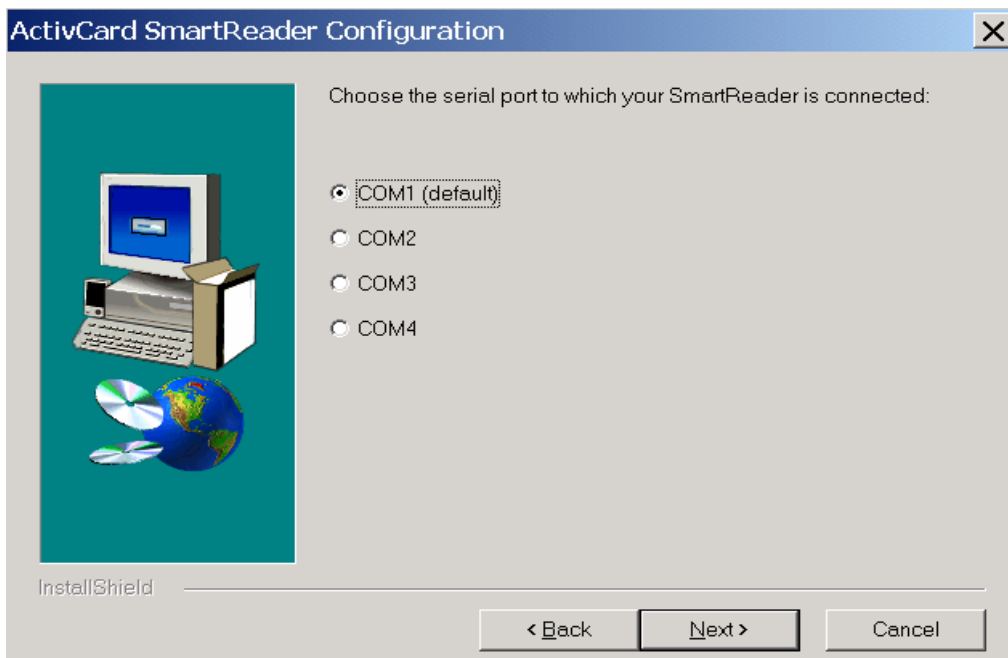
2. When the Welcome screen appears, click “*Next*”.



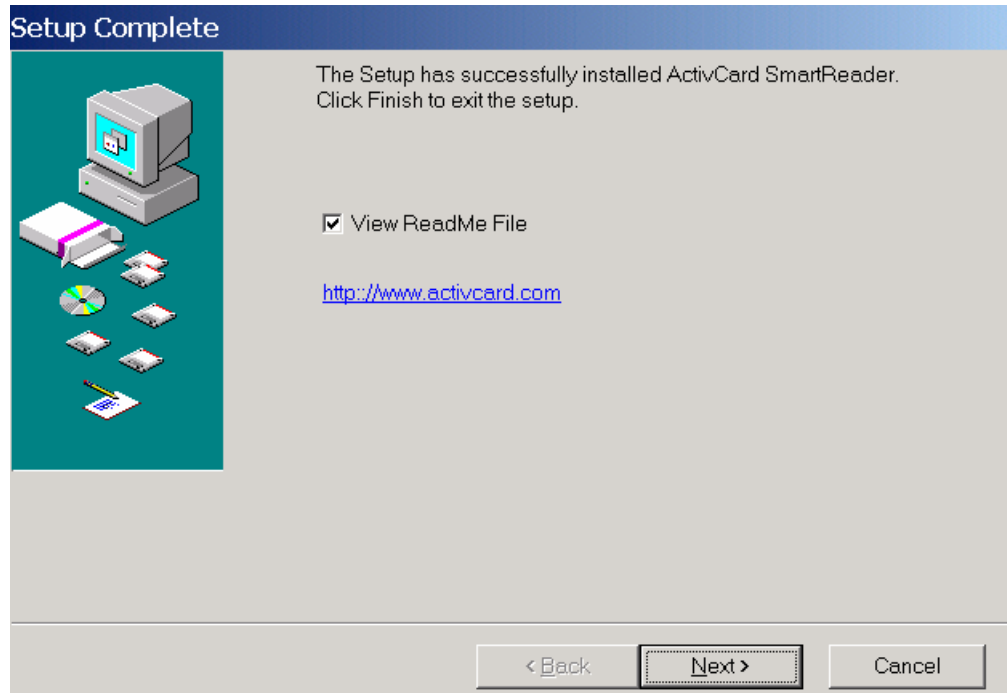
3. Click “*Yes*” to accept the Software License Agreement.



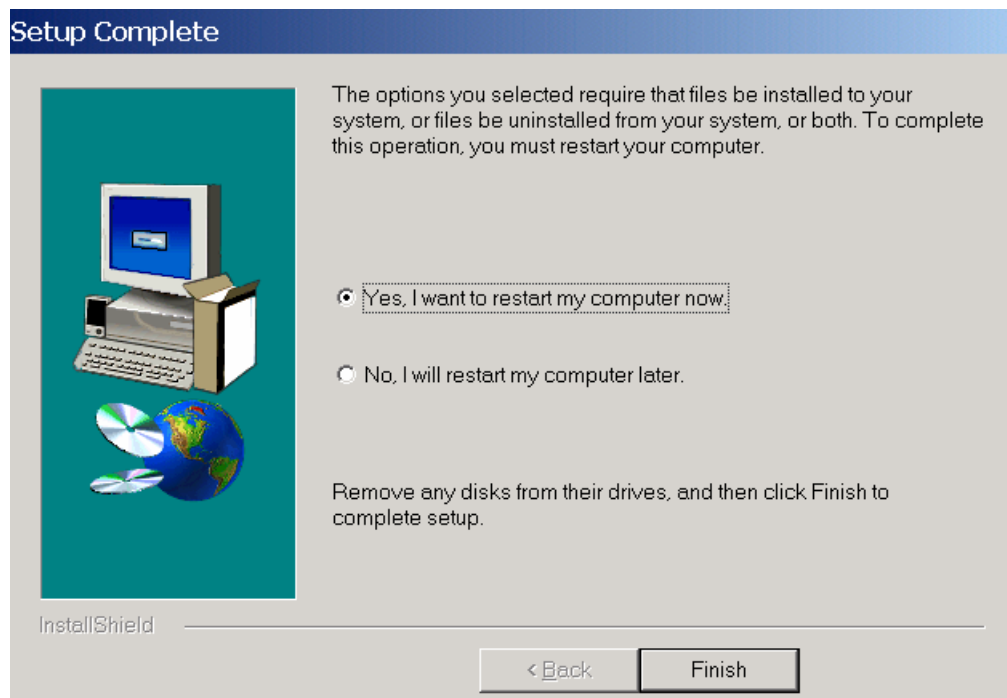
4. Select “*Typical*” for the setup type and then click “*Next*”.



5. Select “*COM1 (default)*” to choose the correct serial port and click “*Next*”.



6. If you would like to view the ReadMe file, leave the “**View ReadMe File**” box checked. If you do not want to view the file, uncheck this box. Click “**Next**” to complete the installation.



7. Click “**Yes, I want to restart my computer now.**” to complete the Setup.



6.3.3 Schlumberger Reflex 72 Serial Smart Card Reader



The Reflex 72 Serial Card Reader has 3 connectors. To connect the reader to the PC:

1. Ensure that the PC is turned off.
2. Connect Connector 1 to an available COM port on your PC or laptop.
3. Connect Connector 2 to either the Keyboard or the Mouse PS/2 port.
4. Connect the Keyboard or Mouse to Connector 3 (if necessary).

NOTE: If you are using a laptop, Connector 3 may be left un-connected. However, both Connectors 1 and 2 MUST be used at all times.

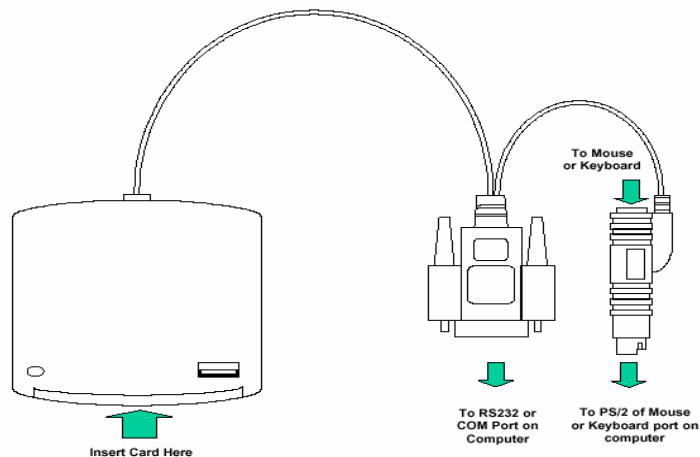


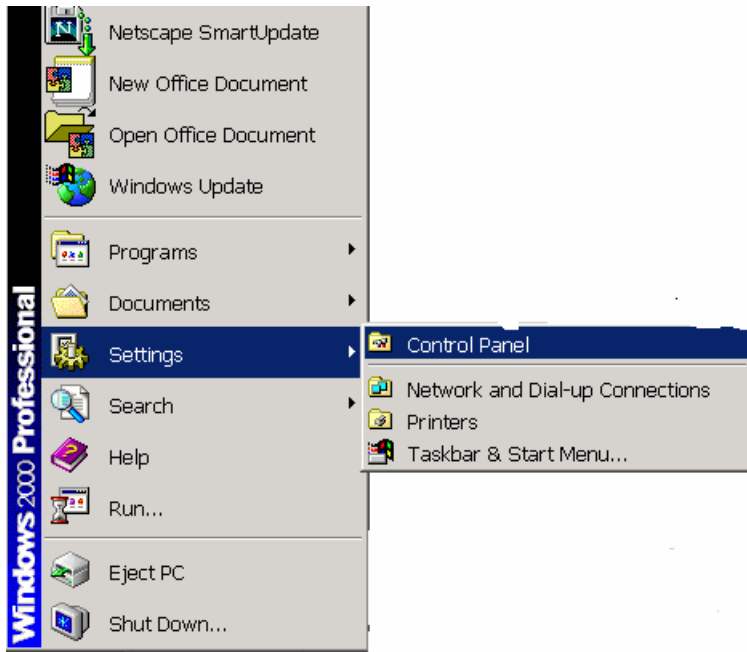
Figure 3: Installation of Serial Card Reader to a PC

5. After the card reader is connected, turn your PC on.

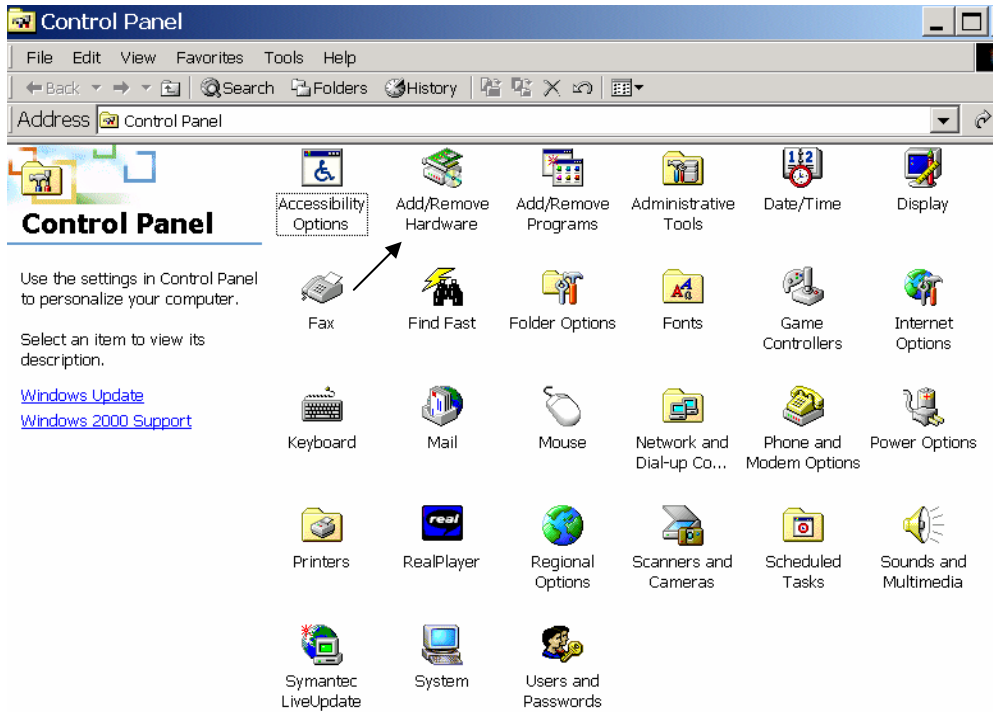


6.3.3.1 Installation on Windows 2000 Platform

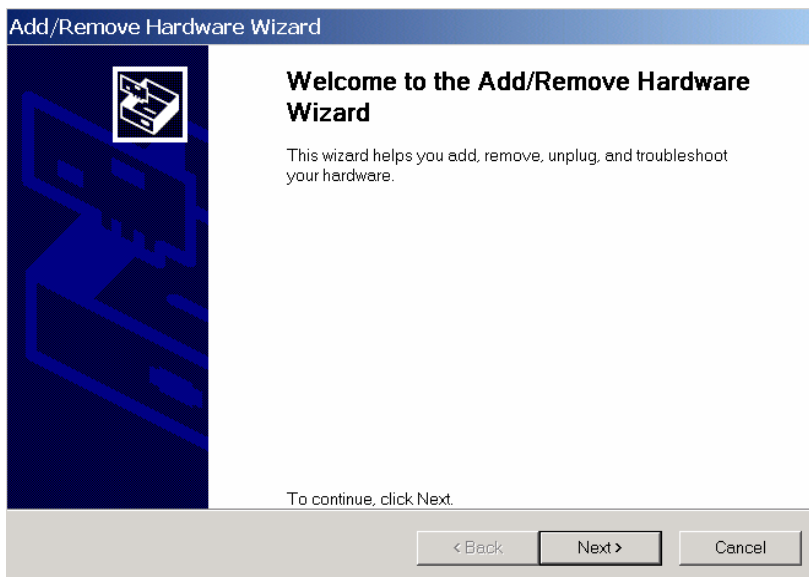
This Schlumberger Reflex 72 Serial Card Reader is a Plug and Play device. Once attached to the PC, the PC should detect this new hardware by itself and launch the *Add/Remove Hardware Wizard*. If the Wizard does not launch:



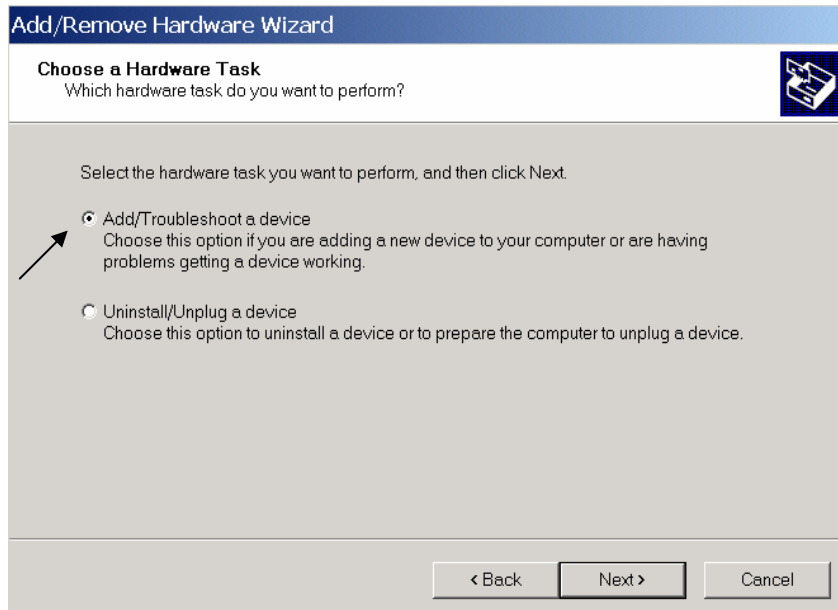
1. Click *Start, Settings, Control Panel*. The Control Panel will open.



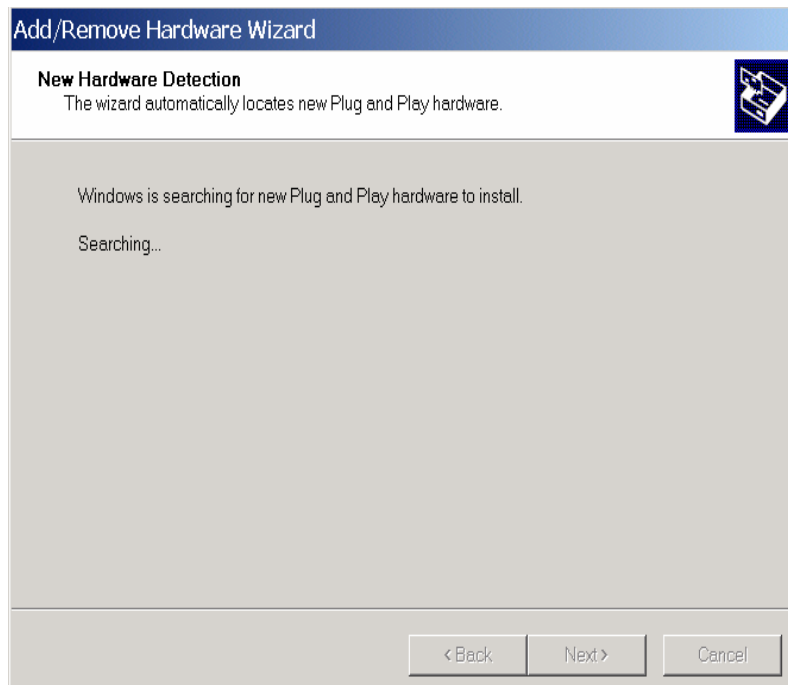
2. Double click the “*Add/Remove Hardware*” icon.



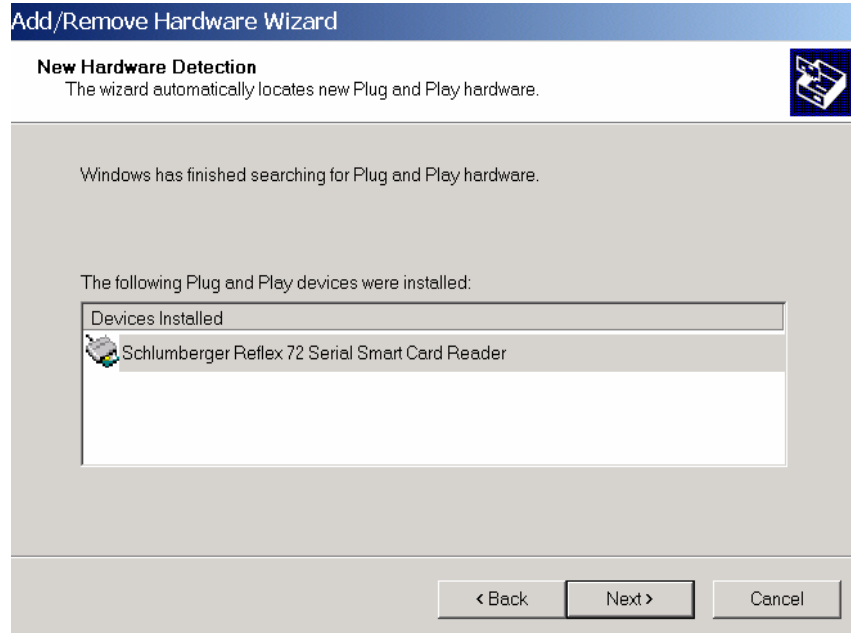
3. The *Add/Remove Hardware Wizard* will appear. If the Wizard launches by itself, this screen will appear. This Wizard will assist you in installing the Card Reader driver on your PC. Click “*Next*” to continue.



4. Click the “*Add/Troubleshoot a device*” radio button then click “*Next*” to continue.



5. The *Add/Remove Hardware Wizard* will search for the Card Reader.



6. The Wizard will automatically detect the Schlumberger Reflex 72 Serial Smart Card Reader and install this device. Click “*Next*” to continue.

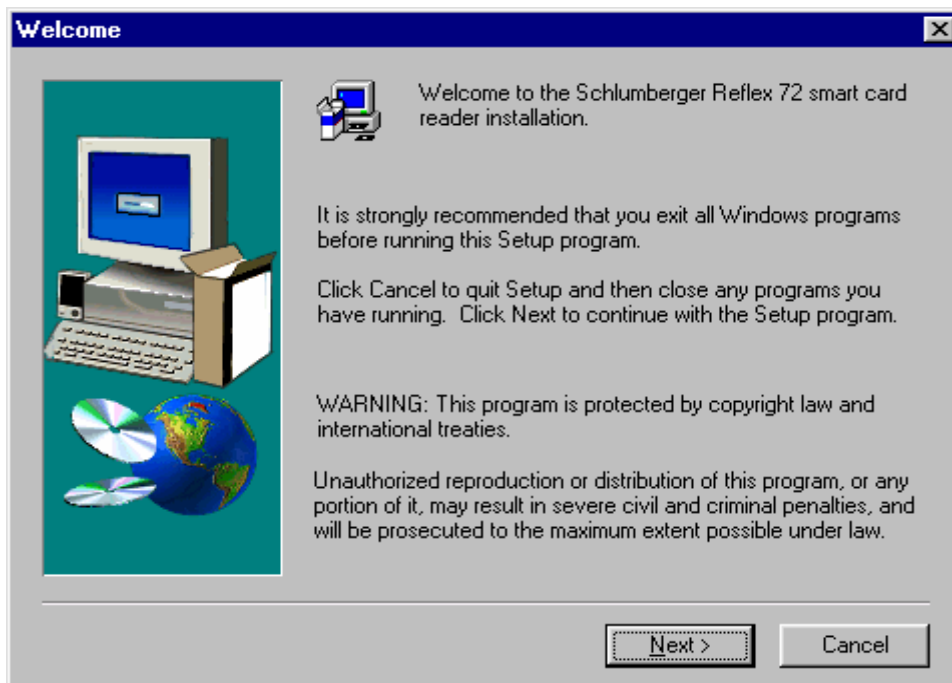


7. Click “*Finish*” to close the *Add/Remove Hardware Wizard*.

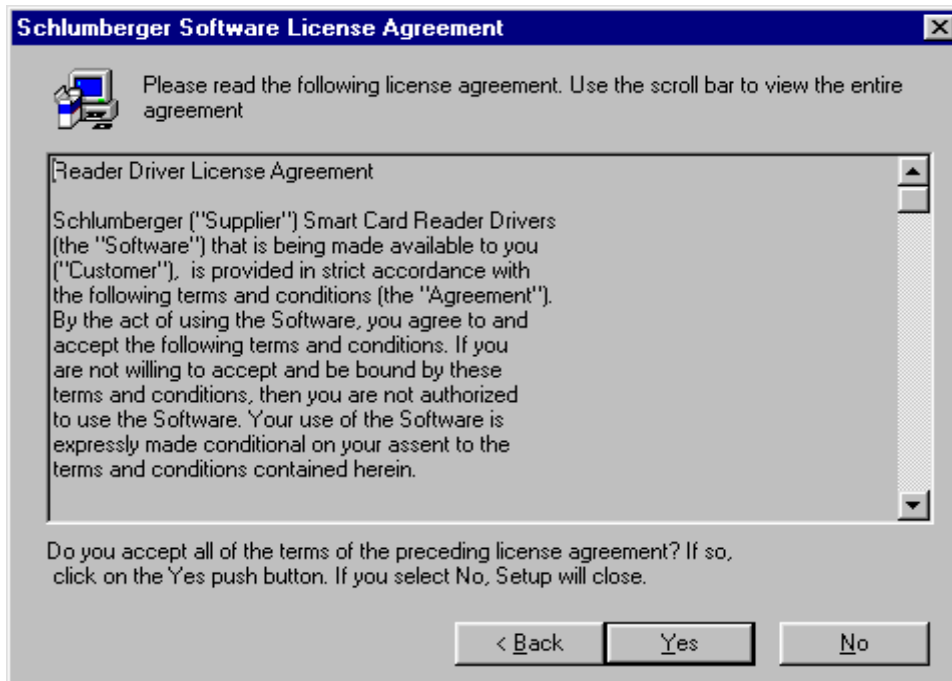


6.3.3.2 Installation on Windows NT & 98 Platform

1. Place the CD in the CD-ROM drive. Browse the CD using *My Computer*. Navigate through the following folders: Card Reader Drivers folder, Schlumberger folder, Serial folder. Double-click the *setup.exe* icon in the Serial folder. The Installation Wizard will launch to begin the card reader installation.



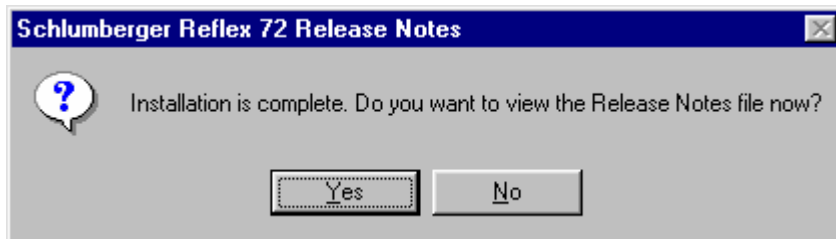
2. When Welcome screen appears, select “*Next*”.



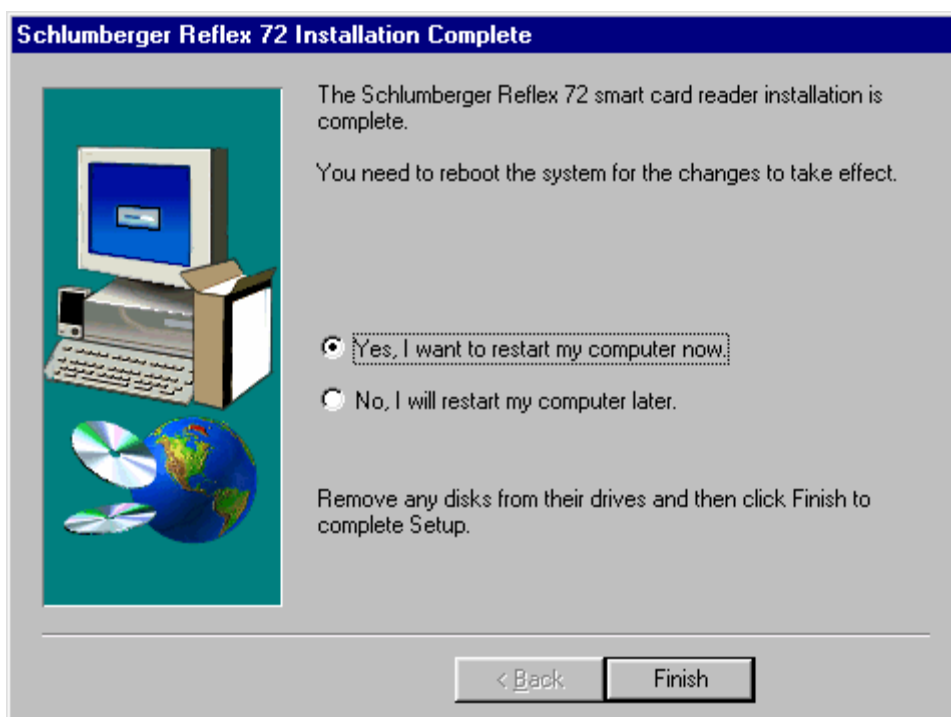
3. Click “*Yes*” to accept the Software License Agreement.



4. Accept the default file folder, click “*Next*” to continue. The necessary files will now be installed.



5. Select “**Yes**” if you would like to view the Release Notes file or “**No**” if you do not.



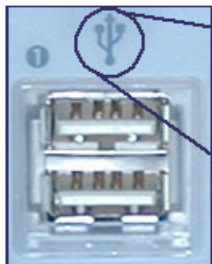
6. Click “**Yes, I want to restart my computer now.**” to complete the installation.



6.3.4 Schlumberger Reflex USB Card Reader



The Schlumberger Reflex USB Card Reader is a Plug and Play Device. A USB Card Reader will attach to the PC differently than a serial Card Reader. The USB Card Reader will connect to your PC via the USB port located on the back of the PC.



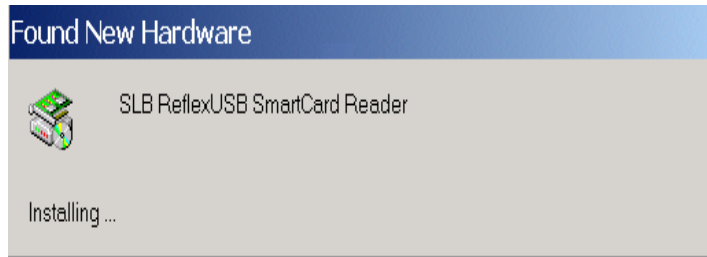
Simply plug the card reader into the USB port as shown above.

NOTE: The Schlumberger Reflex USB Card Reader is NOT SUPPORTED on the Windows NT platform.

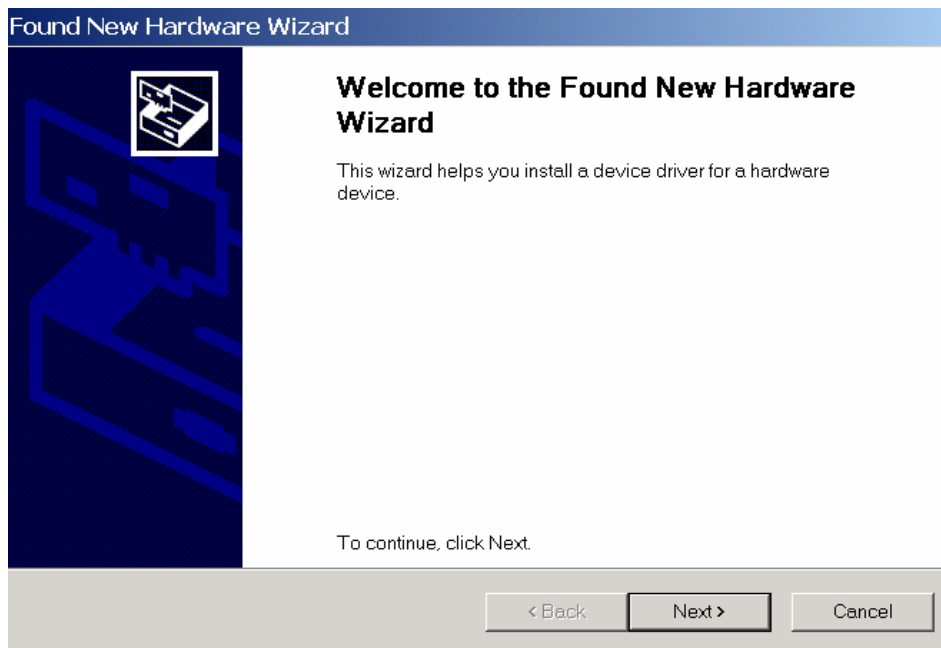
After the card reader is connected, turn your PC on.



6.3.4.1 Installation on Windows 2000 Platform



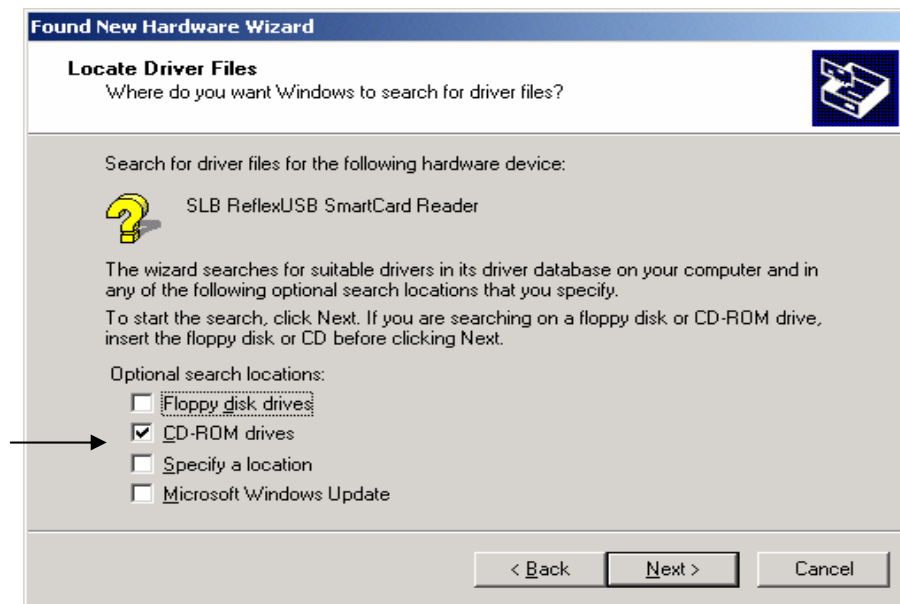
1. Once the Schlumberger USB Card Reader is plugged into the back of the PC, the ***Found New Hardware Wizard*** should appear.



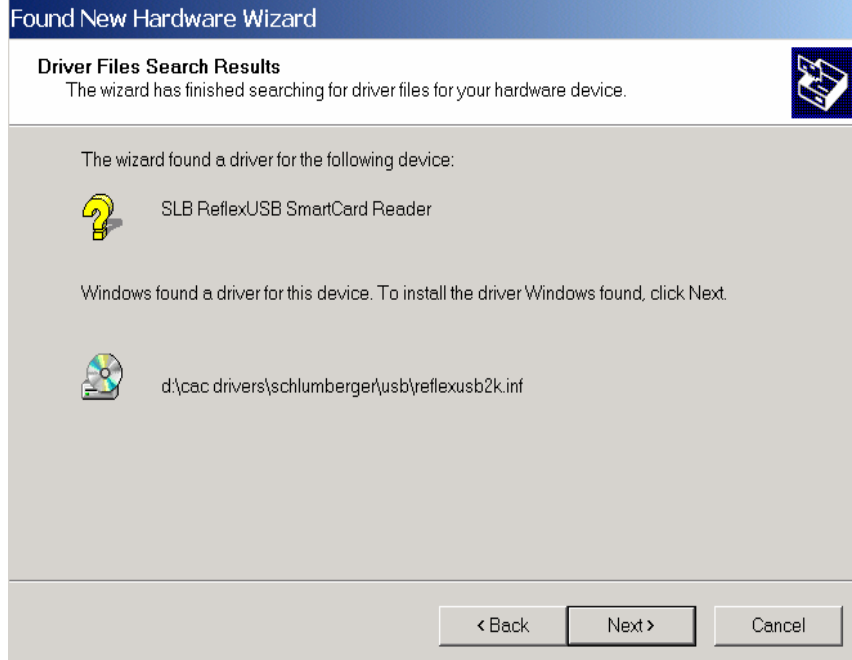
2. Click "***Next***" to install a device driver for the Card Reader.



- The **Found New Hardware Wizard** will look for a device driver for this Card Reader. Click the “**Search for a suitable driver for my device (recommended)**”. Click “**Next**” to continue.



- Place the CD in the CD-ROM drive. Make sure “**CD-ROM drives**” is checked. Click “**Next**”.



5. The Wizard will find the driver on the CD-ROM. Click “*Next*” to continue.



6. Click “*Finish*” to complete the driver installation.



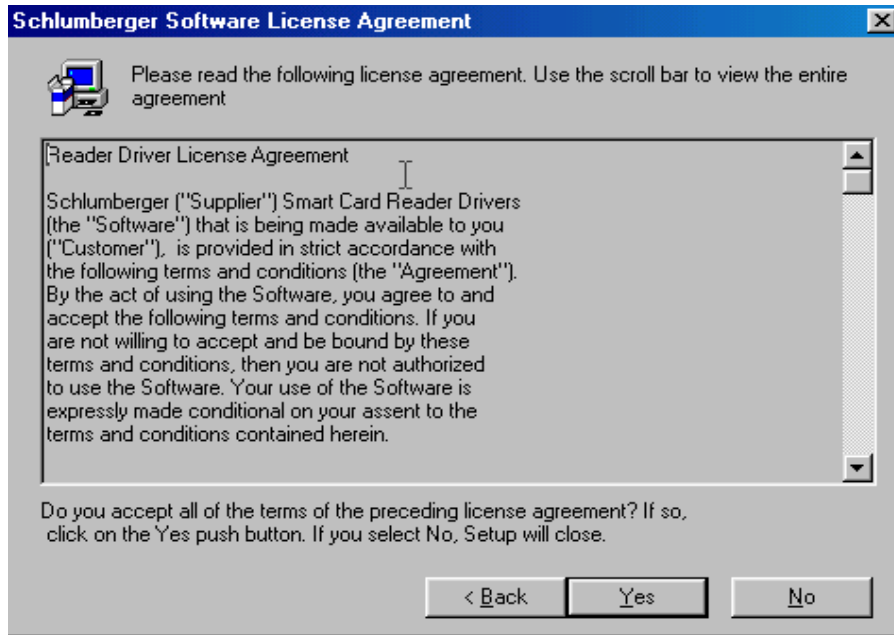
6.3.4.2 Installation on Windows 98 Platform

Do not use the Plug & Play Installation on this Platform. .

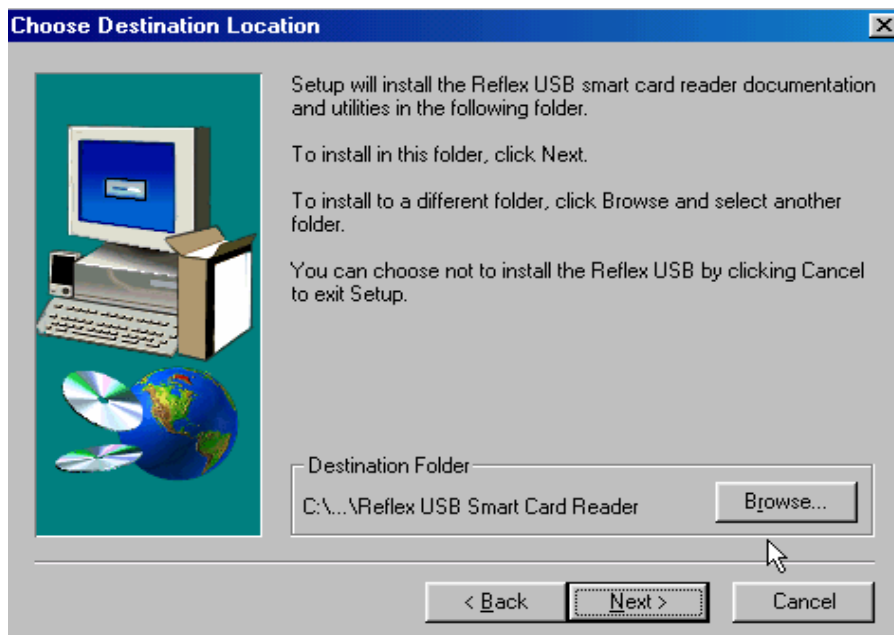
1. Place the CD in the CD-ROM drive. Browse the CD using *My Computer*. Navigate through the following folders: Card Reader Drivers folder, Schlumberger folder, USB folder. Double-click the *ReflexUSB.exe* icon in the USB folder. The Installation Wizard will launch to begin the card reader installation.



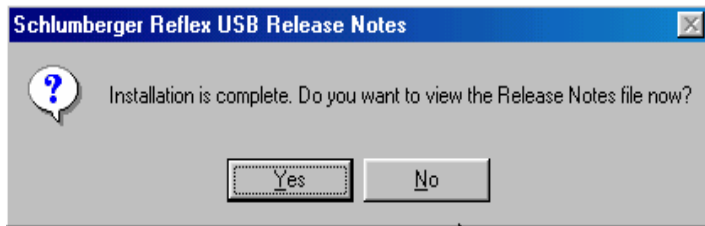
2. When the Welcome screen appears, click “*Next*”.



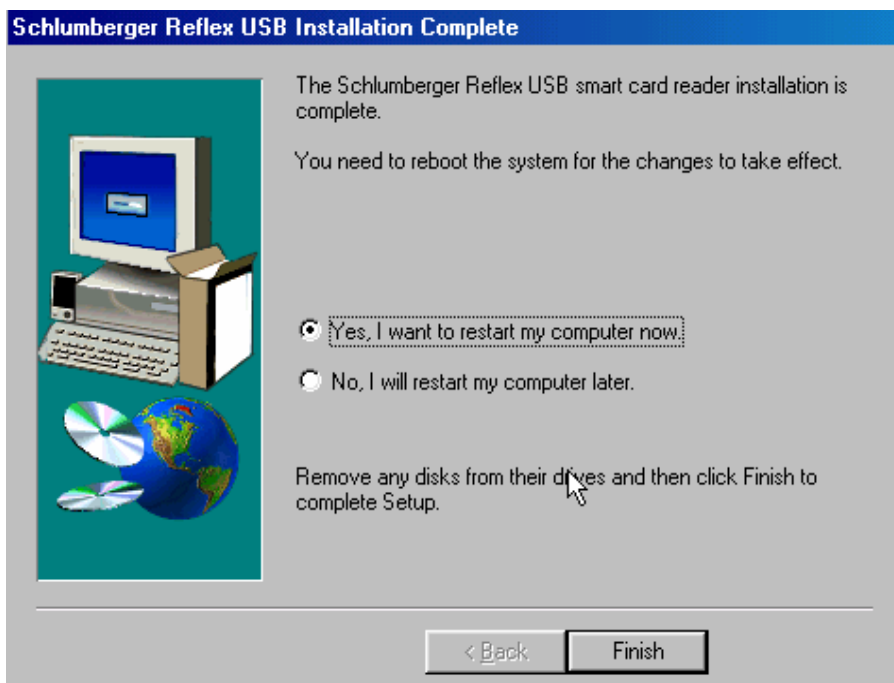
3. Click “*Yes*” to accept the Software License Agreement.



4. Accept the default file folder, click “*Next*” to continue.



5. Select “**Yes**” if you would like to view the Release Notes file or “**No**” if you do not.



6. Click the “**Yes, I want to restart my computer now**” radio button then Click “**Finish**” to complete the installation.



6.3.5 Schlumberger Reflex PCMCIA Card Reader



The PCMCIA Card Reader will connect to your PC or laptop via the PCMCIA slot.



The PCMCIA slot in a standalone PC is shown above.



The PCMCIA slot in a laptop is shown above.

After the card reader is inserted in the PCMCIA slot, turn your PC on.



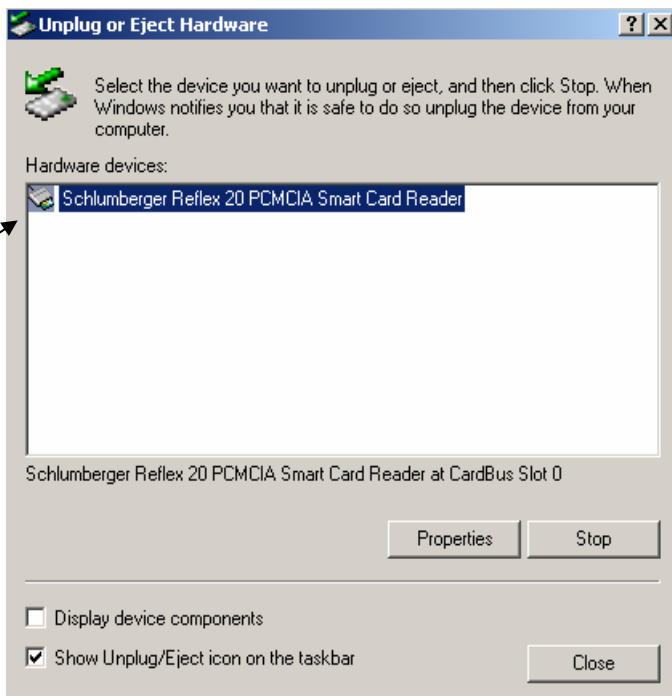
6.3.5.1 Installation on Windows 2000 Platform

1. Shut down and turn off the computer.
2. Insert the PC card reader into an available PCMCIA slot.
3. Restart your computer.

The installation of the driver will take place without any prompting by the user if the device driver software for the smart card reader is available. This driver is installed on the hard drive as part of the Windows 2000 installation. This may take a few minutes.



4. You can confirm that installation has successfully taken place by the appearance of the ***Unplug or Eject Hardware*** icon in the toolbar (shown above). Double-click this icon.

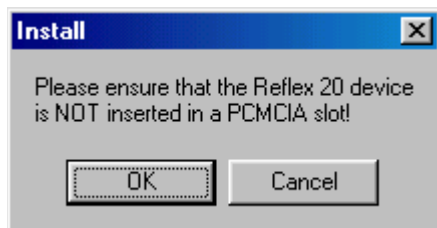


5. The PCMCIA card reader will appear in the list of hardware devices in the ***Unplug or Eject Hardware*** dialog box.



6.3.5.2 Installation on Windows NT & 98 Platform

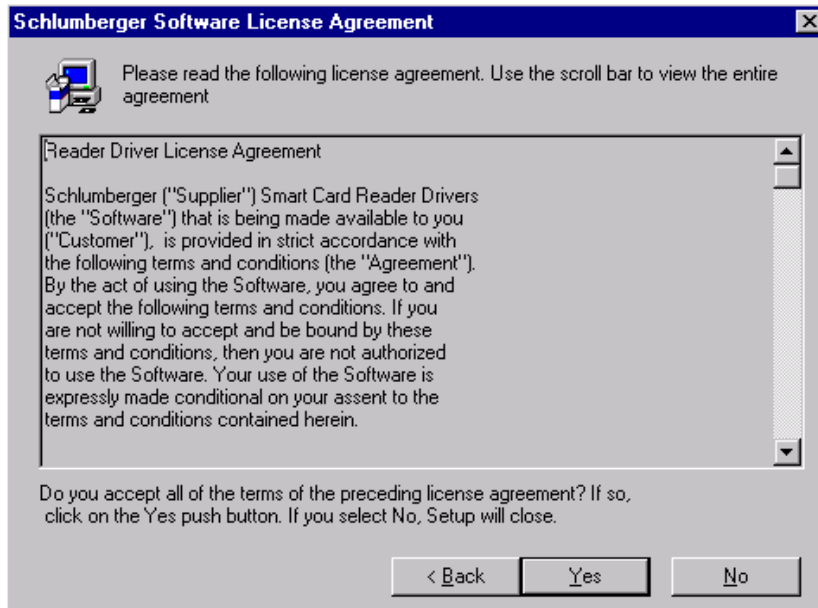
1. Place the CD in the CD-ROM drive. Browse the CD using *My Computer*. Navigate through the following folders: Card Reader Drivers folder, Schlumberger folder, PCMCIA folder. Double-click the *Reflex4NT&9x.exe* icon in the PCMCIA folder. The Installation Wizard will launch to begin the card reader installation.



2. Ensure that the PCMCIA card reader is not inserted in the PCMCIA slot and click “*OK*” to continue.



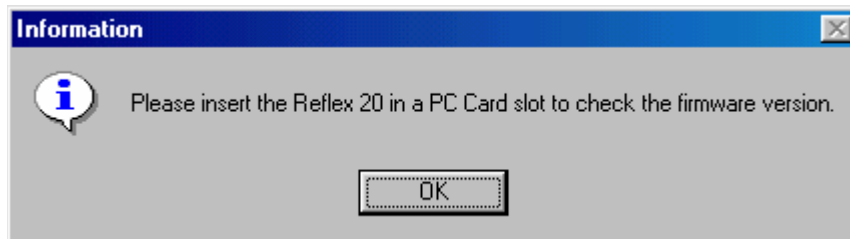
3. When the Welcome screen appears, click “*Next*”.



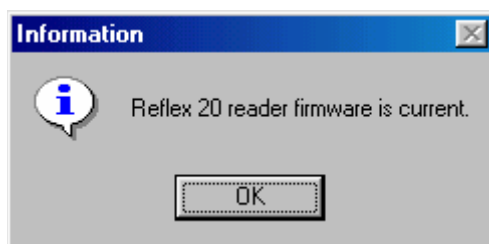
4. Click “*Yes*” to accept the Software License Agreement.



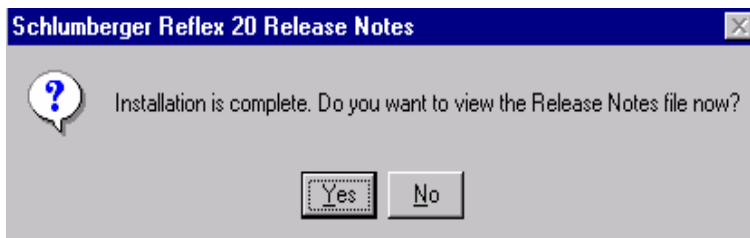
5. Accept the default destination file folder, click ““*Next*”” to continue. The installation program will install the necessary files.



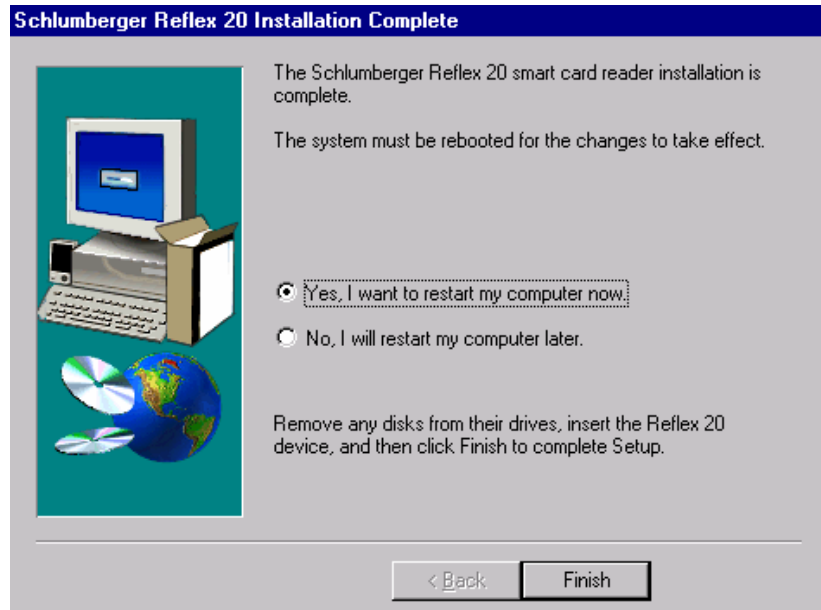
6. Please insert the PCMCIA card reader into the PCMCIA slot and click “**OK**” to check the firmware version.



7. Click “**OK**” to continue with the installation.



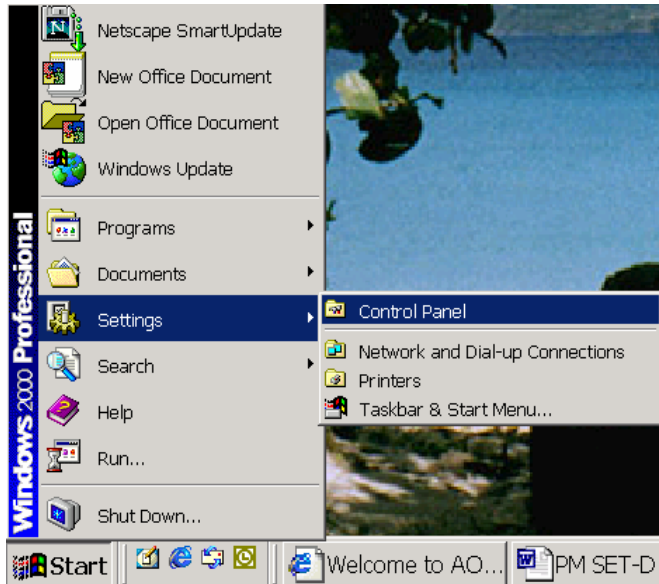
8. Click “**Yes**” if you would like to view the Release Notes file. Click “**No**” if you do not.



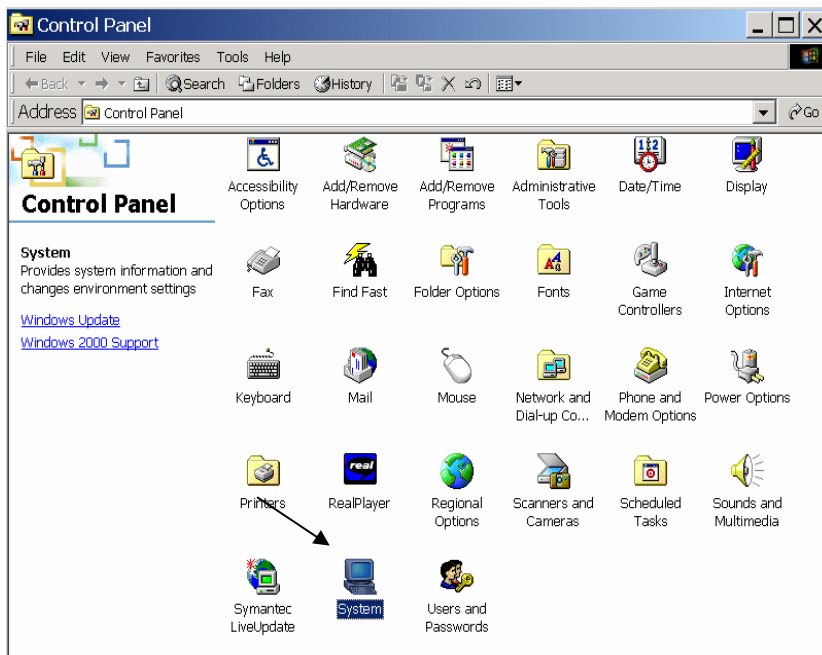
9. Click “*Yes, I want to restart my computer now.*” radio button. Click “*Finish*” to complete the installation.



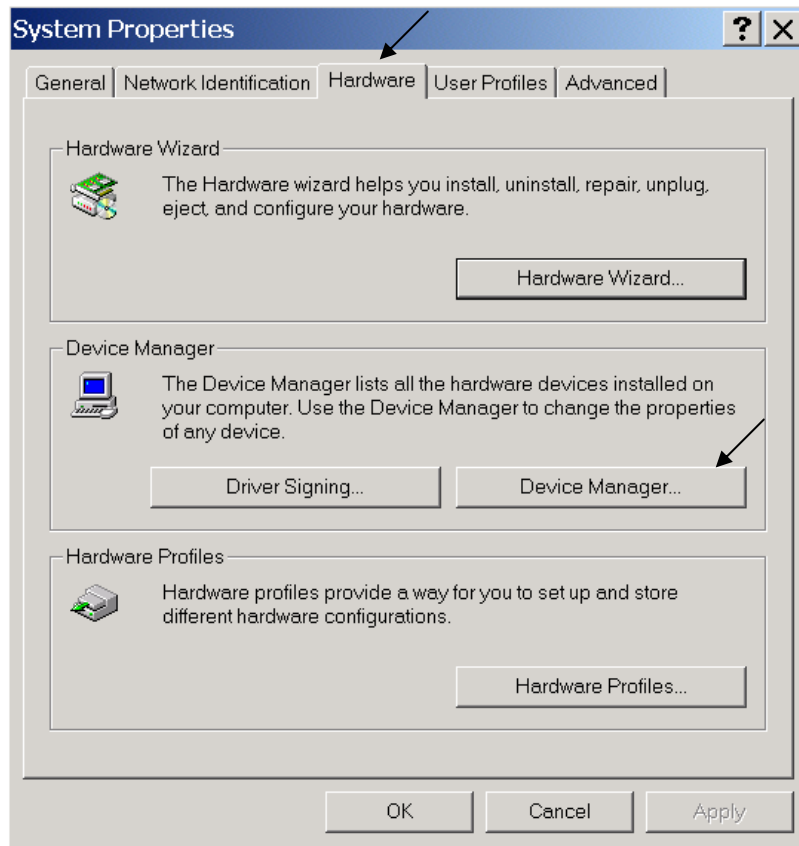
6.4 Checking Card Reader Installation with Device Manager



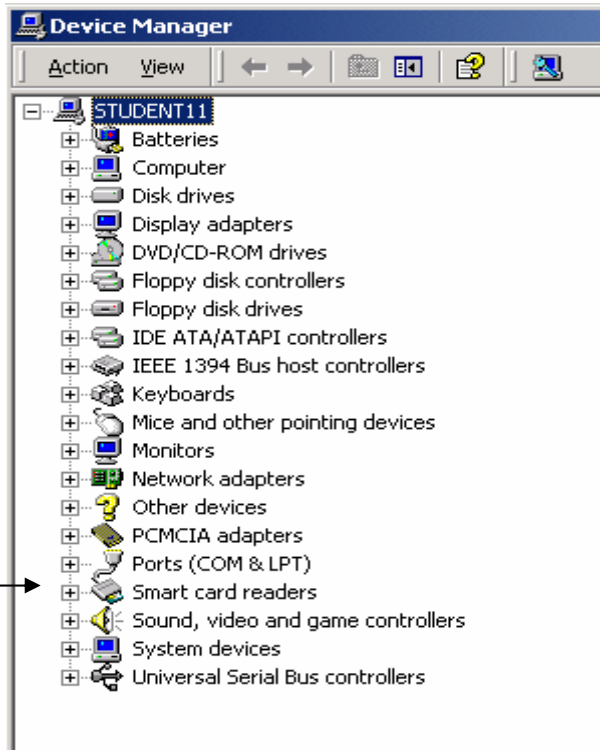
1. Choose *Control Panel* from the Start-Settings menu



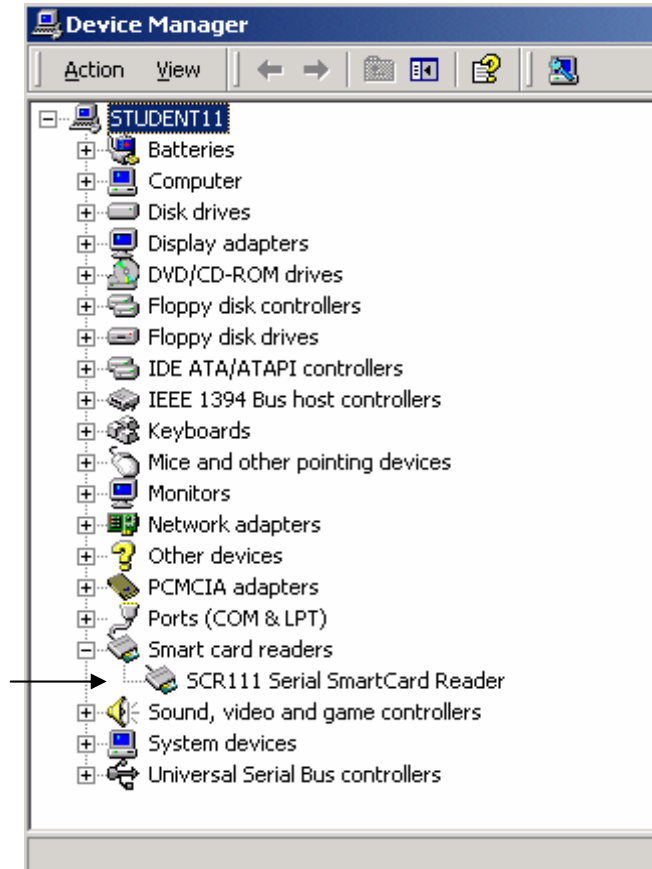
2. Choose *System* from the Control Panel window.



3. Click the “**Hardware**” tab in the *System Properties* window. Once the Hardware tab is visible, click the “**Device Manager**” button.



4. The Device Manger window will appear. Scroll down through the list and find the Smart Card Readers heading. Expand this menu choice by clicking on the “+”.



5. If the smart card reader is not installed properly, a yellow exclamation point will appear next to the Smartcard reader. If the reader is installed properly the screen will look like the one above.

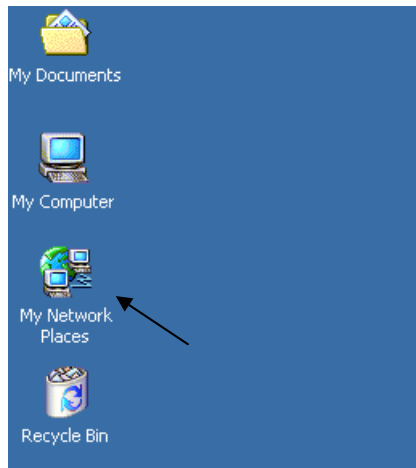


6.5 Obtaining and Installing Root Certificates

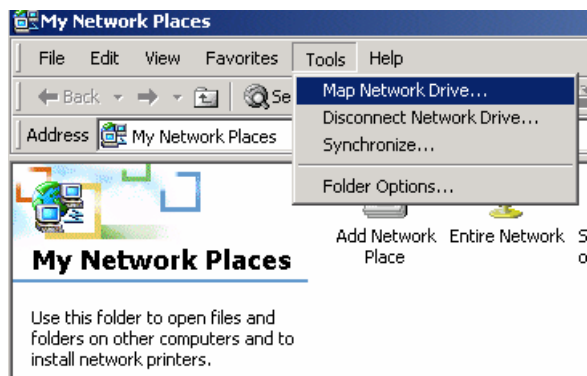
IMPORTANT NOTE:

For training purposes, we will be obtaining and installing 2 sets of Root Certificates. One set is for use with the Test CACs in the Training Classroom. These Test Root Certificates WILL NOT need to be installed during fielding of Card Readers and Middleware. The second set of Root Certificates, the Live CAC Root Certificates, will be obtained from the PKI webpage and saved on your Desktop. A simple installation procedure will follow. Both sets of Root Certificates will need to be installed in order to use your CAC for digitally signing and encrypting email during the Training class. Only the Live CAC Root Certificates will need to be installed for Fielding purposes..

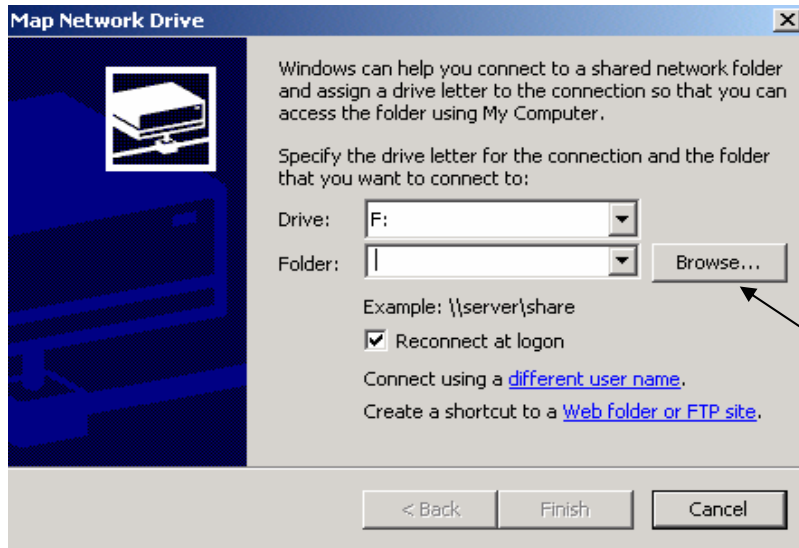
6.5.1 Obtaining and Installing Test CAC Root Certificates



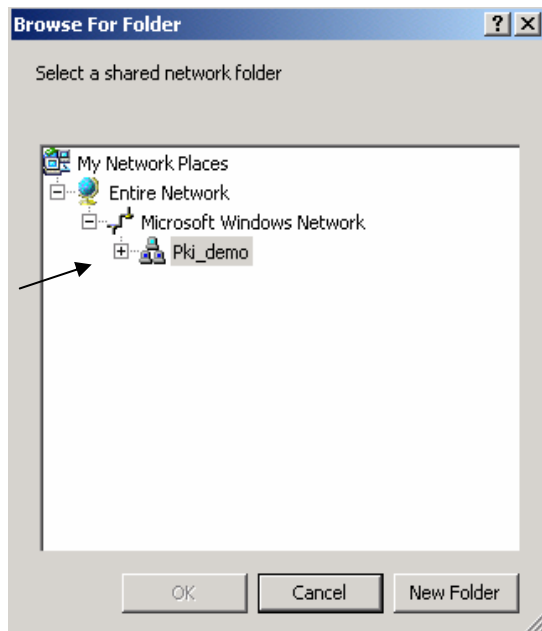
1. Double-click the “*My Network Places*” icon on your desktop.



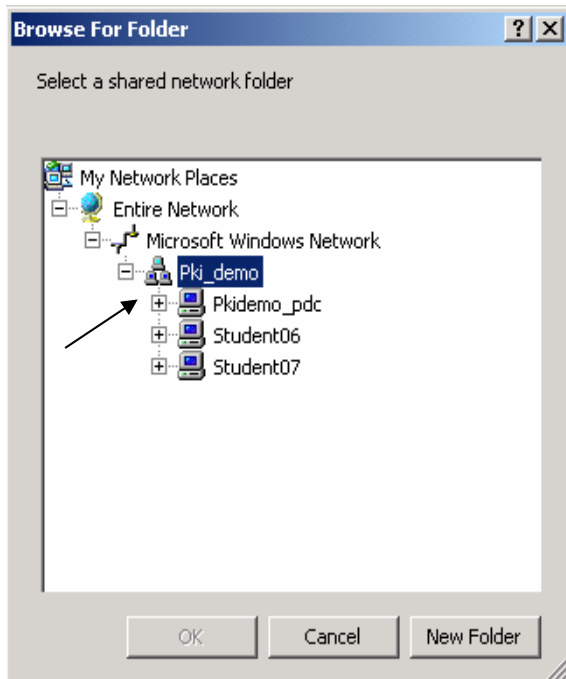
2. The “*My Network Places*” window will appear. Click on the “*Tools*” menu and choose “*Map Network Drive.*”



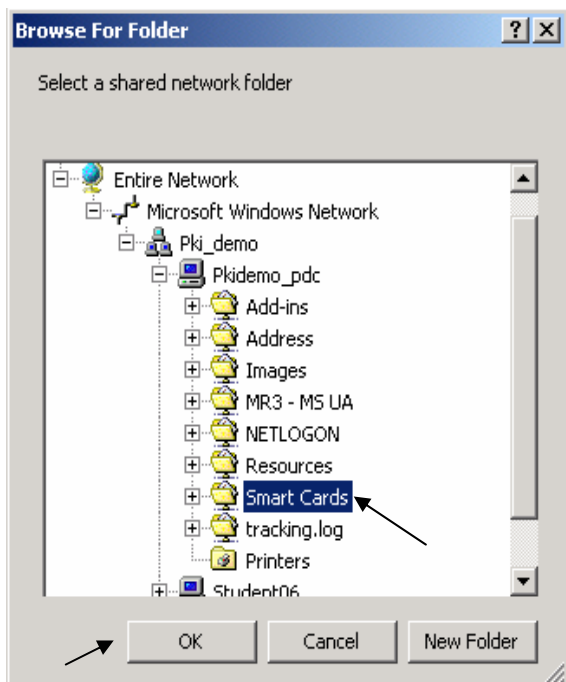
3. Choose “**Browse**” to browse the network for the drive you would like to map.



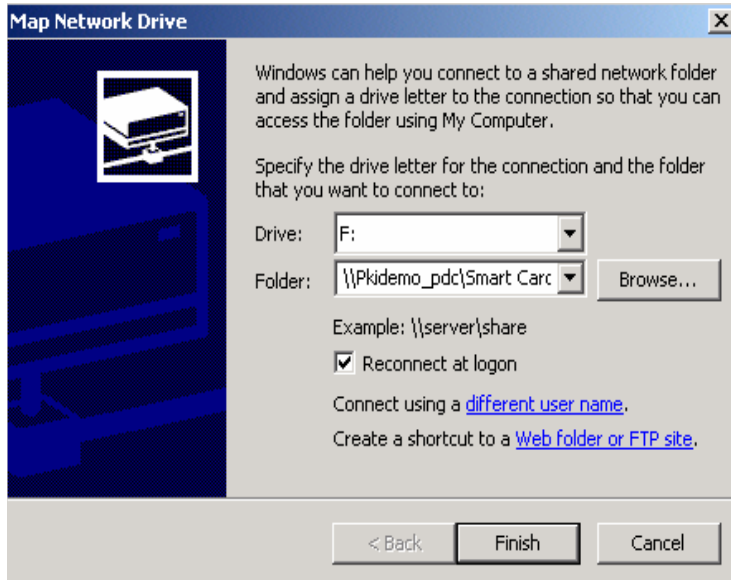
4. Click on the “+” sign to expand the menu next to “**Pki_demo**”.



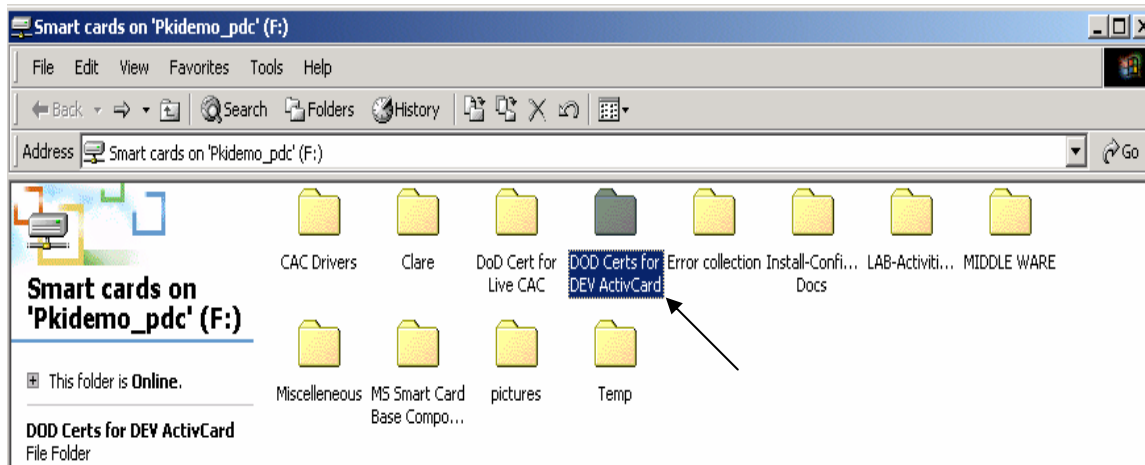
5. Click on the “+” sign next to “*Pkidemo_pdc*” to expand this menu.



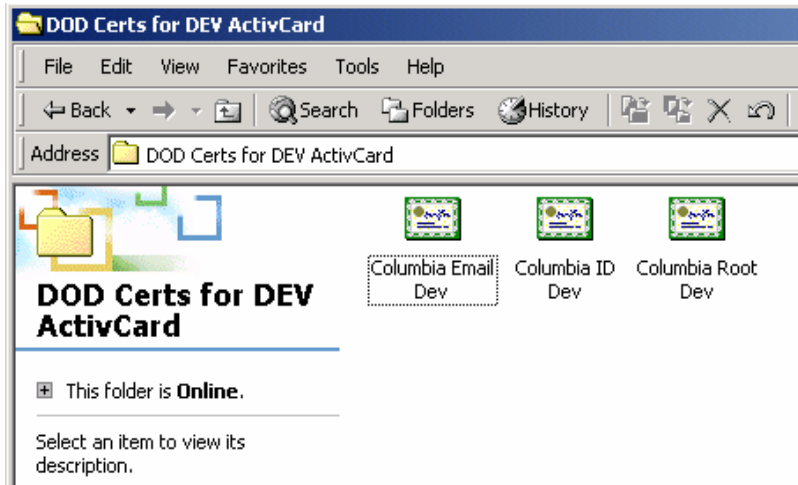
6. Click on “*Smart Cards*” to highlight this folder and then click “*OK*”.



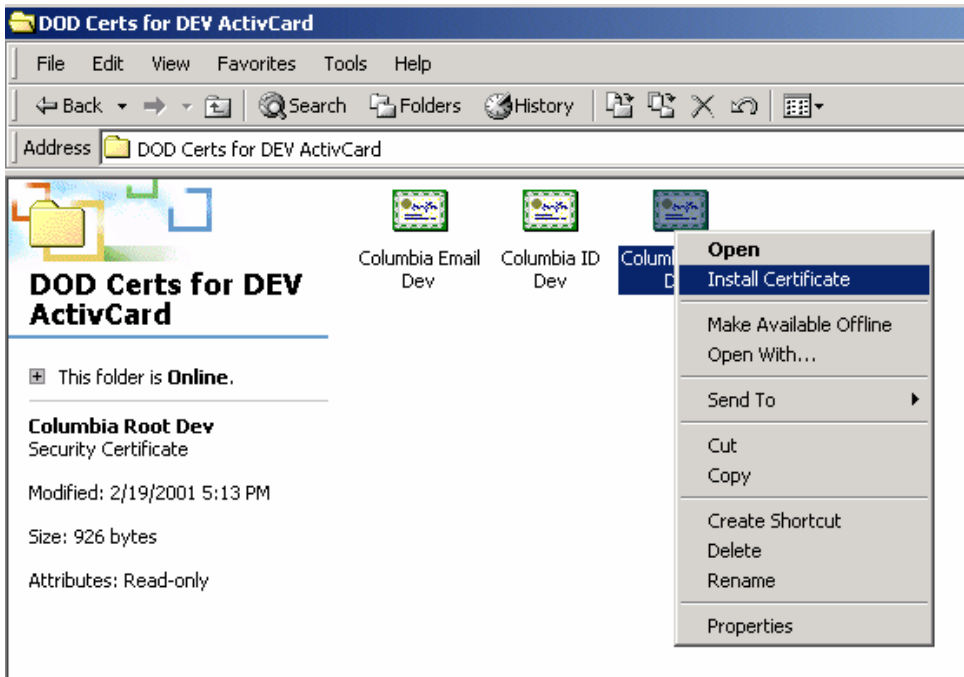
7. Click on “*Finish*” to complete the drive mapping.



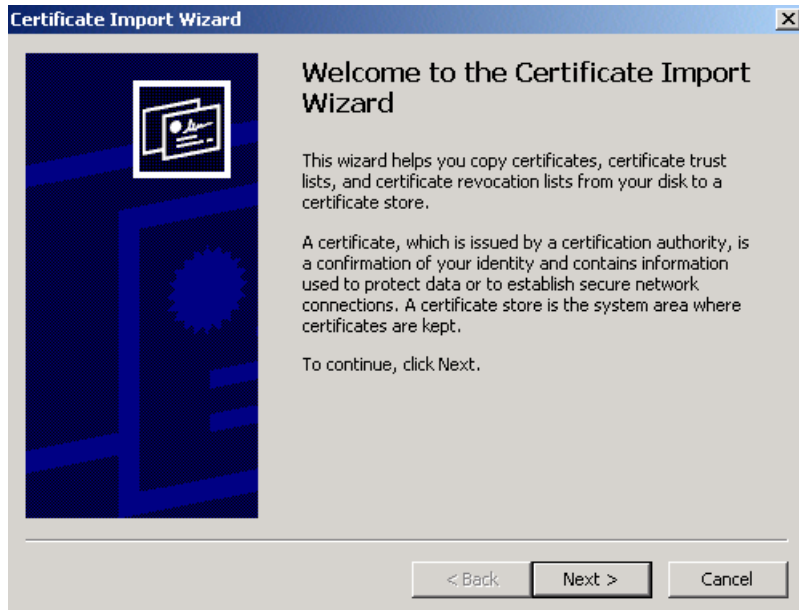
8. A new window will open containing the folders of the newly mapped drive. Double-click the “*DOD Certs for DEV ActivCard*” folder.



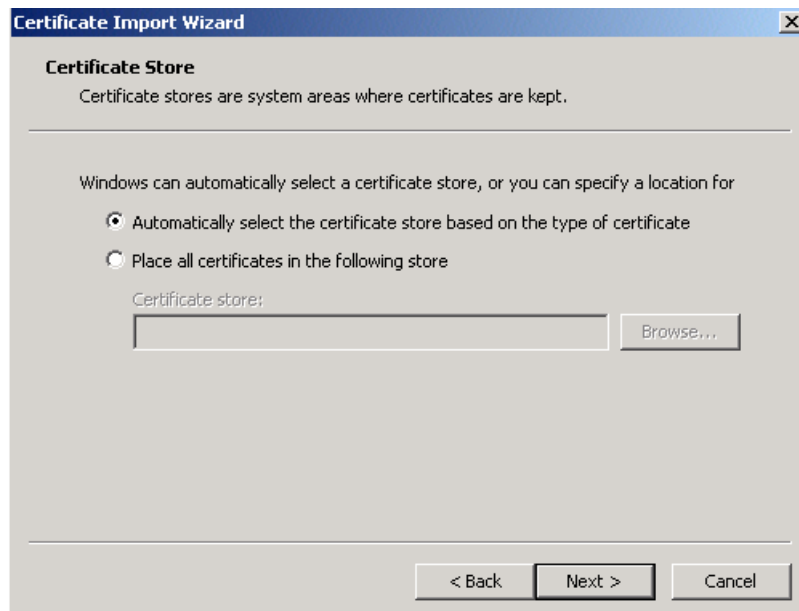
9. This folder contains the 3 Certificates that you will install for use with the Test CACs in our Training environment.



10. Right-click on the “*Columbia Root Dev*” certificate and choose “*Install Certificate*” from the menu.



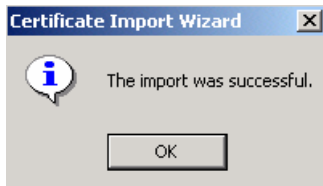
11. The Certificate Import Wizard will launch. Click ***“Next”*** to continue with the installation of the certificate.



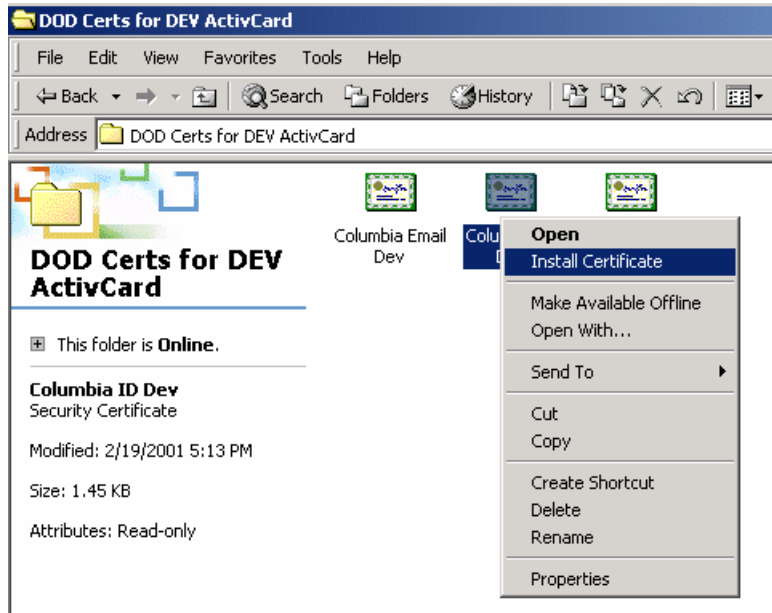
12. Make sure the ***“Automatically select the certificate store based on the type of certificate”*** radio button is selected. Click ***“Next”*** to continue.



13. Click "**Finish**" to complete the Root certificate installation.



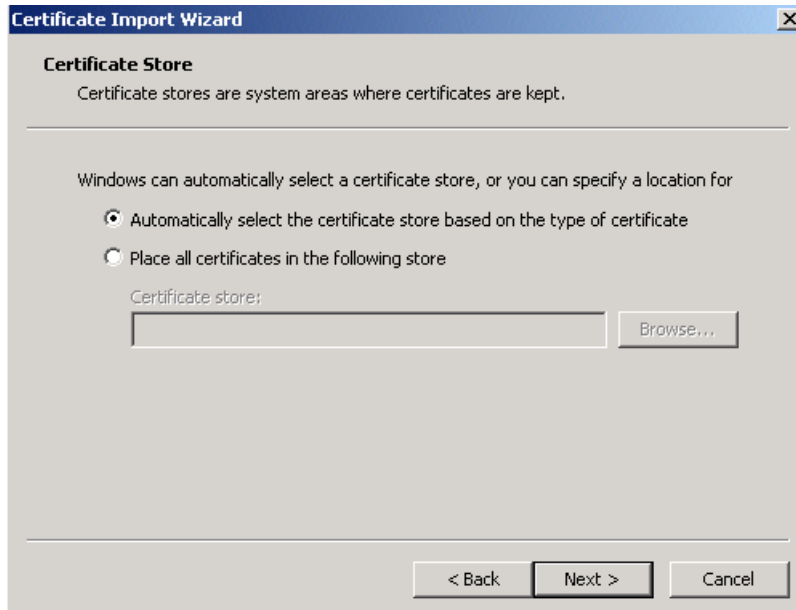
14. Click "**OK**" to close the Certificate Import Wizard.



15. Right-click on the “*Columbia ID Dev*” certificate and choose “*Install Certificate*” from the menu. This certificate will install exactly like the last certificate.



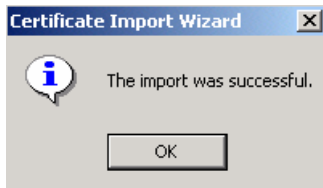
16. Click “*Next*” to continue with the installation of the certificate.



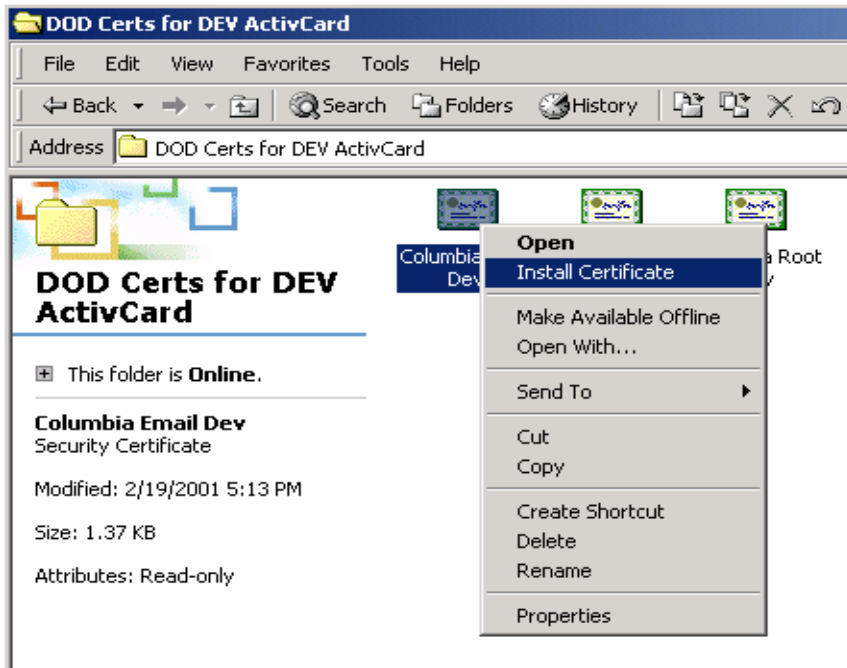
17. Make sure the “*Automatically select the certificate store based on the type of certificate*” radio button is selected. Click “*Next*” to continue.



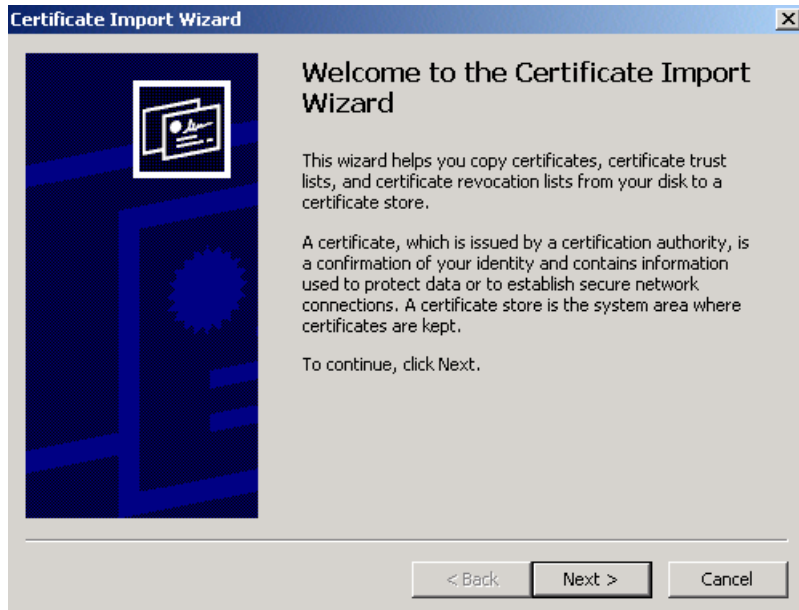
18. Click “*Finish*” to complete the Root certificate installation.



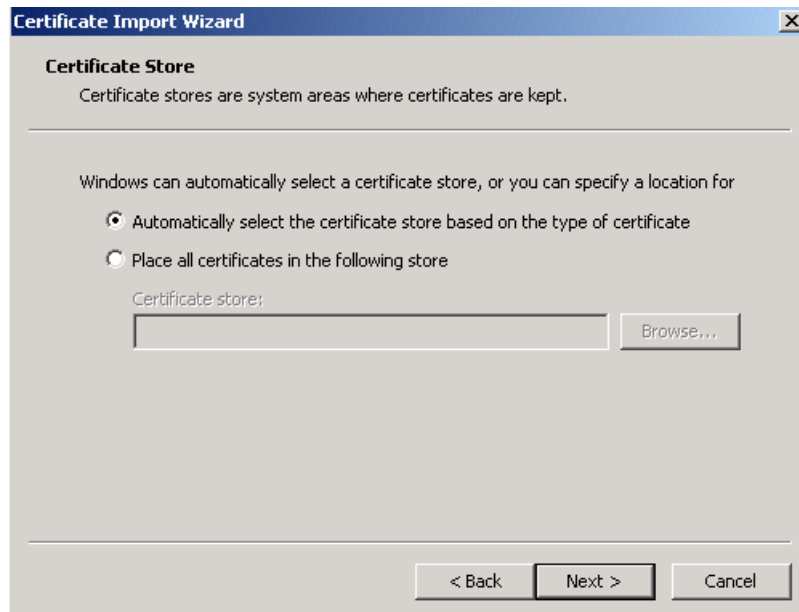
19. Click “**OK**” to close the Certificate Import Wizard.



20. Right-click on the “*Columbia ID Dev*” certificate and choose “*Install Certificate*” from the menu. This certificate will install exactly like the last certificate.



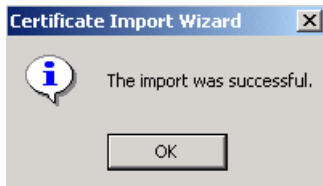
21. Click “*Next*” to continue with the installation of the certificate.



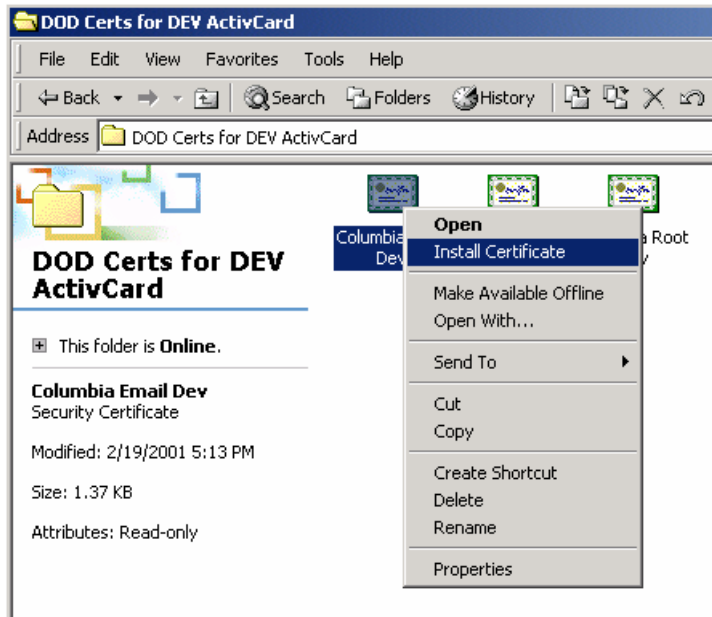
22. Make sure the “*Automatically select the certificate store based on the type of certificate*” radio button is selected. Click “*Next*” to continue.



23. Click “*Finish*” to complete the Root certificate installation.



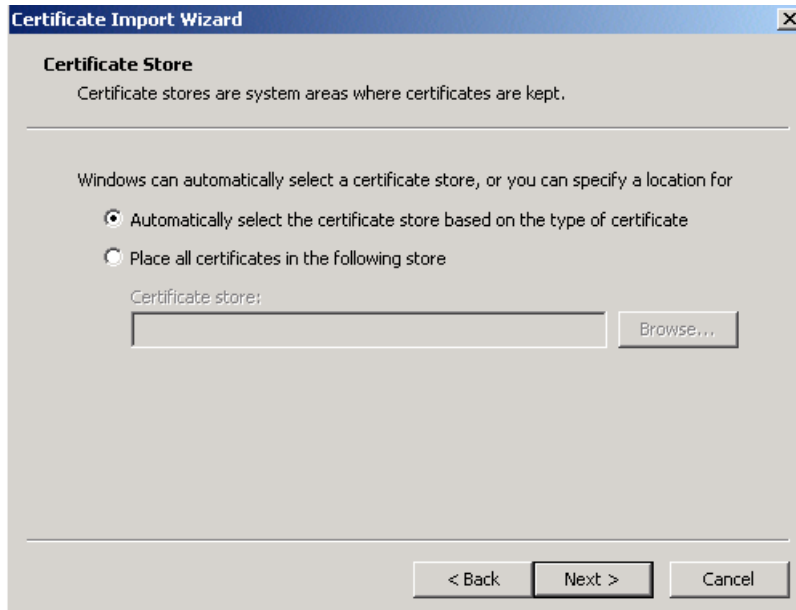
24. Click “*OK*” to close the Certificate Import Wizard.



25. Right-click on the “*Columbia E-mail Dev*” certificate and choose “*Install Certificate*” from the menu. This certificate will install exactly like the last certificate.



26. Click “*Next*” to continue with the installation of the certificate.



27. Make sure the “*Automatically select the certificate store based on the type of certificate*” radio button is selected. Click “*Next*” to continue.



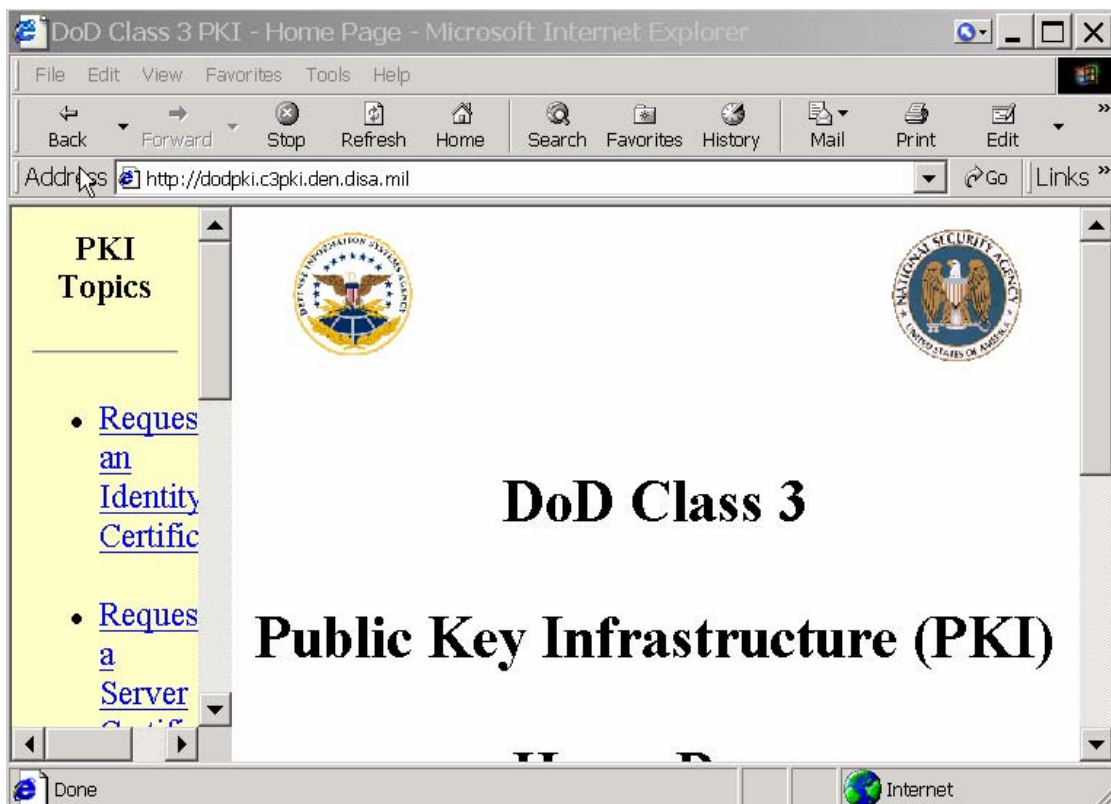
28. Click “*Finish*” to complete the Root certificate installation.



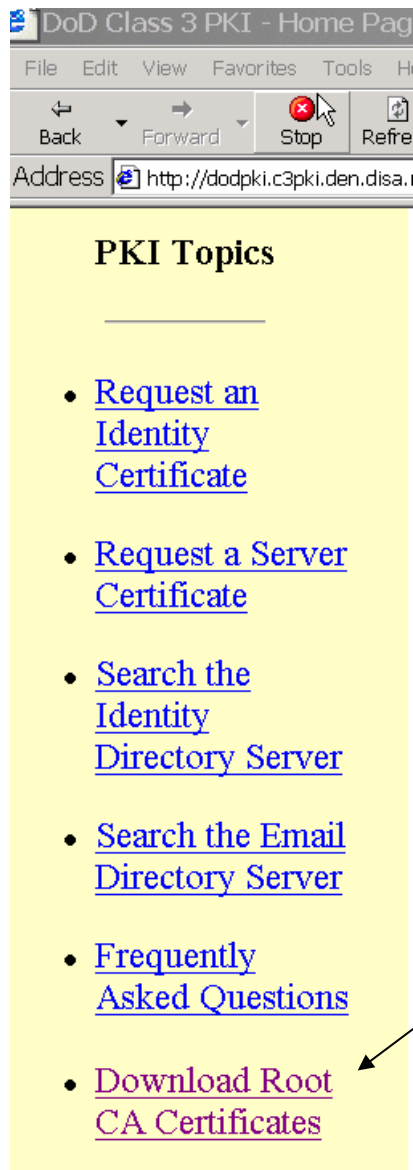
29. Click “**OK**” to close the Certificate Import Wizard.

You have now successfully obtained and installed all 3 Test CAC Certificates.

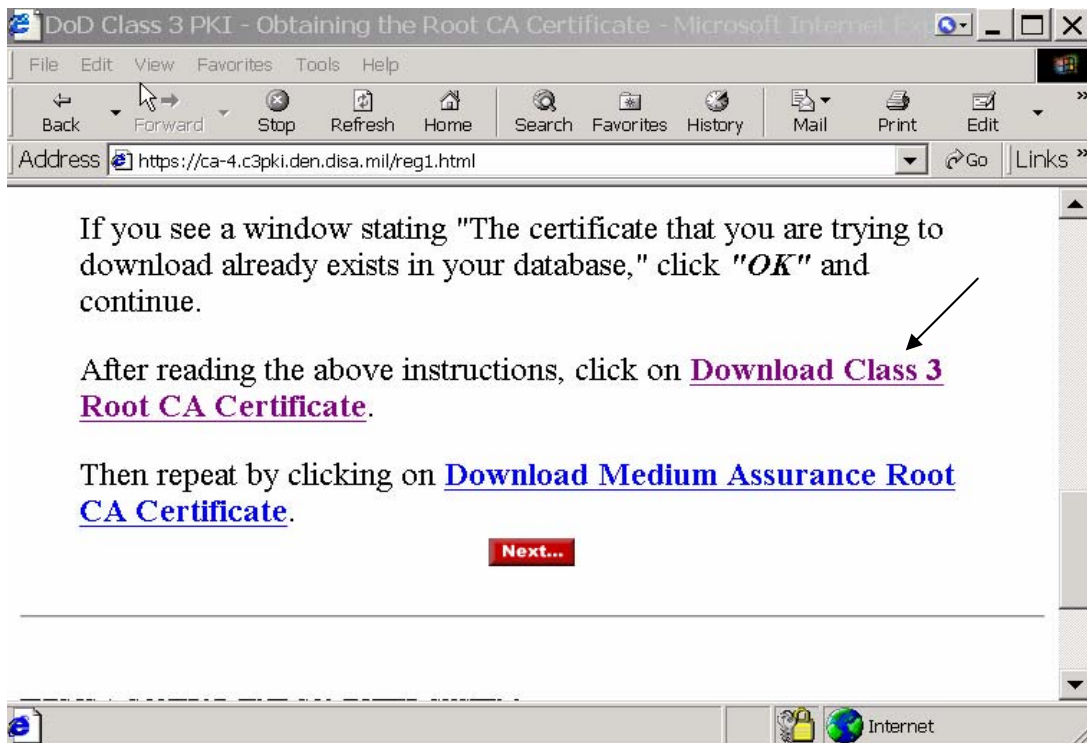
6.5.2 Obtaining Root Certificates



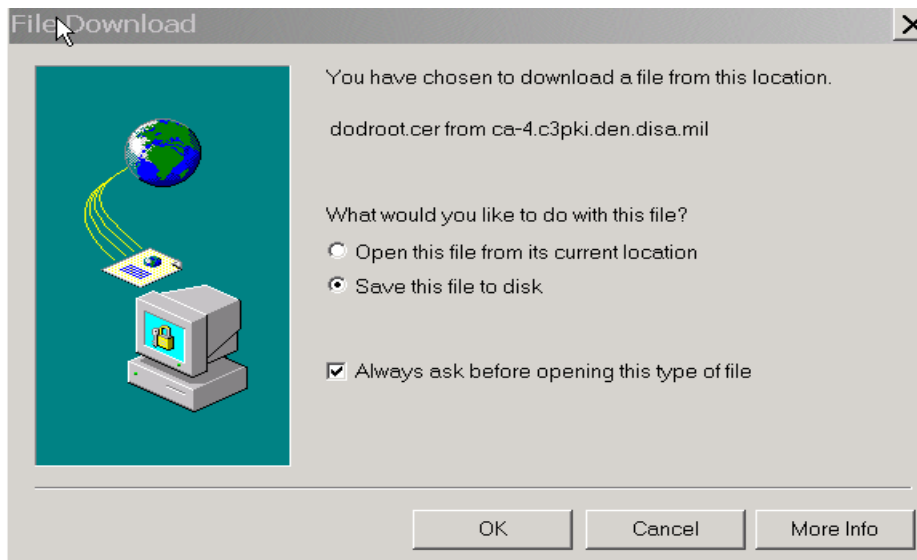
1. Start Internet Explorer and connect to PKI home page:
<http://dodpki.c3pki.chamb.disa.mil> or <http://dodpki.c3pki.den.disa.mil>



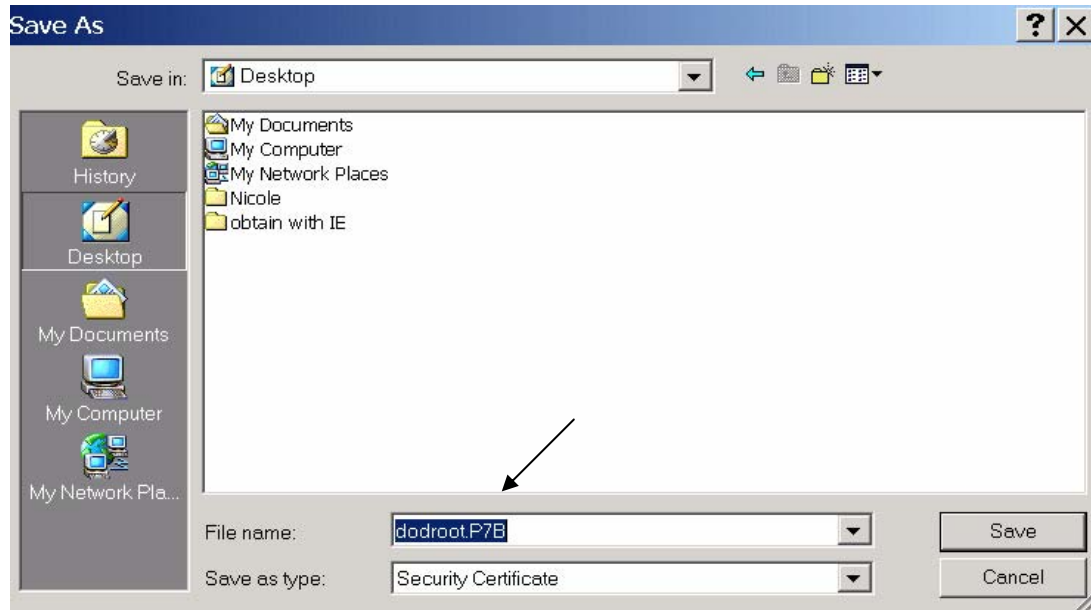
2. Click the “*Download Root CA Certificates*” link on the left side of the webpage.



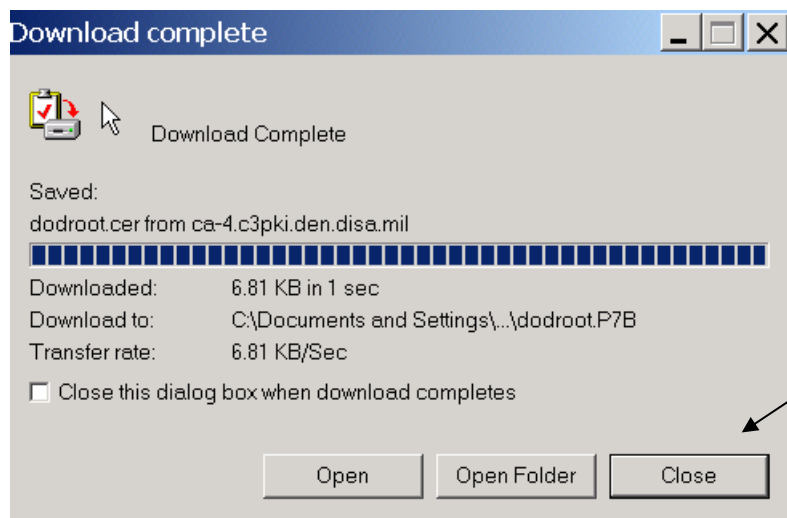
3. The User Registration page will appear. Scroll down to the bottom of the page and click ***“Download Class 3 Root CA Certificate”***.



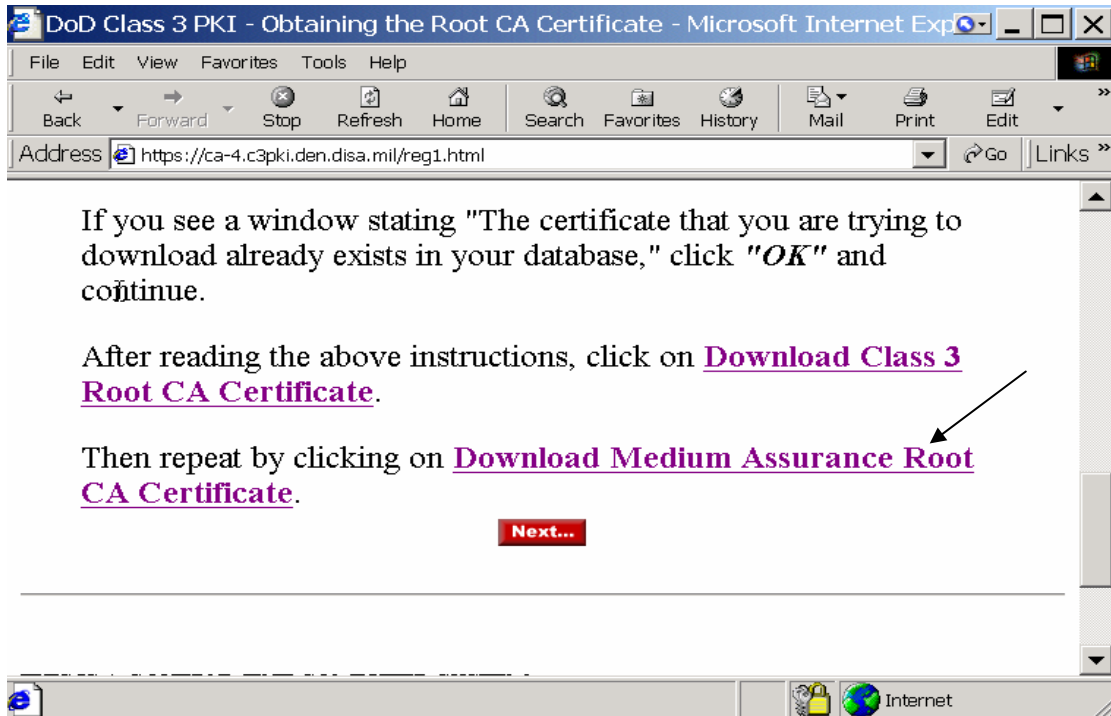
4. Click the ***“Save this file to disk”*** radio button. Click ***“OK”*** to continue.



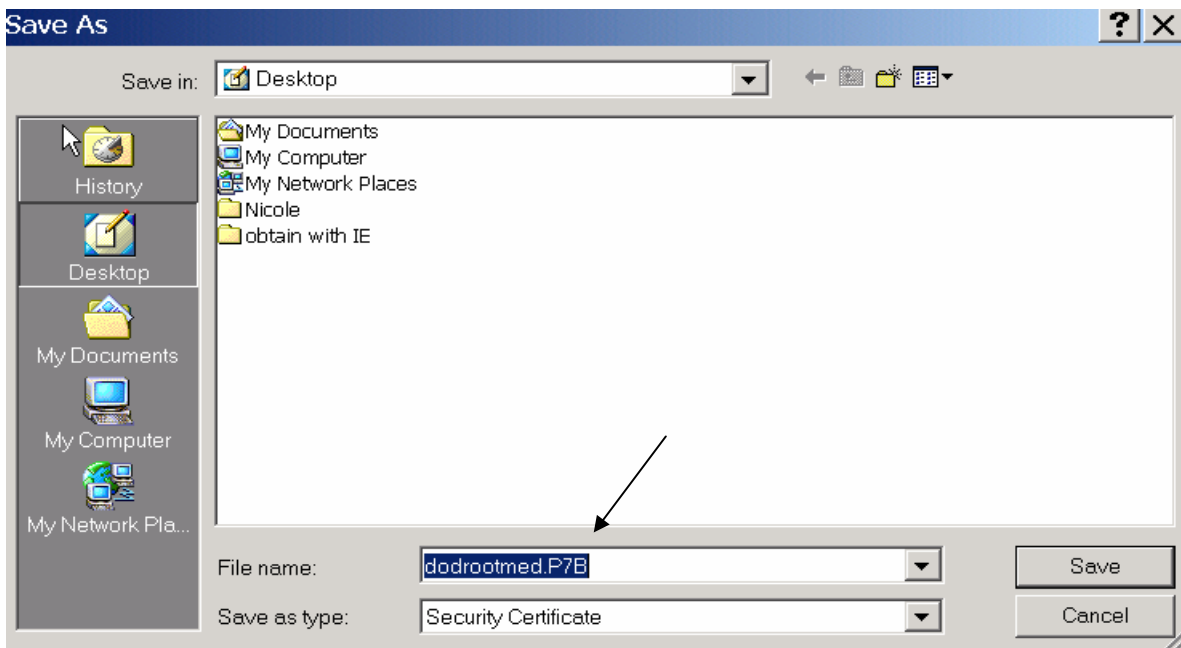
5. Select your Desktop and ensure file name is ***DODROOT.P7B*** click “***Save***”.



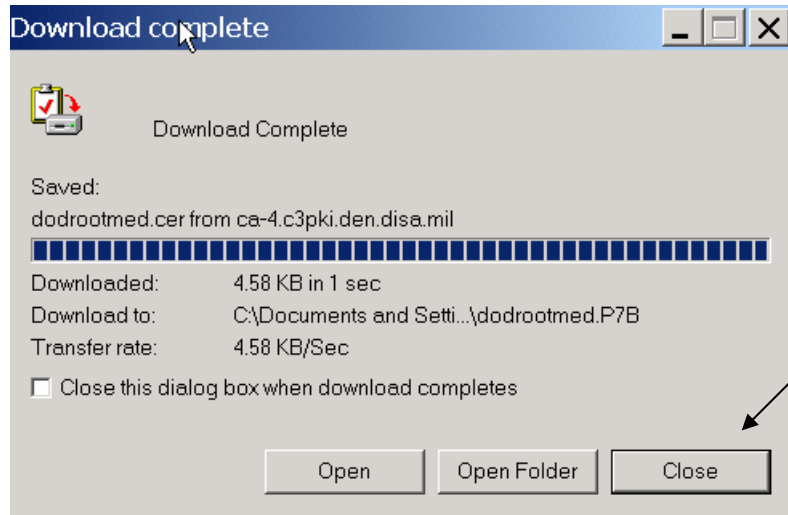
6. When you receive this message that the download is complete, click “***Close.***”



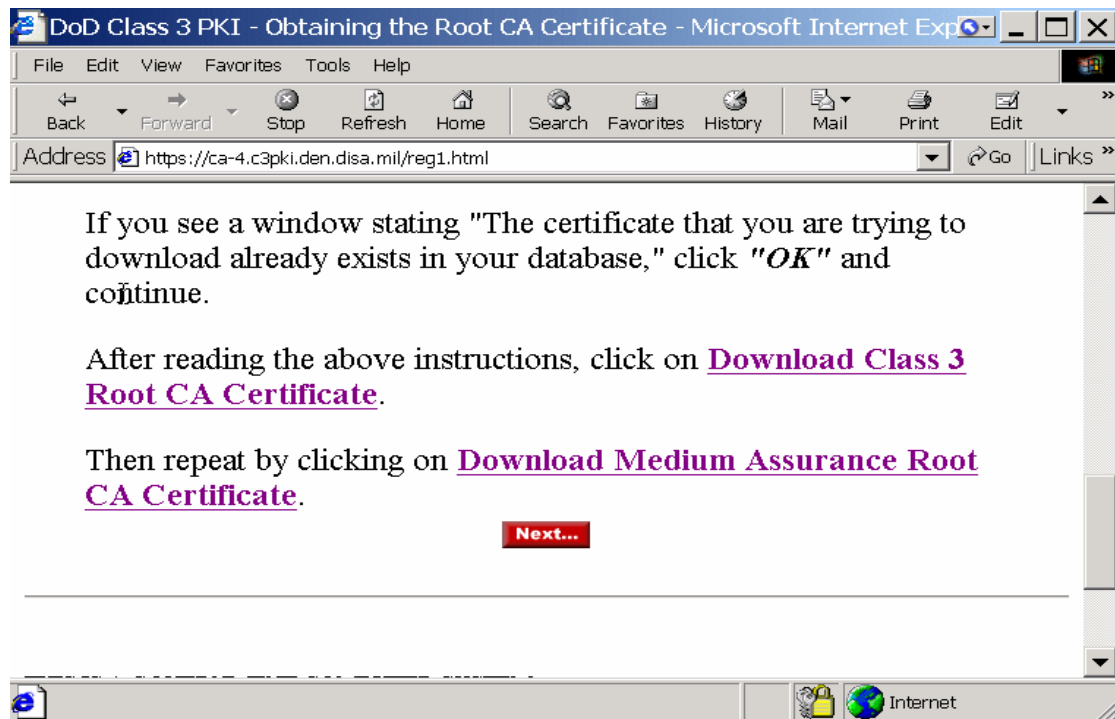
7. You will be returned to the User Registration page. Click “*Download Medium Assurance Root CA Certificate*”



8. Select your Desktop and ensure file name is *DODROOTMED.P7B* and click “*Save*”.



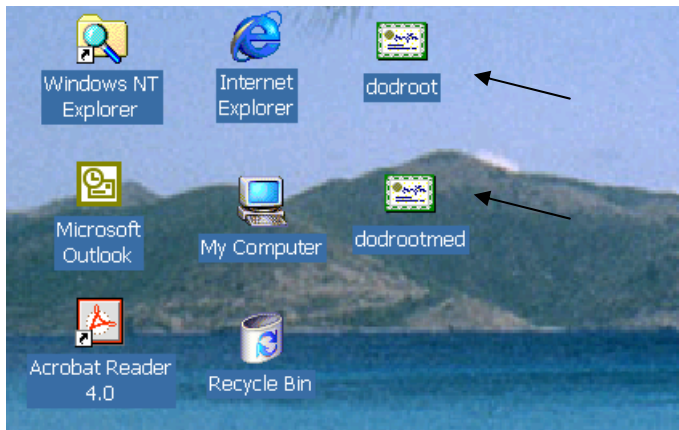
9. When you receive the message that the download is complete, click “Close”.



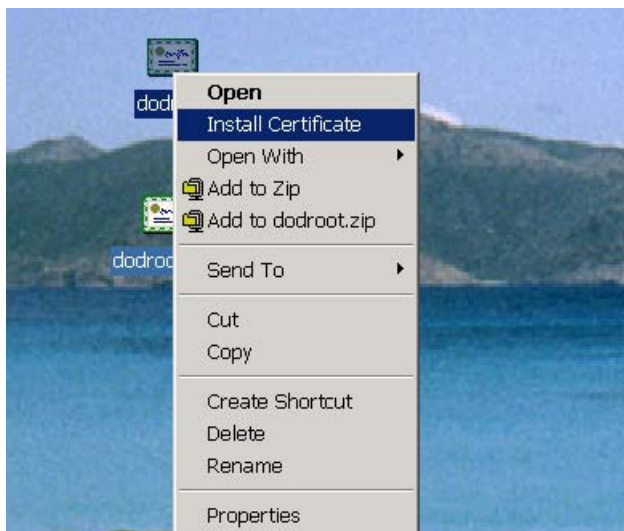
10. Certificate download is now complete. Click the “X” to close the window.



6.5.3 Installing Root Certificates



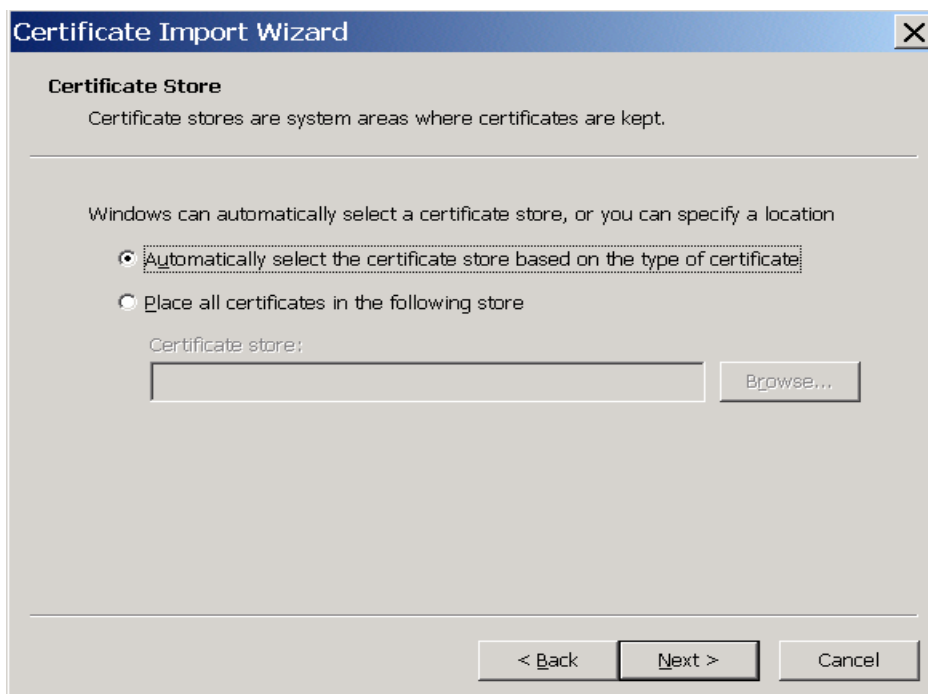
1. There should be 2 certificates saved on your desktop: ***DODROOT.P7B*** and ***DODROOTMED.P7B***.



2. For Outlook 2000 users: Right-click DODROOT.P7B and choose “***Install Certificate***”.
For Outlook 98 users, Double-click the Certificate icon and the Installation Wizard will begin.



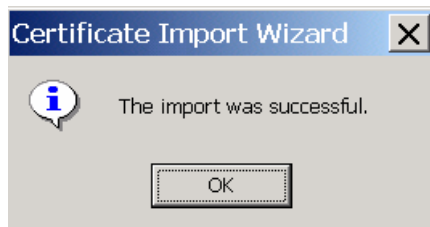
3. The Certificate Import Wizard will start. Click “Next”.



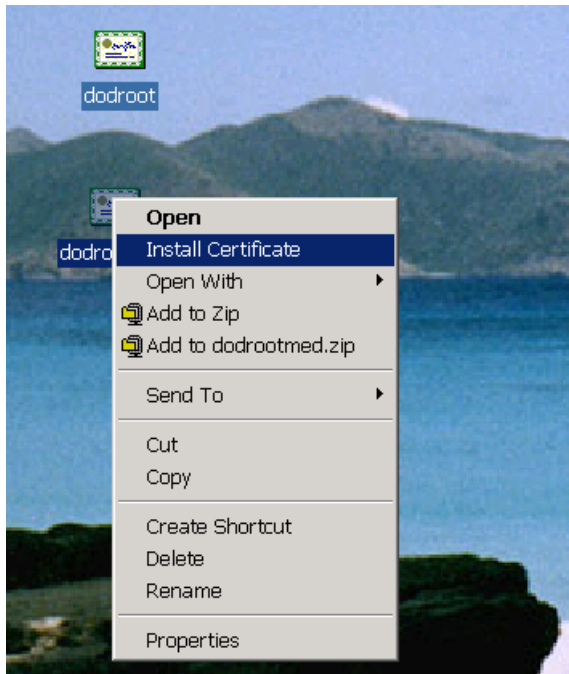
4. Accept the default of “Automatically select the certificate store based on the type of certificate” radio button. Click “Next”.



5. Click “**Finish**” to complete the DODROOT certificate import.



6. The Certificate Import Wizard should display this message stating the import was successful. Click “**OK**”.

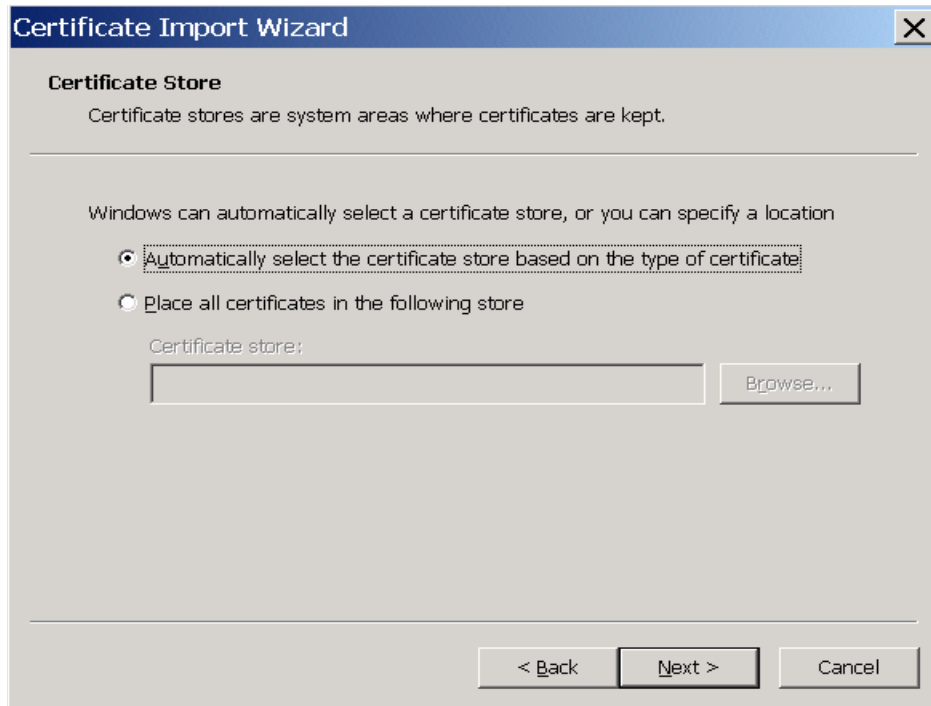


7. For Outlook 2000 users, Right click **DODROOTMED.P7B** and choose “**Install Certificate**”.

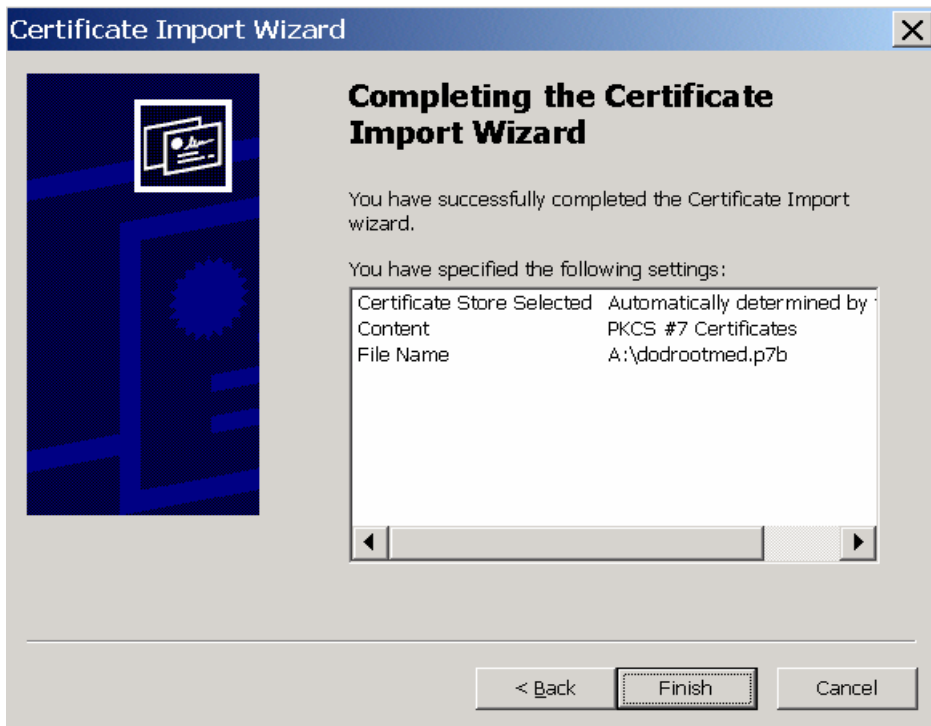
For Outlook 98 users, Double-click the icon and the Installation Wizard will begin.



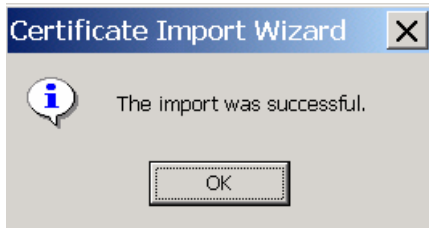
8. The Certificate Import Wizard will start. Click “**Next**”.



9. Accept the default of “*Automatically select the certificate store based on the type of certificate*” and then click “*Next*”.



10. Click “*Finish*” to complete the DODROOTMED certificate import.

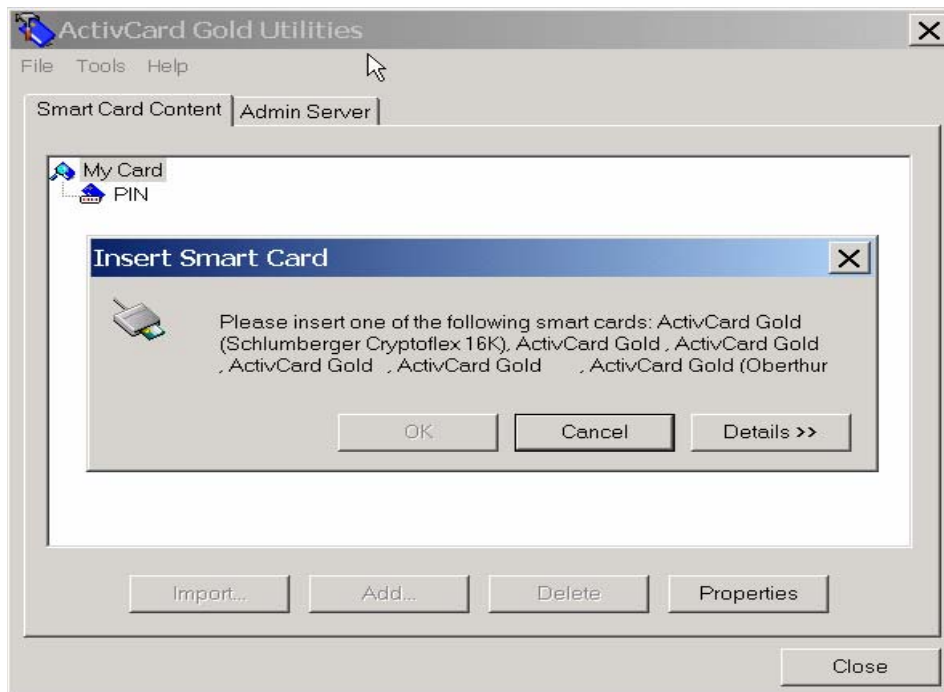


11. The Certificate Import Wizard should display this message stating the import was successful. Click “**OK**”.

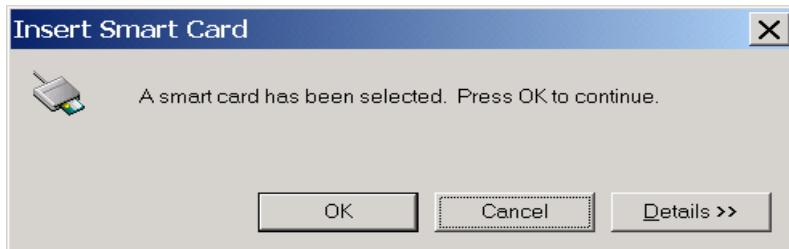
6.6 Registering CAC PKI Certificates



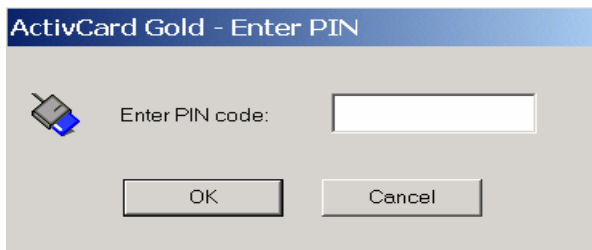
1. Double click the **ActivCard icon** (looks like a smart card reader) displayed in the Windows SysTray or run **ActivCard Gold Utilities** from the Windows Start/Programs menu. The ActivCard icon was placed in the SysTray during the ActivCard 2.0 Middleware installation.



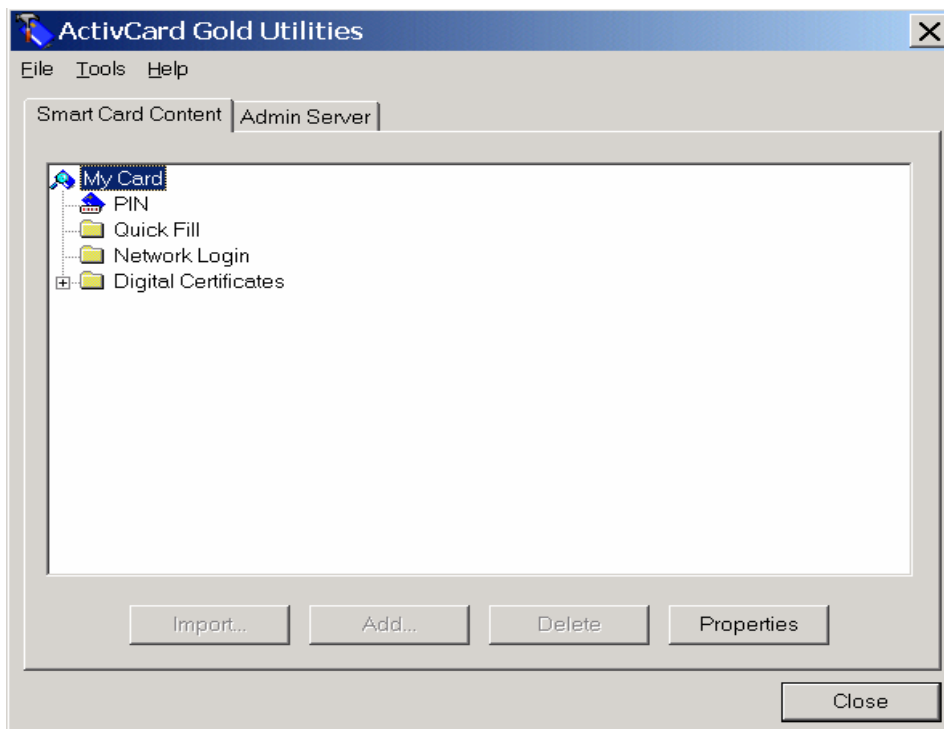
2. After launching the ActivCard Gold Utilities, insert your CAC into the smart card reader. The “**OK**” button will be highlighted once the CAC is recognized by the card reader.



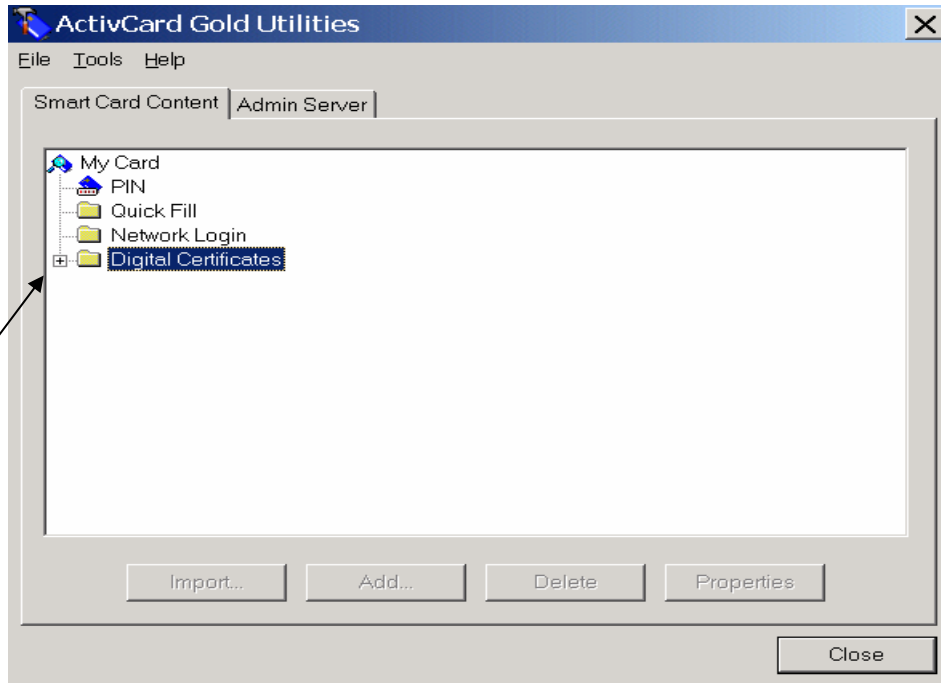
3. Click “**OK**” to continue.



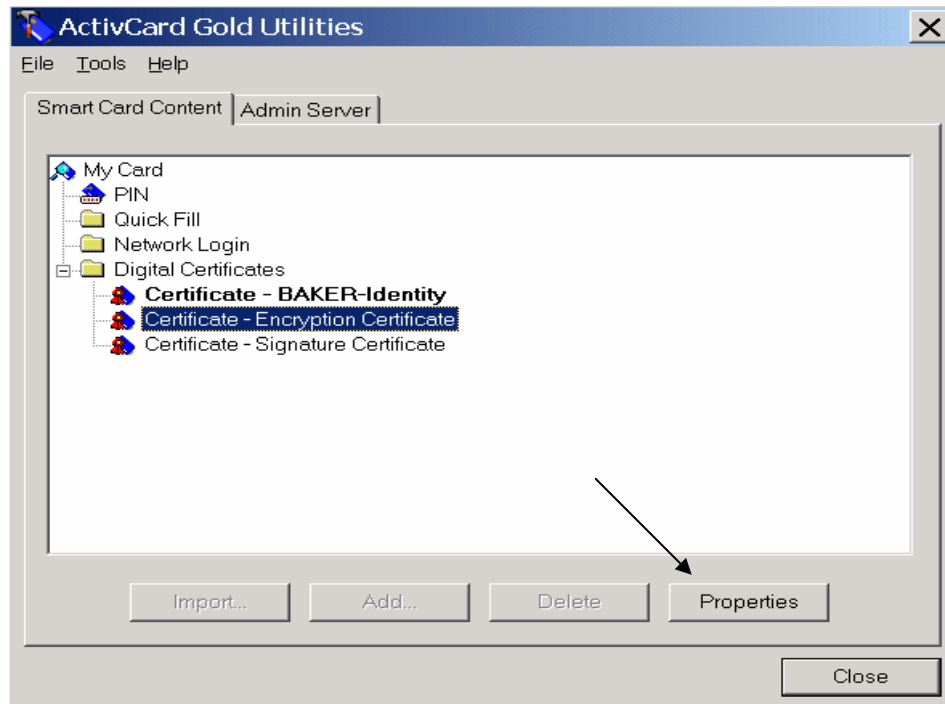
4. You will be prompted to provide a PIN (personal identification number). This PIN was chosen when the CAC was issued. Enter the **PIN** and click “**OK**”.



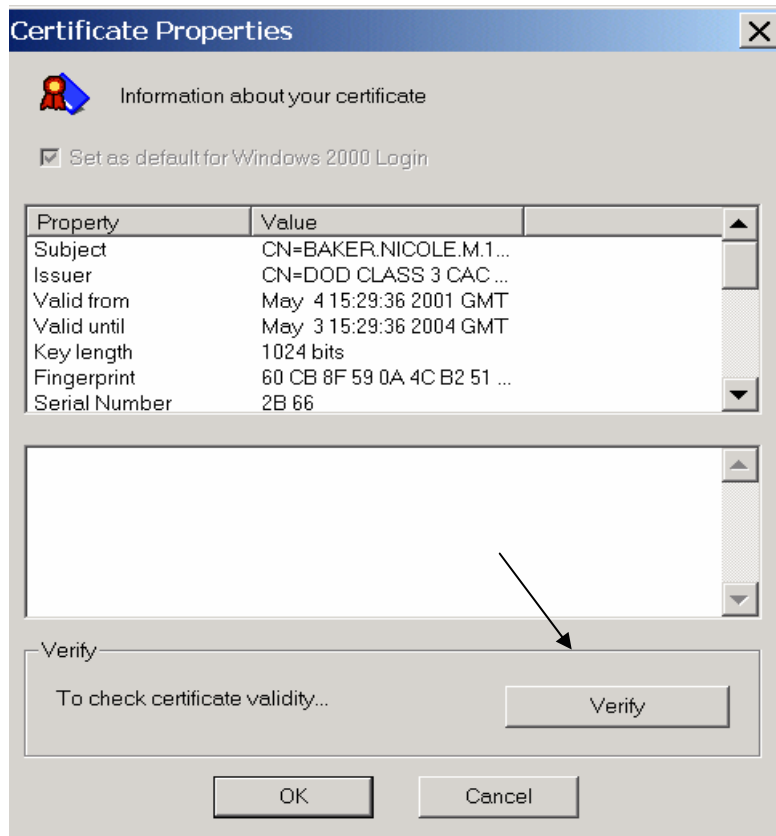
5. The ActivCard Gold Utilities window will appear.



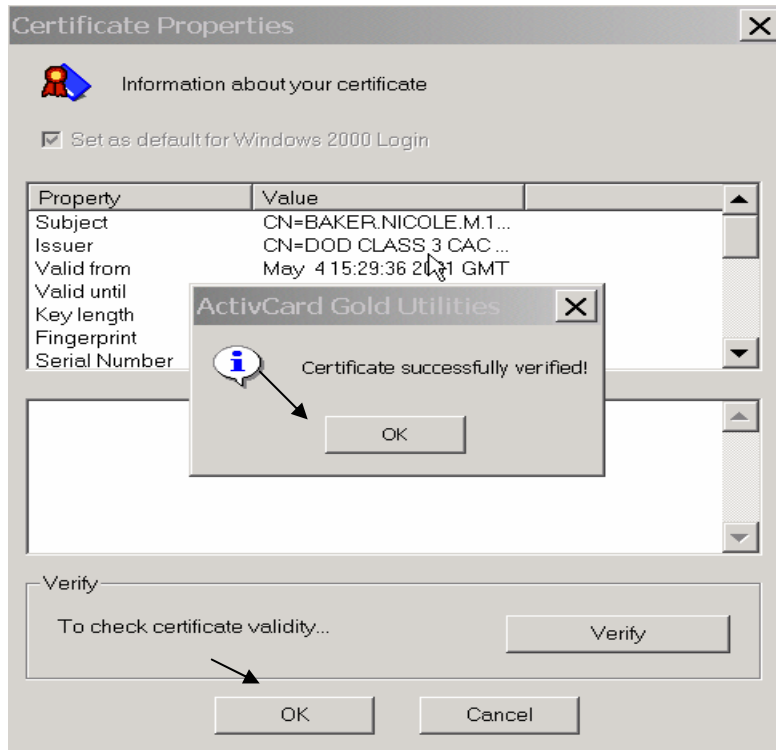
6. Click the “+ sign” to expand the Digital Certificates folder so the certificates on the CAC can be viewed.



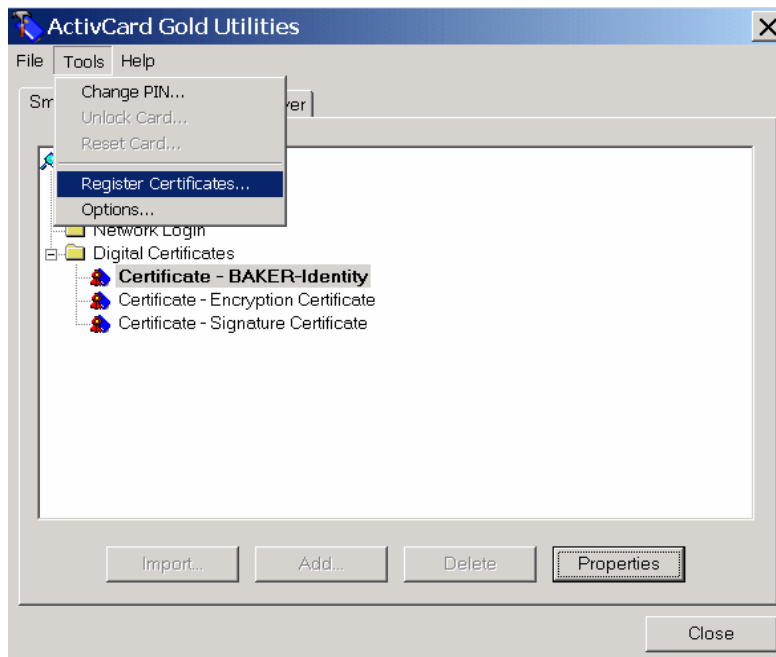
7. Highlight a certificate and click “*Properties*” to verify details of the certificates.



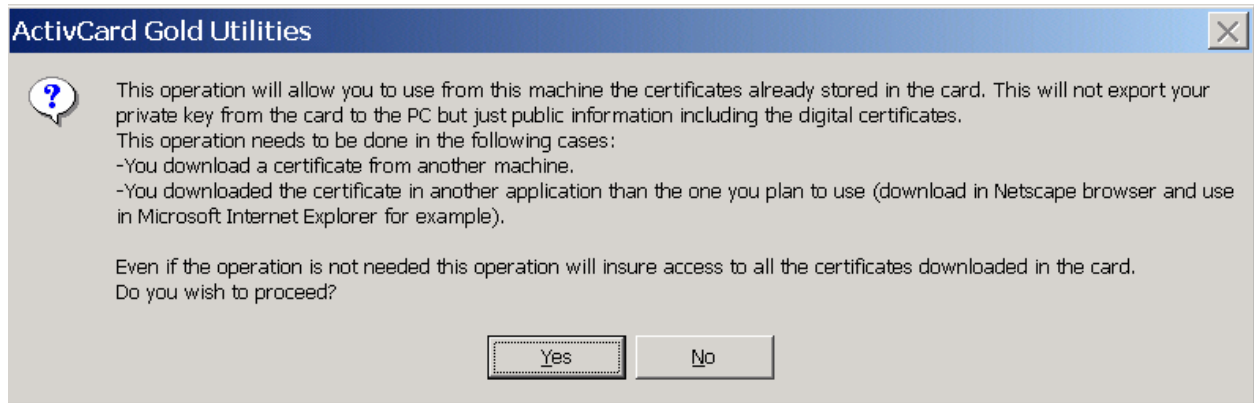
8. Click “*Verify*” to verify the Certificate.



9. Once verification is complete, click **”OK”** to close the Verification message. Close the Properties window by clicking **”OK”**. You may do this for each of the Certificates.



10. To register all Certificates, click the **”Tools”** menu then click **”Register Certificates”**.



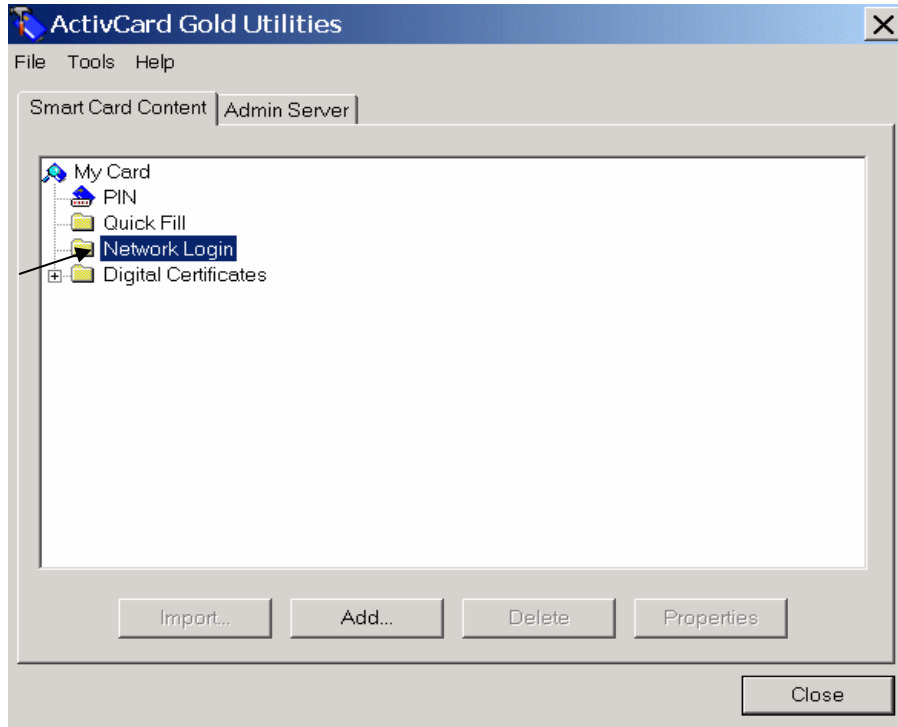
11. Click “**Yes**” to proceed.



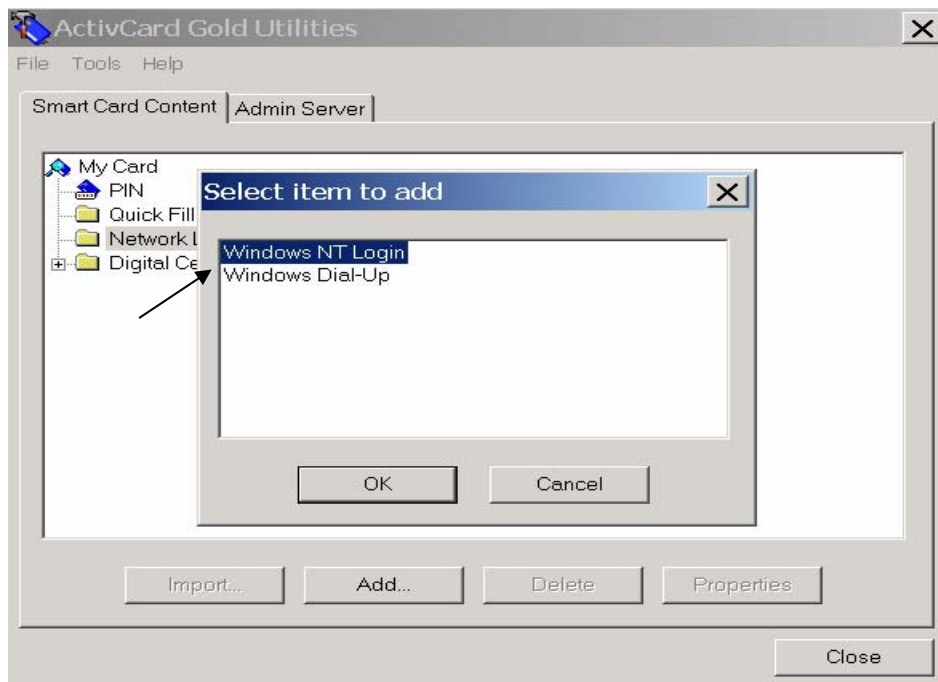
12. To complete Certificate installation click “**OK**”.



NOTE: *The use of the Network Login feature will be determined by Site/DOIM/Unit policy.*



13. To configure Network Login, click the “*Network Login*” folder then click “*Add*”.



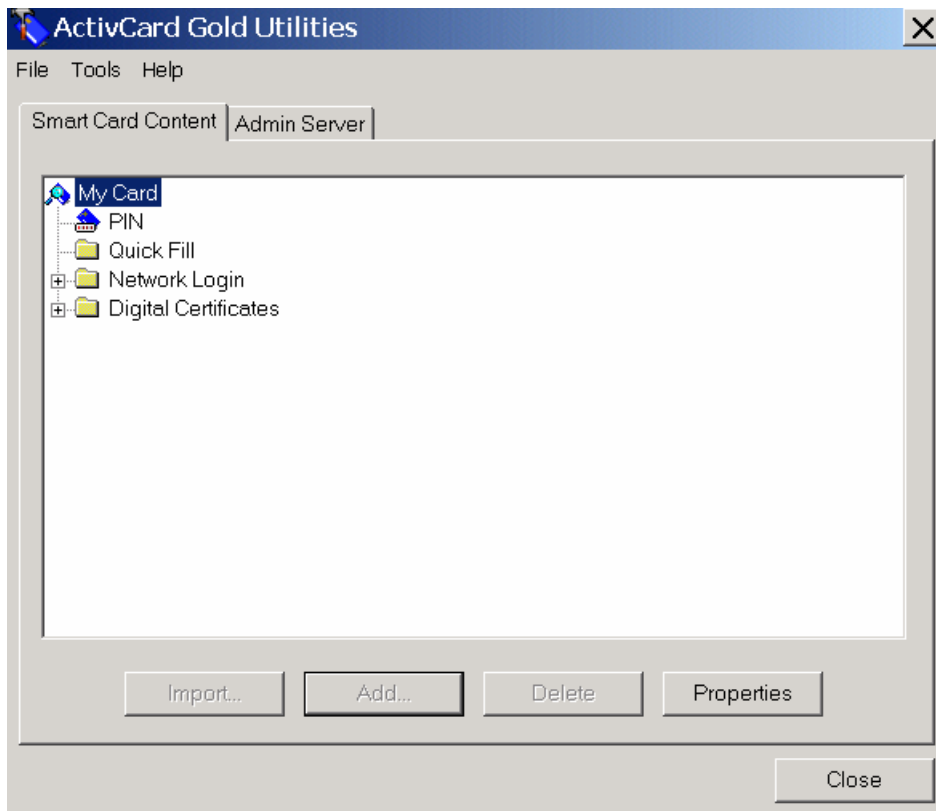
14. Highlight “*Windows NT Login*” then click “*OK*”.



15. Enter **Username**, **Domain** and **Password** information. This information will be the Username, Password and Domain used for normal network login. Retype password to confirm it is correct.

*One of the features of Network Login for Windows 2000 & NT is the option to define the workstation behavior upon removal of the smart card from the card reader. If the option “Lock workstation” is selected from the drop-down menu, when the smart card is removed from the card reader the workstation will lock. If the box next to “Unlock only with smart card” is checked the workstation can only be unlocked by re-inserting the smart card and entering the PIN number.

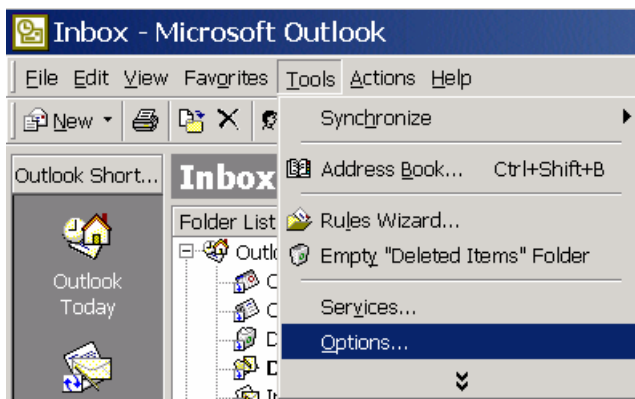
Click “**OK**” to close window.



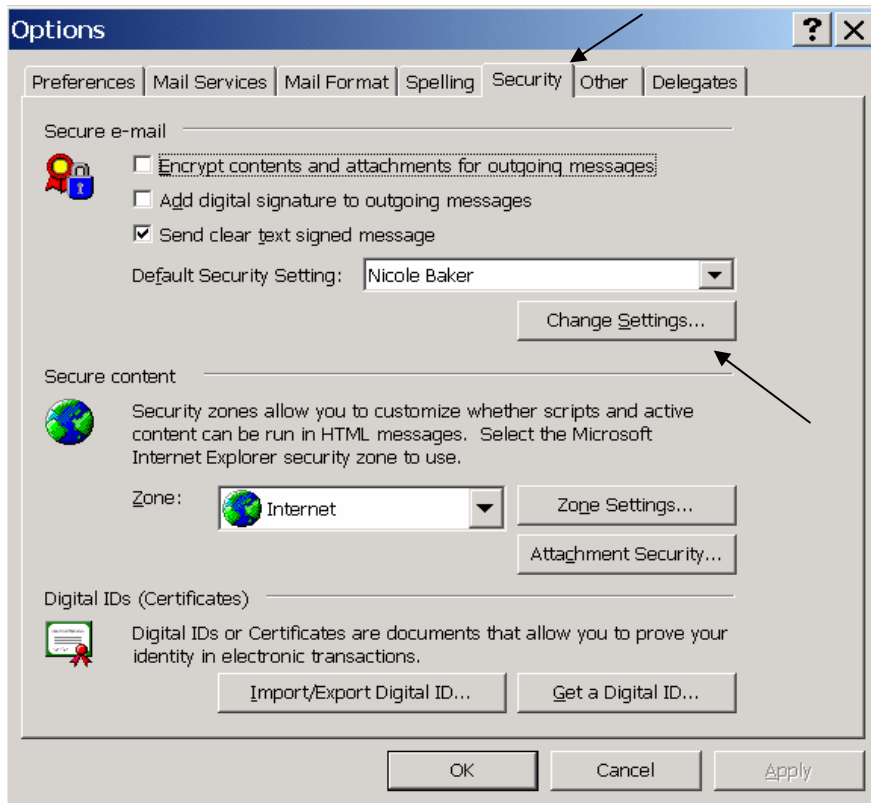
16. Click “*Close*” to complete configuration.

6.7 Configure Outlook 98/2000 Client Security Profile

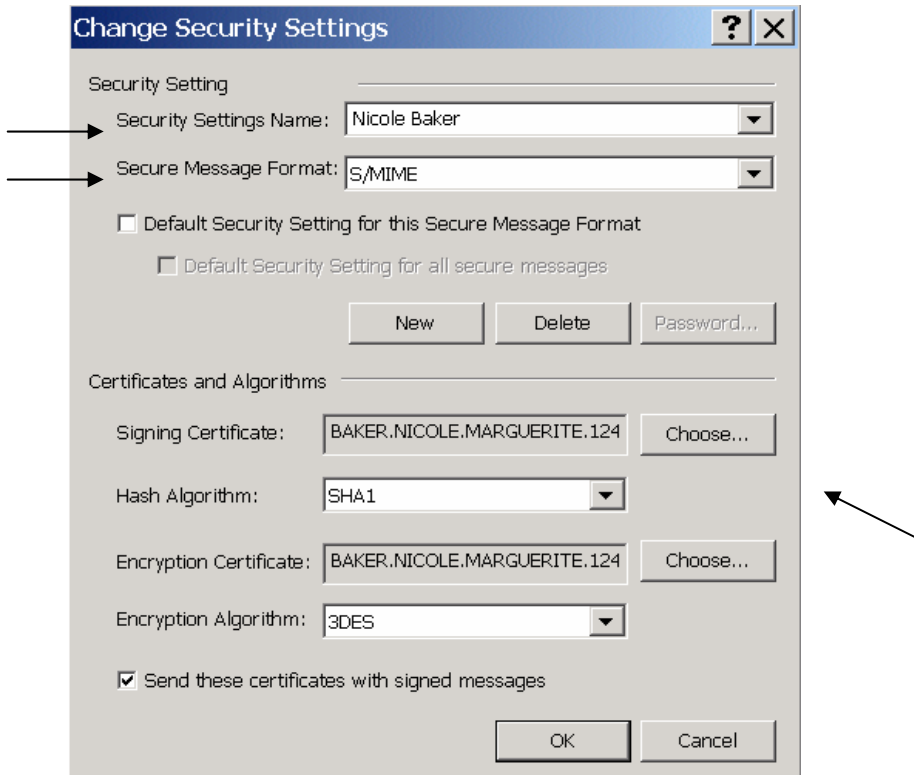
1. Open Microsoft Outlook 98/2000.



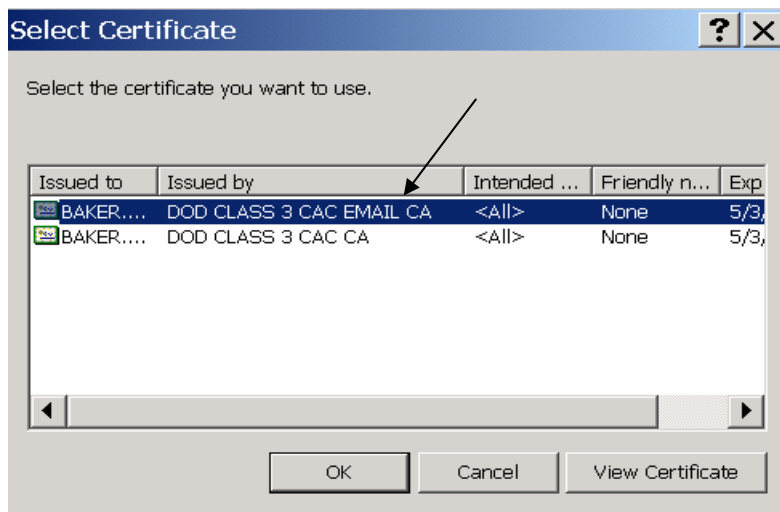
2. In the “*Tools*” pull-down menu, select the “*Options*” menu item.



3. The Options window will appear. Click on the Security tab.
Once the *Security* tab appears, click on the “*Change Settings*” button.



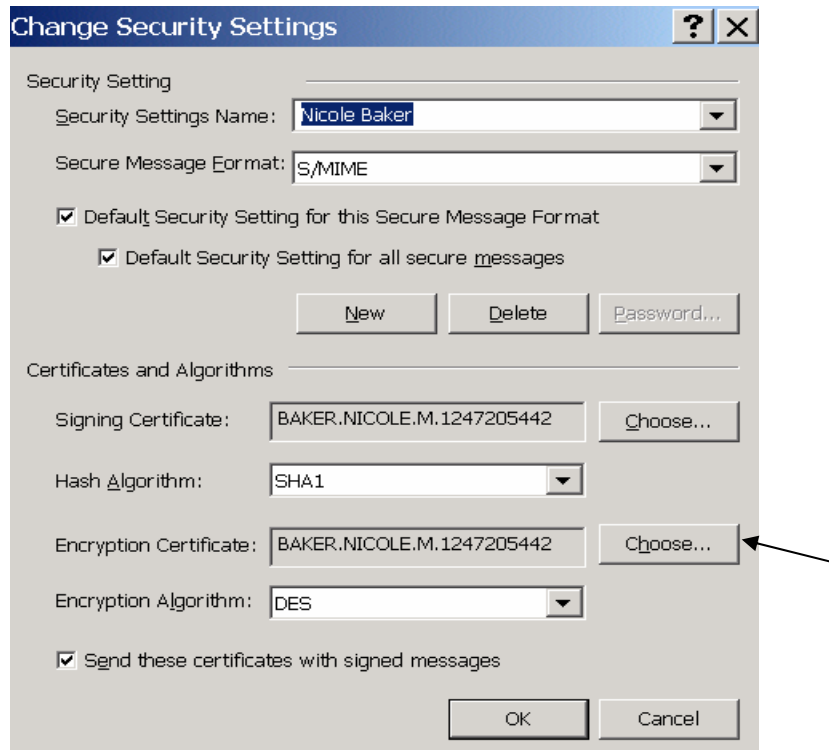
4. In the *Change Security Settings* window, type your name in the *Security Settings Name* field. Choose *S/MIME* from the drop-down menu in the *Secure Message Format* field. Click the “*Choose*” button to the right of *Signing Certificate*.



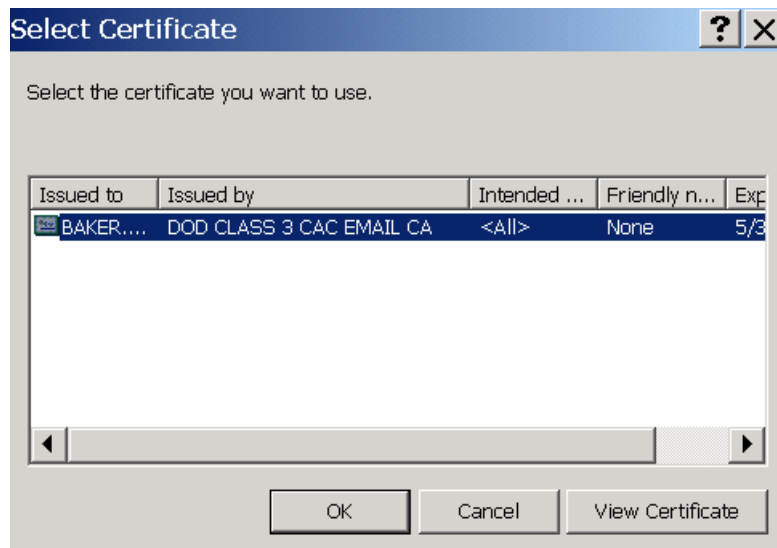
5. In the *Select Certificate* window, identify the correct certificate by examining the *Issued By* column. Highlight the Certificates issued by the *DoD Class 3 CAC Email CA*. Click the “*OK*” button to continue.

The image shows a "Change Security Settings" dialog box. It has a title bar with a question mark and a close button. The dialog is divided into two sections: "Security Setting" and "Certificates and Algorithms". In the "Security Setting" section, there are two dropdown menus: "Security Settings Name" (set to "Nicole Baker") and "Secure Message Format" (set to "S/MIME"). Below these are two checked checkboxes: "Default Security Setting for this Secure Message Format" and "Default Security Setting for all secure messages". There are three buttons: "New", "Delete", and "Password...". In the "Certificates and Algorithms" section, there are four fields: "Signing Certificate" (set to "BAKER.NICOLE.M.1247205442"), "Hash Algorithm" (set to "SHA1" with a dropdown arrow pointing to it), "Encryption Certificate" (set to "MD5"), and "Encryption Algorithm" (set to "DES"). There are two "Choose..." buttons next to the "Signing Certificate" and "Encryption Certificate" fields. At the bottom, there are two checked checkboxes: "Send these certificates with signed messages" and two buttons: "OK" and "Cancel".

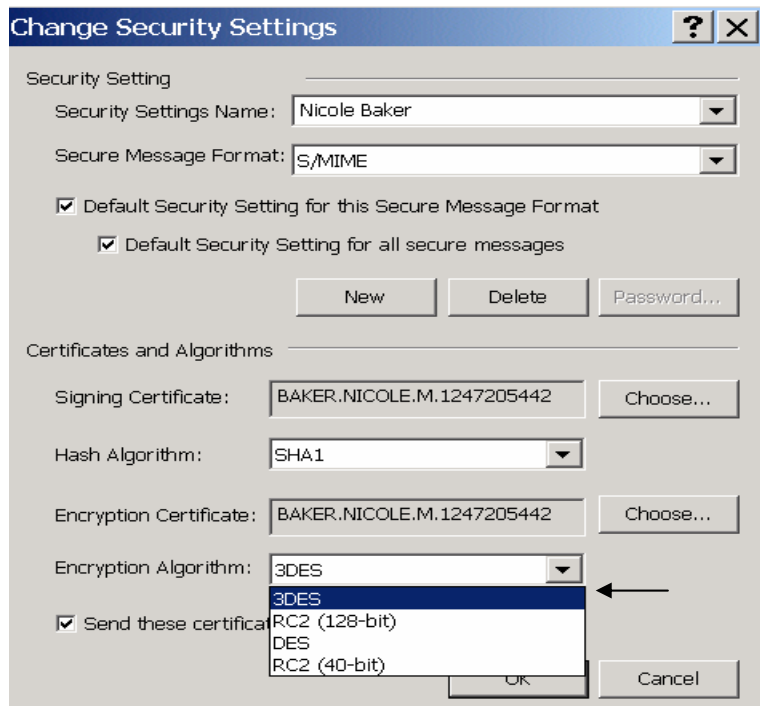
6. You will be returned to the *Change Security Settings* screen. Ensure that *SHA1* is selected in the *Hash Algorithm* drop down menu. If it is not, click on the drop down menu and select “*SHA1*”.



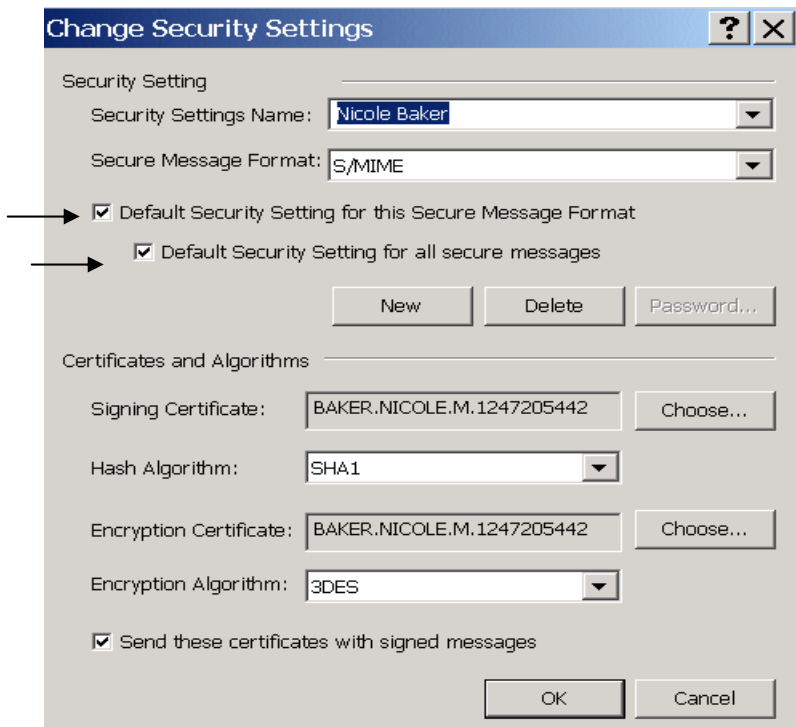
7. In the *Change Security Settings* window, click the “*Choose*” button to the right of Encryption Certificate.



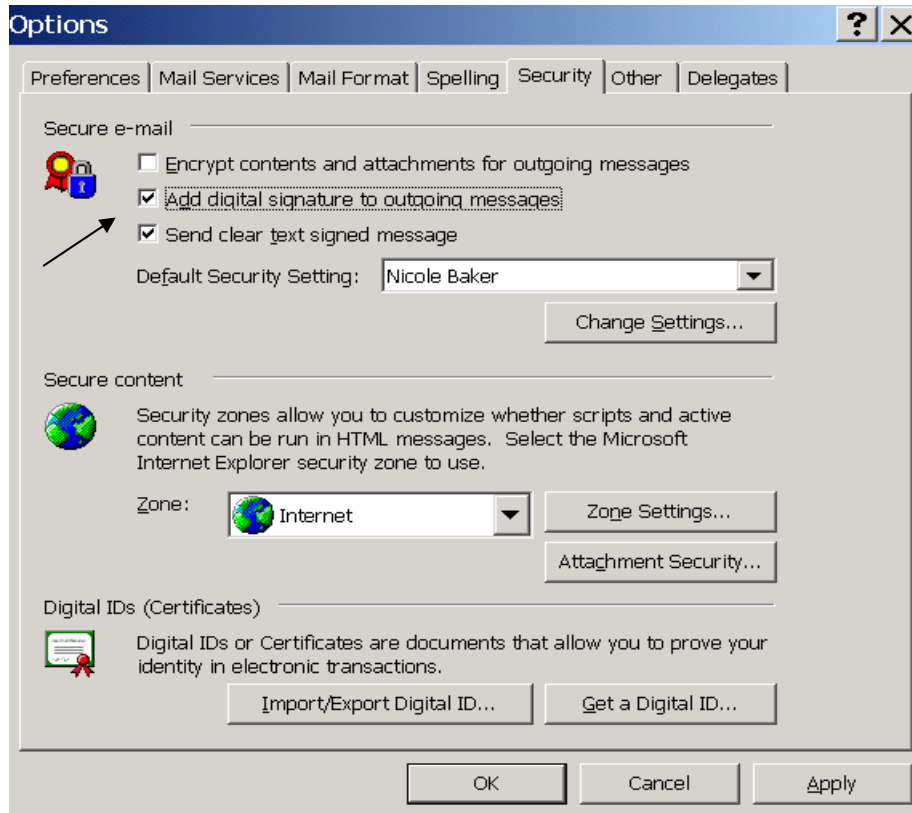
8. In the *Select Certificate* window, identify the correct certificate by examining the *Issued By* column. Highlight the Certificate issued by *DoD Class 3 CAC Email CA*. Click “*OK*.”



9. Ensure **3DES** is selected in the **Encryption Algorithm** drop down menu. If not, select **3DES** from the menu.



10. Make sure both boxes are checked under **Security Setting Preferences**. Click “**OK**” to continue.

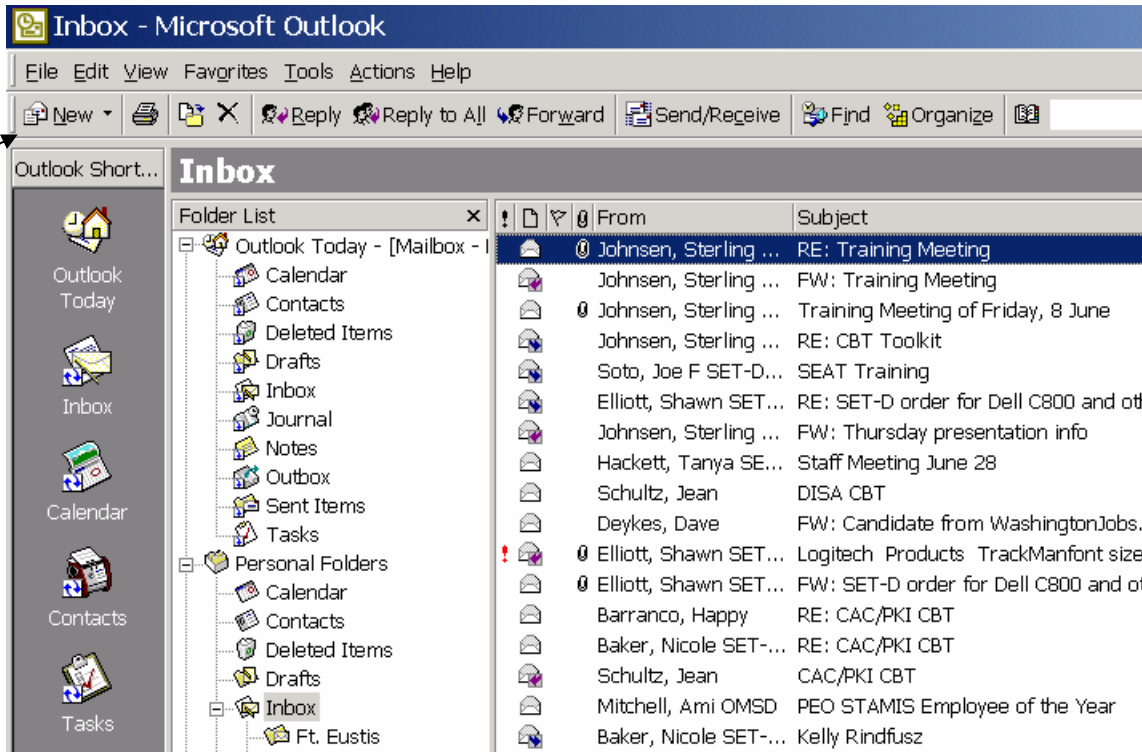


11. You will be returned to the *Options* window showing the *Security* tab. Enable the check box next to “*Add digital signature to outgoing messages*”. This will automatically sign every message you send. Ensure that the “*Send clear text signed message*” check box is also enabled.

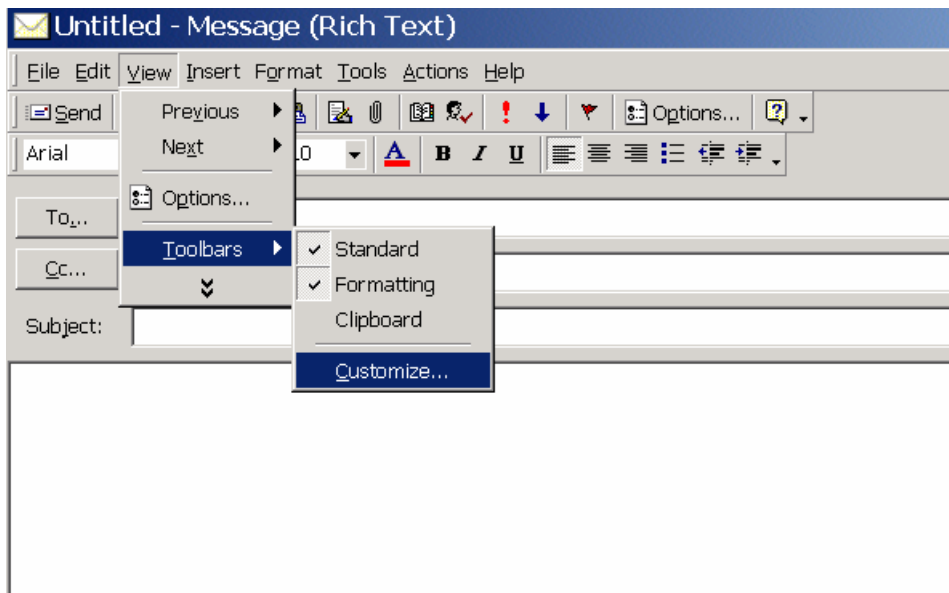
12. Click “OK” button to close the window.

Adding Signing and Encrypting Icons to the Toolbar

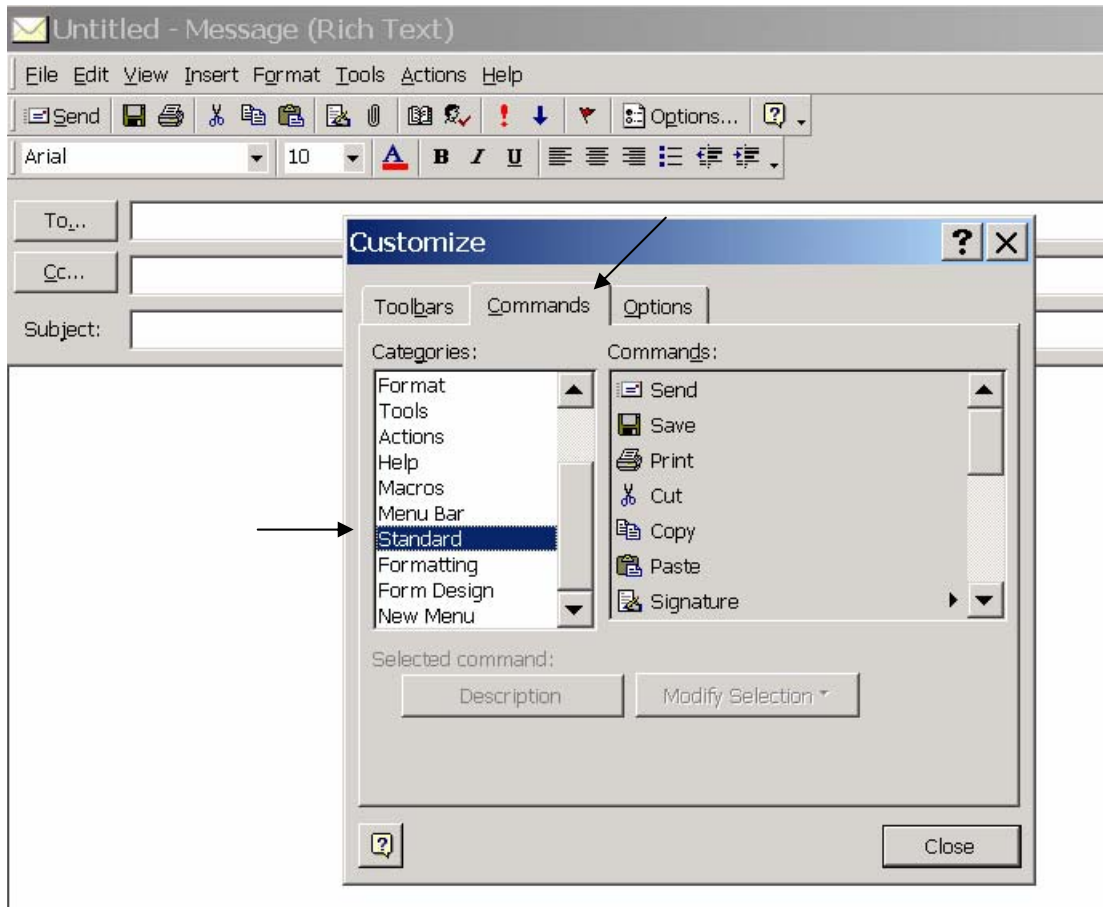
An optional step is to add Signing and Encrypting icons to your toolbar.



1. Open a New Mail Message by clicking the “*New*” button in the top left of the Outlook window.



2. Once the New Mail Message opens, click “*View*”, choose *Toolbars*, then *Customize*.



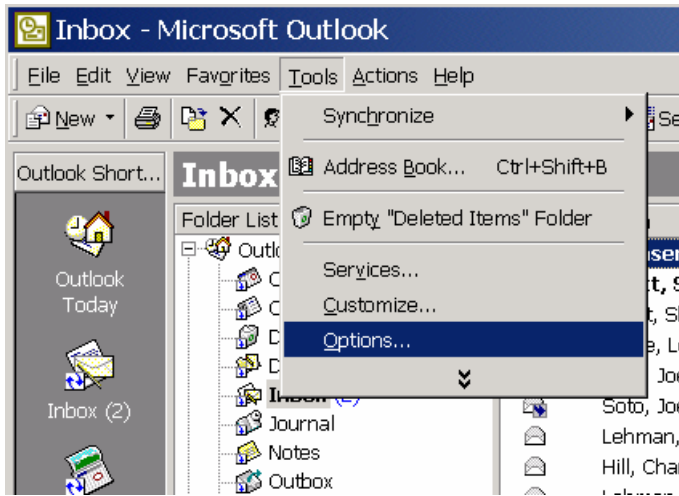
3. Make sure the *Commands* tab is chosen. Click “*Standard*” under the *Categories:* menu. Scroll through the list of choices under the *Commands* menu. Look for the “*Encrypt Message Contents and Attachments*” icon and the “*Digitally Sign Message*” icon in the menu choices.

NOTE: If the “*Encrypt Message Contents and Attachments*” icon and the “*Digitally Sign Message*” icon are NOT present in this menu, you may have MS Word selected as your Email Editor. When this option is chosen, you cannot customize the toolbar with the Signing and Encrypting icons. Complete the additional steps below to turn off this functionality and then place the icons on your toolbar.

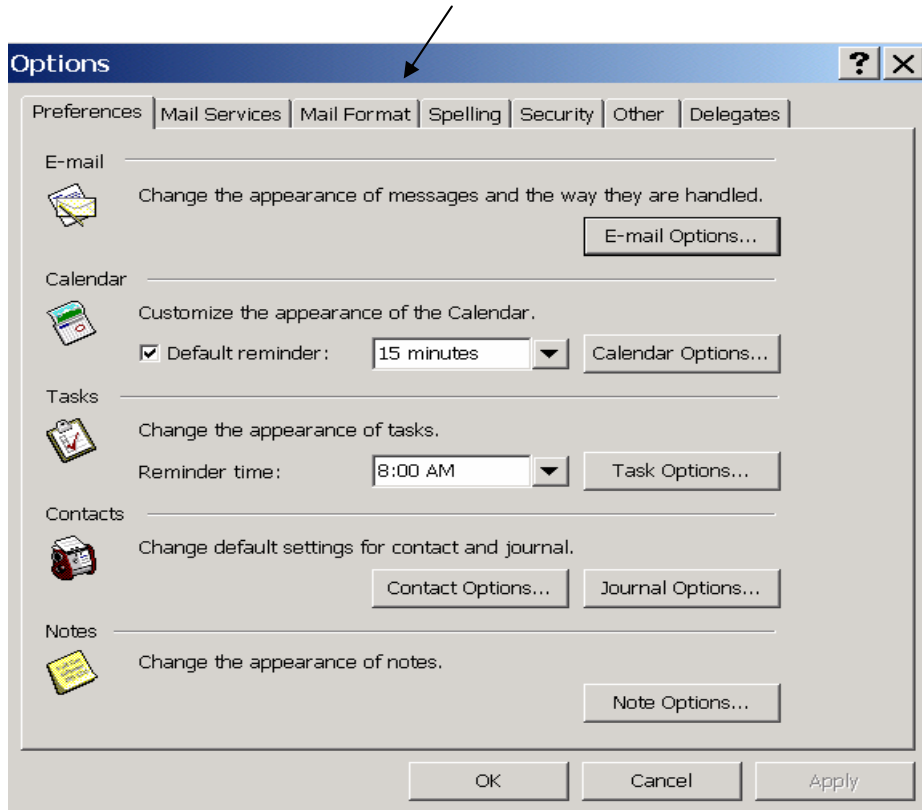
If the icons are in the *Commands* menu, continue to #4.



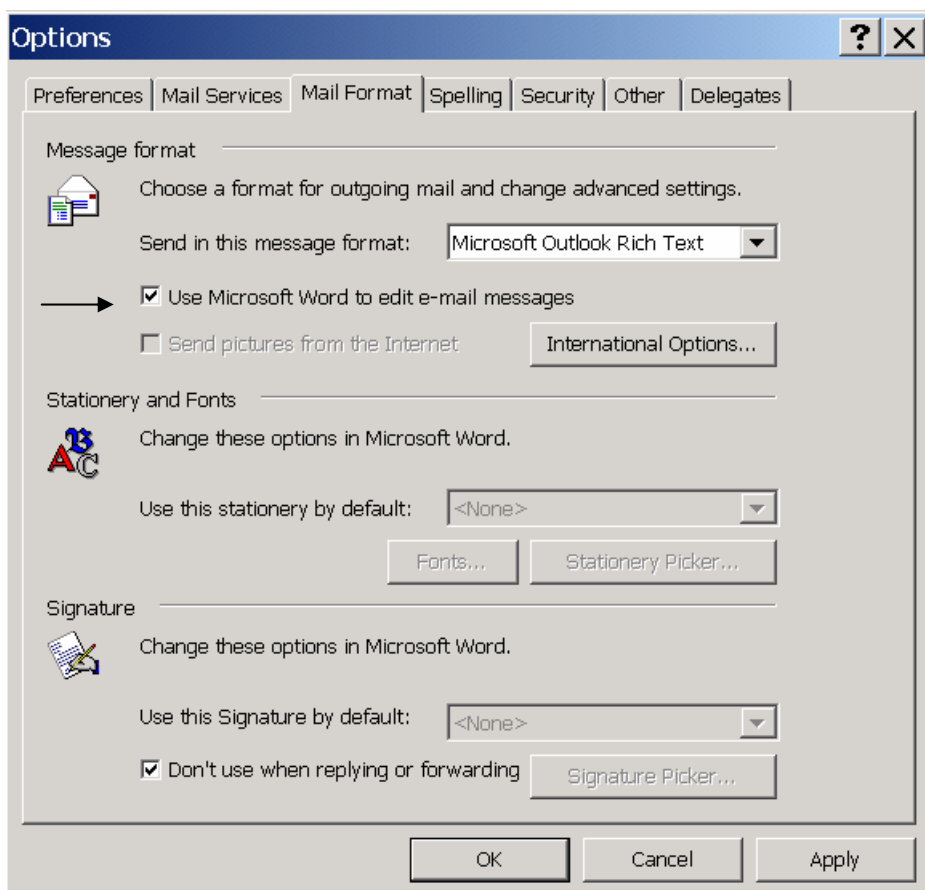
To turn off MS Word as an Email Editor:



In the “*Tools*” pull-down menu, select the “*Options*” menu item.

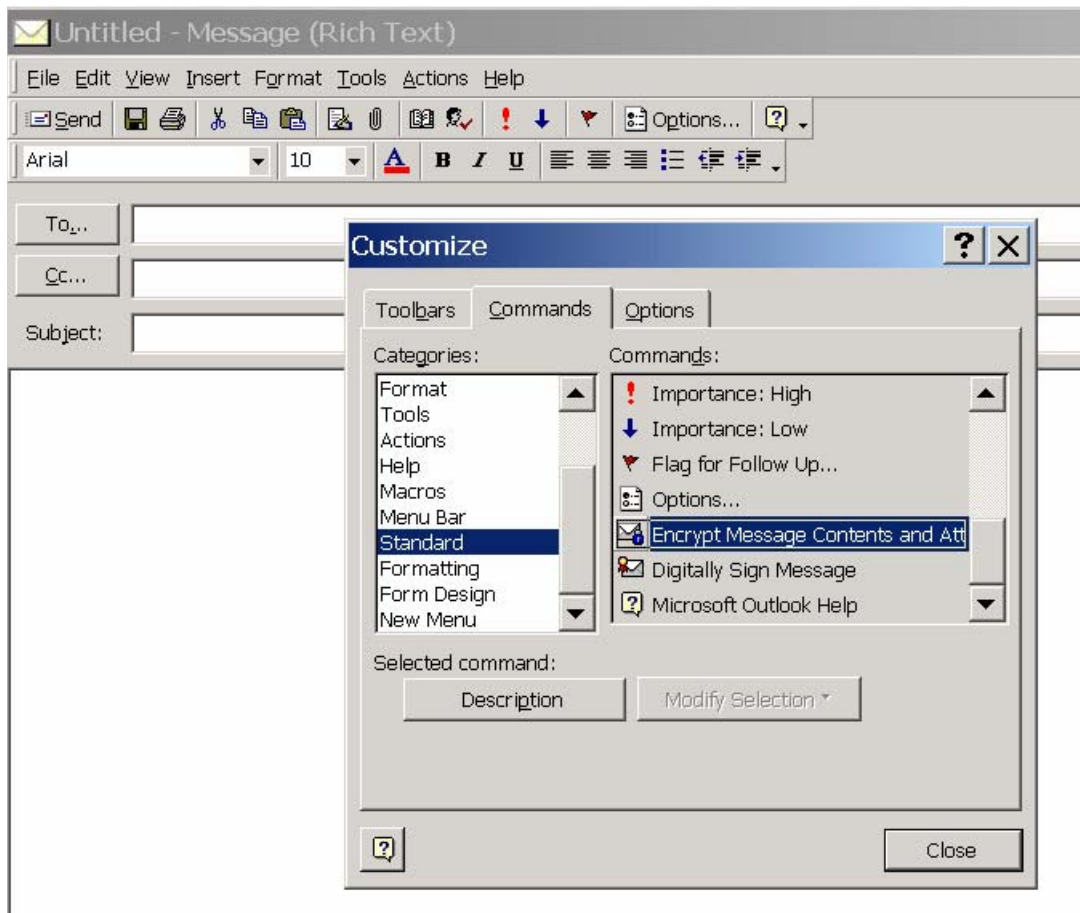


Click the “*Mail Format*” tab.

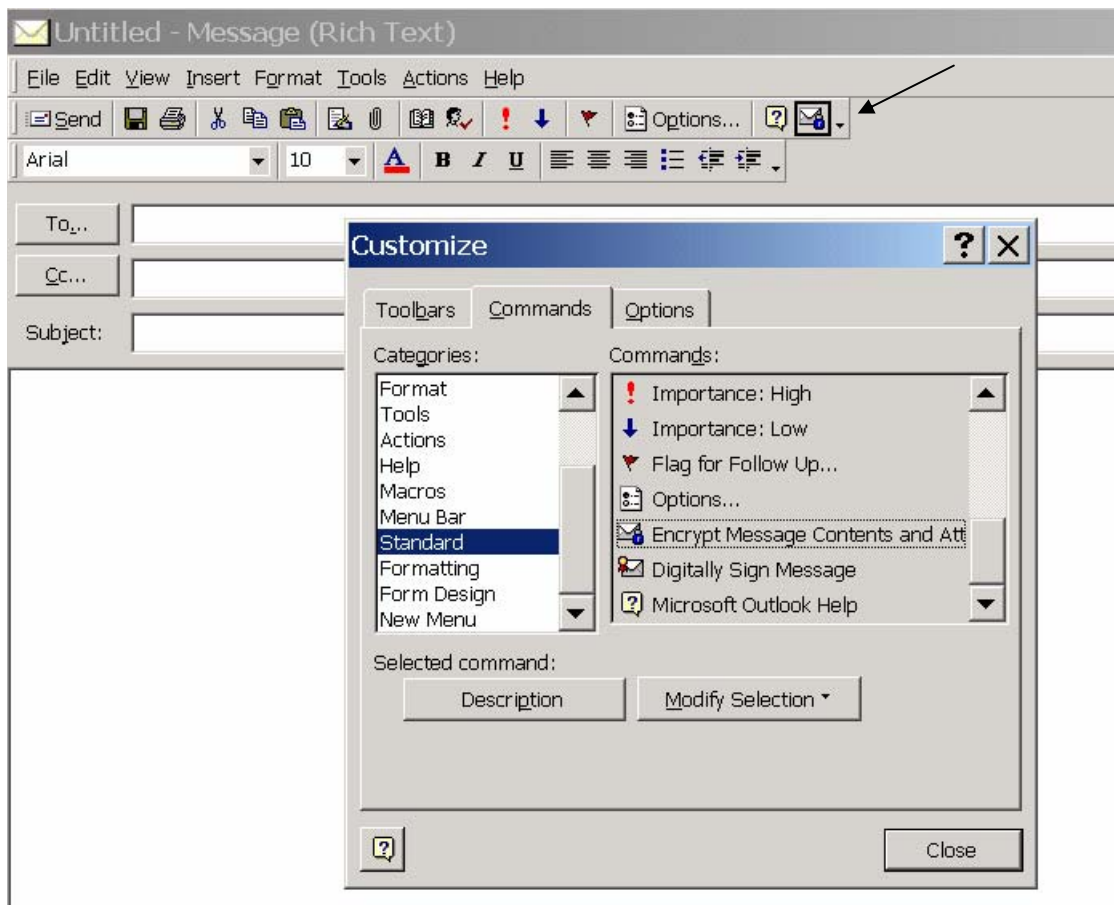


Uncheck the box next to “Use Microsoft Word to edit my e-mail messages”. Click “OK” to close the window.

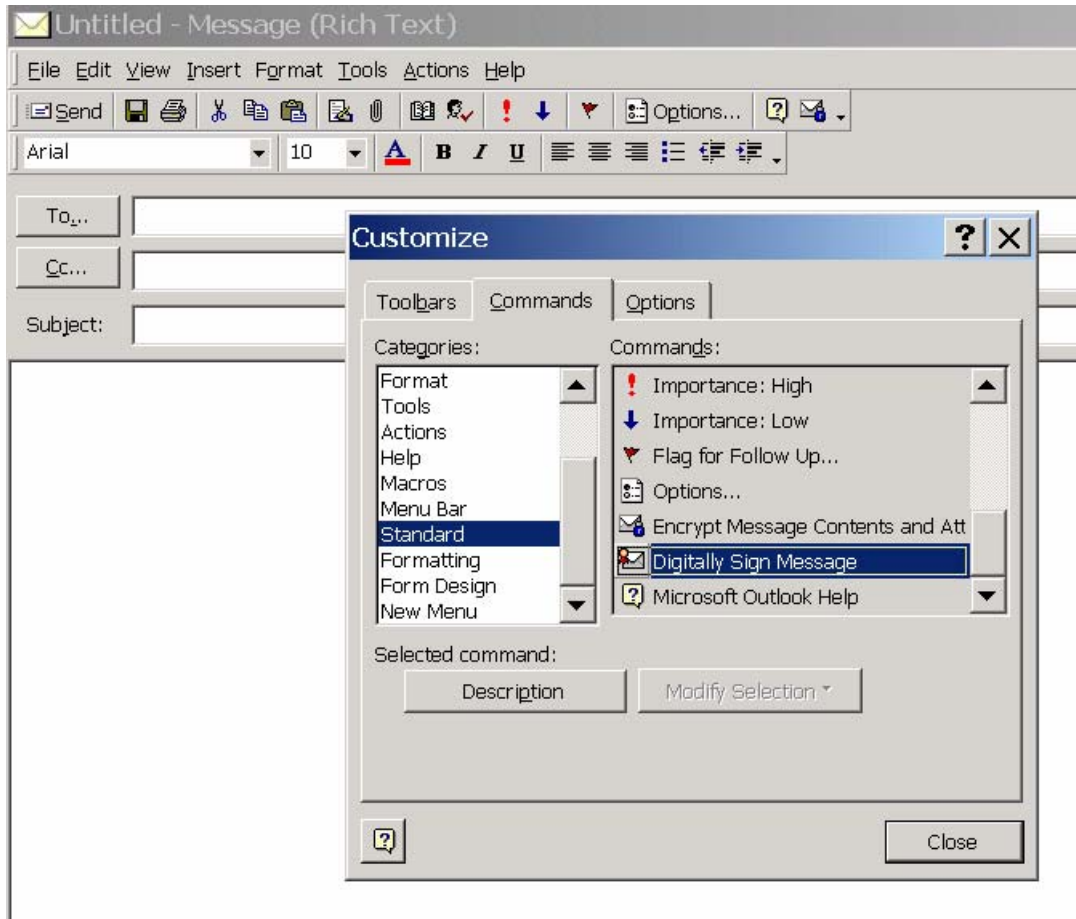
Continue with the following instructions to place the Signing and Encrypting Icons on your toolbar.



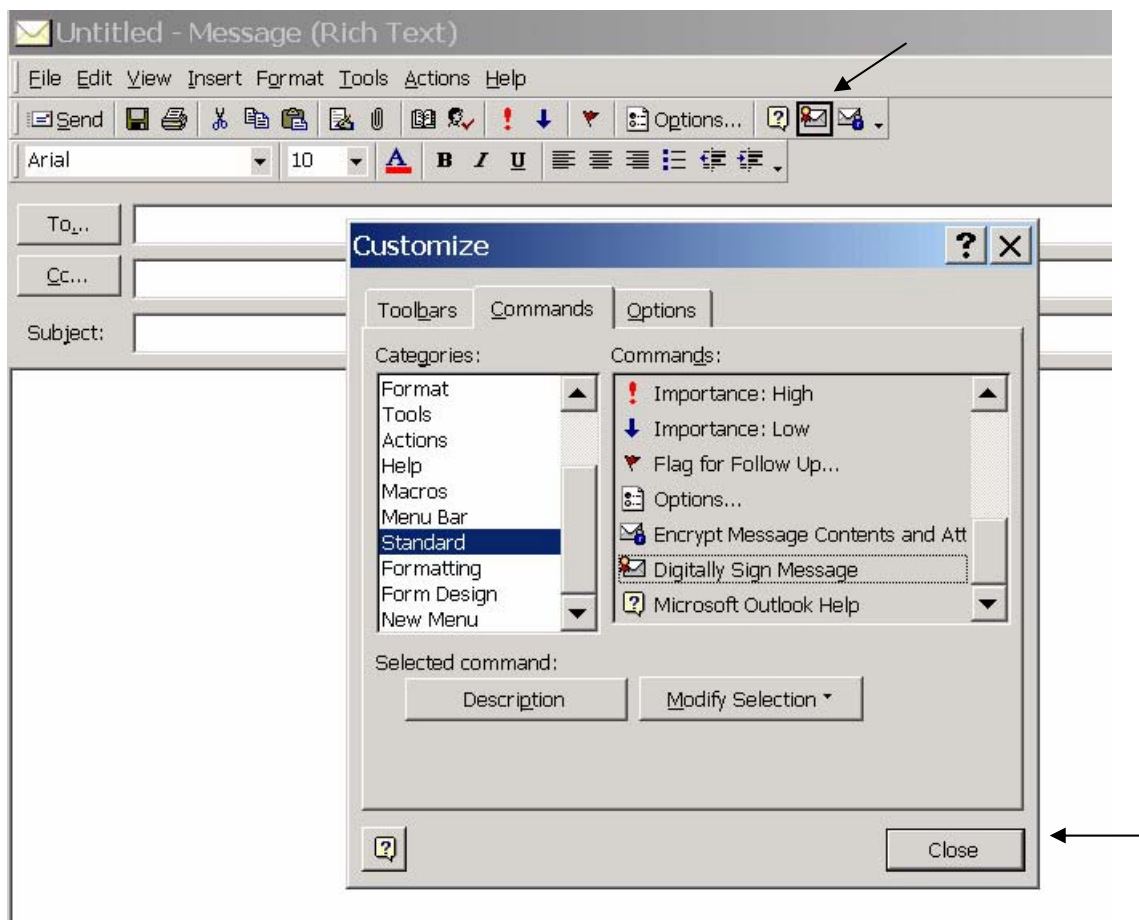
4. Scroll through the list of commands. Click on “*Encrypt Message Contents and Attachments*.”



5. Drag and drop this icon on top of your toolbar.



6. Click on “*Digitally Sign Message*”.



7. Drag and drop this icon onto your toolbar.
8. Click “*Close*”.

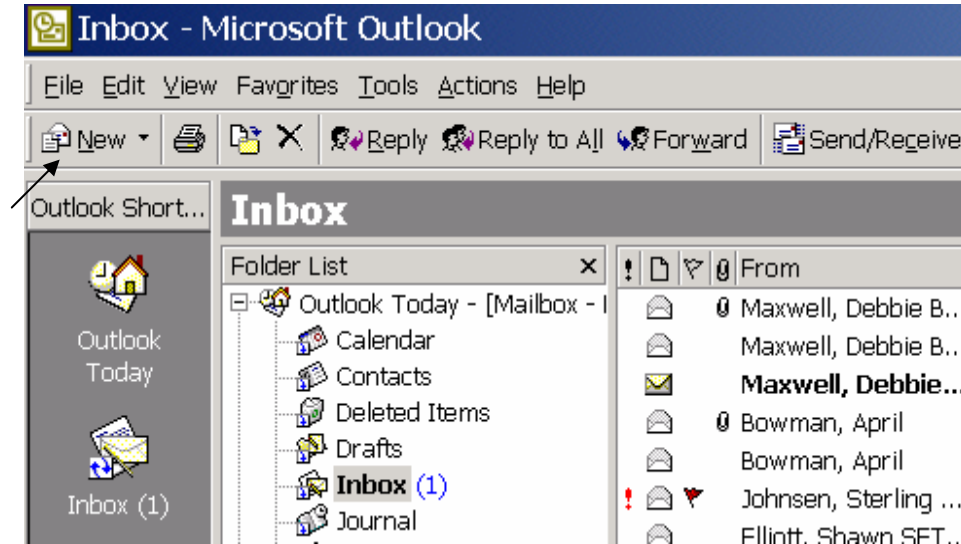
Both icons should appear on this toolbar every time you open a *New Mail Message*.



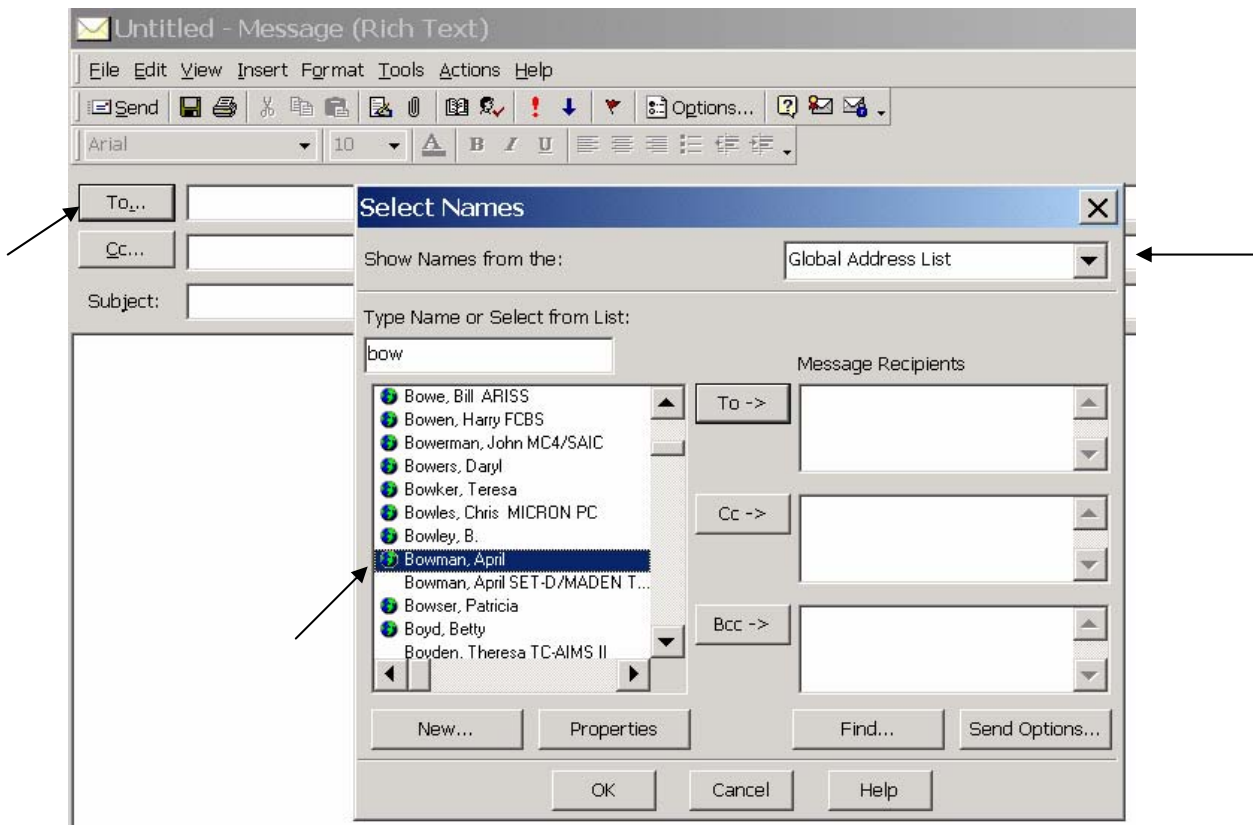
7 Functional Training Scenarios

7.1 Sending and Receiving Digitally Signed and Encrypted Email

7.1.1 Sending Email



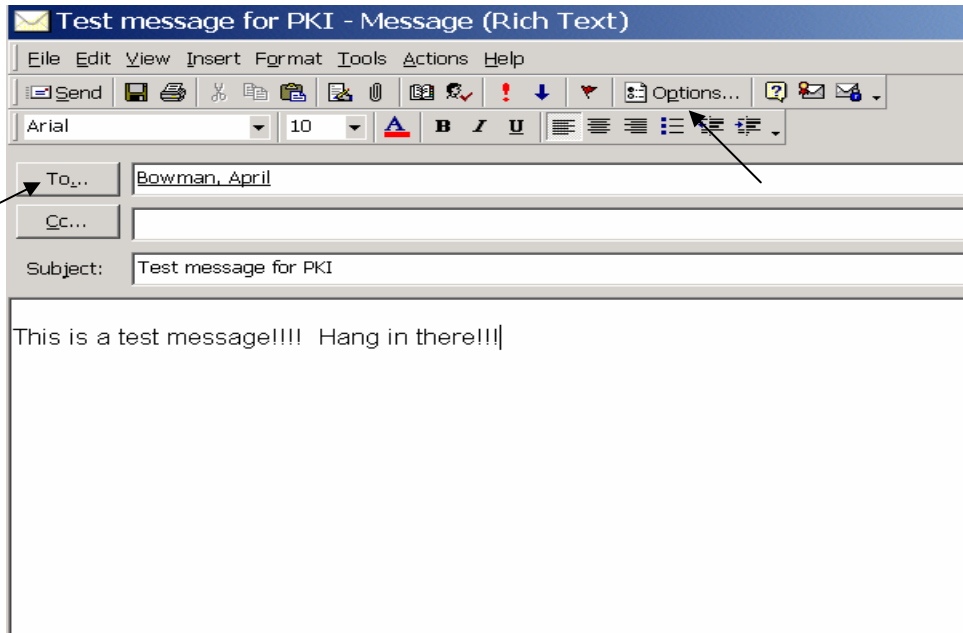
1. Open Microsoft Outlook (98 or 2000) and click the “New” Mail Message icon located on the upper left-hand corner of the menu bar.



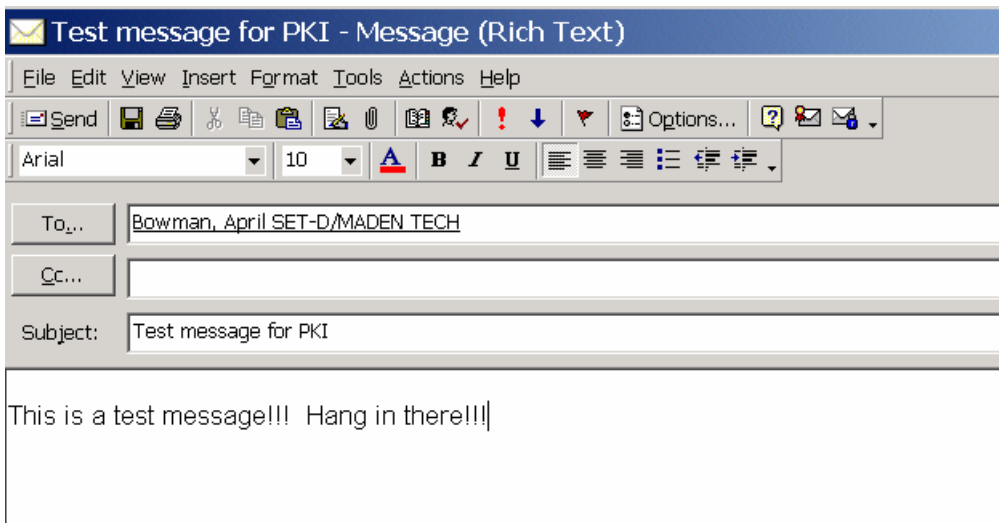
2. Click the **“To”** button. This will open the **Select Names** window.

*To send a digitally signed message you may choose the recipients name from any address list. Choose an address list from the **Show Names from the:** drop down box in the right hand corner of the **Select Names** window. April Bowman is the selected recipient in the diagram. Double click on the recipient’s name. Click **“OK”** to close the address book.

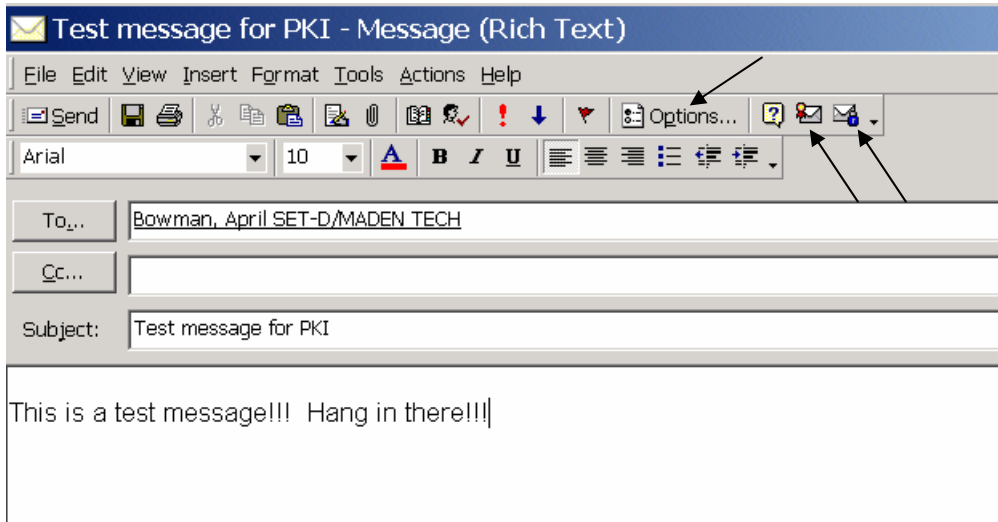
*To send an encrypted message you must have the recipients Certificate. Certificates are stored in the Contacts list. Use the **Show Names from the:** pull down menu and choose **“Contacts”**. Double-click a recipient’s name. Click **“OK”** to close the address book.



3. The recipient's name appears in the *To* box, type a subject and finish typing in the main body of the message.

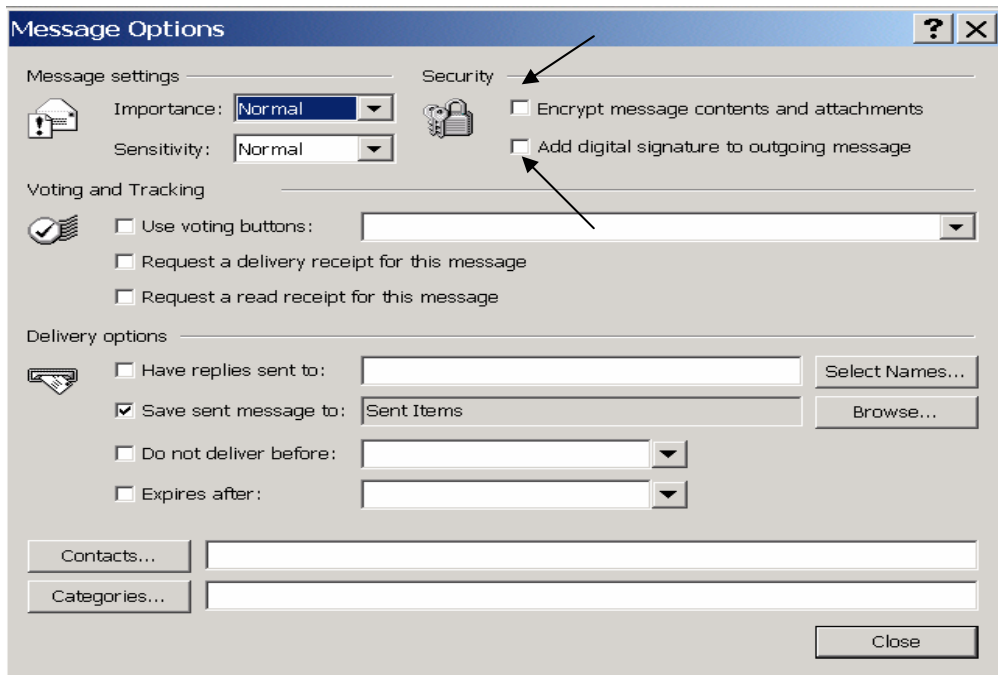


4. As the writer of the message, you must decide how to send the message: **Encrypted or with a Digital Signature or both.**

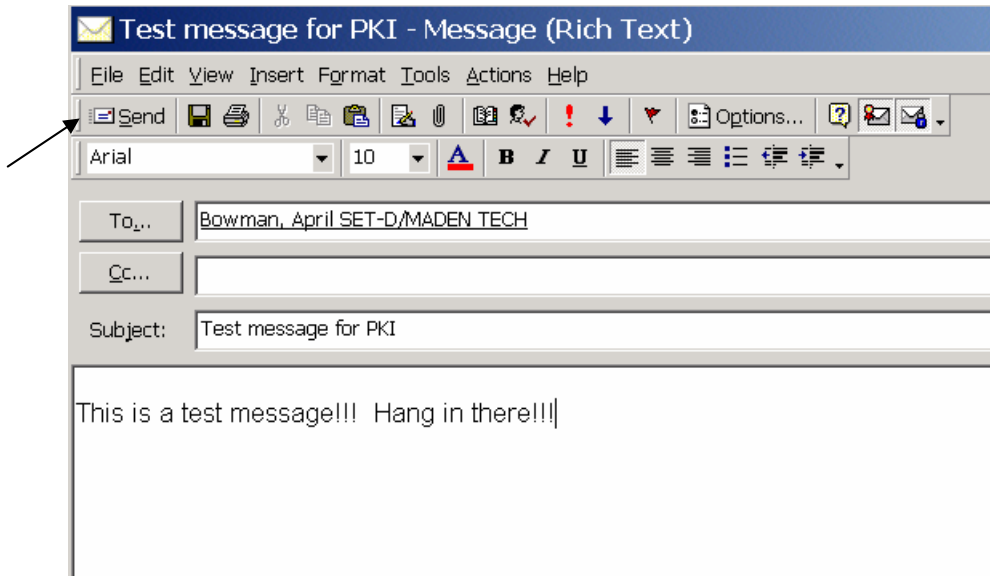


5. Click the envelope icon with the red seal to Digitally Sign the message. Click the envelope icon with the blue lock to Encrypt the message. Click both icons to Digitally Sign AND Encrypt the message.

If the icons do not appear on the toolbar, click the Options button.

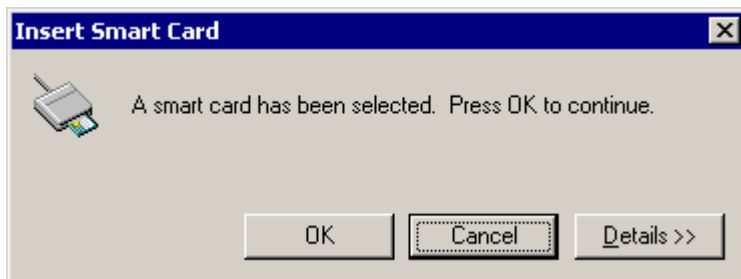
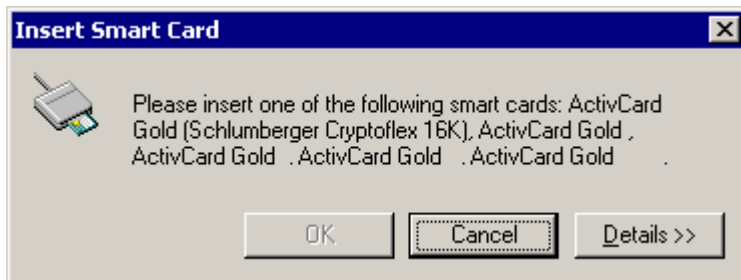


6. In the Message Options window, check the box next to the type of message you would like to send. Click “Close” to close this window.



7. Click “**Send**” to send the message to the recipient.

8. If your CAC is in the reader and you have already logged in with your PIN, you will not be prompted for your PIN to send a signed message. However, if you removed the CAC from the reader, the following display will appear indicating you need to reinsert your card in the reader.

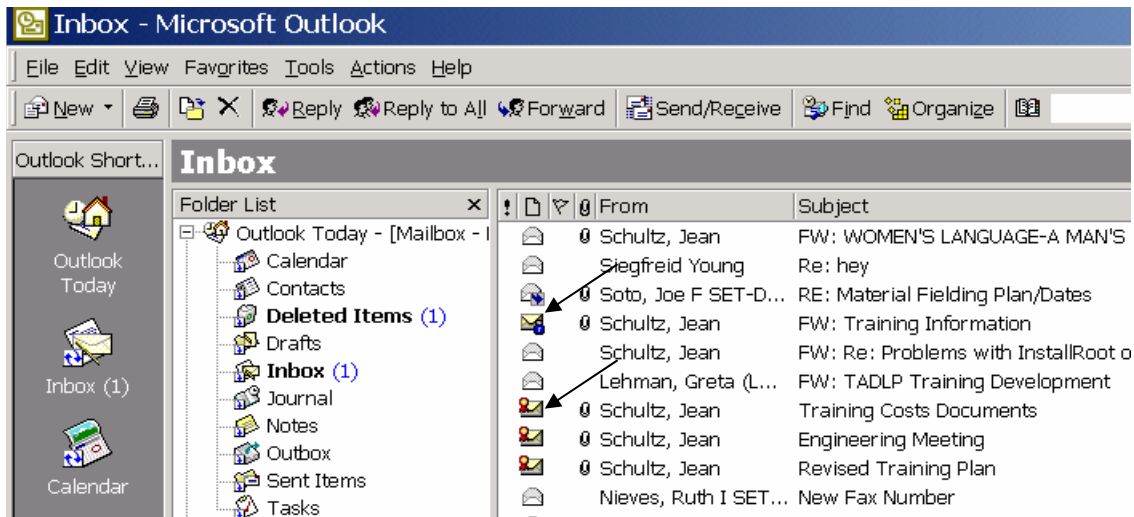


7. Insert your CAC into the reader then click “OK”.



8. Enter your PIN code and click **“OK”**. The email will then be sent to the recipient.

7.1.2 Receiving Email



1. An encrypted message received from another PKI user will be indicated by the **Encrypted icon** (a blue lock symbol over an envelope) in the Outlook Inbox.

A digitally signed message received from another PKI user will be indicated by the **Digital Signature icon** (a red seal over an envelope) in the Outlook Inbox.



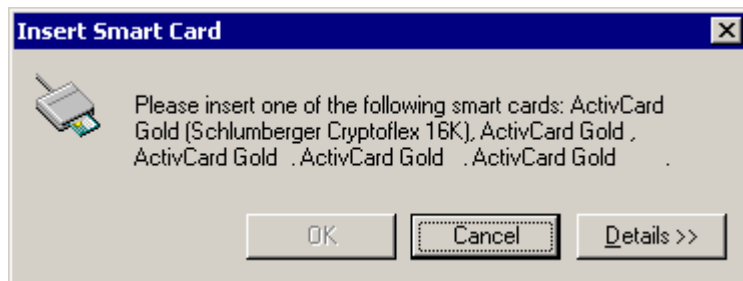
Product Manager Secure Electronic Transactions – Devices

	Hill, Charles A MS...	X120	Tue 6/5/2001 3
	Soto, Joe F SET-D...	RE: Material Fielding Plan/Dates	Tue 6/5/2001 3
	Flinn, Monica SET-...	FW: Training Kit Specs	Tue 6/5/2001 8
	Wright, James W ...	FW: Training Kit Specs	Tue 6/5/2001 7
	Schultz, Jean	FW: Training Information	Mon 6/4/2001 3
	Schultz, Jean	FW: Re: Problems with InstallRoot on an NT4 SP6 platform and the work around	Sun 6/3/2001 8
	Johnsen, Sterling ...	RE: Fielding/Training Working Group Meeting	Thu 5/31/2001

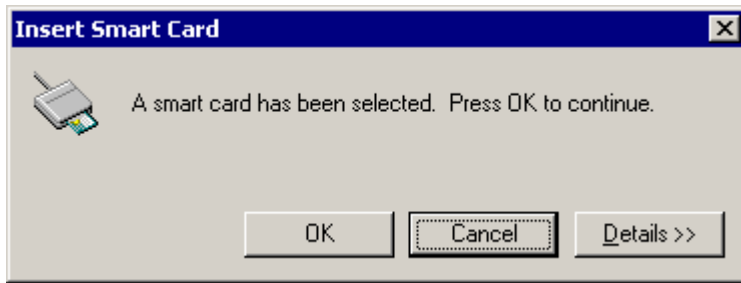


Encrypted or encoded items cannot be shown in the Preview Pane. Open the message to read it.

2. Highlight the Encrypted message by clicking on it. Notice that the Encrypted message does not appear in the preview pane. The contents will not be displayed until the item is opened with your CAC in the reader. (Encrypted messages only).



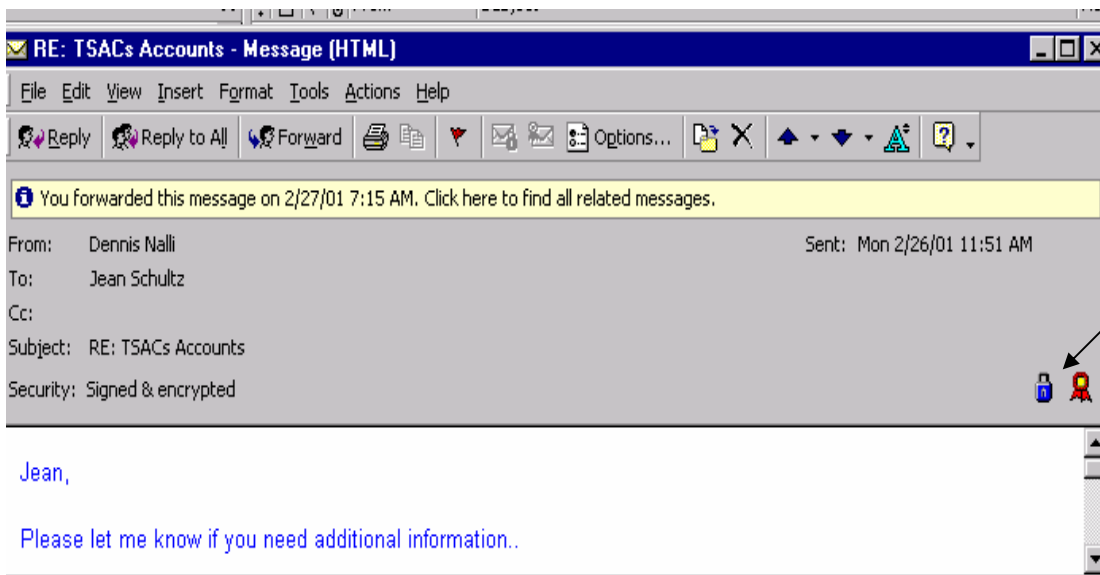
3. Double click on the encrypted message. If your CAC is in the reader and you have already logged in with your PIN, you will not be prompted to open the encrypted message. However, if you removed the CAC from the reader, the following display will appear indicating you need to reinsert your card in the reader.



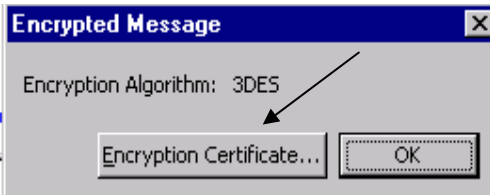
4. Insert your CAC into the reader and click “**OK**”.



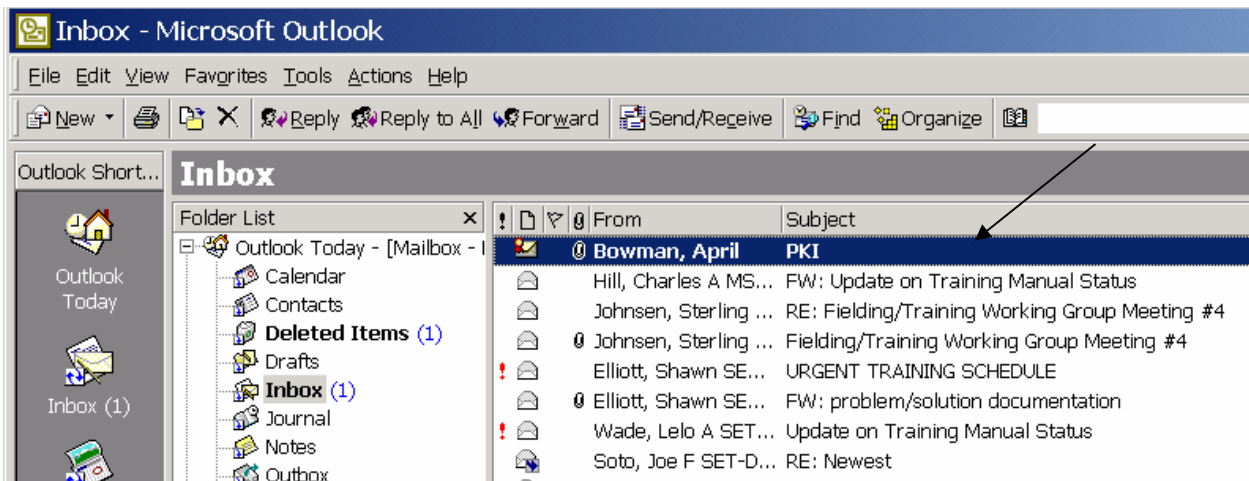
5. Enter your PIN code and click “**OK**”. You will now be able to view the contents of the encrypted message.



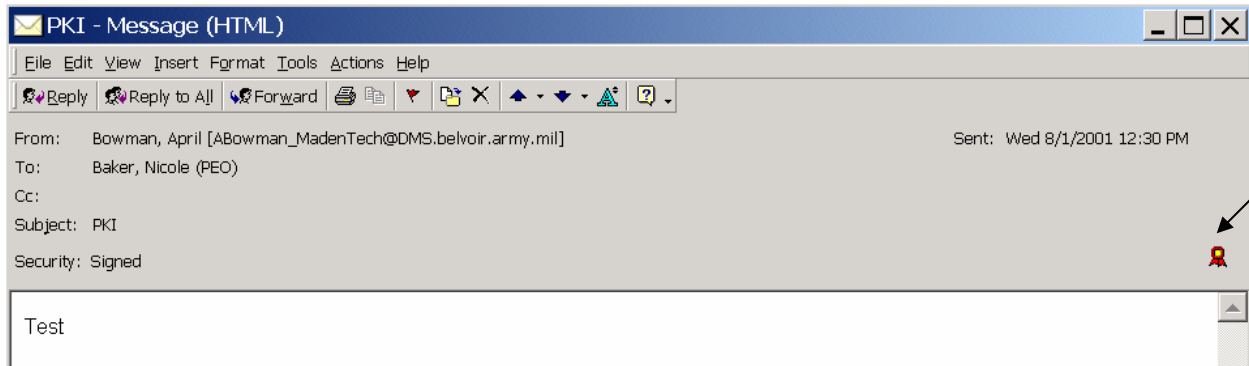
6. Click the “**Encryption**” icon. This icon (symbolized by a blue lock) is located on the far right corner of the email message.



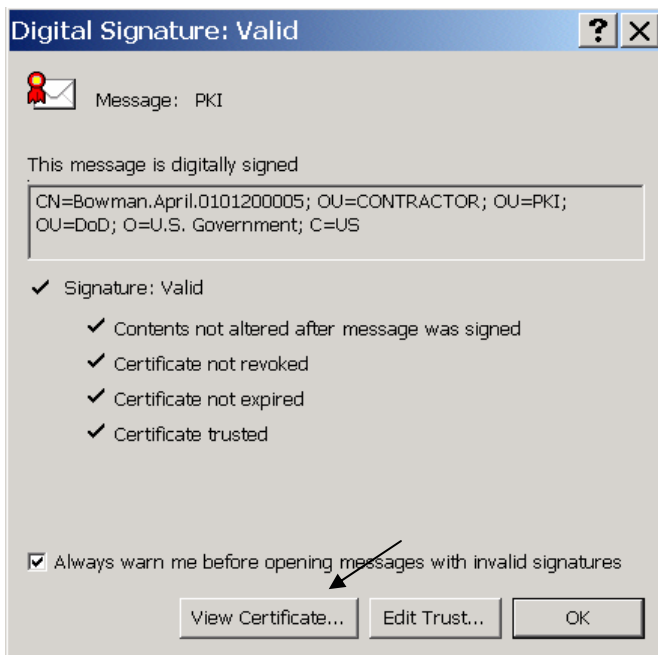
7. The *Encrypted Message* window will appear. You can click the “*Encryption Certificate*” button to open the *View Certificate* window. Close this window when you are finished viewing the Certificate information.



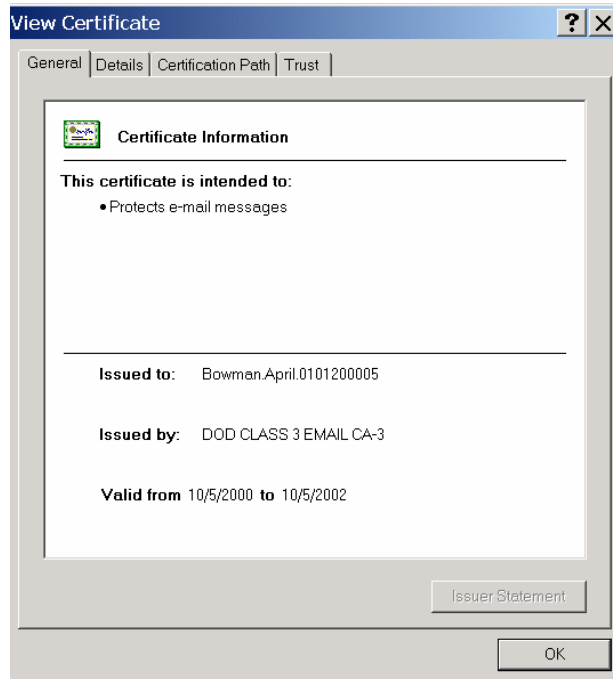
8. Double-click on the Digitally Signed message. Notice you do not need to enter your PIN to open this message.



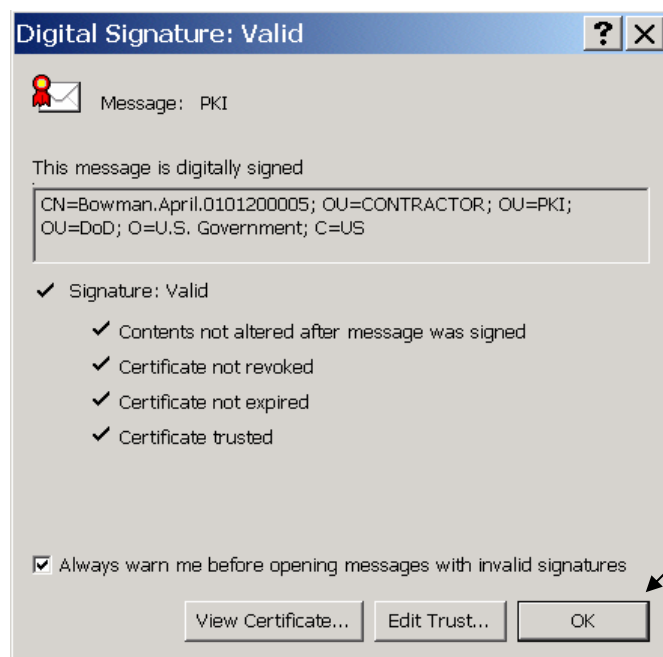
9. Click the **Digital Signature** icon. This icon (symbolized by a red ribbon) is also located on the far right corner of the email message.



10. The Digital Signature window will appear. You can click the “**View Certificate**” button to open the **View Certificate** window.



11. Click “OK” to close this window when you are finished viewing the Certificate information.

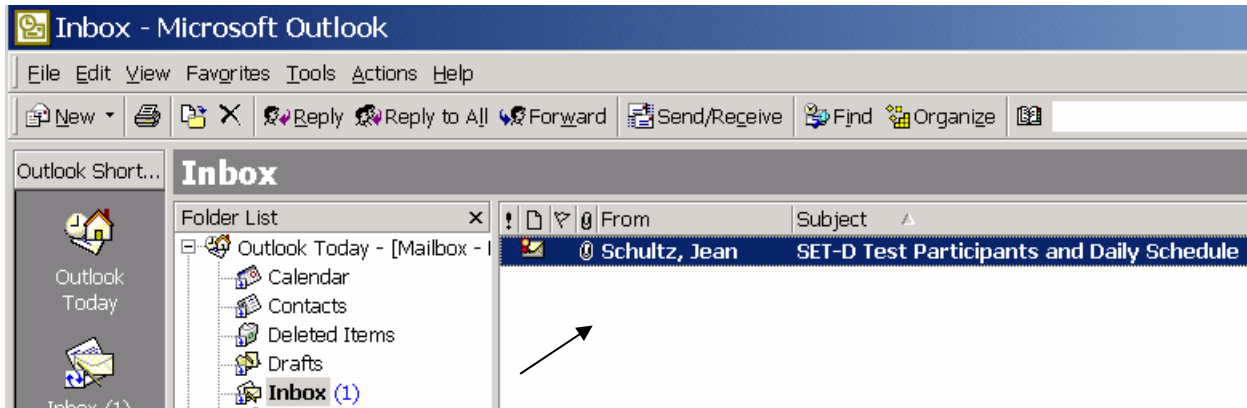


12. Click “OK” to close the Digital Signature window.

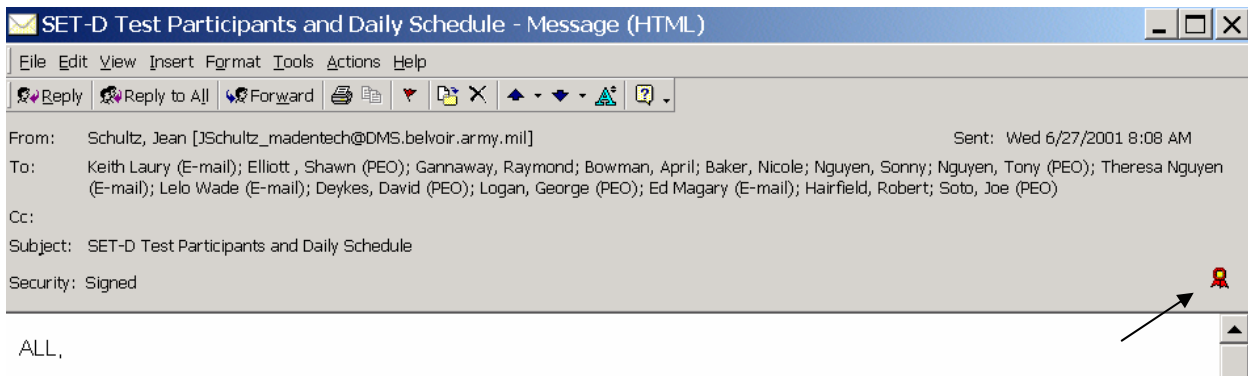


7.2 Retrieving Other Users Certificates

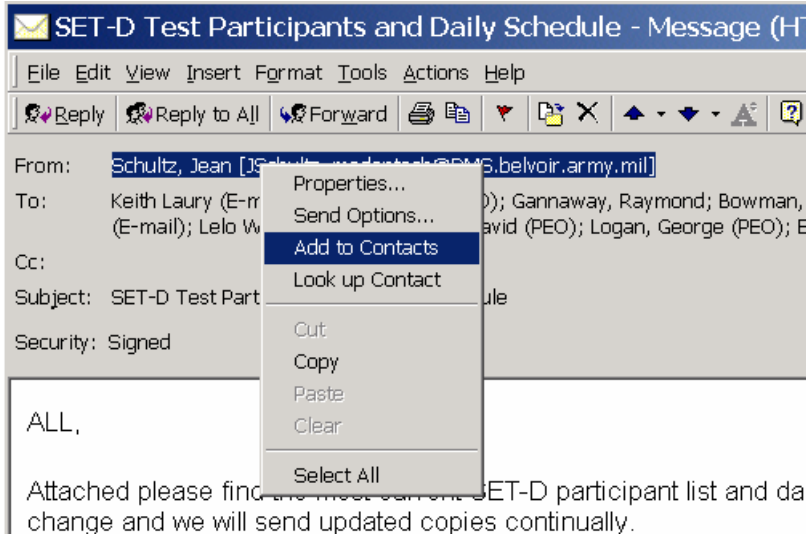
7.3.1 From a Signed Message



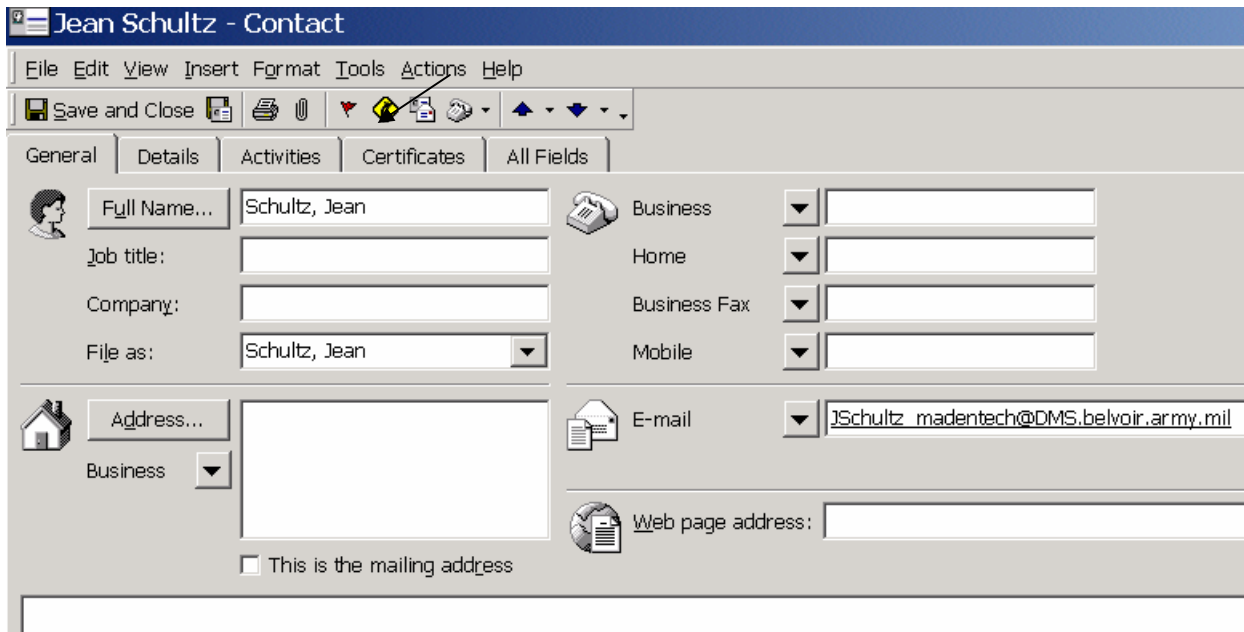
1. Open Microsoft Outlook (98 or 2000). When a new-signed message is received, select the message and double-click to open it.



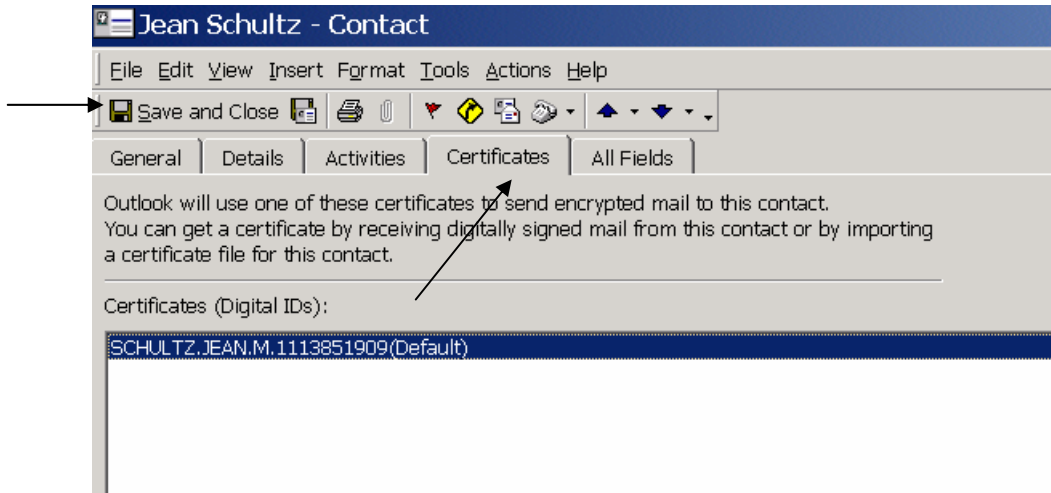
2. Notice the red ribbon in the upper right hand corner of the message.



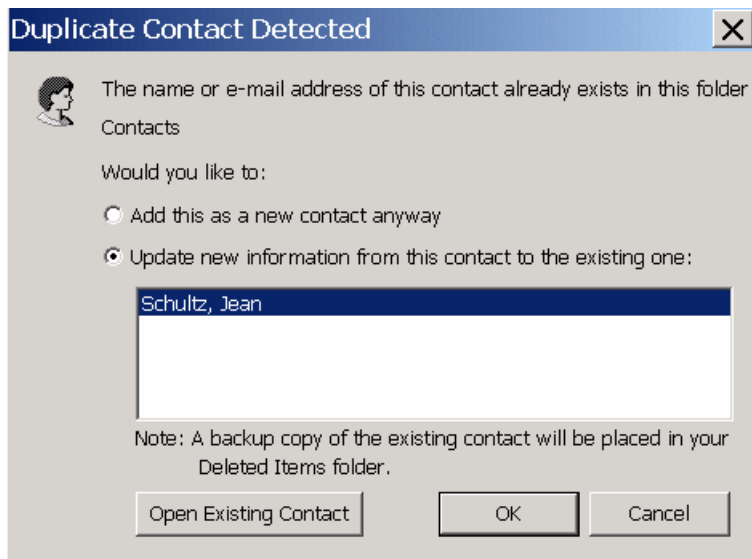
3. Right click on the message sender's name. Select *"Add to Contacts"*.



4. MS Outlook creates the Contacts entry for you. You should see the name and email address of the Sender.



5. Click on the *Certificates* tab to view the certificate. Click the *Save and Close* button.

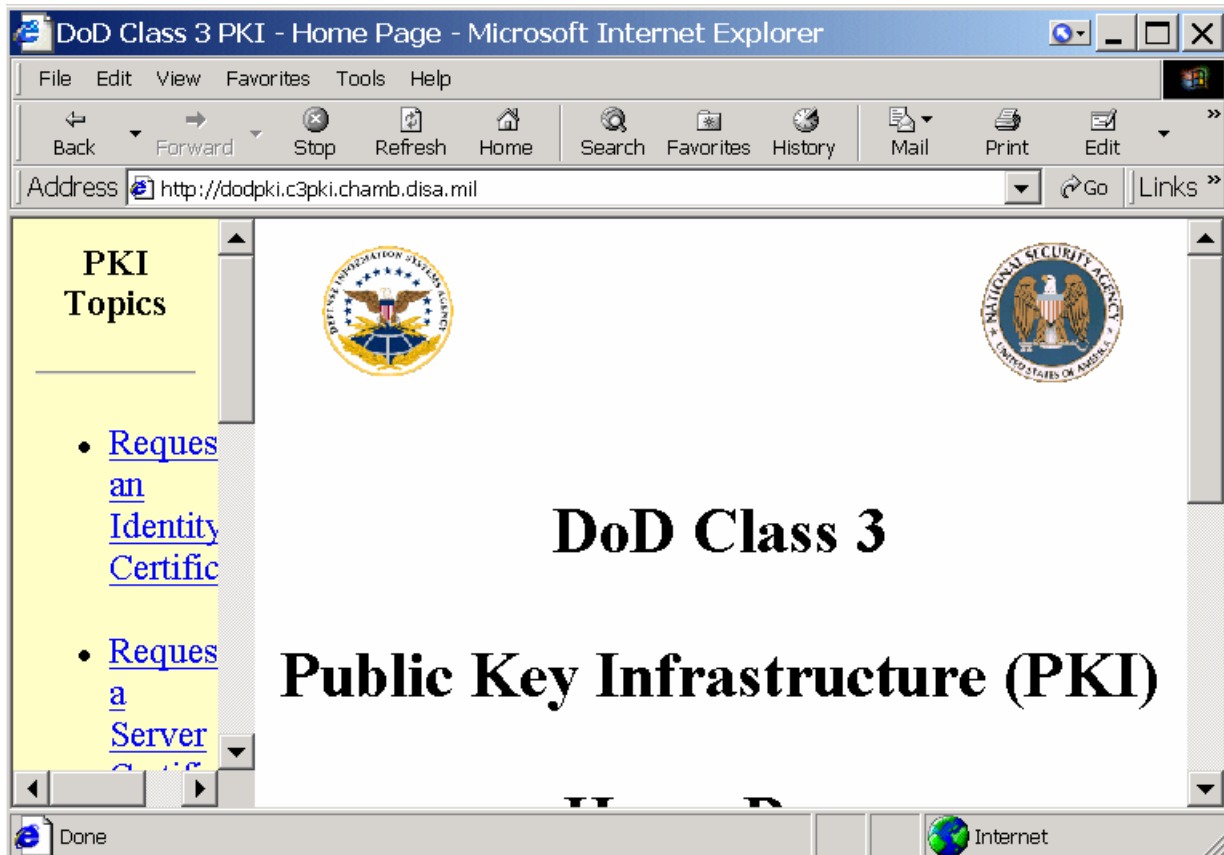


6. In some instances the Contact entry already exists. If it does, update the new information by selecting “*Update new information from this Contact to the existing one*”. Click “*OK*”.

The sender has now been added to your Contacts Folder.



7.3.2 Retrieval from DOD PKI Directory



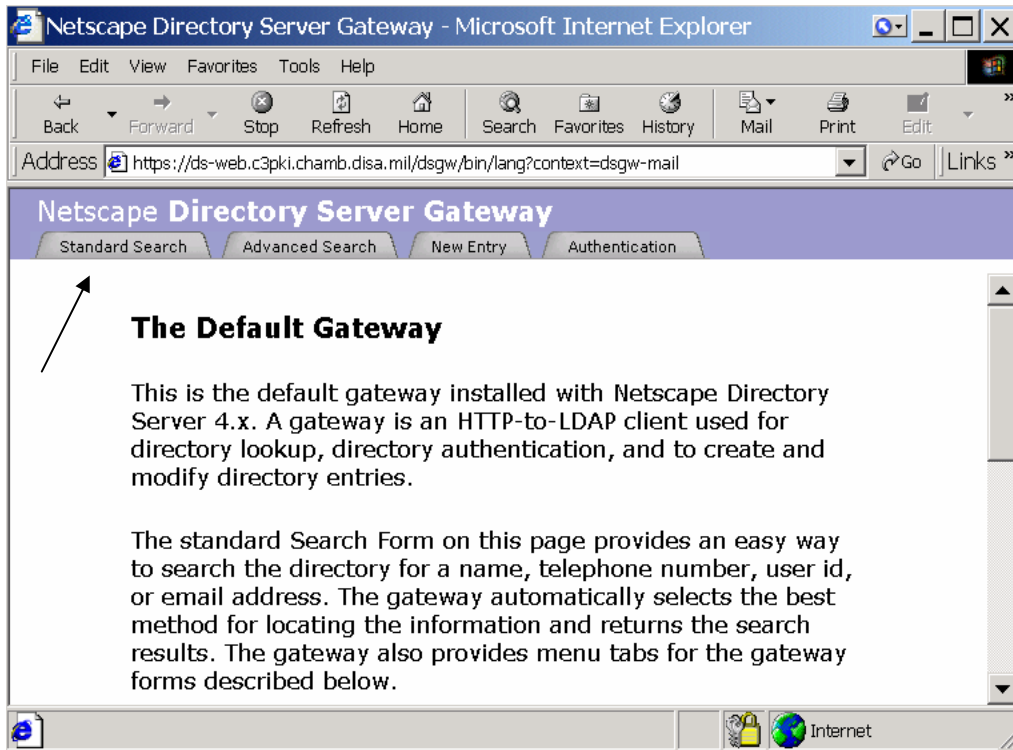
1. To receive a Class 3 Release 2 Certificate from the global directory, open your web browser and connect to either PKI home page:

<http://dodpki.c3pki.chamb.disa.mil> or <http://dodpki.c3pki.den.disa.mil>.

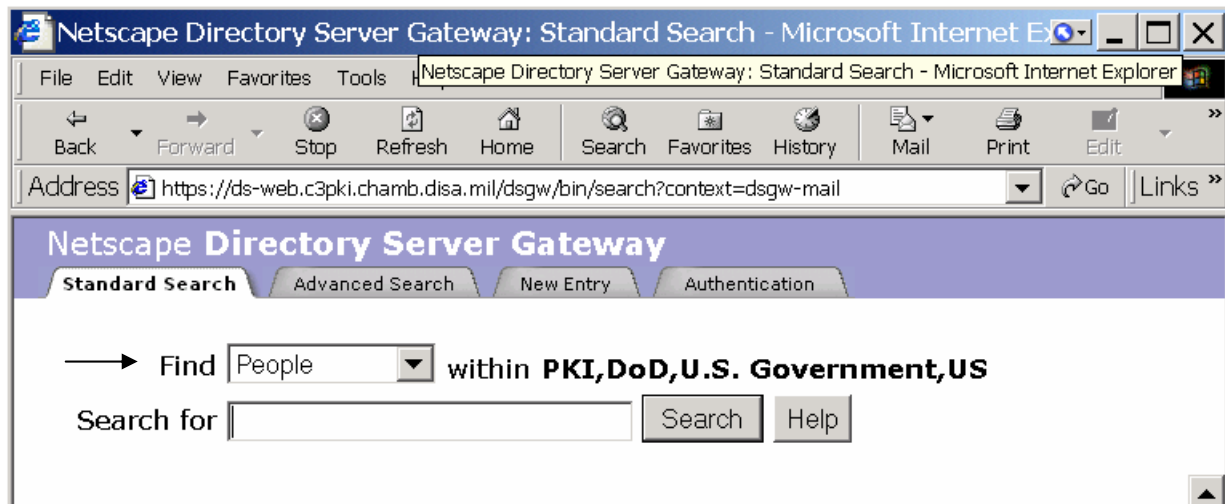


A screenshot of a Microsoft Internet Explorer browser window. The title bar reads "DoD Class 3 PKI - Home Page - Microsoft Inte". The menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The toolbar contains "Back", "Forward", "Stop", "Refresh", "Home", and "Search" buttons. The address bar shows "http://dodpki.c3pki.chamb.disa.mil". The main content area has a yellow background on the left with the heading "PKI Topics" and a list of links: "Request an Identity Certificate", "Request a Server Certificate", "Search the Identity Directory Server", "Search the Email Directory Server", "Frequently Asked Questions", and "Download Root CA Certificates". An arrow points to the "Search the Email Directory Server" link. On the right, there is a circular seal of the Department of Defense Information Systems Agency (DISA) and the text "THIS IS A GOVERN".

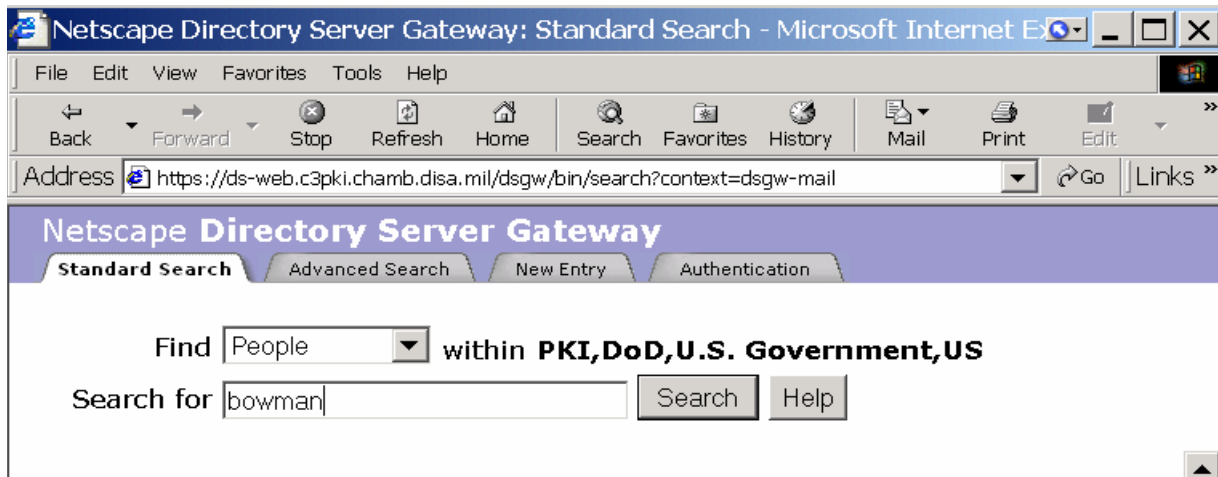
2. Click "*Search the Email Directory Server*".



3. Select the “*Standard Search*” tab at the top of the window.



4. Ensure *People* is selected in the *Find* drop down menu.



5. Type in the last name of the person you wish to receive the certificate for in the **Search For:** field. Click the **“Search”** button.



Found 11 entries where the name or user id is 'bowman'.

Name	ID	Phone
Bowman.April.0101200005	Bowman.April.0101200005	
Bowman.Betty.0606052026	Bowman.Betty.0606052026	
Bowman.Brian.D.0101068799	Bowman.Brian.D.0101068799	
Bowman.Bruce.E.0300086392	Bowman.Bruce.E.0300086392	
Bowman.Daniel.R.0300043766	Bowman.Daniel.R.0300043766	
Bowman.Donald.J.Jr.0300106012	Bowman.Donald.J.Jr.0300106012	
Bowman.George.M.0101308142	Bowman.George.M.0101308142	
Bowman.John.M.0300062184	Bowman.John.M.0300062184	
Bowman.Teresa.A.0300116075	Bowman.Teresa.A.0300116075	
Bowman.Terry.L.0300023020	Bowman.Terry.L.0300023020	
LRA.Bowman.April.D.0101200200	LRA.Bowman.April.D.0101200200	703-769-4518

6. The directory will list all individuals that meet the criteria listed in the search. Select your entry from the list.



Netscape Directory Server Gateway: Standard Search - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Real.com

Address <https://ds-web.c3pki.chamb.disa.mil/dsgw/bin/search?context=dsgw-mail>

Netscape Directory Server Gateway

Standard Search Advanced Search New Entry Authentication

Find within **PKI,DoD,U.S. Government,US**

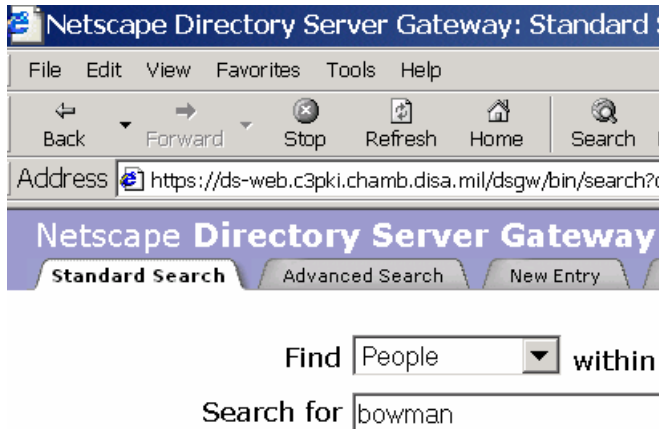
Search for

Bowman.April.0101200005, CONTRACTOR, PKI, DoD

[Download Certificate](#)

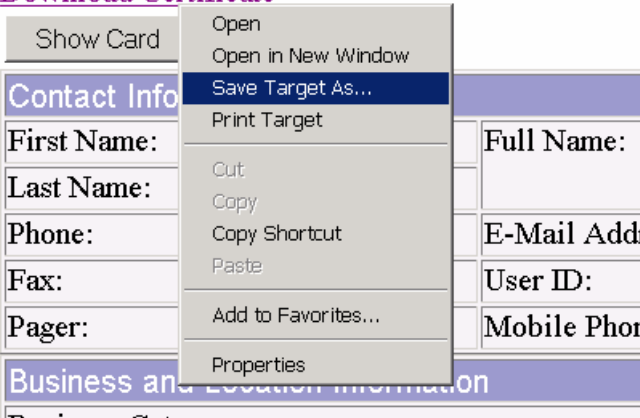
Contact Information			
First Name:	April	Full Name:	Bowman.April.0101200005
Last Name:	Bowman		
Phone:		E-Mail Address:	abowman_madentech@dms.belvoir.army.mil
Fax:		User ID:	0101200005
Pager:		Mobile Phone:	

7. Once the screen has loaded with the results of the search, review the information to ensure the certificate is for the correct person.



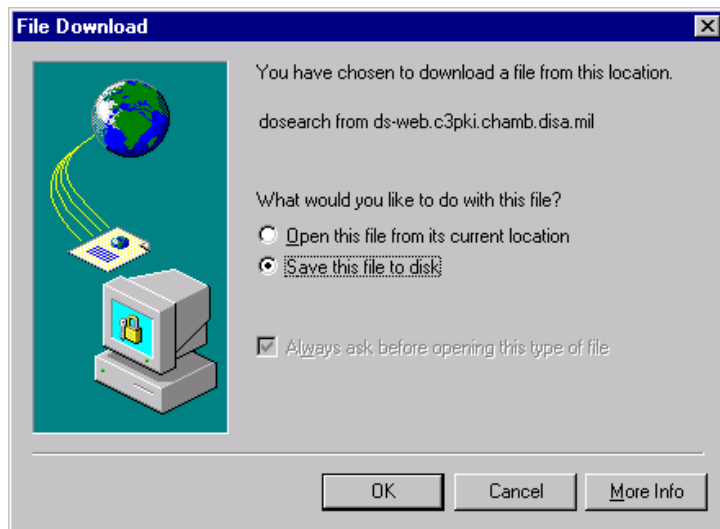
 **Bowman, April.0101200005,**

[Download Certificate](#)

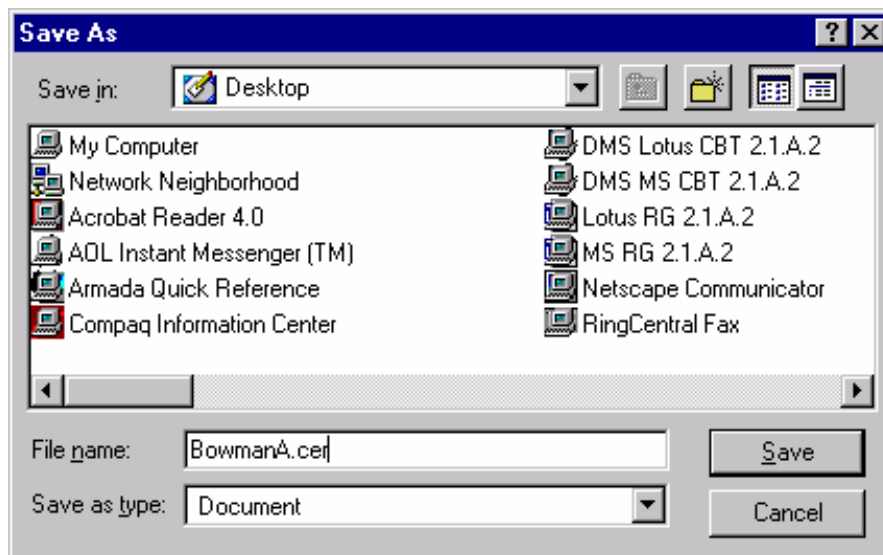


8. If you are using Netscape, right click on “*Download Certificate*” and choose “*Save Link As...*” from the menu.

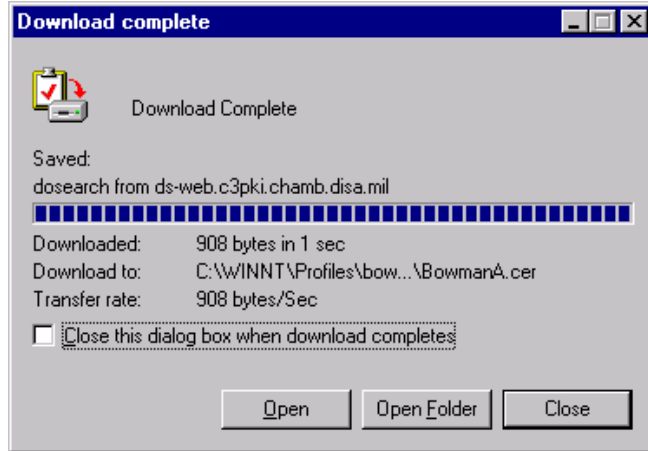
If you are using Internet Explorer, right click on “*Download Certificate*” and click “*Save Target As...*”.



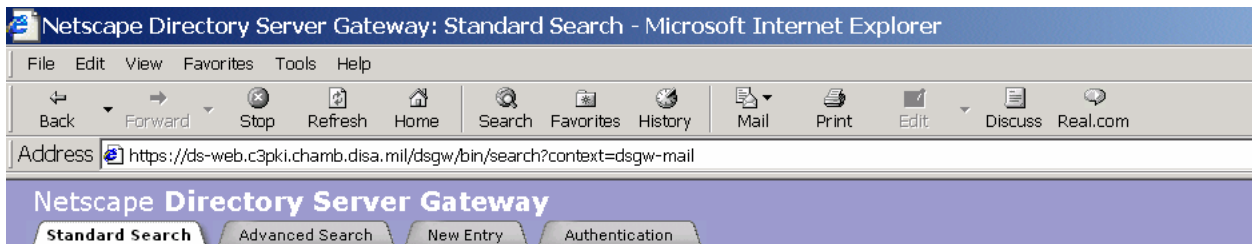
9. Select “*Save this file to disk*”. Click “*OK*”.



10. Save the file to your Desktop as LastnameFirstinitial.cer. For example: bowmana.cer for April Bowman. Select “*Save*”.



11. When Download is complete, click “Close”.



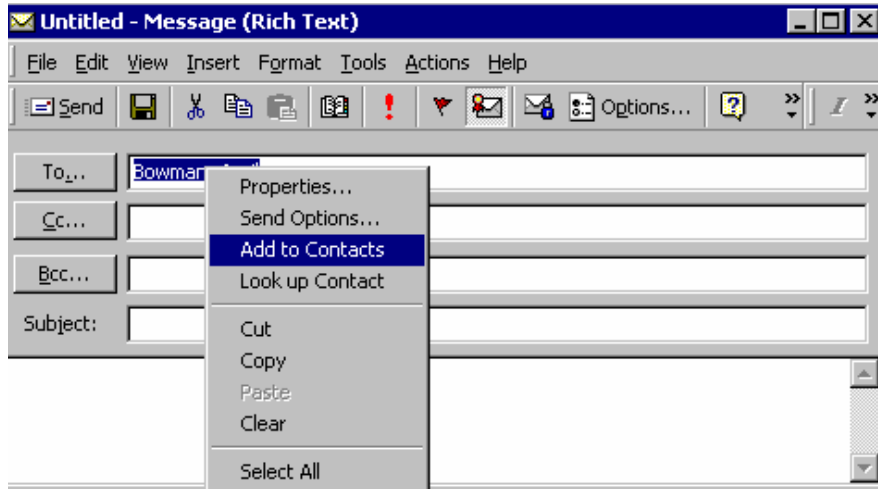
Find within **PKI, DoD, U.S. Government, US**
Search for

Bowman.April.0101200005, CONTRACTOR, PKI, DoD

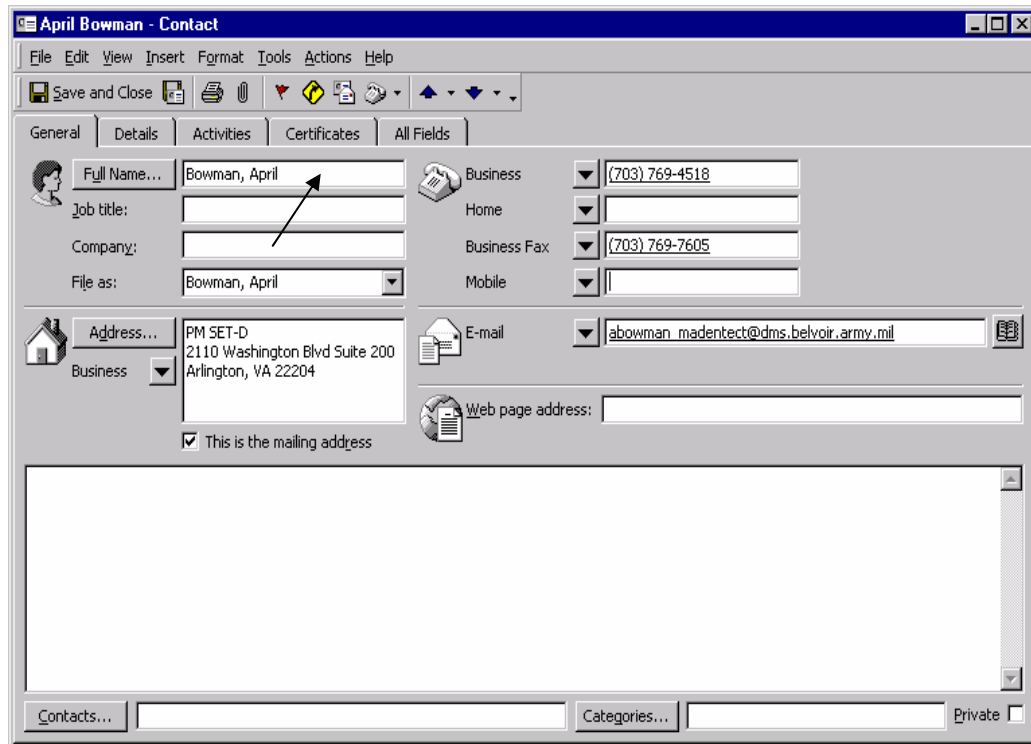
[Download Certificate](#)

Contact Information			
First Name:	April	Full Name:	Bowman.April.0101200005
Last Name:	Bowman		
Phone:		E-Mail Address:	abowman_madentech@dms.belvoir.army.mil
Fax:		User ID:	0101200005
Pager:		Mobile Phone:	

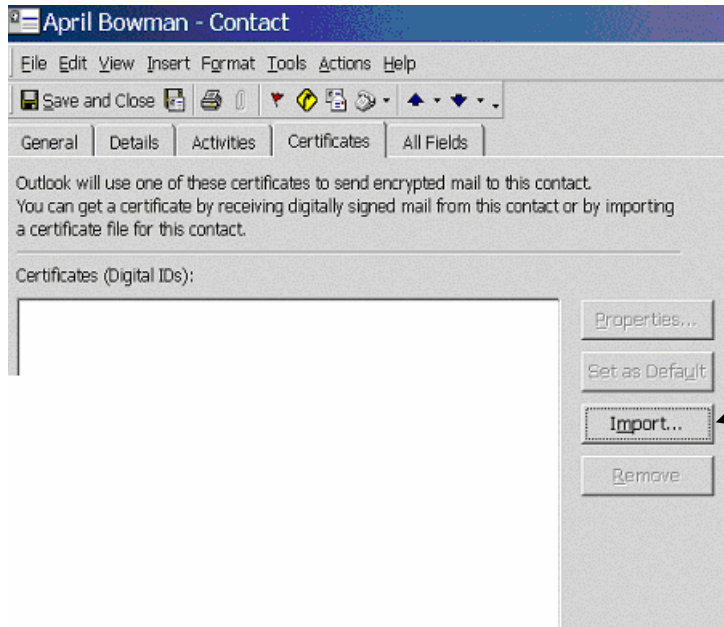
12. Click on the link for the email address located on the far right side of the window.



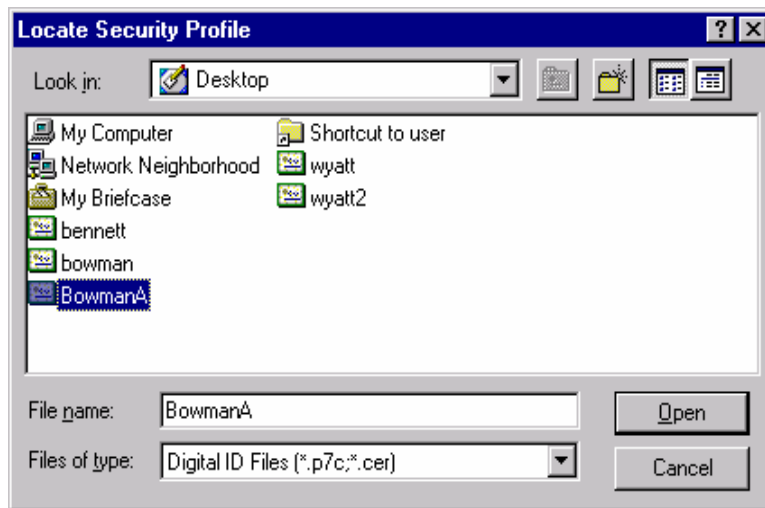
13. When the new mail message opens, right-click on the recipient's name and select ***“Add to Contacts”***.



14. Fill out additional information. Mandatory fields have been completed for you. Once complete, click on the ***“Certificates”*** tab.



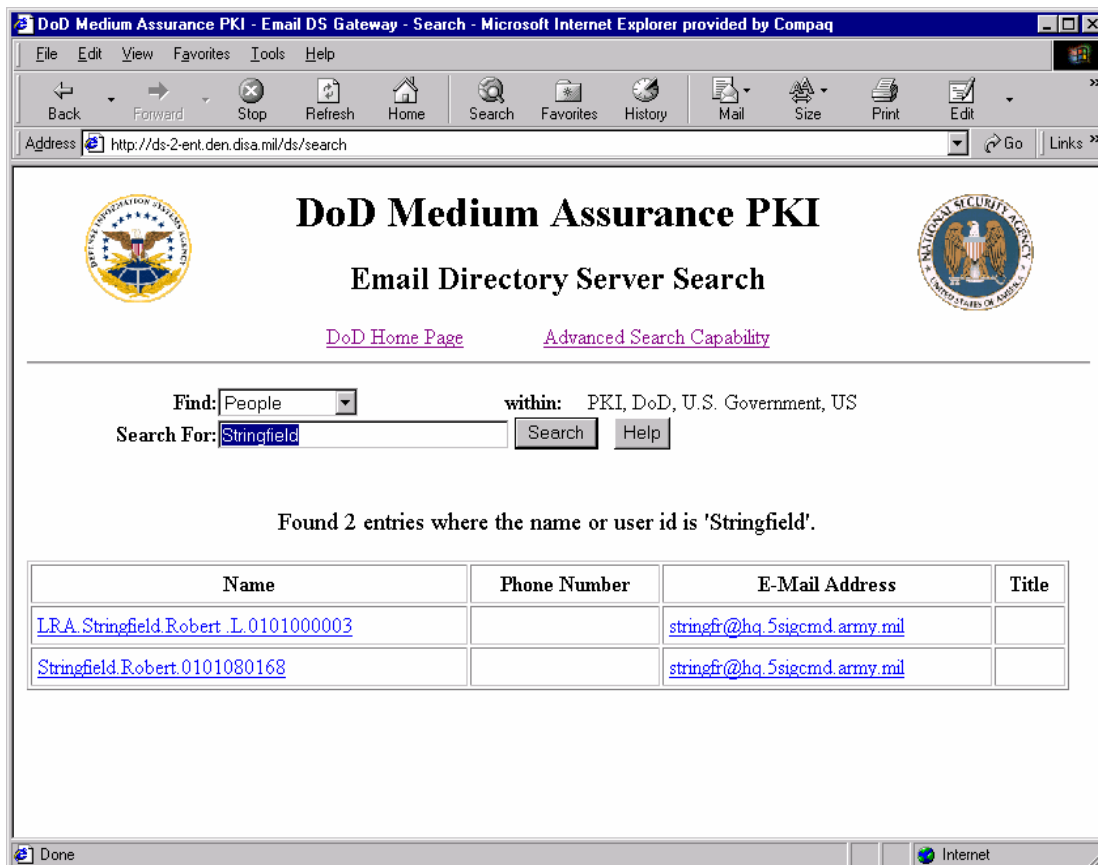
15. Select “*Import*” on the far right side of the window.



16. Select the file you previously saved on your Desktop. Click “*Open*”.



17. The Public Key has now been imported. Click “*Save and Close*”.



To retrieve a Class 3 Release 1 certificate from the global directory, go to <http://ds-2-ent.disa.mil/ds/search> to search for users. The rest of the process is the same as C3R2.



7.3 Network Login

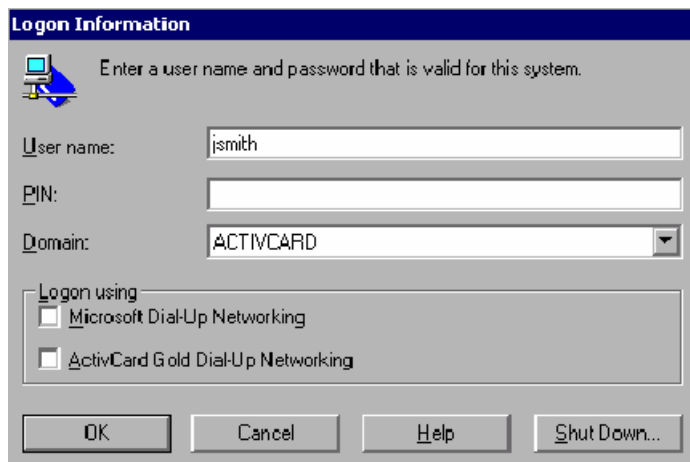
The Network Login feature is configured during the CAC Registration process. The use of this feature will be determined by Site/DOIM/Unit policy.

7.3.1 Windows NT & 2000 Network Login

1. Insert your smart card into the reader (chip side up and chip first).
2. Turn on your machine.
3. A message will appear asking you to press **Ctrl, Alt, Del** to login. Press **Ctrl, Alt, Del**.
4. The Windows Logon window will now appear. Once ActivCard Gold detects the smart card, the **Password** field automatically changes to **PIN**.

NOTE: If the login screen displays the **Password** field instead of the **PIN** field, then:

- a) Verify that the smart card is inserted properly in the reader.
- b) When the login screen displays the **PIN** field, repeat step 3 above.



5. Enter your smart card's PIN code in the **PIN** field and click "**OK**". After a few moments, you are logged in to your network and your desktop displays.

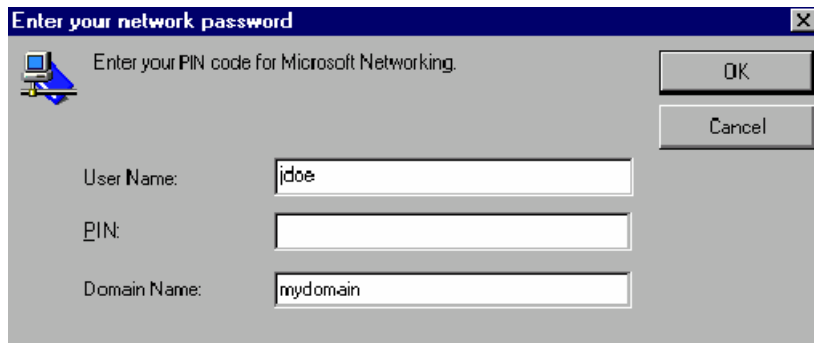


7.3.2 Windows 98 Network Login

1. Insert your smart card into the reader (chip side up and chip first).
2. Turn on your machine.
3. A message will appear asking you to press **Ctrl, Alt, Del** to login. Press **Ctrl, Alt, Del**.
4. The Windows Logon window will now appear. Once ActivCard Gold detects the smart card, the **Password** field automatically changes to **PIN**.

NOTE: If the login screen displays the **Password** field instead of the **PIN** field, then:

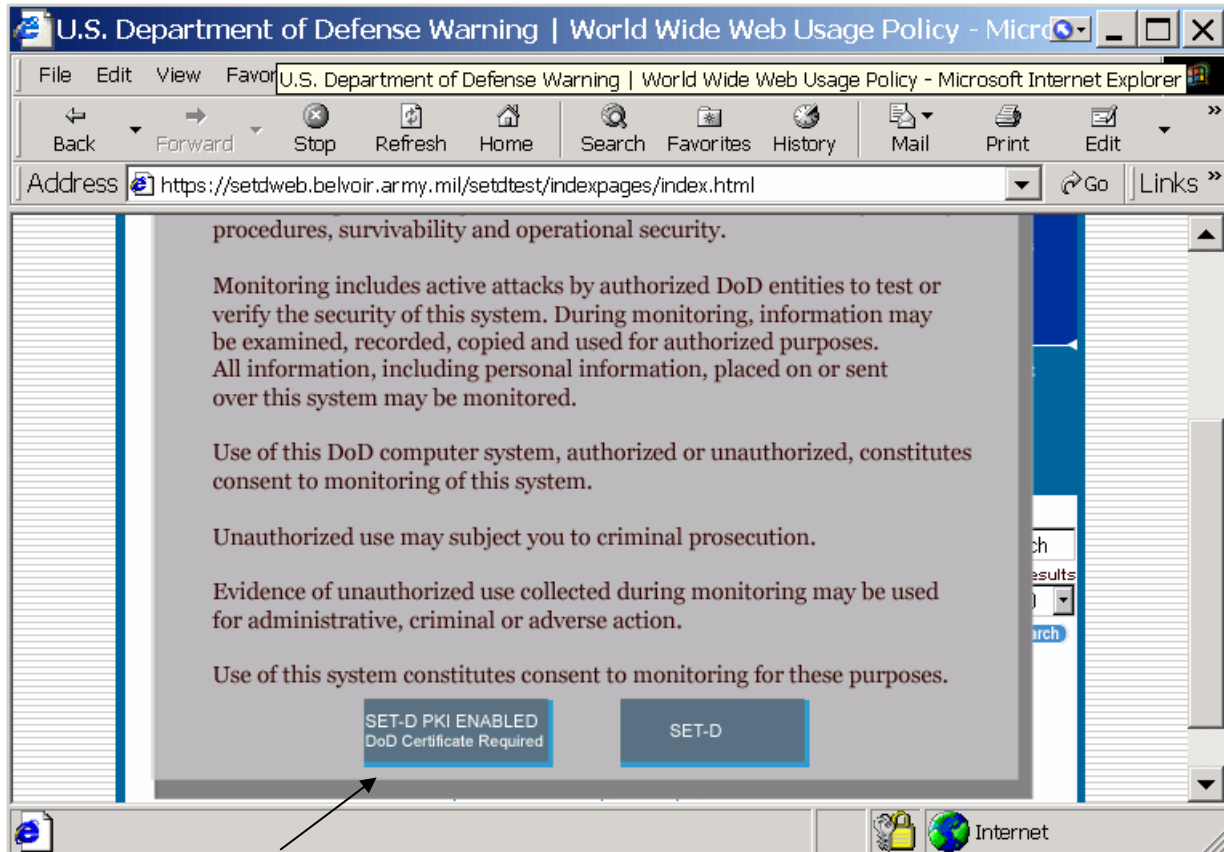
- a) Verify that the smart card is inserted properly in the reader.
- b) When the login screen displays the **PIN** field, repeat step 3 above.



5. Enter your smart card's PIN code in the **PIN** field and click on the "**OK**" button. After a few moments, you are logged in to your network and your desktop displays.



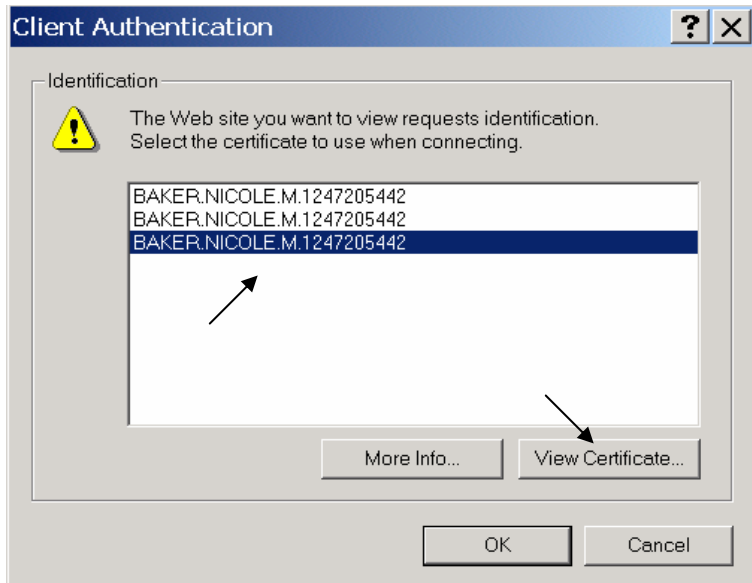
7.4 Login to a PK-Enabled Website



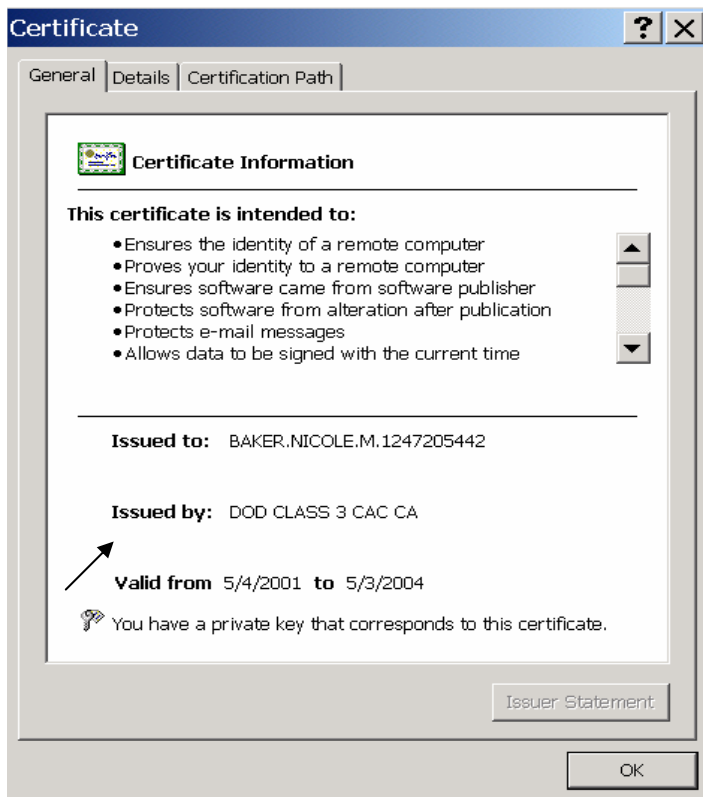
1. Start Internet Explorer or Netscape and connect to a PK-Enabled website. For this example we are using:

<https://setbweb.belvoir.army.mil/setdtest/indexpages/index.html>

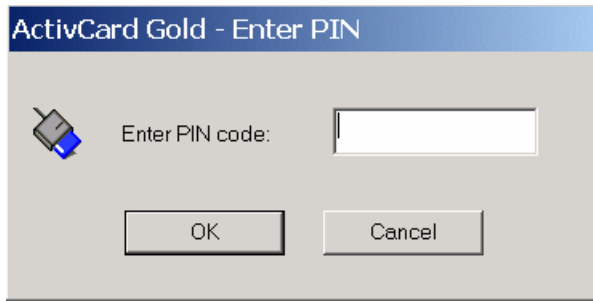
2. Click on the “*SET-D PKI ENABLED*” link.



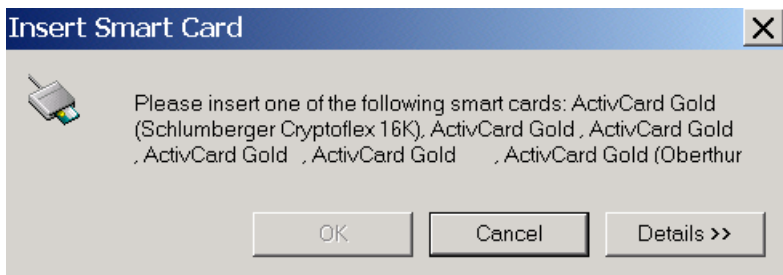
3. Highlight your ID Certificate. Typically your ID Certificate is listed last, to double-check, click on “*View Certificate*”.



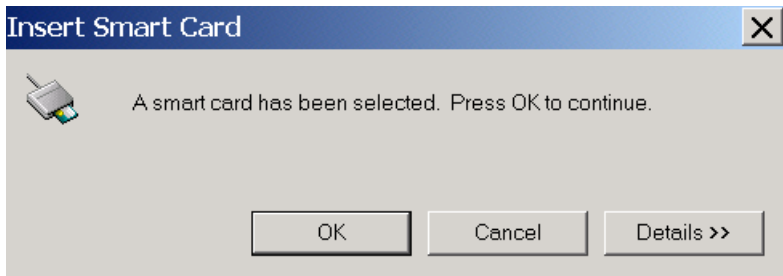
4. Examine the *Issued by:* field. It should say *DoD Class 3 CAC CA*. Click “OK”. You will be returned to the Client Authentication window. Click “OK” to continue.



5. If the smart card (CAC) is already inserted into the card reader, you will be prompted to enter you PIN code. Enter the *PIN* code and click “**OK**”.




6. If your smart card is not already in the reader, you will see the above message. Insert your CAC into the card reader.



7. Click “**OK**” to continue.



ActivCard Gold - Enter PIN

 Enter PIN code:

8. Enter your PIN at the prompt.

U.S. Army SET-D Program - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit

Address <https://setdweb.belvoir.army.mil/setdtest/indexpages/index2test.html> Go Links

SET-D

NEW SET-D Material Fielding Plan

PMO SET-D (Secure Electronic Transactions - Devices) Program:

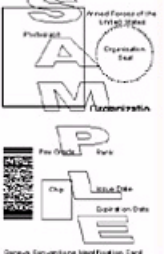
LTC Greta Lehman,
Product Manager

Mr. Robert Hairfield,
Deputy Product Manager

Notice: DOIMs: MACOMs:
For Pre-Fielding
Site Survey Information
Contact: **MSG Charles Hill**

What does the Smart Card (CAC) do?

The Common Access Card (CAC), also known as the Smart Card, is the primary focus of the SET-D program. CAC is an identification card with a tiny



What is SET-D?
How do I get a CAC?
How do I use a CAC?
Support
Points of Contact
FAQ
Sitemap

Site Search
Max. Results
10

Done Internet

9. If the PIN is correct, access to the web site will be granted.



8 Troubleshooting Guide

8.1 Frequently Asked Questions

Frequently Asked Questions

This page contains answers to common questions about Public Key Infrastructure (PKI) and Common Access Card (CAC)/Smart Cards. Some of the questions are linked to the Army's website, they can be accessed by a simple click.

1. What is Common Access Card (CAC)?

The Common Access Card (CAC) is a Department of Defense-wide Smart Card that will serve as:

- Standard ID card for active-duty military personnel (to include the Selected Reserve), DoD civilian employees, and eligible contractor personnel
- Principle card used to enable physical access to buildings and controlled spaces
- Principle card used to enable computer network and system access
- Primary platform for the PKI authentication token.

2. How do I use the CAC?

By the end of FY 2002 every military member, selected reservist, civilian employee, and on-site contractor in the Department of the Army will have a smart card that they will be able to use in their everyday life. Initially, the CAC will be used to enable building access, network access, and personnel identification. For example, service members may use the CAC to enter their post/camp/station, log onto their computers, or to verify their eligibility for benefits at a medical or dining facilities. These will be the primary uses of the CAC for its initial release. As technology matures, the Army will use the CAC to enable many business processes to improve current business processes and enhance support to people throughout the Army. One of the efforts currently underway is the development of the process and criteria by which new requirements for the CAC will be evaluated and prioritized.



3. Who will receive a CAC?

Initially, the Army will issue 1.4 million cards to active-duty military, Selected Reserve, National Guard, Army civilian, and eligible contractor personnel. Retirees and military dependents will not receive the CAC at this time, but will continue receiving their current identification cards.

4. Who will issue the CACs?

Verifying Official (VO)/Local Registration Authority (LRA) will issue the CACs at the current ID issuance facilities.

The following steps will be performed:

- Authenticate Based Upon Documentation Review
- Update DEERS Data
- Issue Uniformed Services ID Cards/Smart Cards

5. When will the CACs be issued?

During October 2000, a select group of personnel stations were issued the CACs starting with the Beta Tests at selected DoD installations. This will be followed by expanded beta tests in selected CONUS and OCONUS Army installations through June 2001. Full implementation of the CAC starts in May 2001 and continues through the end of 2002. This is a gradual process because the personnel stations must receive upgraded equipment to issue the CACs. Local Commanders or personnel offices will notify their staff when it's time to get the new card.

6. Where will the CAC be used?

CACs can be used at all locations where current ID cards are accepted. Additional locations, services, and functions that accept or support the new ID card will depend initially on the local command.

7. What is purpose of the CAC?

By the end of FY 2002 every military member, selected reservist, civilian employee, and on-site contractor in the Department of the Army will have a smart card that they will be able to



use in everyday life. Initially, the CAC will be used to enable building access, network access, and personnel identification. For example, service members may use the CAC to enter their post/camp/station, log onto their computers, or to verify their eligibility for benefits at a medical office or mess hall. These will be the primary uses of the CAC for its initial release.

8. How often will the CAC be re-issued?

On average, the CAC expires 3 years from the issue date, but new cards may be issued during that time period if the card is lost, damaged, or if the individual is promoted, married, or has a status change.

9. What should I do if my CAC is lost?

Individuals should report them as lost to their command and the nearest RAPIDS issuance station. Authorized operators at the issue station will request revocation of the digital certificates and issue new certificates.

10. What if a cardholder forgets their PIN?

The cardholder has three chances (in a row) to enter the PIN correctly. After the third time, the system will lock the cardholder out and the cardholder needs to return to the CAC issuance station to have the card "unlocked."

11. How does this card work with the different Microsoft Operating Systems out there?

DMDC has issued a "Validated Reader List." A card reader as well as a middleware product is needed to interoperate with the card and the Microsoft Operating System.

12. What is the Hardware/Software requirement for PKI?

Client computers must meet the following requirements:

- Hardware:
 - Pentium 166 processor or higher



- 64 MB RAM
- Software:
 - Microsoft Windows 98/NT/2000 Professional
 - Microsoft Outlook 98/2000
 - SmartCard reader/driver
 - Middleware

13. I am trying to send a signed and encrypted message but I keep getting the following error: “Your Key set cannot be found by the underlying security system.” Why is this happening?

You may not have the 128-bit version of Internet Explorer 5 installed on your system. To check this, Open Internet Explorer and select the Help drop down menu. Click on About Internet Explorer and make sure that the cipher strength says 128-bit. If it says anything else you will need to install the 128-bit Security Patch.

14. When trying to send an encrypted message, I keep getting the following error message: “This message cannot be secured using the selected Security Settings. Your email address may not match the email address on the certificate, or some other problem exists with the certificate. Do you want to proceed with the message without security?”

On occasion the Email and ID certificate will flip-flop and this error will occur. To fix this all you will need to do is go into Tools, Options, Security, Change Settings and making sure both the Signing Certificate and Encryption certificates are both pointing to the e-mail PKI certificate. If the ID and Email certificates have not flip-flop'd, you will need to verify that the e-mail address on the certificate matched your e-mail address listed in the Global Address List on the server.

15. I have an extensive Personal Address book. Is there a way to transfer my personal address list into my contacts without having to retype everything?

Yes. Follow these instructions:

Using Outlook, add a personal folder to your profile. Create a temporary Contacts folder in the new personal folder you just created. On the Tools menu, click **Address Book**. Click to select the recipients you want to add as Outlook contacts. Right-click the selected recipients and click **Add to Personal Address Book**. On the File menu, click



Import and Export. Click Import from another program or file, and then click *“Next”*. In the Select file type to import from list, click **Personal Address Book**, and then click *“Next”*. Select the temporary Contacts folder previously created, and then click *“Next”*. Click Finish to import the users from your PAB to the Contacts folder in your personal folder. You can now drag the contacts to any Microsoft Exchange Server location, whether it is a Mailbox Contacts folder, or a Contacts public folder.

16. Why can't I “Reply” to an encrypted message?

You cannot **Reply** to an encrypted message. When you receive a message and **Reply**, the "To" addressee is pointing to the global or the directory services of the Exchange server instead of your contact list. Since the certificate is linked to the contact folder, the "To" addressee must point to the SMTP address from the contact folder.

Outlook 98: Customize option unavailable when attempting to customize toolbar.

Use any Mail Format other than Microsoft Word: TOOLS/OPTIONS/MAILFORMAT TAB, Select any option other than Microsoft Word from the "Send in this message format" and select OK. REFERENCE: **Microsoft Technet: ID Number Q189919**

17. Is there a way to change the security level without reloading the cert? (User wants to change it from ‘High’ to perhaps ‘Low’)

The security setting should be set to HIGH to support the regular usage of the password protecting the private key. This procedure would require a password each time you encrypt or decrypt. That way only the person with the password would be able to open or send encrypted messages. If the security setting is not set to HIGH, it will require the user to reload the certificate.

18. When I attempt to open an encrypted message, I receive an error message saying, “Cannot open this item. Your digital ID name cannot be found by the underlying Security System.”

Check your security settings within Outlook and verify that all possible encryption certificates are installed. Even if more than one certificate is listed within the Outlook Security Settings, you will be able to decrypt any message as long as the necessary certificate is installed. If the message still cannot be opened, it is possible that the sender used an encryption certificate from the directory that you do not have locally installed. Download your encryption certificate from the web directory (save it as a .cer file) and compare the serial number on it to your locally installed certificates. If you do not have a certificate installed locally that matches the serial number from the directory certificate, you will not be



able to decrypt the message. If you have another certificate on a floppy disk or a different machine, you will need to install it locally in order to open the message.

If you do not have a “private” certificate matching this serial number on any other machine or floppy disk, you will need to contact your LRA to have it revoked. Once it is revoked, the certificate you do have should then appear in the directory so that others will be able to use it to send you encrypted mail.

19. How do I know if a digital signature has been checked against a valid certificate revocation list (CRL)?

CRL checking is not built in to Outlook, but it is available as a separate patch. This patch is included in Internet Explorer 5.5 Service Pack 1, but Outlook 2000 SR-1 security features must also be enabled for it to work properly.

To validate a digital signature once the CRL patch and SR-1 have been applied, open a signed message. Click on the red ribbon for the digital signature and view the large white box for the Message Security Properties.

If there are green check marks throughout the list of security properties, the signature has been verified and you can trust the signature.

However, if there is a triangle yellow warning icon with an exclamation point in this list, click to highlight it and view the description box underneath to determine why the signature could not be fully verified.

20. Why aren't any signatures released from the DOD CLASS 3 EMAIL CA-3 or CA-4 intermediate certification authorities successfully verified against the CRL?

Many of these “Release 2” email certificates do not have a CRL Distribution Point listed in the certificate itself. The PKI office temporarily removed this line from the email certificates to resolve a technical problem. The CRL Distribution Point will be added back to the certificates in the near future. Thus, a CRL check against one of the Release 2 certificates will not appear to be successfully verified.

21. When I open an email message with Outlook, I get an error saying that the certificate is not trusted. What is wrong?

The error means that the certificates used to sign and/or encrypt cannot be validated based on the root certificates currently in your root store. To resolve this issue, you will need to install



the root certificate authority that issued the certificate the sending is using. You can obtain the trusted root certificate authorities from:

DOD PKI Release 1 & 2: <https://ca-3.c3pki.chamb.disa.mil/reg1.html>

ORC IECA: <http://eca.orc.com/trust.html>

DST IECA: <http://www.digistrust.com/certificates/policy/ieca/ieca.cacert>

Verisign IECA:

<https://onsite.verisign.com/services/USGovernmentDODIECA3Encryption/cgibin/privateCA/getcacert>

GD IECA: <http://webex.gdpsc.com/ieca/GDIECARoot.cer>

The DOD PKI root certificate authorities and 4 IECA's are the only certificate authorities you should trust. It may be a potential security breach to install any other root certificate authority. Once you have installed these root certificate authorities, the error message will not appear the "*Next*" time you open the message.

22. People I send messages to who are not using MGS claim that they cannot read my messages. The messages aren't being sent encrypted, so why can't they read them?

If the recipient is not using an email client capable of supporting S/MIME, the digital signature will make a message unreadable on these clients. To prevent this problem from occurring, make sure you select the check box for "Send clear text signed message when sending signed messages." This check box specifies that recipients whose email clients do not support S/MIME signatures be allowed to read the message without verification of the digital signature.

If this check box is not selected, recipients using Outlook will notice the blue encryption icon "*Next*" to a message in their inbox. However, after opening the message, you will notice that it has been digitally signed.

23. When I sign a forward of a signed attachment, why do the recipients get the error "An error occurred in the underlying security subsystem"?

This error will appear in Outlook when you sign and forward a signed message. If only the original message is signed, and not your forward, the recipient will be able to read it. A possible workaround is to configure Outlook so that you forward messages as inline



text rather than attachments. However, this configuration will forward the original message unsigned, with no assurance that the text hasn't been modified.

8.2 Where Do I Go For Help?

PKI Army Help Desk
703 769-4499
DSN 327-4004
Hours: 0700 – 1700 (M-F)

Website:
<http://setdweb.belvoir.army.mil>

PKI Web Sites:
<http://dodpki.c3pki.chamb.disa.mil>

<http://dodpki.c3pki.den.disa.mil>



APPENDIX A – ACRONYMS

Abbreviation of Term	Explanation
API	Application Programming Interface
CA	Certificate Authority
CAC	Common Access Card
CD	Compact Disc
CD-ROM	Compact Disc-Read Only Memory
CRL	Certificate Revocation List
D/RPO	DEERS/RAPIDS Program Office
DEERS	Defense Enrollment Eligibility Reporting System
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DOIM	Director of Information Management
DSO	DMDC Support Office
EDI	Electronic Data Exchange
FSR	Field Service Representative
ICC	Integrated Circuit Chip
IMO	Information Management Officer
IO	Issuing Officer
KB	Kilobyte
LRA	Local Registration Authority
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
OS	Operating System
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RAPIDS	Real-Time Automated Personnel Identification System
SLCPP	Senior Leadership Communication Protection Program
SSN	Social Security Number
USB	Universal Serial Bus
VO	Verifying Officer
VO/LRA	Verifying Officer/Local Registration Authority



APPENDIX B – DEFINITIONS

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Certificate: A digital representation of information that binds the user's identification with the user's public key in a trusted manner. At minimum, this information (1) identifies the certification authority issuing it, (2) names or identifies its user, (3) contains the user's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.

Certification Authority (CA): An authority trusted by one or more users to create and assign certificates.

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in managing and issuing certificates in relation to a specific Certificate Policy.

Certificate Revocation List (CRL): A computer-generated record that identifies certificates that have been revoked or suspended prior to their expiration dates. It is periodically issued by each CA and posted to the directory.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Defense Eligibility & Enrollment Reporting System (DEERS): A system that contains accurate and timely information on all eligible Uniformed Services members (Active Duty, Reserve and Retired) and their families as well as DoD Civilians (23 million records). It includes detailed information on DoD Benefit Program eligibility.

Digital Signatures: "Digital signature" or "digitally signed" refers to a transformation of a message using an asymmetric cryptosystem such that a person who has the initial message and the signer's public key can accurately determine: (1) whether the transformation was created using the private key that corresponds to the signer's public key; and (2) whether the initial message has been altered since the transformation was made.

Directory: The directory is a repository or database of certificates, CRLs, and other information available online to users.

Encryption: The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (*one-way encryption*) or cannot be obtained without using the inverse decryption process.

Integrity (Data Integrity): Protection against unauthorized modification or destruction of information.



Interoperability – Refers to a system or a product that is capable of operating with another system or product directly without additional developmental effort by the user.

Local Registration Authority (LRA): A type of Registration Authority with responsibility for a local community.

Logical Access Control – Refers to an automated system that controls an individual's ability to access one or more computer system resources such as a workstation, a network, an application, or a database.

Mission Category: (GIG IA 6-8510 G&PM) Applicable to information systems, the mission category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the war fighter's combat mission. Mission categories are primarily used to determine requirements for availability and integrity services. DoD will have three mission categories:

- **Mission Critical¹:** Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. Information in these systems must be absolutely accurate and available on demand (may be classified information, as well as sensitive and unclassified information).
- **Mission Support:** Systems handling information that is important to the support of deployed and contingency forces. The information must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).
- **Administrative:** Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term (may be classified information, but is much more likely to be sensitive or unclassified information).

Non-Repudiation: Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.

Private Key: The part of a key pair to be safeguarded by the owner. A private key is used to generate a digital signature. Private keys are used to decrypt information, including key encryption keys during key exchange. It is computationally infeasible to determine a private key given the associated public key.



Public Key: The part of a key pair released to the public. A private key can be either a signature or key exchange key. The signer's public signature key is used to verify a digital signature.

Public Key Infrastructure (PKI): Framework established to issue, maintain, and revoke public key certificates.

Private Web Server: A web server that is designed for and/or provides information resources that are limited to a particular audience (i.e., DoD) or a subset thereof. (This includes web servers that provide interfaces to e-mail systems.) A private web server restricts or attempts to restrict general public access to it. The common means of restriction are by the use of domain restriction (e.g., .mil and/or .gov), filtering of specific Internet Protocol (IP) addresses, user ID and/or password authentication, encryption (i.e., DoD certificates) and physical isolation. Any DoD operated web server that provides any information resources that are not intended for the general public shall be considered a private web server and is subject to this policy. Personal web servers (i.e., those that only allow one user and are only accessible from the machine to which it is installed) are not subject to this memorandum.

Real-Time Automated Personnel Identification System (RAPIDS): This is an automated, cost-effective and currently operation ID Card System for Military, Retired and their Families.

Registration Authority (RA): Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.

Root Certification Authority: The Root CA is a trusted entity responsible for establishing and managing a PKI domain by issuing CA certificates to entities authorized and trusted to perform CA functions.

Smart Card – Credit card size card with an Integrated Circuit Chip (ICC).

Token: A device (e.g., *floppy disk, Common Access Card, smart card, PC Card, Universal Serial Bus device, etc.*), that is used to protect and transport the private keys of a user.