II. Installing RSA Public and Private Key Generation Software

➤ ***The software for the RSA Public and Private Key Generation can be found on the GinnieNET 2020 desktop CD. If you cannot locate the Key Generation software, call GinnieNET Customer Service at 1-800-234-4662, option #1.***

RSA Public and Private Key Generation

The objective of this course is to train Issuers and Custodians on the installation process of the RSA Public and Private Key Generation system. The Private and Public Keys are generated to store the authorized signatory. At this point, an authentication password for each authorized signer will also be assigned for subsequent use in shipping and certifying the pools.

This chapter will provide details on how to:

- Install the RSA Public and Private Key Generation;
- Create a Public and Private Key certificate; and
- Use the Public and Private Key certificate to enroll your fingerprint.

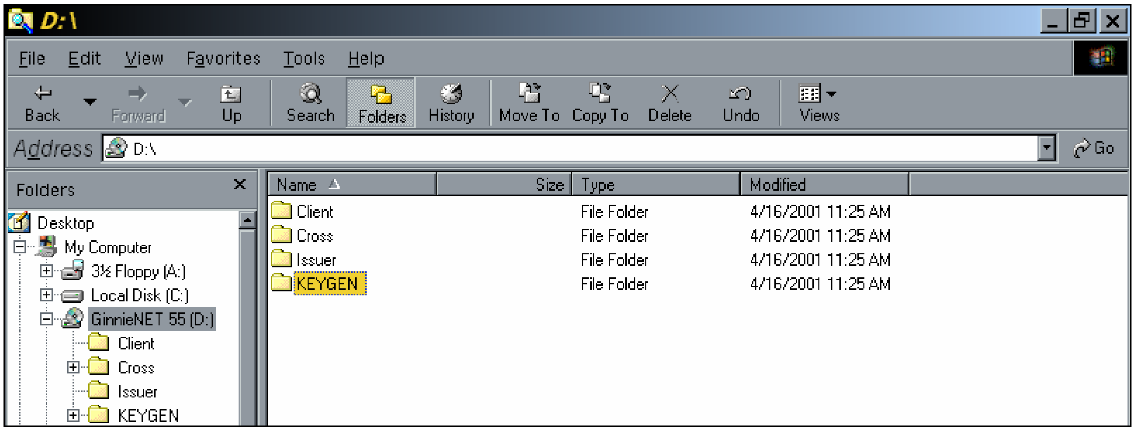
II. INSTALLATION

RSA Public and Private Key generation software is used to create one Public Key diskette and one Private Key diskette per user. The information contained on these RSA diskettes enables a user to work with functions requiring security access in the Communications and Signature Enrollment menus on Ginnie*NET* 2020. Your RSA password is contained on the RSA Public Key diskette.

Each Issuer should have a designated security officer who is responsible for creating the RSA diskettes. The RSA Public and Private Key generation software is to be installed *only* on the PC utilized by the security officer. **This software must be loaded on a local drive on a resident PC. It should not be installed in a LAN environment.**

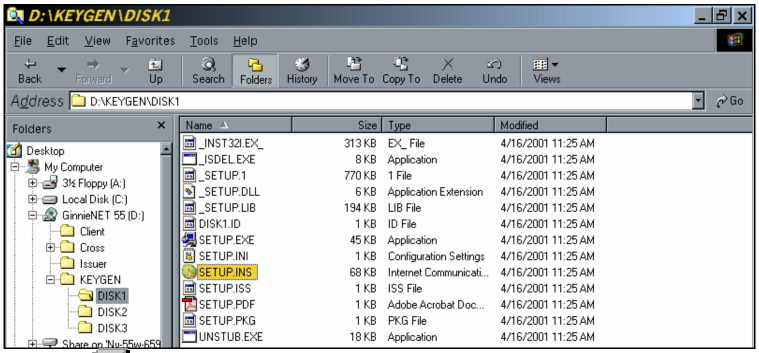
Note: If there is only one user working with Ginnie*NET* at a particular site and no security officer has been designated, the individual user will function as the security officer.

1. Select on the KEYGEN .



Name	Size	Type	Modified
Client		File Folder	4/16/2001 11:25 AM
Cross		File Folder	4/16/2001 11:25 AM
Issuer		File Folder	4/16/2001 11:25 AM
KEYGEN		File Folder	4/16/2001 11:25 AM

2. Double-click on DISK1 folder in the left windowpane to open it and gain access to SETUP.EXE in the right windowpane.

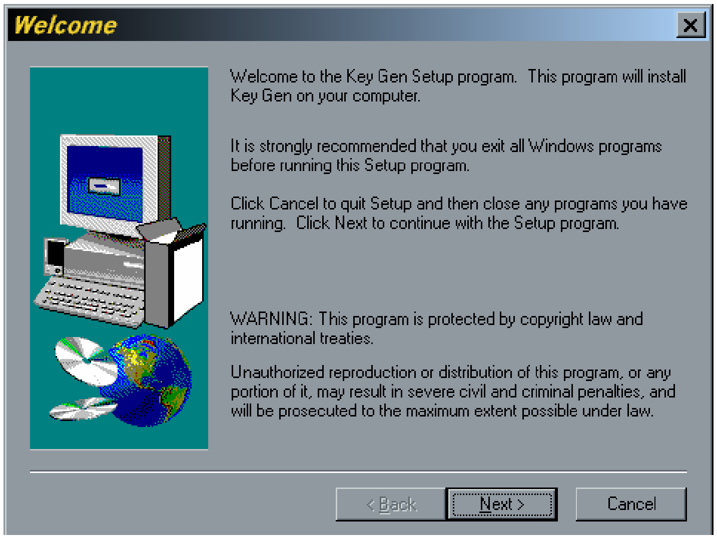


Name	Size	Type	Modified
INST32I.EX	313 KB	EX_ File	4/16/2001 11:25 AM
_ISDEL.EXE	8 KB	Application	4/16/2001 11:25 AM
_SETUP.1	770 KB	1 File	4/16/2001 11:25 AM
_SETUP.DLL	6 KB	Application Extension	4/16/2001 11:25 AM
_SETUP.LIB	194 KB	LIB File	4/16/2001 11:25 AM
DISK1.ID	1 KB	ID File	4/16/2001 11:25 AM
SETUP.EXE	45 KB	Application	4/16/2001 11:25 AM
SETUP.INI	1 KB	Configuration Settings	4/16/2001 11:25 AM
SETUP.INS	68 KB	Internet Communicati...	4/16/2001 11:25 AM
SETUP.ISS	1 KB	ISS File	4/16/2001 11:25 AM
SETUP.PDF	1 KB	Adobe Acrobat Doc...	4/16/2001 11:25 AM
SETUP.PKG	1 KB	PKG File	4/16/2001 11:25 AM
UNSTUB.EXE	18 KB	Application	4/16/2001 11:25 AM

3. Double-click on in the right windowpane to start the installation process.

SETUP takes over and provides systematic instructions until the process is complete.

4. Make sure that you read the instructions on the **Setup** screens. If there is a discrepancy between this manual and the instructions on a **Setup** screen, follow the instructions on the **Setup** screen.



Welcome to the Key Gen Setup program. This program will install Key Gen on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

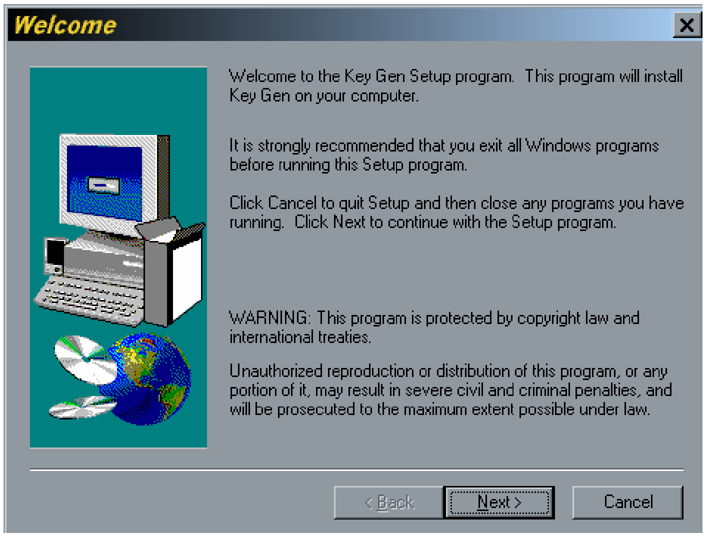
WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

5. Select Next > on the **Welcome!** Screen to proceed to the **User Information** screen.

6. Enter your **Name** and **Company** on the User Information screen.

7. Select Next > to proceed to the Choose **Destination Location** screen.



Welcome to the Key Gen Setup program. This program will install Key Gen on your computer.

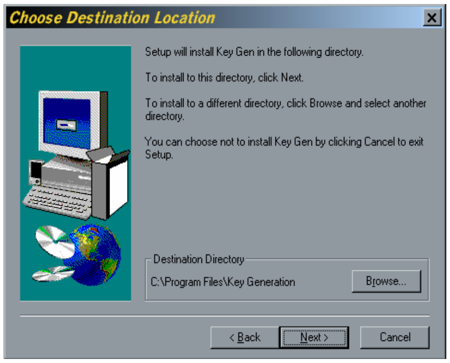
It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

8. The default destination directory for your RSA Public and Private Key generation software is a directory on your local hard drive as shown above. You may choose a different drive or directory by using the Browse... command button. Accepting the SETUP default is simple and safe. Change the directory if you need to do so and Select Next > to proceed.



Choose Destination Location

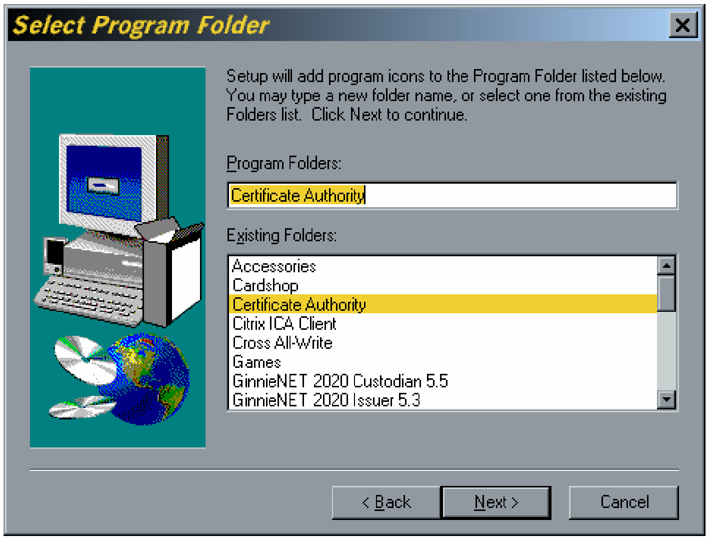
Setup will install Key Gen in the following directory.

To install to this directory, click Next.

To install to a different directory, click Browse and select another directory.

You can choose not to install Key Gen by clicking Cancel to exit Setup.

Destination Directory: C:\Program Files\Key Generation



Select Program Folder

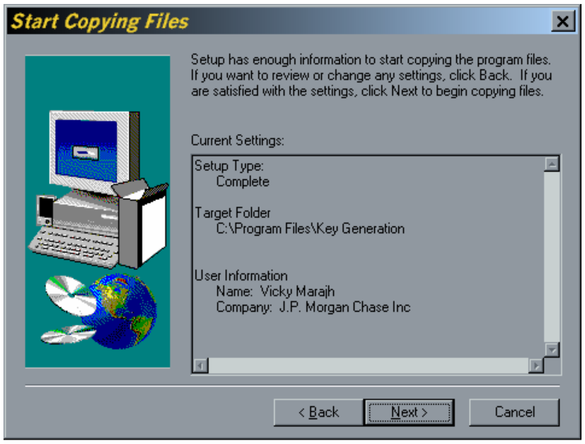
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.

Program Folders: Certificate Authority

Existing Folders:

Accessories
Cardshop
Certificate Authority
Citrix ICA Client
Cross All-Write
Games
GinnieNET 2020 Custodian 5.5
GinnieNET 2020 Issuer 5.3

9. The **Program Folder** (or group) is the window in which the RSA program icons will be located. The program folder name, which appears in the **Program Folders** field above, is the default. This name will used on the Windows™ **Programs Menu**. Change it if you need to do so and Select Next > to review your entries.



Start Copying Files

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

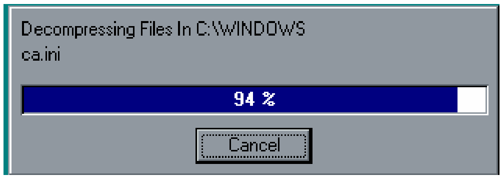
Current Settings:

Setup Type:
    Complete

Target Folder
    C:\Program Files\Key Generation

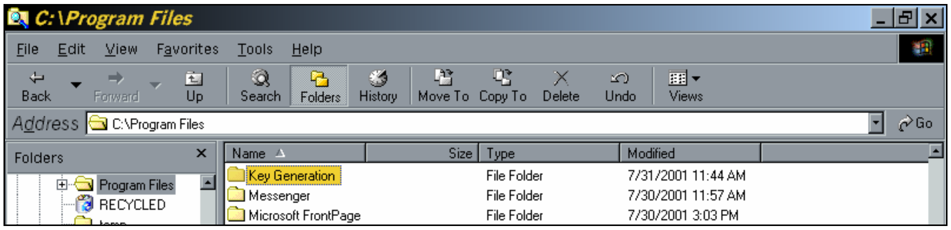
User Information
    Name: Vicky Marajh
    Company: J.P. Morgan Chase Inc

10. After confirming your selections, Select Next > again to start copying files.



Decompressing Files In C:\WINDOWS
ca.ini

- When the process is complete, a new program group will be placed on your **Programs Menu** and on your desktop.

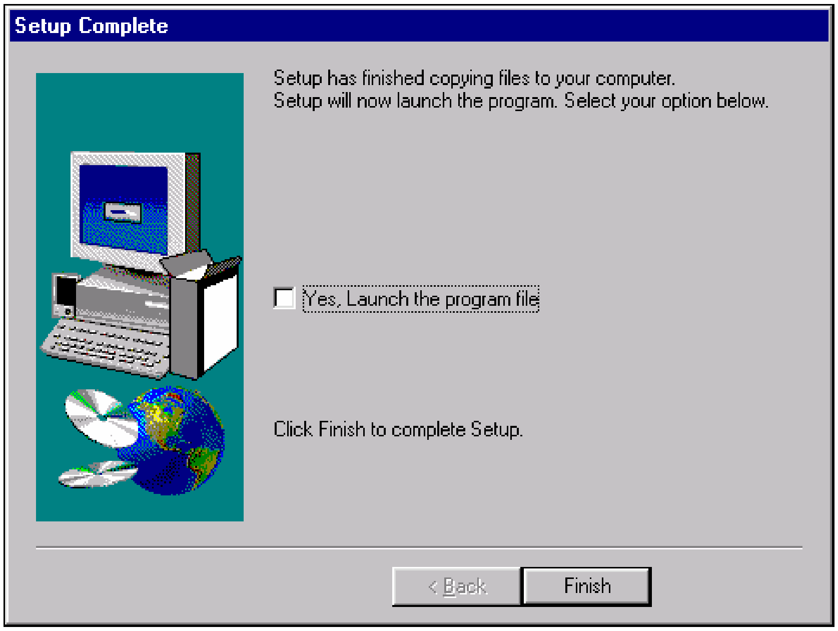


C:\Program Files
File Edit View Favorites Tools Help
Back Forward Up Search Folders History Move To Copy To Delete Undo Views
Address C:\Program Files
Go
Folders
Program Files
RECYCLED

Name	Size	Type	Modified
Key Generation		File Folder	7/31/2001 11:44 AM
Messenger		File Folder	7/30/2001 11:57 AM
Microsoft FrontPage		File Folder	7/30/2001 3:03 PM

- Finally, you will be invited to "Launch the program file." You can run it now or later. **Run it now**. The process takes only a few minutes.

You will need two IBM-formatted, 3 ½ " floppy diskettes or CDs.



Setup Complete

Setup has finished copying files to your computer.
Setup will now launch the program. Select your option below.

□ Yes, Launch the program file

Click Finish to complete Setup.

11. To launch the program, Select the □ Yes box and then Select Finish. To run the program later, leave the check box empty. Instructions for creating Public and Private Key certificates are provided in the next section.

RSA Public and Private Key Certificates

You will need two blank, IBM-formatted, 3 ½ " floppy diskettes to proceed.
Label them Disk 1: Private Key Disk and Disk 2: Public Key Disk.

RSA Private and Public Key certificates are created by the security officer to establish Ginnie*NET* security. These certificates are required for the **Fingerprint Enrollment** process.

Fingerprint enrollment requires…..

a. …that the user has a Private Key certificate stored on Disk 1 and

b. …that the Public Key certificate stored on Disk 2 has been properly certified and authenticated by Ginnie*NET* Customer Service.

After the security officer creates the Public and Private Key certificates, the Public Key Disk (Disk 2) must be sent to Ginnie*NET* Customer Service for authentication. Public Keys that have not been authenticated will not allow a user to complete the fingerprint enrollment process.

Mail each user's Public Key Disk to:

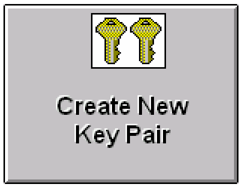
Ginnie*NET* Customer Service
Bank of New York
101 Barclay Street, 8E
New York, New York 10286

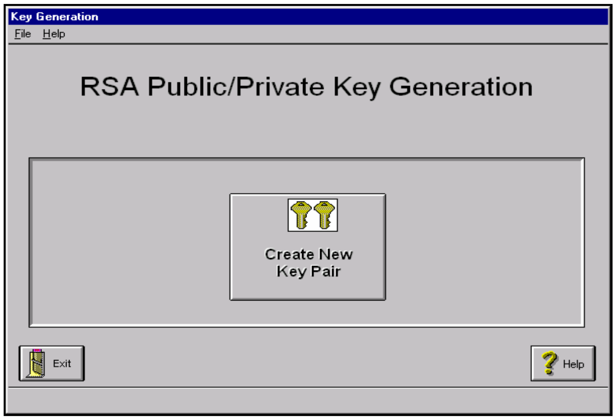
There will be a 48-hour turnaround time for Public Keys authentication once Ginnie*NET* Customer Service receives the Public Keys.

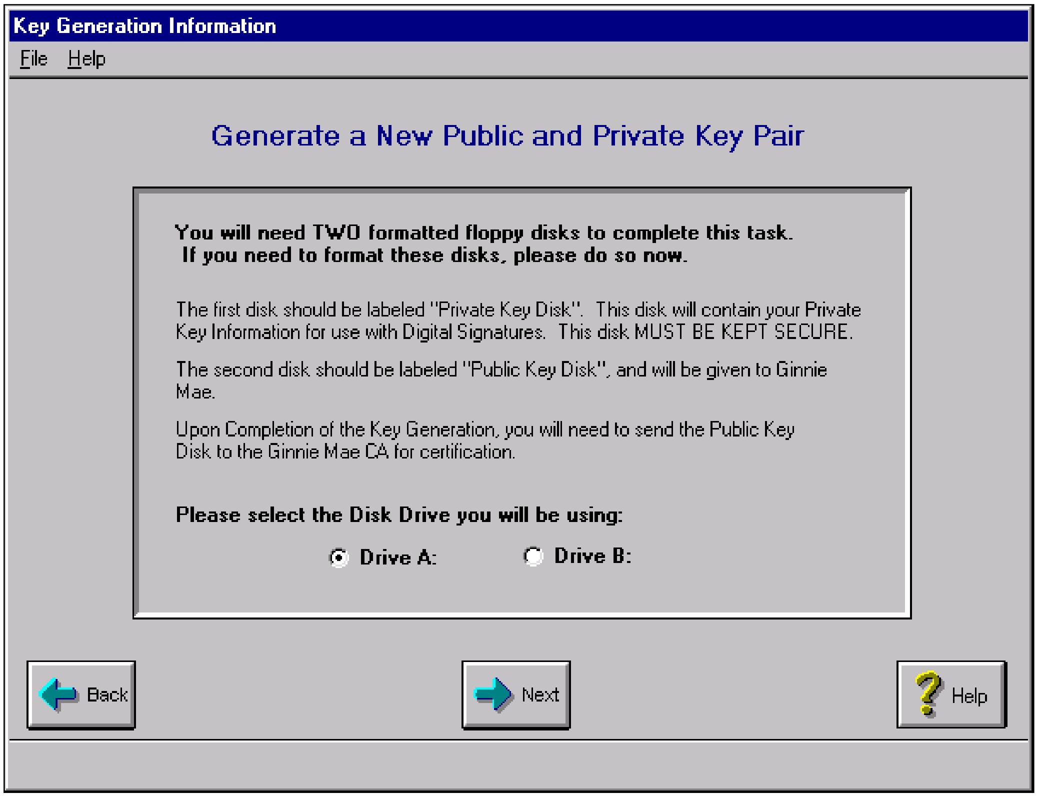
1. Double-Click on the **RSA Key Generation icon** in your Certificate Registration program group to start the process. Alternatively, you can run the program from the Windows™ Taskbar by choosing the following menu options:

Start , **Programs, Certificate Authority, Key Generation.**

2. Select **Create New Key Pair** to create Public and Private Key disks.







Key Generation Information

Generate a New Public and Private Key Pair

You will need TWO formatted floppy disks to complete this task.
If you need to format these disks, please do so now.

The first disk should be labeled "Private Key Disk". This disk will contain your Private Key Information for use with Digital Signatures. This disk MUST BE KEPT SECURE.

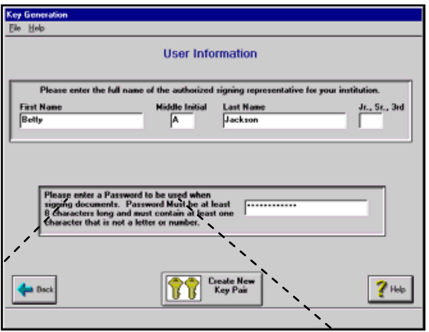
The second disk should be labeled "Public Key Disk", and will be given to Ginnie Mae.

Upon Completion of the Key Generation, you will need to send the Public Key Disk to the Ginnie Mae CA for certification.

Please select the Disk Drive you will be using:

● Drive A: ○ Drive B:

3. Select the appropriate disk drive and Select Next to access the **User Information** screen.



Key Generation

User Information

Please enter the full name of the authorized signing representative for your institution.

First Name	Middle Initial	Last Name	Jr., Sr., 3rd
Betty	A	Jackson	

Please enter a Password to be used when signing documents. Password Must be at least 8 characters long and must contain at least one character that is not a letter or number. ************

Please enter a Password to be used when signing documents. Password Must be at least 8 characters long and must contain at least one character that is not a letter or number.

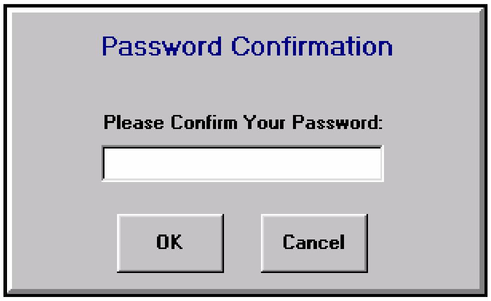
4. Follow the instructions carefully. Enter the full name of the authorized signing representative.
   Use Tab and Shift-Tab to move between fields.

☞ Select Help for additional information.

5. Follow the directions to create a valid RSA password. Choose a password that you can remember without writing it down.

6. Select Create New Key Pair to move on.

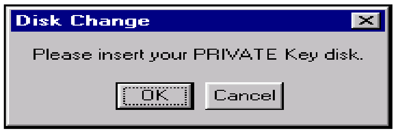
7. The system will prompt you to confirm your new RSA password. Enter it again on this screen and Select OK to proceed.



Password Confirmation

Please Confirm Your Password:

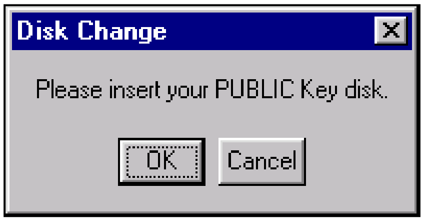
8. You will be instructed to insert the Private Key Disk.
Insert one of the blank, formatted floppy diskettes in
the floppy drive and Select OK.



Disk Change

Please insert your PRIVATE Key disk.

9. Then the system will ask for your Public Key Disk. Remove the Private Key Disk from the floppy drive and replace it with the second formatted floppy diskette.



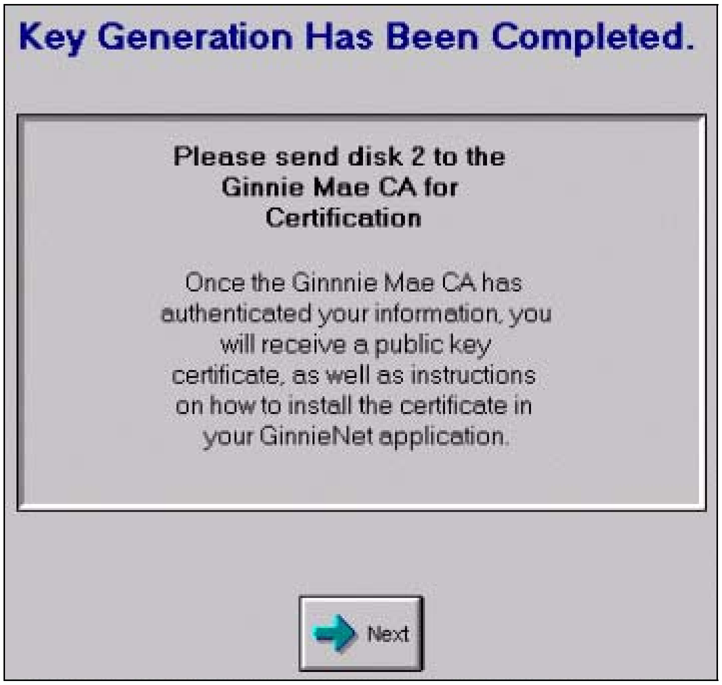
Disk Change

Please insert your PUBLIC Key disk.

RSA - Key Generation

☞ Label Disk 1 now (Private Key disk), while Disk 2 (Public Key Disk) is still in the drive avoid mixing up the diskettes.

- When the system returns, **you're done**.



Key Generation Has Been Completed.

Please send disk 2 to the Ginnie Mae CA for Certification

Once the Ginnie Mae CA has authenticated your information, you will receive a public key certificate, as well as instructions on how to install the certificate in your GinnieNet application.

⚠ Follow the instructions for the disposition of the Public Key disk and submission of supporting documentation including (a) instructions on the screen above; (b) instructions in the beginning of this section and those in Program Enrollment and Set-Up. You are responsible for submitting required materials and supporting documentation. If you have questions, call Ginnie*NET* Customer Service at 1-800-234-4662, option 1.

10. Select Next to exit the program.

INSTALLING FINGERPRINT SCANNER SYSTEM

The fingerprint reader is a desktop device. The Web application triggers an ActiveX control*. The ActiveX control communicates with the Fingerprint Server using TCPIP over port 1200. The Web Application generally changes C:\Program Files\BioPlugin\Client.ini to point to the Fingerprint Server (in the Server section the IP key value is changed to www.ginnienet.net).

If there are constraints in your organization requiring that you run through a proxy server, the workaround is as follows:

1. Install the Fingerprint Reader software. Make certain REGISTRATION_ID value in the KEY Section of C:\Program Files\BioPlugin\Client.ini matches the LID on the Reader.

2. Edit C:\Program Files\BioPlugin\Client.ini. Change the value of IP in the Server section to the address needed to reach the Proxy Server.

3. Change the attributes for C:\Program Files\BioPlugin\Client.ini so that it is “read-only”.

4. The proxy server needs to be configured so it will pass the communications via port 1200 on to the IP address 160.254.60.14.

5. Port 1200 is required to be open only for outbound initiated communication which minimizes the risk. Additionally, communication can be restricted to specified sites, which further reduces the risk.

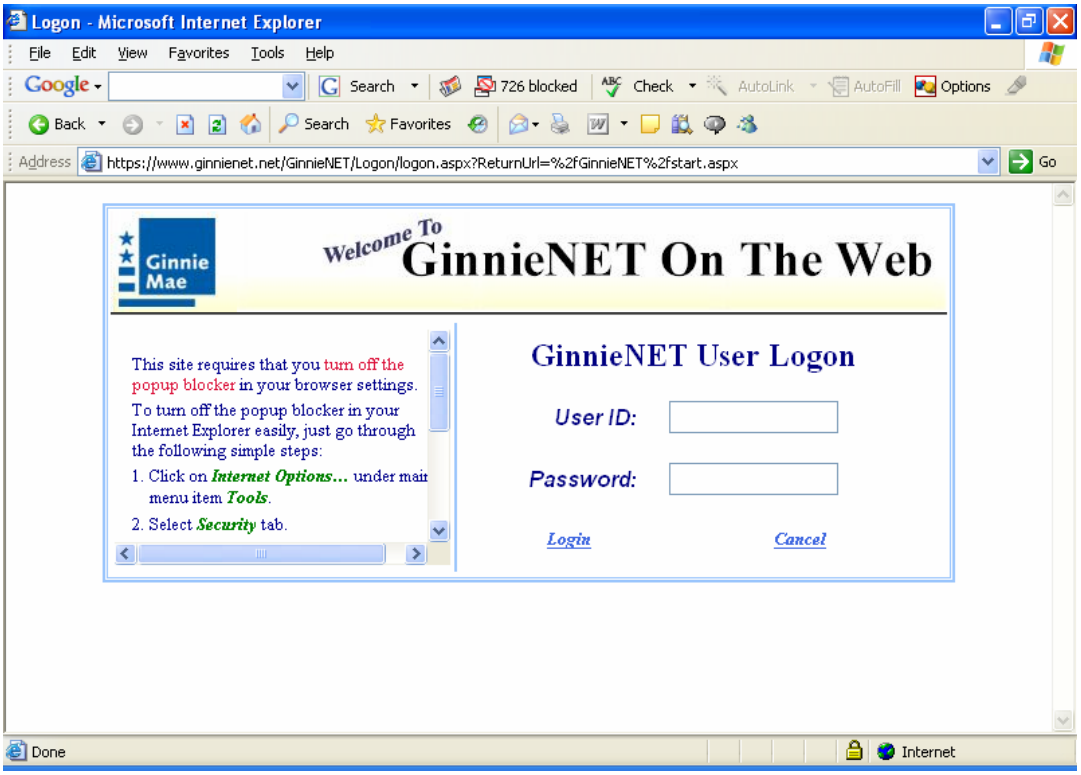
Your infrastructure team should be able to restrict the availability of the port to a discrete segment of your network. It does not need to be opened universally.

Note: The ActiveX control can be downloaded from ginnienet.net and is to be installed on the workstation. The installation creates the directory C:\Program Files\BioPlugin.

INSTALLATION

- ***<u>Do not attach fingerprint scanner until installation is complete and your system has been restarted.</u>***

To begin the installation process log onto the Ginnie*NET* website at www.ginnienet.net to download software.


Logon - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Google Search 726 blocked Check AutoLink AutoFill Options
Back Search Favorites
Address
Go
Ginnie Mae
Welcome To
GinnieNET On The Web
Login
Cancel
Done
Internet

Address: https://www.ginnienet.net/GinnieNET/Logon/logon.aspx?ReturnUrl=%2fGinnieNET%2fstart.aspx

This site requires that you turn off the popup blocker in your browser settings.

To turn off the popup blocker in your Internet Explorer easily, just go through the following simple steps:

1. Click on ***Internet Options...*** under mai menu item ***Tools***.
2. Select ***Security*** tab.

GinnieNET User Logon

User ID:

Password:

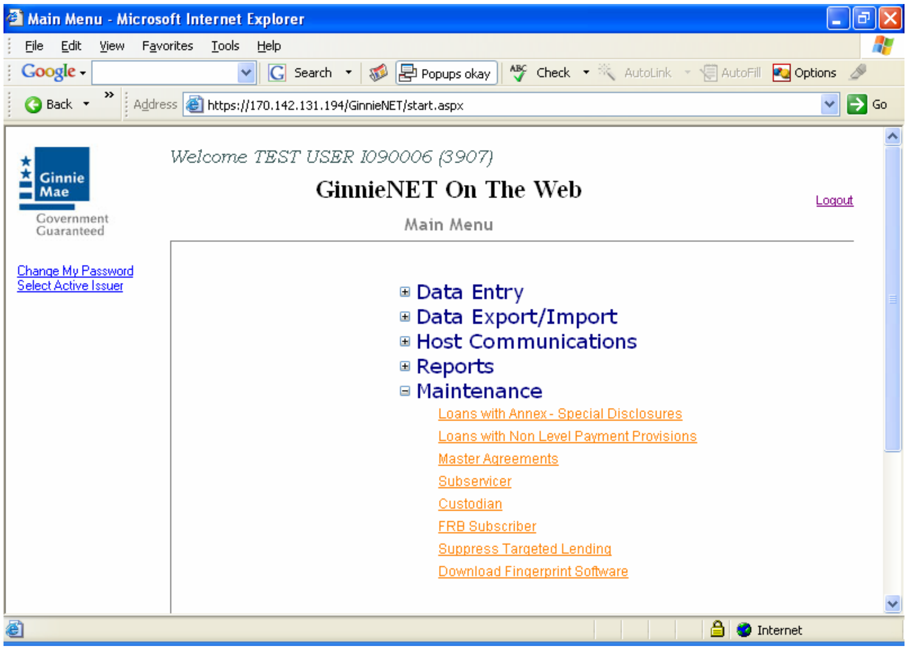
Site Requirements

1. This site requires that you turn off the popup blocker in your browser settings.

Turning Off Popup Blocker:

2. Select on ***Internet Options…*** under main menu item ***Tools***.
3. Select ***Security*** tab.
4. Select on ***Internet*** icon if you are accessing our web on the internet, or ***Local intranet*** if you are accessing within our intra-net environment.
5. Select on ***Custom Level…*** button.
6. Find **Use *pop-up Blocker*** item, and disable it.
7. Select on ***OK*** button to save the new setting.

1. Select ***Maintenance*** and ***Download Fingerprint Software***.



Main Menu - Microsoft Internet Explorer

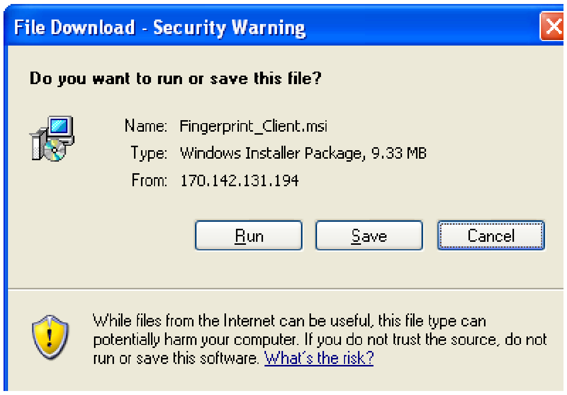
Address https://170.142.131.194/GinnieNET/start.aspx

Welcome TEST USER I090006 (3907)

GinnieNET On The Web

Main Menu

2. Select ***Run*** to install software.

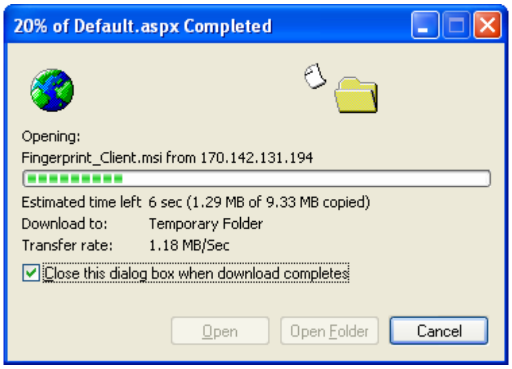


File Download - Security Warning

Do you want to run or save this file?

Name: Fingerprint_Client.msi
Type: Windows Installer Package, 9.33 MB
From: 170.142.131.194

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?



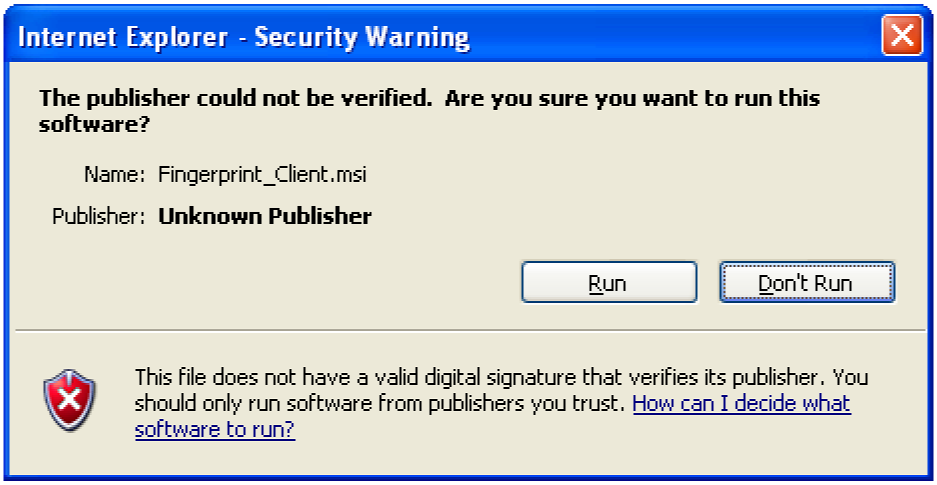
20% of Default.aspx Completed

Opening:
Fingerprint_Client.msi from 170.142.131.194

Estimated time left 6 sec (1.29 MB of 9.33 MB copied)
Download to: Temporary Folder
Transfer rate: 1.18 MB/Sec

☑ Close this dialog box when download completes

3. Security verification select ***Run*** to continue installing software.



Internet Explorer - Security Warning

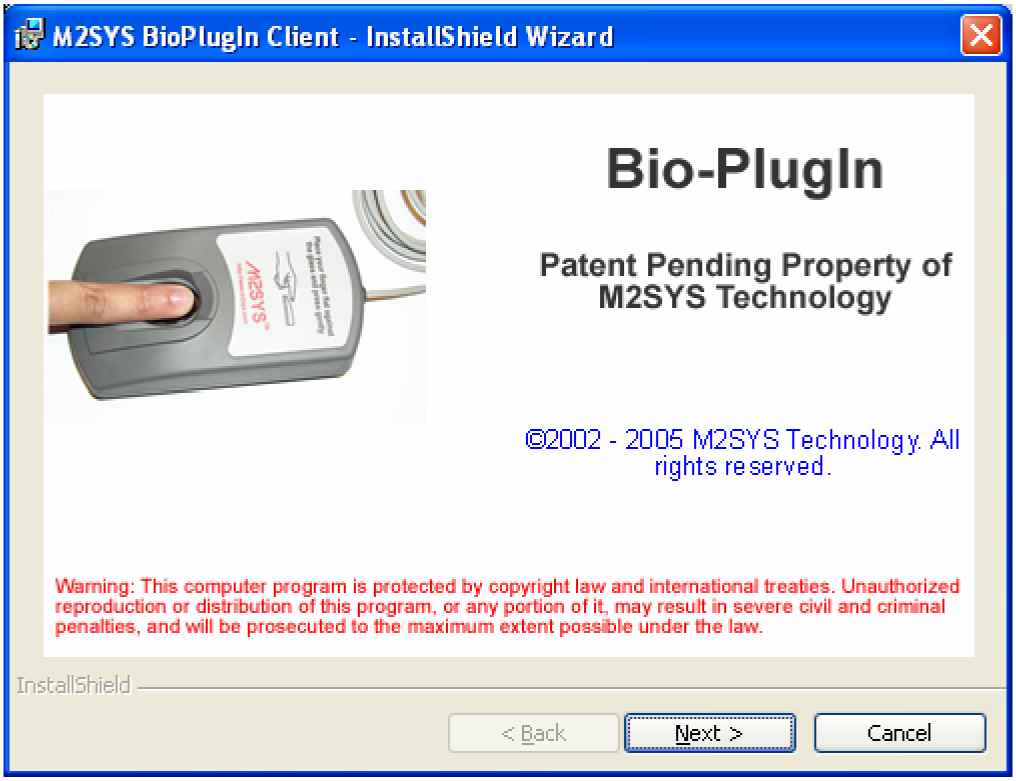
The publisher could not be verified. Are you sure you want to run this software?

Name: Fingerprint_Client.msi

Publisher: **Unknown Publisher**

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

4. Select ***Next*** to install the Bio-PlugIn software.



M2SYS BioPlugIn Client - InstallShield Wizard

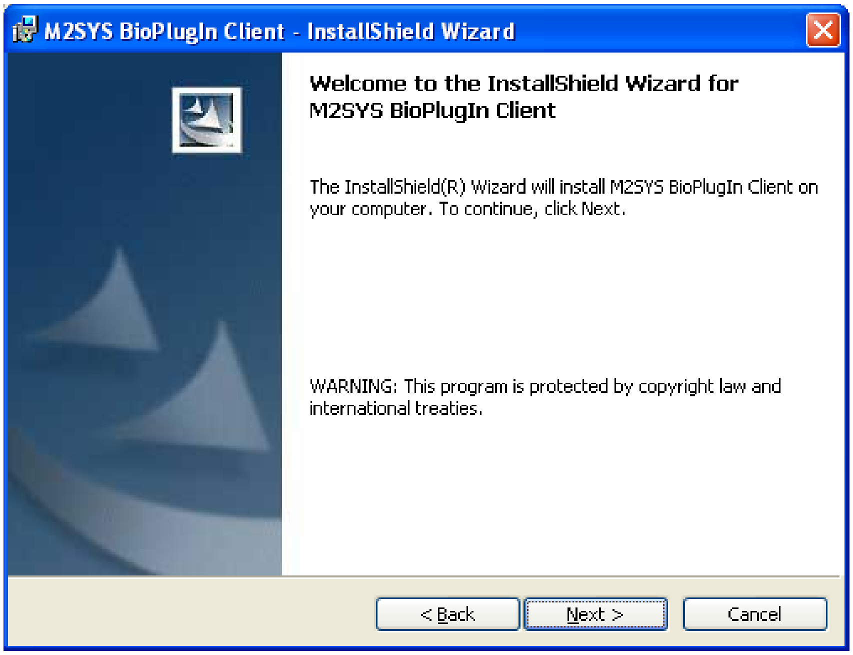
Bio-PlugIn

Patent Pending Property of M2SYS Technology

©2002 - 2005 M2SYS Technology. All rights reserved.

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

5. Once initialized, Setup presents a Welcome screen. Select ***Next*** to acknowledge the welcome, the warning and the copyright.



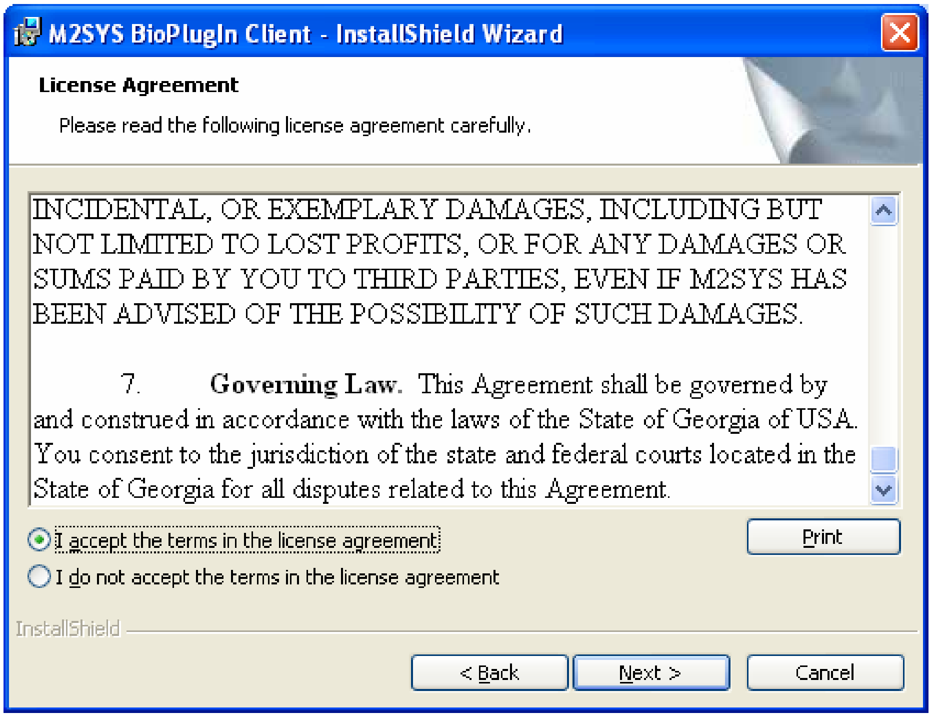
M2SYS BioPlugIn Client - InstallShield Wizard

Welcome to the InstallShield Wizard for M2SYS BioPlugIn Client

The InstallShield(R) Wizard will install M2SYS BioPlugIn Client on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

6. Please read the License Agreement select Print for a copy of the license. Select on ***Accept*** and ***Next*** to continue with the installation.



M2SYS BioPlugIn Client - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

INCIDENTAL, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO LOST PROFITS, OR FOR ANY DAMAGES OR SUMS PAID BY YOU TO THIRD PARTIES, EVEN IF M2SYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the State of Georgia of USA. You consent to the jurisdiction of the state and federal courts located in the State of Georgia for all disputes related to this Agreement.

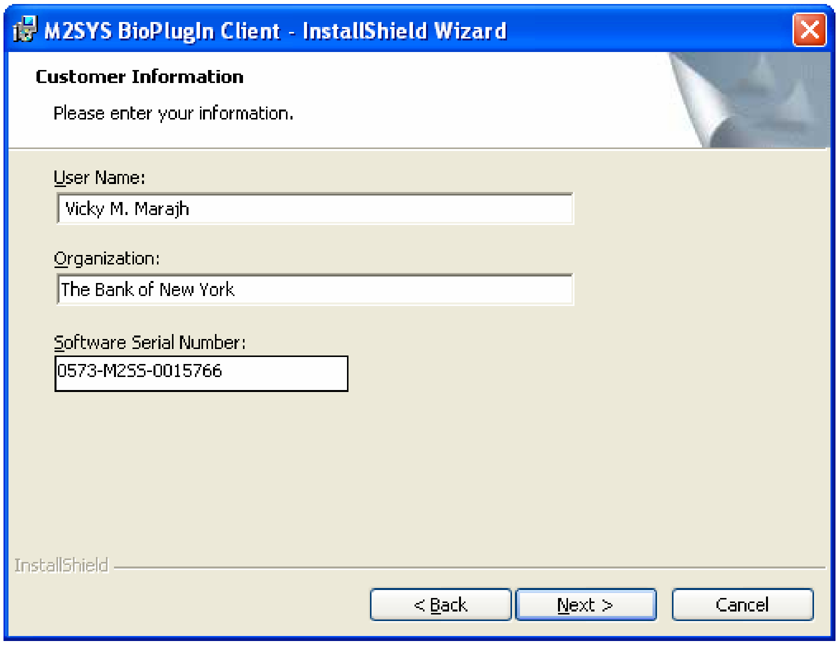
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

7. Enter your ***User Name, Organization and Software Serial Number***.

Software Serial Number

0573-M2SS-0015766



Customer Information

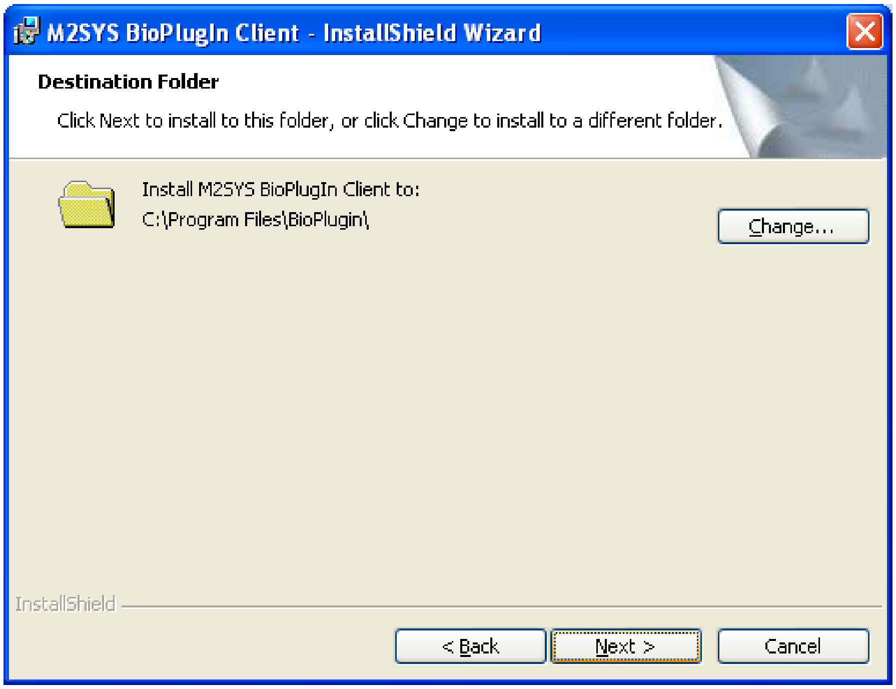
Please enter your information.

User Name:
Vicky M. Marajh

Organization:
The Bank of New York

Software Serial Number:
0573-M2SS-0015766

8. Setup will recommend a default installation if you need to change to a different folder or create a new folder Select on ***Change.*** Select ***Next*** when you are comfortable with the Program Group name.

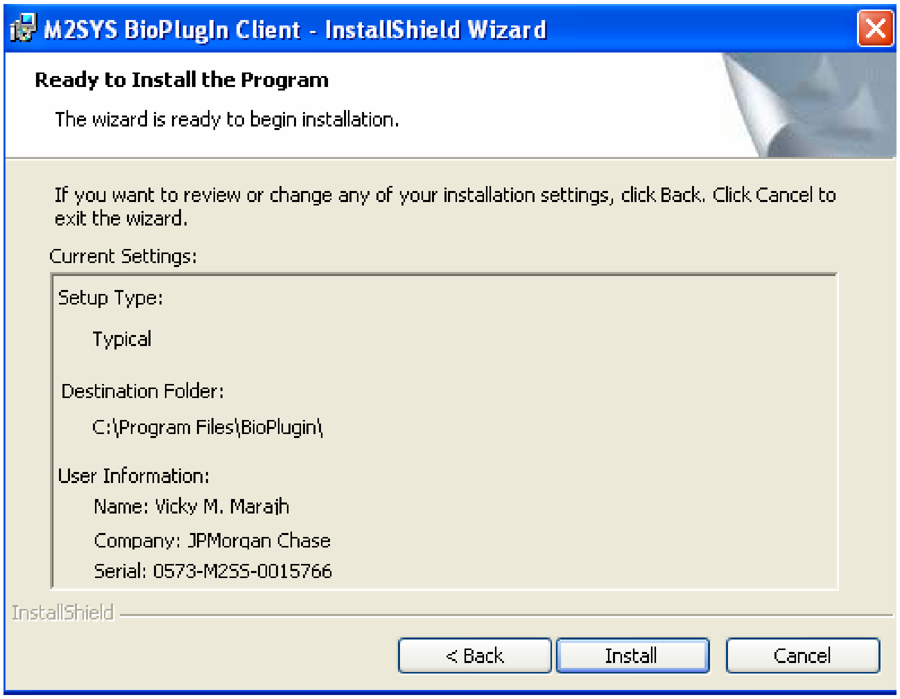


Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install M2SYS BioPlugIn Client to:
C:\Program Files\BioPlugin\

9. The Program Folder (or group) is the window in which the Bio-Plugin program will be located. The program folder name, which appears in the Program Folders field above, is the default. To make change Select the ***Back*** or ***Install*** to accept enters and start coping files.



M2SYS BioPlugIn Client - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Current Settings:

Setup Type:

Typical

Destination Folder:

C:\Program Files\BioPlugin\

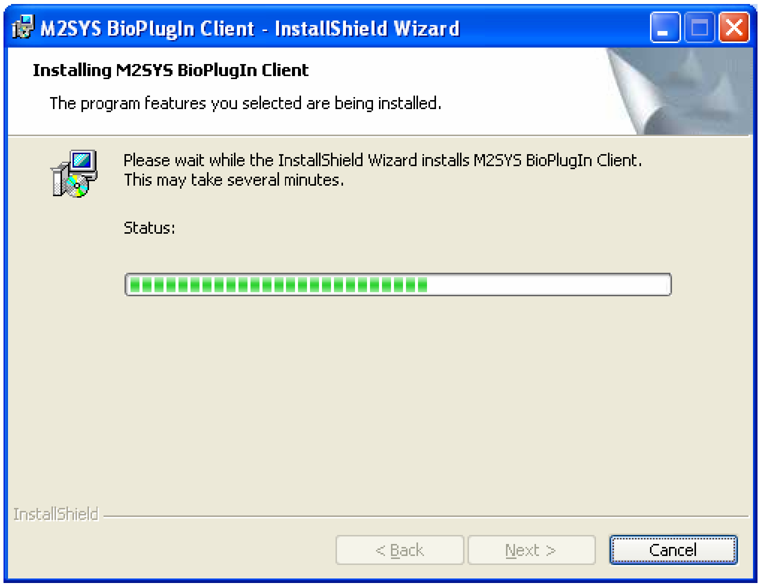
User Information:

Name: Vicky M. Marajh

Company: JPMorgan Chase

Serial: 0573-M2SS-0015766

10. The system may take several minutes to copy files.



M2SYS BioPlugIn Client - InstallShield Wizard

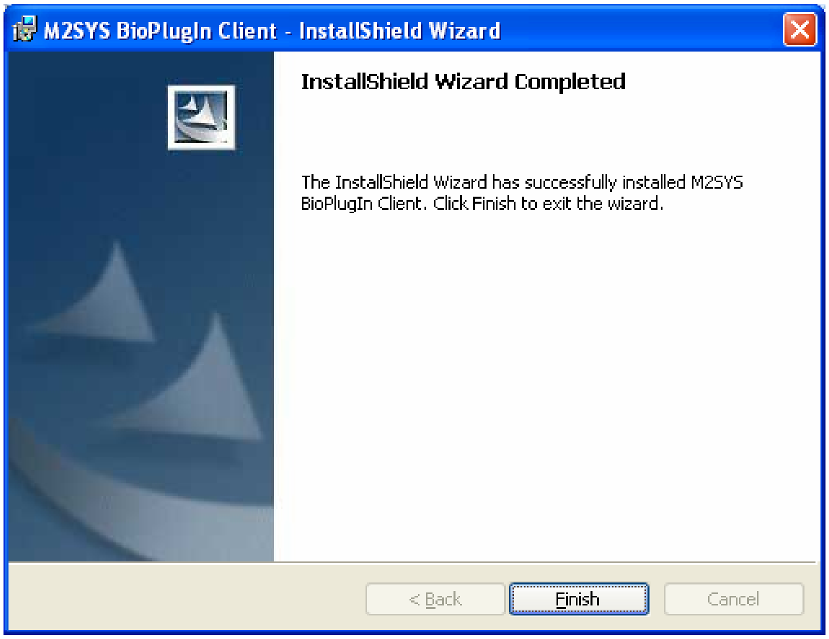
Installing M2SYS BioPlugIn Client

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs M2SYS BioPlugIn Client. This may take several minutes.

Status:

11. Select on ***Finish*** to complete installation.

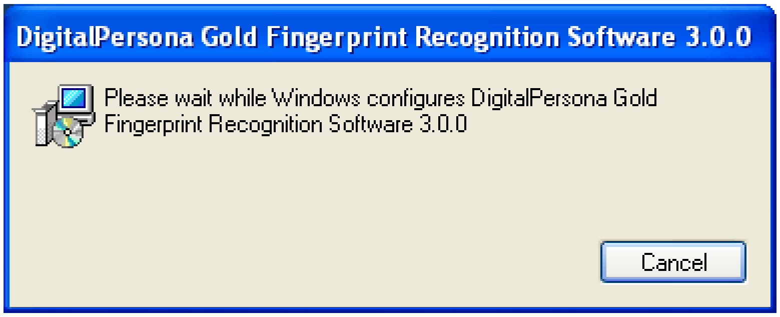


M2SYS BioPlugIn Client - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed M2SYS BioPlugIn Client. Click Finish to exit the wizard.

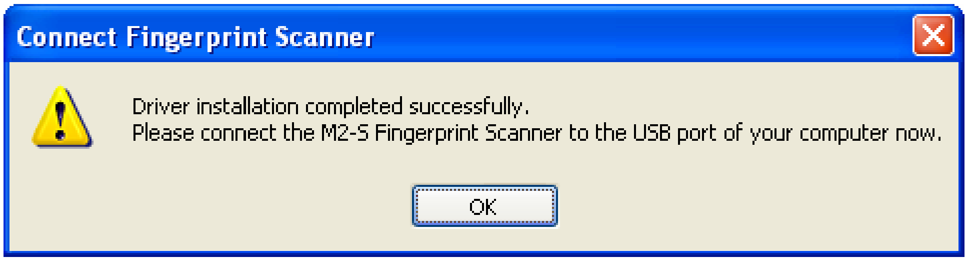
12. System will configure fingerprint software.



DigitalPersona Gold Fingerprint Recognition Software 3.0.0

Please wait while Windows configures DigitalPersona Gold Fingerprint Recognition Software 3.0.0

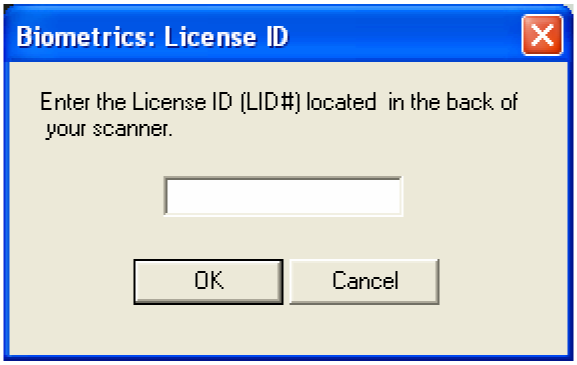
13. Select on ***OK*** to restart your system.



Connect Fingerprint Scanner

Driver installation completed successfully.
Please connect the M2-S Fingerprint Scanner to the USB port of your computer now.

14. Once you log into your system attach the Fingerprint Scanner to your USB port. The system will prompt you for the License ID (LID#) at the back of your scanner.



Enter the License ID (LID#) located in the back of your scanner.

15. Installation is complete.