คู่มือการใช้งาน PGP บน Windows

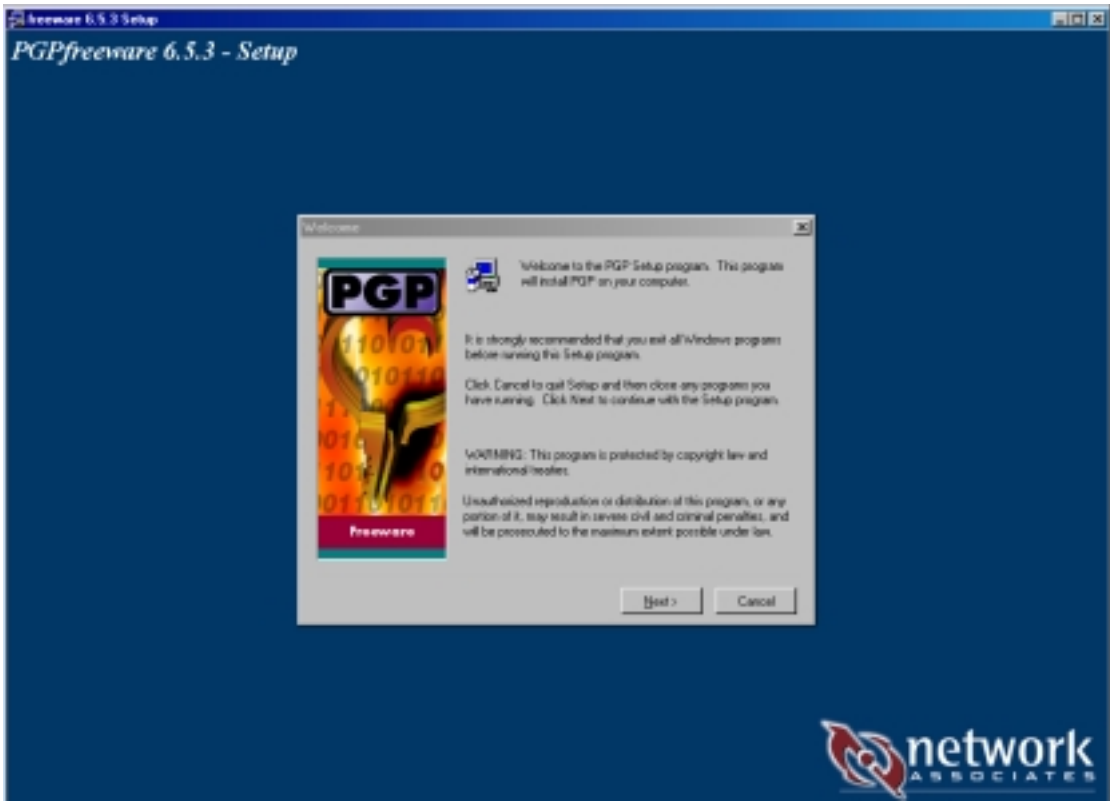
คู่มือฉบับนี้ได้จัดทำขึ้นเพื่อการใช้งาน PGP เพื่อสร้างความปลอดภัยในการติดต่อสื่อสารด้วย email โดยใช้ email application ใน Windows ซึ่งยังไม่ครอบคลุมรายละเอียดการใช้งาน PGP ในด้านอื่นๆ หากท่านต้องการข้อมูลเพิ่มเติม ท่านสามารถอ่านรายละเอียดได้ในเอกสารที่มาพร้อมกับโปรแกรม PGP หลังการติดตั้งแล้ว

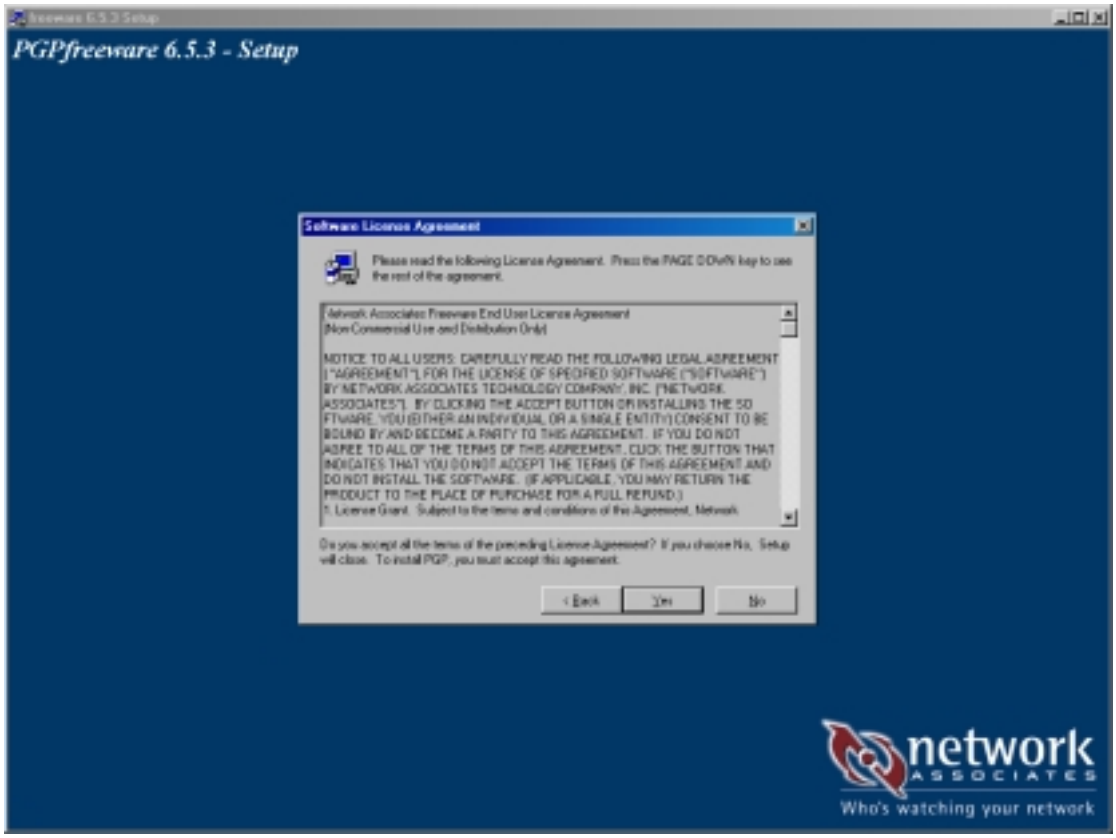
วิธีติดตั้ง PGP Desktop (PGP for windows)

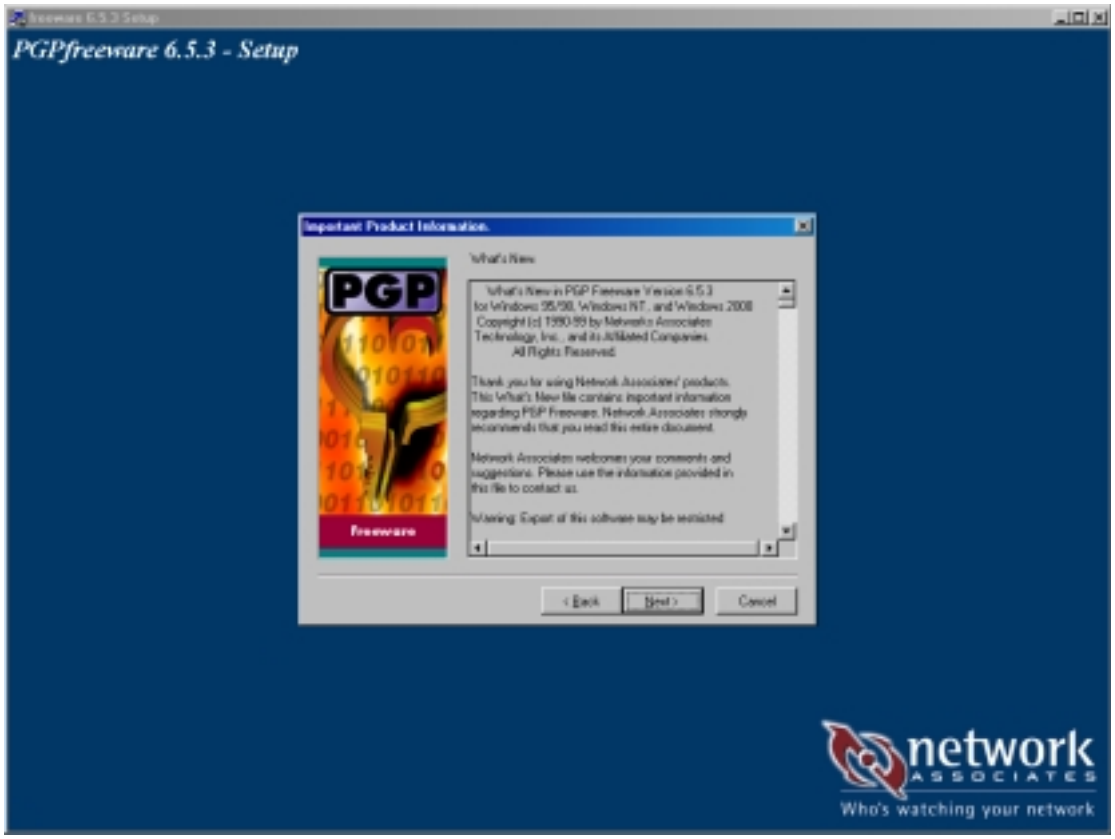
1. ทำการ unzip โปรแกรม PGP freeware ซึ่งเป็น zip file ชื่อ PGPfreeware_6.5.3.zip อยู่ในแผ่น CD ROM นี้ หรือ ท่านสามารถ download ได้จาก

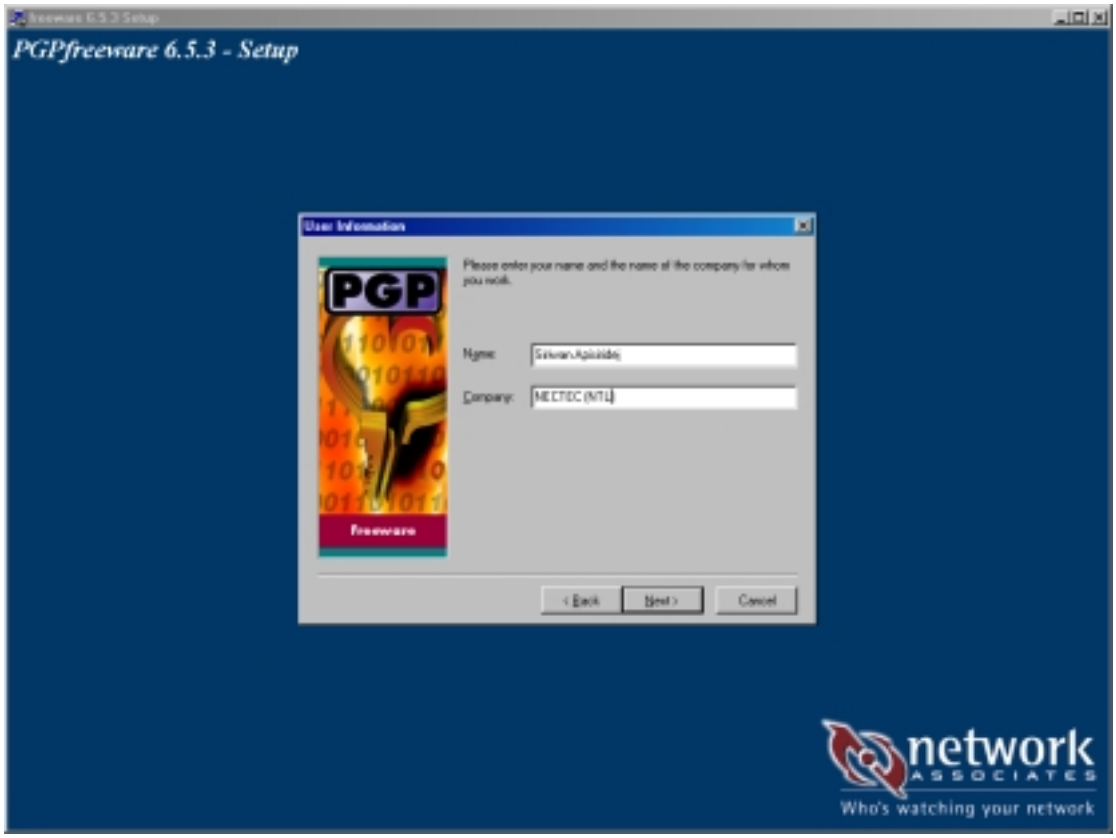
   http://www.pgpi.org/cgi/download.cgi?filename=PGPfreeware_6.5.3.zip หรือ

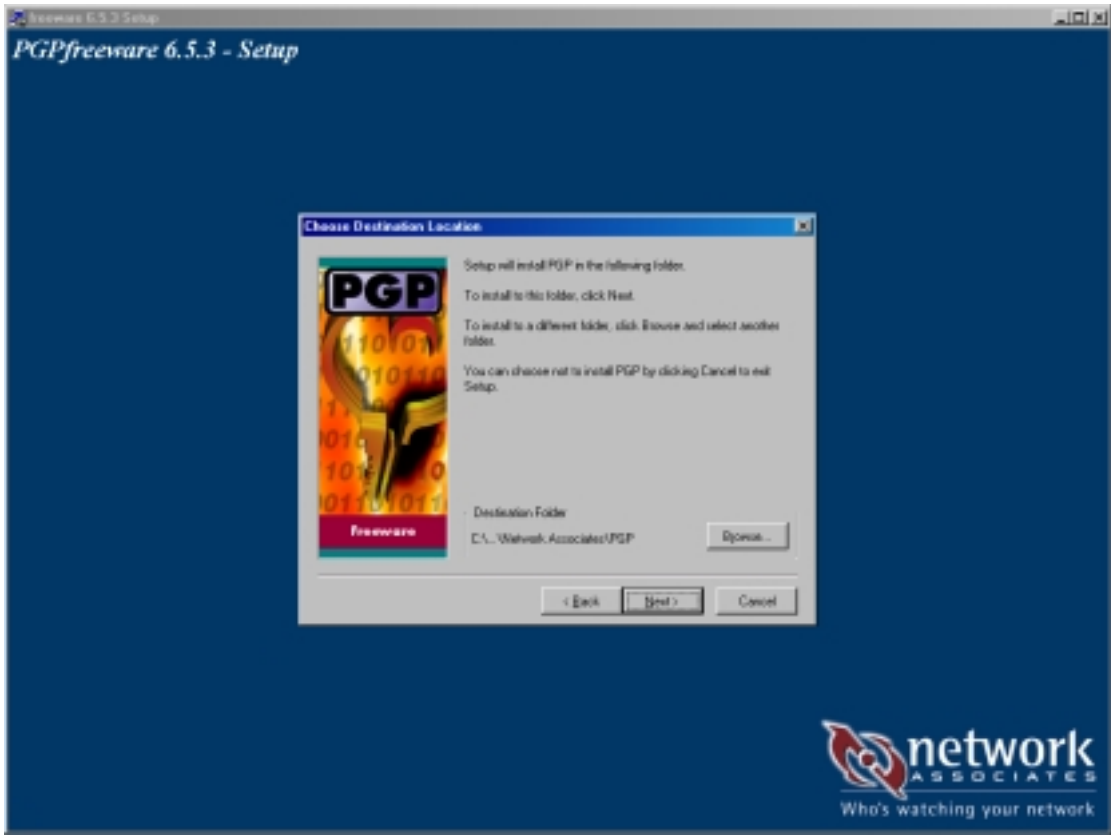
   http://www.nectec.or.th/thaicert
2. เริ่มติดตั้งได้โดย double click ที่ file ชื่อ setup ซึ่งอยู่ภายใต้ directory ที่ทำการ unzip ไว้
3. จากนั้นทำการติดตั้งตามขั้นตอนดังรูปข้างล่างนี้โดยกดปุ่ม **Next** และ/หรือ **OK** รวมทั้งกรอกข้อมูลที่จำเป็นไปเรื่อยๆ

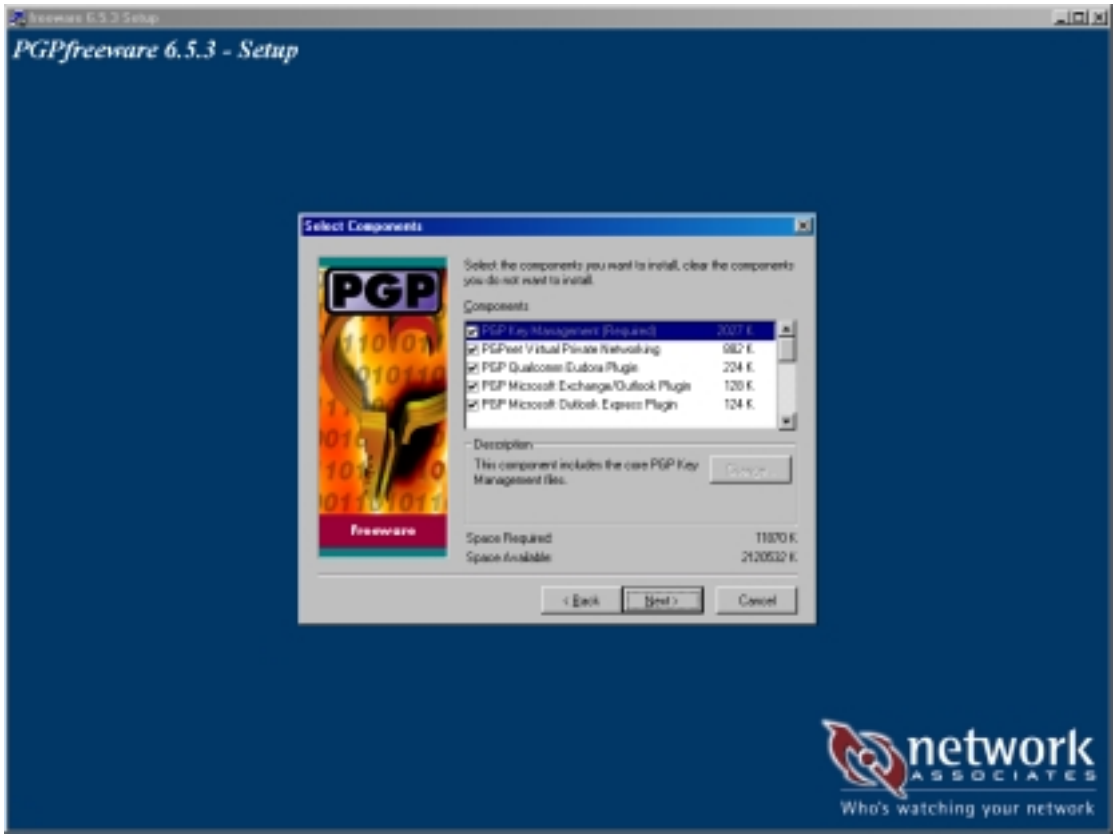


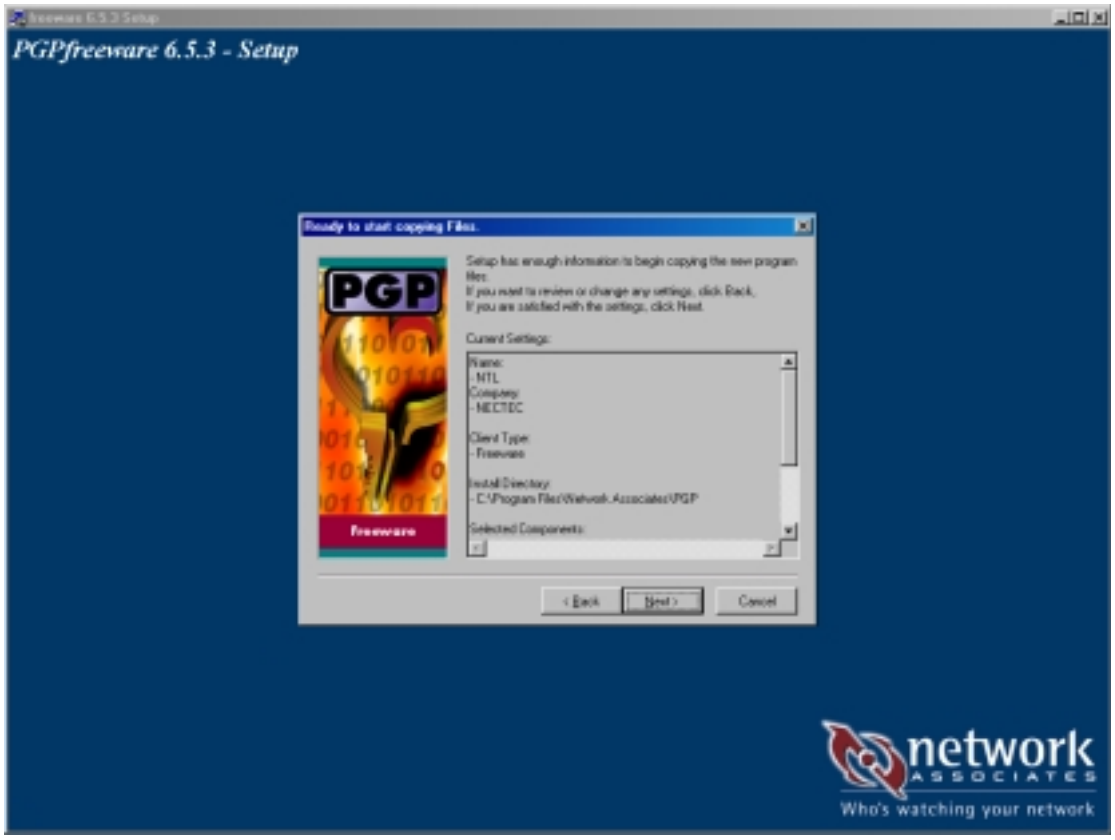

PGPfreeware 6.5.3 - Setup
Software License Agreement
Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.
Network Associates Freeware End User License Agreement
(Non-Commercial Use and Distribution Only)
NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT") FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") BY NETWORK ASSOCIATES TECHNOLOGY COMPANY, INC. ("NETWORK ASSOCIATES"). BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)
1. License Grant. Subject to the terms and conditions of this Agreement, Network
Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install PGP, you must accept this agreement.
< Back
Yes
No
network ASSOCIATES
Who's watching your network

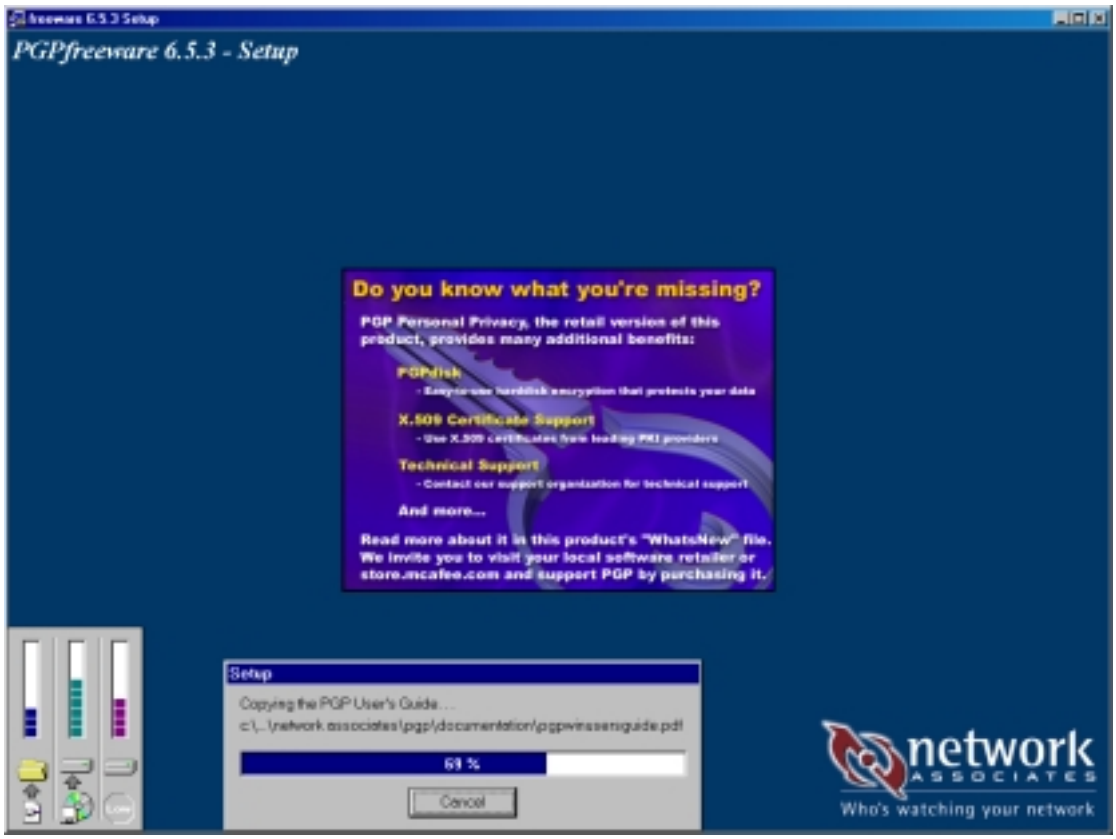

PGPfreeware 6.5.3 - Setup
Important Product Information.
What's New
What's New in PGP Freeware Version 6.5.3
for Windows 95/98, Windows NT, and Windows 2000
Copyright (c) 1990-99 by Network Associates
Technology, Inc., and its Affiliated Companies
All Rights Reserved
Thank you for using Network Associates' products.
This What's New file contains important information
regarding PGP Freeware. Network Associates strongly
recommends that you read this entire document.
Network Associates welcomes your comments and
suggestions. Please use the information provided in
this file to contact us.
Warning: Export of this software may be restricted
PGP
Freeware
< Back
Next >
Cancel
network ASSOCIATES
Who's watching your network

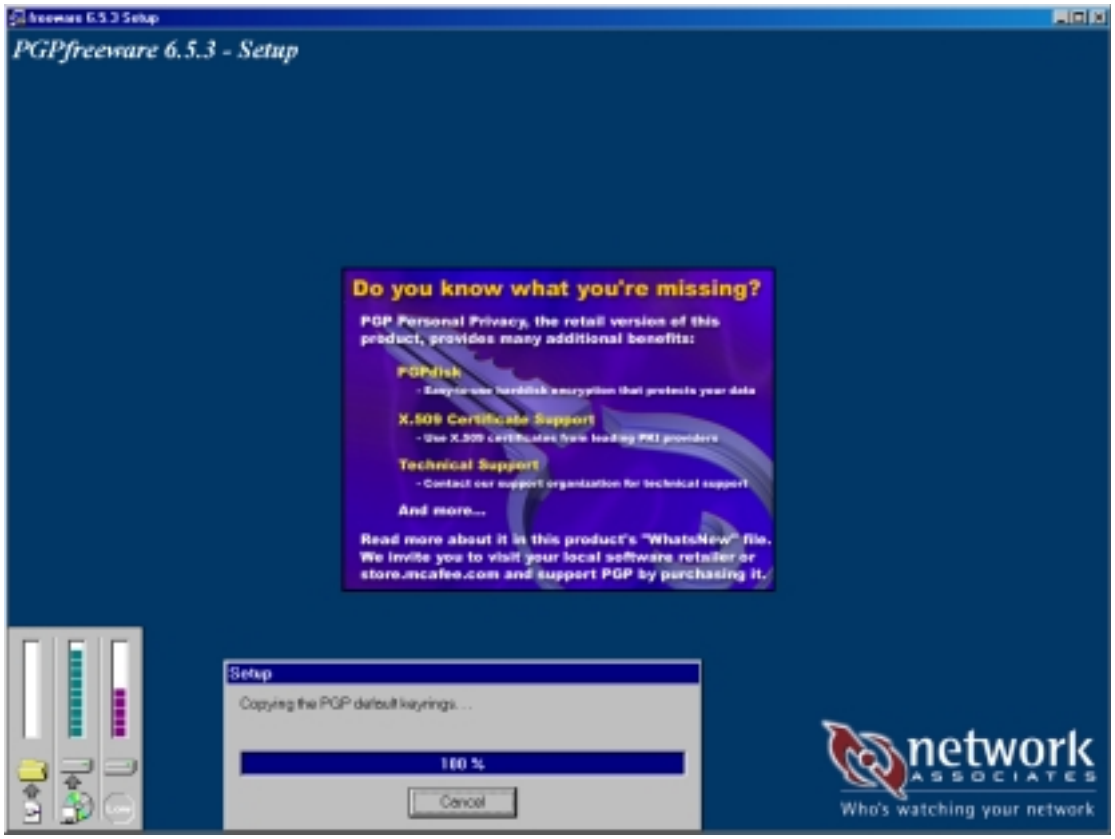

PGPfreeware 6.5.3 - Setup
User Information
Please enter your name and the name of the company for whom you work.
Name:
Company:
MECTEC (NTL)
< Back
Next >
Cancel
network ASSOCIATES
Who's watching your network


PGPfreeware 6.5.3 - Setup
Choose Destination Location
Setup will install PGP in the following folder.
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
You can choose not to install PGP by clicking Cancel to exit Setup.
Destination Folder
C:\...\Network Associates\PGP
Browse...
< Back
Next >
Cancel
network ASSOCIATES
Who's watching your network

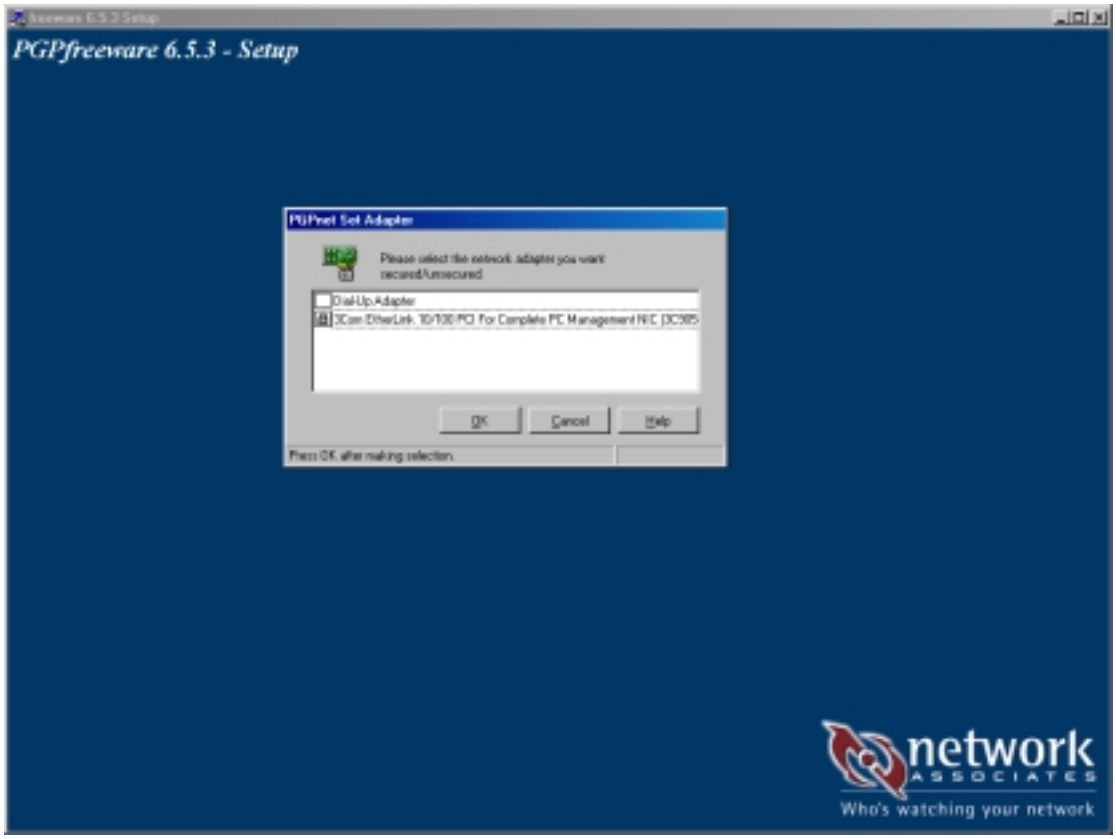

PGPfreeware 6.5.3 - Setup
Select Components
Select the components you want to install, clear the components you do not want to install.
Components
PGP Key Management (Required) 2027 K
PGPnet Virtual Private Networking 982 K
PGP Qualcomm Eudora Plugin 224 K
PGP Microsoft Exchange/Outlook Plugin 120 K
PGP Microsoft Outlook Express Plugin 124 K
Description
This component includes the core PGP Key Management files.
Change...
Space Required: 11870 K
Space Available: 2120532 K
< Back
Next >
Cancel
PGP
freeware
network ASSOCIATES
Who's watching your network


PGPfreeware 6.5.3 - Setup
Ready to start copying Files.
Setup has enough information to begin copying the new program files.
If you want to review or change any settings, click Back.
If you are satisfied with the settings, click Next.
Current Settings:
Name:
- MTL
Company:
- NECTEC
Client Type:
- Freeware
Install Directory:
- C:\Program Files\Network Associates\PGP
Selected Components:
< Back
Next >
Cancel
PGP
freeware
network ASSOCIATES
Who's watching your network

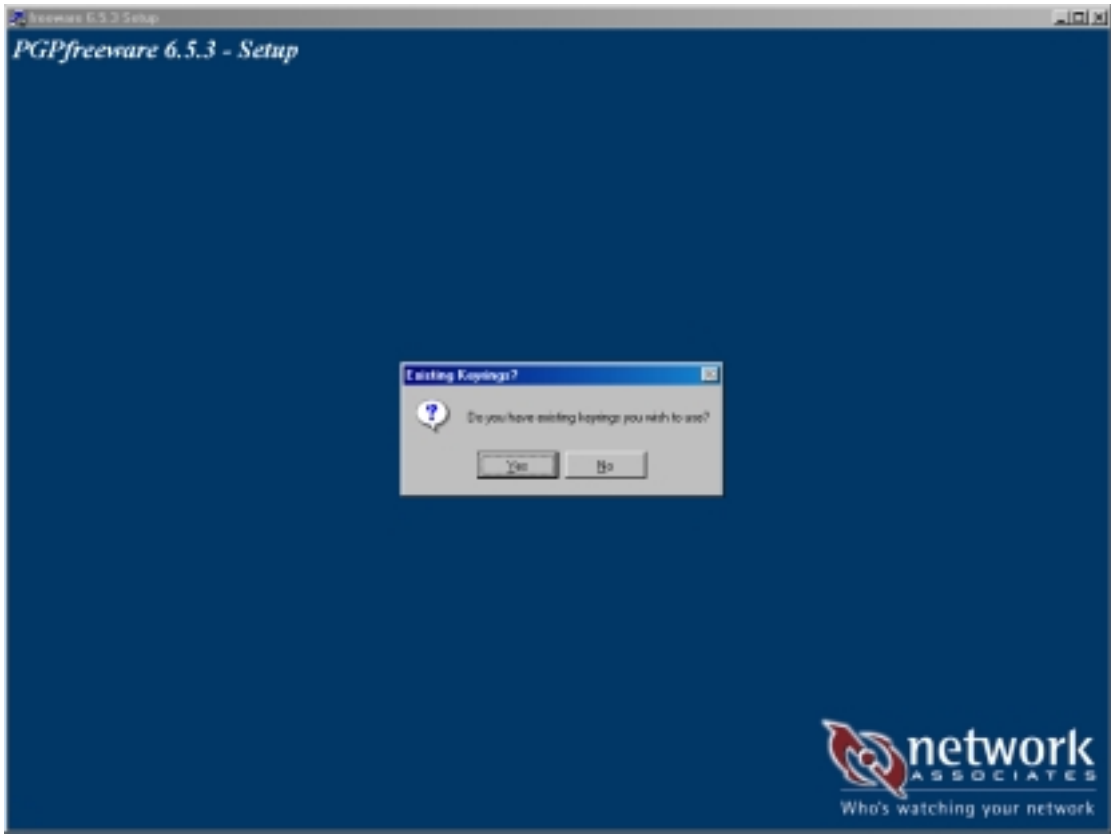

PGPfreeware 6.5.3 - Setup
Do you know what you're missing?
PGP Personal Privacy, the retail version of this product, provides many additional benefits:
PGPdisk
X.509 Certificate Support
Technical Support
And more...
Read more about it in this product's "WhatsNew" file. We invite you to visit your local software retailer or store.mcafee.com and support PGP by purchasing it.
Setup
Copying the PGP User's Guide...
c:\...\network associates\pgp\documentation\pgpwinuserguide.pdf
69 %
Cancel
network ASSOCIATES
Who's watching your network


PGPfreeware 6.5.3 - Setup
Do you know what you're missing?
PGP Personal Privacy, the retail version of this product, provides many additional benefits:
PGPdisk
X.509 Certificate Support
Technical Support
And more...
Read more about it in this product's "WhatsNew" file. We invite you to visit your local software retailer or store.mcafee.com and support PGP by purchasing it.
Setup
Copying the PGP default keyrings...
100 %
Cancel
network ASSOCIATES
Who's watching your network

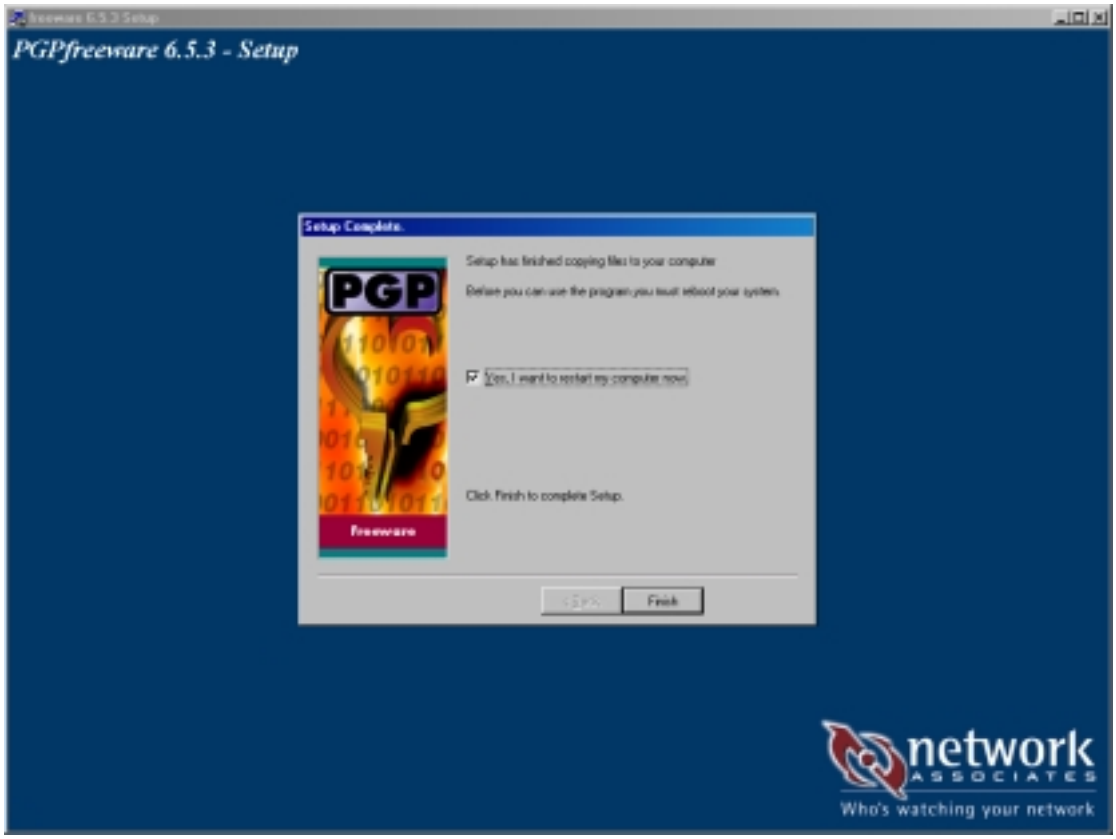
4. ในหน้าต่างนี้ กรณีที่เครื่อง PC ของท่านต่อ LAN ให้เลือก 3Com Etherlink แต่ถ้าใช้ modem ให้เลือก Dial-Up Adapter



5. ในหน้าต่างนี้ ถ้าท่านเคยสร้าง key หรือมี keyring files อยู่แล้วให้เลือก **Yes** แต่ถ้าไม่มีให้เลือก **No**



6. เมื่อถึงขั้นตอนนี้แล้ว ท่านสามารถเลือกให้เครื่องทำการ restart ทันทีหลังจากกดปุ่ม **Finish** หรือ ท่านจะทำการ restart ทีหลังก็ได้



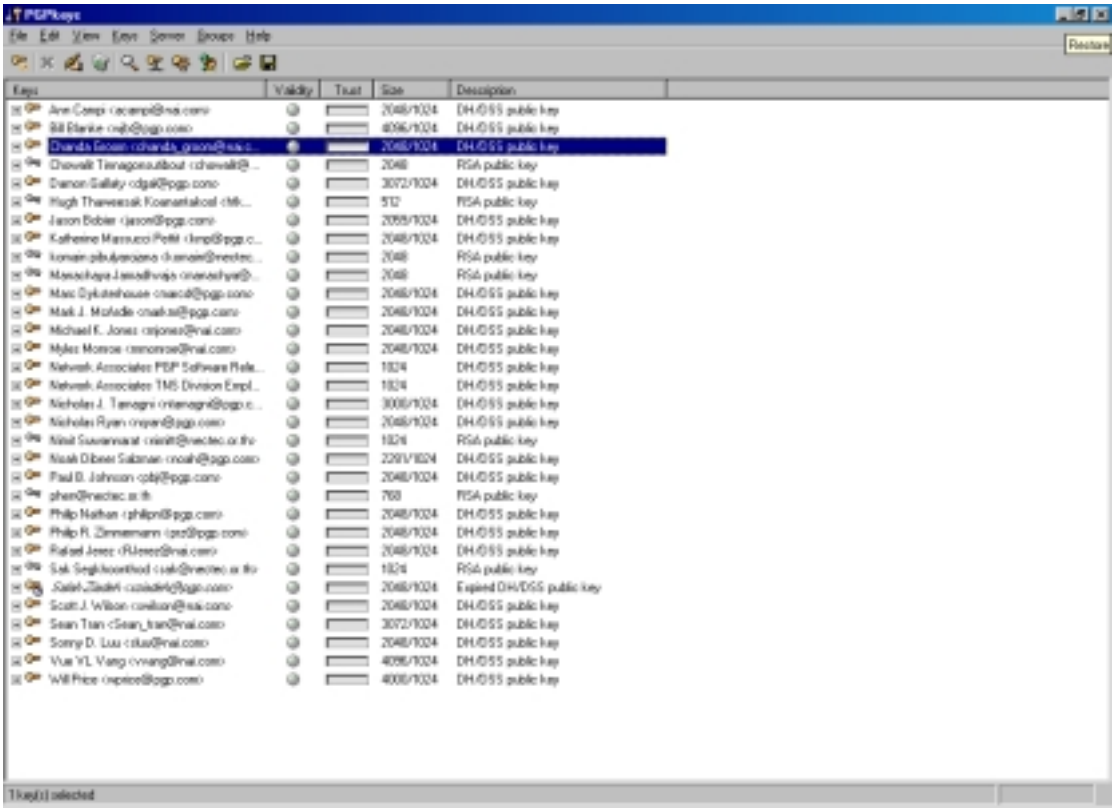
เมื่อ restart แล้วท่านก็จะสามารถใช้งาน PGPได้ แต่ก่อนจะใช้ท่านจำเป็นจะต้องมี key pair ซึ่งท่านสามารถทำตามขั้นตอนต่อไปนี้

วิธีสร้าง key pair

ในกรณีที่ท่านทำการ upgrade PGP เวอร์ชันที่มีอยู่ก่อนแล้ว แสดงว่าท่านได้สร้าง private key ไว้เรียบร้อยแล้วและแจกจ่าย public key ที่เข้าคู่กันให้แก่ผู้ที่จะติดต่อด้วยแล้ว ดังนั้นท่านก็ไม่จำเป็นต้องสร้าง key pair ใหม่อีก แต่เพียงระบุตำแหน่งที่เก็บ key ของท่านเมื่อทำการ run PGPkeys application โดยเลือก **Files** panel ของ **Option** dialog box แล้วกรอกตำแหน่ง keyring files

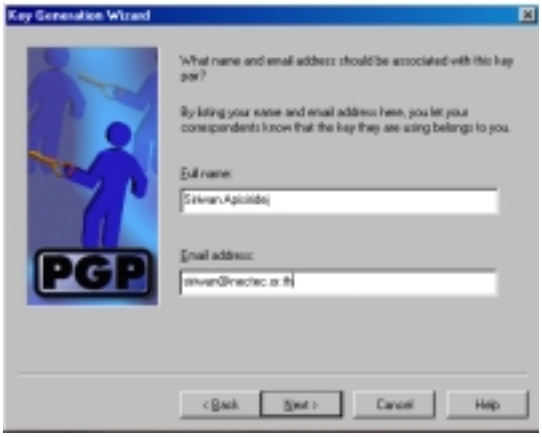
การสร้าง key pair ใหม่ทำได้โดย

1. เปิด PGPkeys โดยกดปุ่ม Start→ Programs→PGP→PGPkeys หรือ กดที่ PGPtray icon ใน System tray แล้วกดที่ PGPkeys หรือ กดปุ่มรูปกุญแจใน toolbar ของ email application จะปรากฏ PGPkeys ดังรูปต่อไปนี้



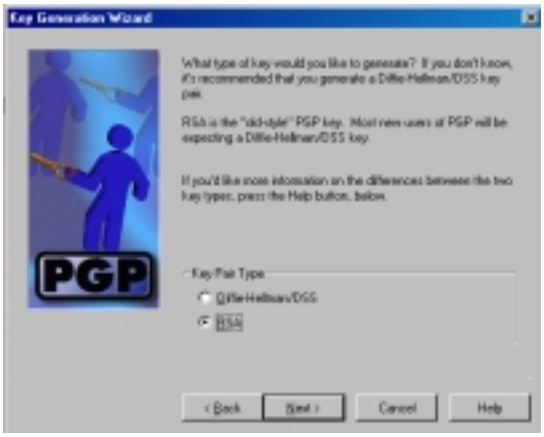
2. กดปุ่มรูปกุญแจด้านซ้ายสุดของ **PGPkeys menu bar** แล้วจะปรากฏข้อมูลเบื้องต้นบน screen แรก ดังนี้

3. เมื่ออ่านเสร็จ ก็กดปุ่ม **Next** จะมีหน้าต่างของ **PGP Key Generation Wizard** ให้ท่านกรอก ชื่อและ email address ดังรูป



ชื่อและ email address อาจจะไม่จำเป็นต้องเป็นของจริง แต่การใช้ชื่อจริงจะทำให้ง่ายต่อผู้อื่นในการชี้ว่าท่านเป็นเจ้าของ public key นั้น และ การใช้ email addressจริงก็ทำให้ท่านและผู้อื่นได้รับประโยชน์จาก plug-in feature ในการหา key ที่เหมาะสมใน keying ของท่านโดยอัตโนมัติเมื่อท่านระบุผู้รับที่เฉพาะเจาะจงในการส่ง email

6. กดปุ่ม **Next** จะมี dialog box ต่อไปให้ท่านเลือกชนิดของ key ดังรูป

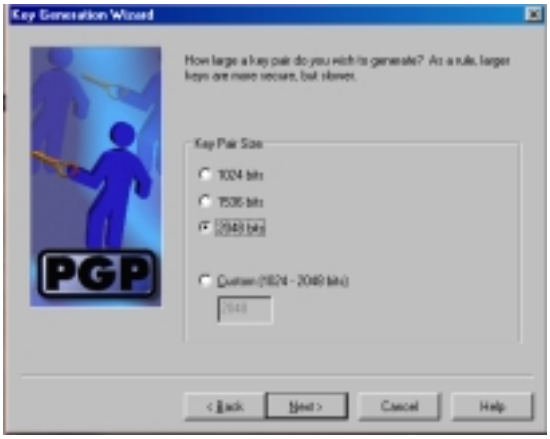


สำหรับ PGP เวอร์ชันเก่าจะใช้เทคโนโลยีที่เก่ากว่า (RSA) ในการสร้าง key ส่วน PGP เวอร์ชัน 5.0 ขึ้นไป ท่านสามารถเลือกสร้าง key ใหม่ด้วยเทคโนโลยีที่ดีขึ้นคือ Diffie-Hellman technology

- ถ้าท่านวางแผนว่าจะติดต่อกับบุคคลซึ่งยังคงใช้ RSA keys อยู่ ท่านจะต้องสร้าง RSA key pair เพื่อให้เข้ากันได้
- ถ้าท่านวางแผนว่าจะติดต่อกับบุคคลซึ่งใช้ PGP เวอร์ชัน 5.0 ขึ้นไป ท่านก็สามารถสร้างใช้เทคโนโลยีใหม่สร้าง pair of Diffie-Hellman/DSS keys
- ถ้าท่านต้องการแลกเปลี่ยน email กับผู้ใช้ PGP ทุกคน ท่านก็สามารถสร้างทั้ง RSA key pair และ Diffie-Hellman/DSS key pair แล้วใช้อันที่เหมาะสมขึ้นอยู่กับเวอร์ชันของ PGP ของผู้รับ

หมายเหตุ ถ้า PGP ของท่านไม่ support RSA ขั้นตอนนี้ท่านอาจจะใช้ไม่ได้ ท่านสามารถดูข้อมูลเพิ่มเติมเกี่ยวกับ RSA support ใน WhatsNew file ที่มากับโปรแกรม PGP

7. หลังจากเลือกชนิดของ key แล้ว ท่านก็จะต้องระบุขนาดของ keys ใหม่ของท่าน โดยเลือกจาก 1024 ถึง 3074 bit หรือ เลือก custom key size จาก 1024 ถึง 4096 bits custom key size อาจจะใช้เวลานานในการสร้าง ขึ้นอยู่กับ ความเร็วของเครื่องคอมพิวเตอร์ของท่านด้วย



หมายเหตุ ขนาดของ key เป็นไปตามจำนวน bit ที่ใช้ในการสร้าง digital key ถ้า key ขนาดใหญ่ ความเสี่ยงจากการถูก crack ก็ลดลง แต่จะใช้เวลานานขึ้นในการทำกระบวนการ decryption และ encryption ขนาดที่เหมาะสมและปลอดภัยเพียงพอคือ key ที่ประกอบด้วย 1024 bits

8. จากนั้นกดปุ่ม **Next** จะมีหน้าต่างให้ท่านกำหนดวันหมดอายุของ key pair

ท่านสามารถเลือก **Never** ซึ่งเป็น default selection เพื่อใช้ไปเรื่อยๆ หรือ ระบุวันที่จะให้ keys หมดอายุ ในกรณีที่ท่านต้องการใช้ key นั้นในช่วงเวลาจำกัดเท่านั้น กรณีนี้เมื่อ public key หมดอายุ บุคคลอื่นจะไม่สามารถทำการ encrypt mail ให้ท่าน แต่มันยังสามารถใช้ตรวจสอบ digital signature ของท่านได้ และเมื่อ private key หมดอายุ มันยังคงถูกใช้ในการ decrypt mail ที่ท่านได้รับก่อน public key จะหมดอายุได้แต่จะไม่สามารถใช้ในการ sign mail ให้แก่บุคคลอื่น

9. เมื่อกดปุ่ม **Next** ท่านจะต้องใส่ passphrase

ช่อง **Passphrase** สำหรับใส่ตัวอักษรหรือคำที่ท่านต้องการใช้ในการเข้าถึง private key ของท่าน และท่านจะต้องยืนยันอีกครั้งในช่อง **Confirmation** ตัวอักษรที่ท่านพิมพ์จะไม่ปรากฏ แต่ถ้าท่านแน่ใจว่าไม่มีใครแอบดูอยู่และท่านต้องการดูตัวอักษรของ passphrase ที่ท่านพิมพ์ ก็ทำได้โดยการเอาเครื่องหมายถูก ออกจาก **Hide Typing** checkbox

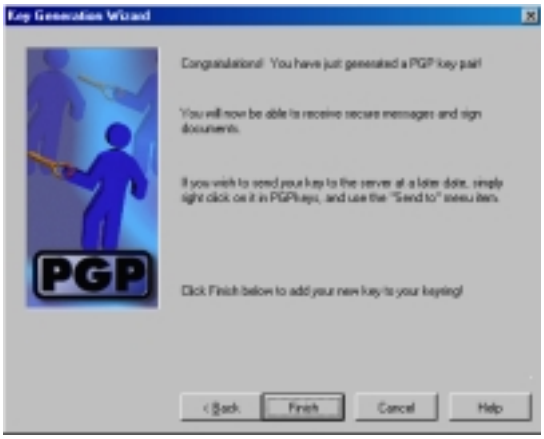
หมายเหตุ passphrase ควรประกอบด้วย คำที่หลากหลายรวมถึงตัวเลข, ช่องว่าง หรือ เครื่องหมายวรรคตอนต่างๆ เพื่อความปลอดภัยจากการเดาและนำไปใช้โดยผู้ไม่ประสงค์ดี แต่ท่านจะต้องจำให้ได้ด้วยเพราะไม่มีใครสามารถกู้ passphrase ที่ท่านลืมกลับมาได้อีก

10. กดปุ่ม **Next** เพื่อเริ่มกระบวนการสร้าง key ดังรูป

11. เมื่อเสร็จแล้ว กดปุ่ม **Next** จะมีหน้าต่างขึ้นมาถามว่าท่านต้องการส่ง public key ของท่านไปยัง certificate server หรือไม่

เมื่อท่านส่ง public key ไปยัง certificate server บุคคลอื่นๆที่สามารถเข้าถึง certificate server นั้นจะสามารถนำเอา key ของท่านไปใช้ได้เมื่อต้องการ

12. เมื่อระบุว่าจะส่ง key ไปยัง certificate server หรือไม่เรียบร้อยแล้วก็กดปุ่ม **Next** หน้าต่างสุดท้ายจะปรากฏดังรูป



key pair ที่สร้างใหม่จะปรากฏในหน้าต่างของ PGPkeys

11. ท่านอาจทำการแลกเปลี่ยน public key ของท่านกับบุคคลอื่นที่ท่านต้องการติดต่อด้วยโดยการ save public key ของท่านเก็บเป็น file .asc แล้วส่งให้บุคคลนั้นทำการ import file ของท่านลงใน key rings เพื่อให้สะดวกแก่บุคคลนั้นๆแทนการ search หา public key ของท่านจาก certificate server และกรณีที่ท่านก็ได้รับ public key file จากผู้อื่น ท่านก็จะต้องทำการ import file นั้นโดยการ double click ที่ file นั้นแล้วกดปุ่ม **import**

และหลังจากนี้ ท่านก็สามารถนำ key ที่สร้างขึ้นมาใช้ในการรับส่ง email อย่างปลอดภัยด้วยวิธีที่จะอธิบายดังต่อไปนี้

วิธีส่งและรับ email ที่ปลอดภัย

วิธีที่เร็วและง่ายที่สุดในการ encrypt และ sign email messages คือการใช้ application ที่มี PGP email plug-ins ถึงแม้ขั้นตอนการทำจะแตกต่างกันระหว่าง email application ที่ต่างกัน ท่านก็สามารถทำการ encrypt และ sign ได้ด้วยการกดปุ่มที่เหมาะสมบน toolbar ของ application นั้นๆ

ถ้า email application ที่ท่านใช้อยู่ไม่มี PGP plug-ins (เช่น Lotus Notes) ท่านก็สามารถ encrypt และ sign email messages ผ่าน Windows clipboard ได้โดยเปิดหน้าต่างของ email application ที่เขียน message ที่พร้อมจะส่งไว้ แล้วกดที่ icon รูปแม่กุญแจ (PGPtray) ใน System tray แล้วเลือก **current window** และทำการ encrypt และ/หรือ sign ตามต้องการ และท่านยังสามารถ encrypt files จาก Windows Explorer แล้วแนบไปกับ email ได้ด้วย

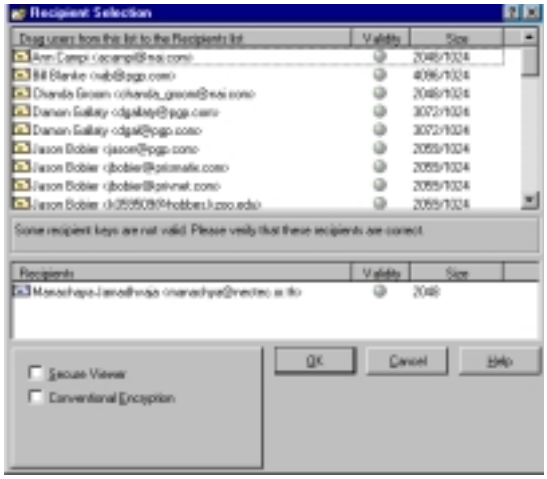
ท่านอาจเลือกใช้ PGPtools ในการ encrypt และ sign email text และ attachments แทนการใช้ plug-ins ได้ ซึ่งจะมีคำอธิบายต่อไปในหัวข้อ “การ encrypt และ sign โดยใช้ PGPtools”

ข้อแนะนำ ในการส่ง email ที่สำคัญ ท่านควรเว้นช่องว่างในส่วนของ subject ไว้ หรืออาจตั้งชื่อหัวข้อที่ไม่เป็นการเปิดเผยเนื้อความใน message ที่ถูก encrypt

การ encrypt และ sign กับ supported email applications

1. ใช้ email application ในการเรียบเรียงข้อความใน email ตามปกติ
2. จากนั้นกดปุ่ม  เพื่อทำการ encrypt ข้อความใน email ของท่าน แล้วกดปุ่ม  เพื่อ sign ข้อความ
3. ทำการส่ง email ของท่านตามปกติ

   เมื่อกดปุ่ม **send** ของ email application จะมีหน้าต่าง **PGP Recipient Selection** ปรากฏให้ท่านระบุ key ของผู้รับเหล่านั้น



4. ลาก public keys ของผู้ที่จะรับ email message ที่ encrypt ลงไปใน Recipients list box หรือ อาจใช้วิธี double-click ที่ key เหล่านั้นเพื่อให้ลงไปใน box นั้นเลย
5. กดปุ่ม **OK** เพื่อ encrypt และ sign email ของท่าน

ถ้าท่านได้เลือกที่จะ sign data ที่ถูก encrypt ก็จะมี **Signing Key Passphrase** dialog box ปรากฏให้ท่านใส่ passphrase (passphrase เดียวกับที่ท่านใส่ในขั้นตอนการสร้าง key pair) ก่อนที่ mail นั้นจะถูกส่งออกไป

6. เมื่อใส่ passphrase แล้วก็กดปุ่ม **OK**

การ encrypt และ sign ข้อความโดยใช้ PGPtools

1. ทำการ copy ข้อความที่ท่านต้องการ encrypt และ sign
2. แล้วกดปุ่ม **Encrypt, Sign** หรือ **Encrypt and Sign** ใน PGPtools ก็จะมี **PGP Key Select File(s)** dialog box ปรากฏ
3. กดปุ่ม Clipboard แล้ว **PGP Key Recipients** dialog box ก็จะปรากฏ
4. แล้วทำตามขั้นตอนที่ 4 ของหัวข้อ “การ encrypt และ sign กับ supported email applications” ไปจนเสร็จสิ้นการ encrypt และ sign

การ decrypt และ verify email

กรณีที่ท่านใช้ email application ที่มี PGP plug-ins ท่านสามารถทำการ decrypt และ verify ข้อความใน email โดยกดปุ่ม **Decrypt/Verify** จาก menu ใน email application ของท่านได้เลยแล้วจะมี **PGP Enter Passphrase** dialog box ปรากฏให้ท่านใส่ passphrase และกดปุ่ม **OK**

กรณีที่ไม่มี PGP plug-ins ท่านก็สามารถทำตามขั้นตอนต่อไปนี้

1. เปิด email message ตามปกติ ท่านจะเห็นกลุ่มของข้อความรหัสลับ (cipher text) อยู่ใน email message ของท่าน
2. ทำการ copy cipher text เก็บไว้ใน Clipboard
3. กดที่สัญลักษณ์รูปแม่กุญแจใน System tray → Clipboard → Decrypt&Verify
   กรณีที่จะ decrypt และ verify files ที่แนบมากับ email ก็สามารถใช้ PGPtools หรือ PGPtray ได้
   จากนั้น **PGP Enter Passphrase** dialog box ก็จะปรากฏให้ท่านใส่ passphrase ของท่าน
4. ใส่ passphrase แล้วกดปุ่ม **OK** ข้อความนั้นๆก็จะถูก decrypt ถ้าข้อความนั้นมีการ sign มาด้วยและท่านมี public key ของผู้ส่ง ข้อความจะปรากฏให้ท่านเห็นว่า signature นั้นถูกต้อง
5. ท่านสามารถ save ข้อความนั้นในรูปแบบ decrypt หรือ อาจจะ save ในรูปแบบ encrypt เพื่อความปลอดภัยก็ได้