
iVEST™ Client 4.1 Release User Guide



Windows Vista/XP

**Documentation Version 4.1.0.0
(25-June-2008)**



MIMOS BERHAD
TECHNOLOGY PARK MALAYSIA
57000 KUALA LUMPUR
<http://www.igest.com.my>
<http://www.mimos.my>

Copyright Notice

Information in this document is subject to change without notice and does not represent a commitment on the part of MIMOS Berhad. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the agreement. It is against the law to copy the software on any medium except as specifically allowed in the license or nondisclosure agreement. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of MIMOS Berhad.

© Copyright 2007, MIMOS Berhad. All right reserved. iVEST™ is the trademark of MIMOS Berhad, Malaysia.

The names used in this document are for internal development purposes only.

IN NO EVENT WILL MIMOS BERHAD BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY DEFECT IN THE SOFTWARE OR ITS DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, ORAL OR WRITTEN, EXPRESS OR IMPLIED.

Contents

COPYRIGHT NOTICE	2
CONTENTS	3
SECTION 1: ABOUT THIS GUIDE	5
WHO SHOULD READ THIS GUIDE?	5
PURPOSE OF THIS GUIDE	6
TECHNICAL SUPPORT	6
SECTION 2: INTRODUCTION	7
WHAT IS iVEST™ CLIENT?	7
iVEST™ PKI ARCHITECTURE	8
SECTION 3: USING YOUR SMART CARD	9
SECURE ACCESS	9
DIGITAL SIGNATURE	9
SECURE E-MAIL.....	9
SECTION 4: INSTALLATION	10
SYSTEM REQUIREMENTS	10
INSTALLATION INSTRUCTION.....	11
Step 1: Plug-in the smart card reader	11
Step 2: Driver installation (USB reader model) under Windows Vista/XP.....	11
Step 3: iVEST™ Client Software Installation	14
Step 4: Configuring Proxy Security Settings in Web Browser	19
Internet Explorer on Dial-up Connection	19
Internet Explorer 7 on LAN Connection	21
Netscape 9 on Dial-up and LAN Connection	22
Mozilla Firefox 2.0 on Dial-up an LAN Connection	23
Using External Proxy Server on LAN environment– additional settings required.....	24
Step 5: Extra Configuration for Internet Explorer	26
Step 6: Test your installation and settings	26
UPGRADE SOFTWARE	27
SECTION 5: iVEST™ GATE	28
INTRODUCTION	28
HOW TO START AND EXIT iVEST™ GATE	28
HOW TO USE iVEST™ GATE	28
View certificate.....	29
Change PIN.....	30
Change settings.....	31
About iVEST Gate Admin	31
About iVEST™ Gate.....	32
SECTION 6: iPROXY	33
INTRODUCTION	33
HOW TO START AND EXIT iPROXY	33
HOW TO USE iPROXY	33
SSL connection details	33
Change setting	34
About iProxy.....	34
SECTION 7: ISIGN	35
INTRODUCTION	35
HOW TO SIGN DATA?	35
SECTION 8: iVEST™ CSP	37

INTRODUCTION	37
SECURING E-MAIL USING OUTLOOK EXPRESS.....	37
Encrypting e-mail	37
Decrypting e-mail	38
Signing e-mail.....	40
Verifying signed e-mail.....	41
MICROSOFT OUTLOOK.....	42
SECTION 9: IVEST™ PKCS #11	43
INTRODUCTION	43
SECURING E-MAIL USING NETSCAPE MESSENGER	43
Enabling Netscape Messenger	43
Log-in to Smart Card Token	47
Encrypting e-mail	48
Decrypting e-mail.....	49
Signing e-mail.....	50
Verifying signed e-mail.....	50
SECTION 10: IVEST™ XBROWSER	51
INTRODUCTION	51
HOW TO START AND EXIT IVEST™ XBROWSER	51
IVEST™ XBROWSER SETTING.....	52
SECTION 11: UNINSTALLATION	53
INTRODUCTION	53
UNINSTALL THROUGH “UNINSTALL IVEST CLIENT”	53
UNINSTALL THROUGH “ADD/REMOVE PROGRAM”.....	54
SECTION 12: SOFTWARE SPECIFICATIONS	57
IVEST™ GATE.....	57
ISIGN	57
IPROXY	57
IVEST™ CSP.....	57
IVEST™ PKCS #11	57
IVEST™ XBROWSER.....	57
SECTION 13: TROUBLESHOOTING	58
INSTALLATION	58
IVEST™ CARD READER AND DRIVER	59
IVEST™ CARD.....	60
IVEST™ GATE.....	60
IPROXY	61
IVEST™ CSP.....	62
IVEST™ PKCS #11	63
WEB BROWSER	64
OPERATING SYSTEM	65
NETWORKING / INTERNET CONNECTION / EXTERNAL PROXY	66
ERROR CODE (WHILE DOWNLOADING CERTIFICATES).....	66
SECTION 14: GLOSSARY OF TERMS.....	68
APPENDIX	71
RECOMMENDED CONFIGURATION STEPS AT SERVER SIDE FOR SIGNING LARGE DATA	71
iVEST Server.....	71
Web/Application Server	71

Section 1: About This Guide

Who should read this guide?

This guide is for anyone with Internet access who wants to secure this channel to perform transactions and communications in a safe and secure environment.

The security services that can be provided by iVEST™ through the Internet are:

1. Services that requires user identity
2. Services that contains private information not to be disclosed to unintended parties
3. Services that requires user signature
4. Services that are legally binding

By securing the Internet with iVEST™, the user can be assured of complete security and peace-of-mind during an Internet transaction and communication.

Some applications that can be used with iVEST™ are:

1. Financial Applications
 - Online Banking
 - Perform all banking functions on Internet.
 - Online Stock Transaction
 - Perform stock trading on Internet.
 - Online Insurance
 - Online Bill Payment
 - Bill presentment and payment on Internet.
 - Online Shopping
 - Shop and Pay on Internet
 - Hard and soft goods.
 - Services.
2. Business Applications
 - Business to Business Transaction
 - Internet Material Sourcing and Procurement
 - Source for material on Internet.
 - Tendering process on Internet.
 - Extranets
 - Virtual Private Networks
 - E-Commerce
3. Government Applications
 - E-Government
 - E-Licensing
 - E-Submission
 - E-Public Services
4. Secure e-mail

Purpose of this guide

The iVEST™ **Client User's Guide** contains installation and configuration steps to install iVEST™ Client software. It provides the instructions on how to use the software which consists of six modules; iVEST™ Gate, iProxy, iSign, iVEST™ PKCS #11, iVEST™ CSP and iVEST™ XBrowser.

This guide is divided into 14 sections:

1. Section 1: About This Guide
2. Section 2: Introduction
3. Section 3: Using Your Smart Card
4. Section 4: Installation
5. Section 5: iVEST™ Gate
6. Section 6: iProxy
7. Section 7: iSign
8. Section 8: iVEST™ CSP
9. Section 9: iVEST™ PKCS #11
10. Section 10: iVEST™ XBrowser
11. Section 11: Uninstallation
12. Section 12: Software Specification
13. Section 13: Troubleshooting
14. Section 14: Glossary of Terms

Technical Support

If you encounter any problem and no solution can be obtained from **Section 13: Troubleshooting** and iVEST™ website, please email support@invest.com.my for assistance. Our operation hours is Monday to Friday, 8:30am to 5:30pm.

Please visit iVEST™ website for latest announcements, product updates, promotions and other information as well: <http://www.invest.com.my>

Section 2: Introduction

What is iVEST™ Client?

iVEST™ Client is a software that establishes secure access and secure transaction over the Internet. By using PKI technology, it protects the integrity and confidentiality of every transaction.

iVEST™ Client is normally available as part of an online kit (e.g. iVEST™ Client Kit or iVEST4MyKad Online Kit). This kit contains all necessary components, e.g. iVEST™ Client software, smart card, digital certificate and smart card reader.

As for the iVEST™ Client software, it consists of 6 modules:

1. iVEST™ Gate (and iVEST™ Gate Admin)
2. iProxy
3. iSign
4. iVEST™ CSP
5. iVEST™ PKCS #11
6. iVEST™ XBrowser

iVEST™ Client functionalities:

1. Supports cryptographic **smart cards**. Currently iVEST™ Client is compatible with 64K MyKad and iVEST™ card.

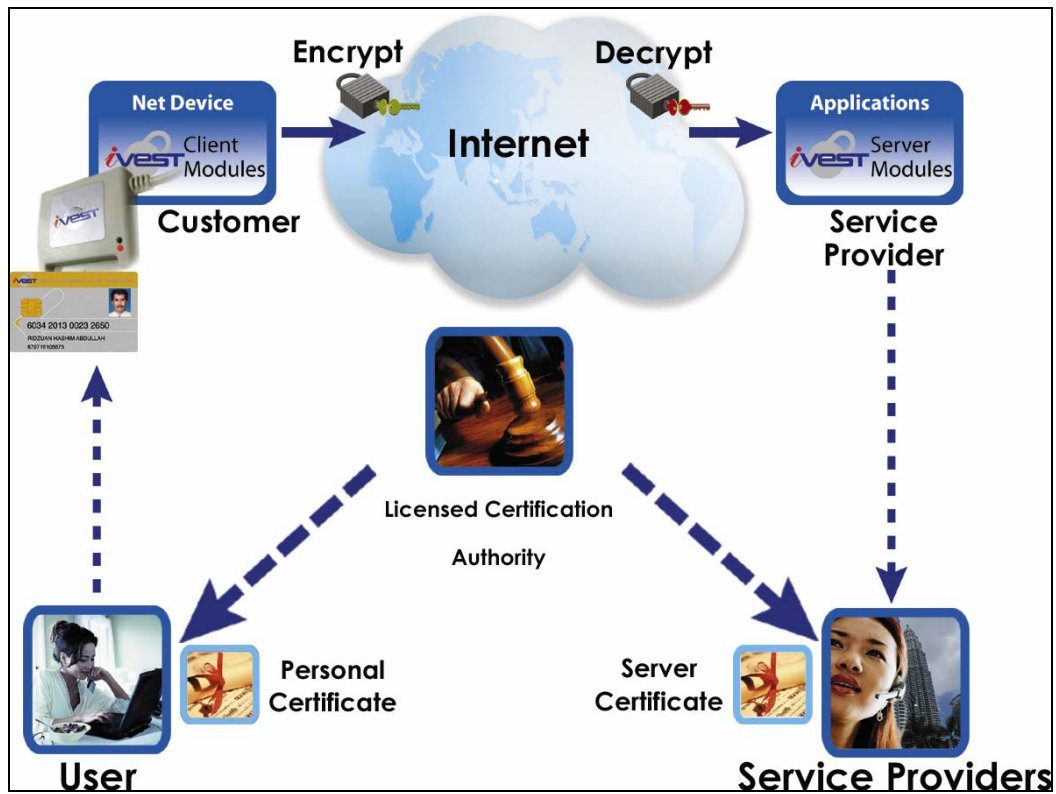
The smart card stores a digital certificate, and a pair of keys (a private key and a public key). The digital certificate is issued by the Certification Authority (CA).

2. Supports PC/SC compliant smart card readers certified by iVEST™.
3. **iVEST™ Gate** is the interface between smart card and iVEST™ modules like iProxy, iVEST™ CSP, iVEST™ PKCS#11 and iSign.

Using **iVEST™ Gate Admin**, users can change their PIN, the smart card reader setting, and view the digital certificate as well.

4. **iProxy** is the local secure proxy that authenticates client and server sides via a Secure Socket Layer (SSL) connection. It supports 128-bit encryption. It also supports X.509 digital certificates issued by licensed Certification Authority.
5. **iSign** is a plug-in to perform digital signature. It uses a *private key* from smart card to generate digital signatures on web form data.
6. **iVEST™ CSP** is a Cryptographic Service Provider for Microsoft platform. With iVEST™ CSP implemented, iVEST™ Client allows secure e-mail using Outlook Express and Microsoft Outlook.
7. **iVEST™ PKCS #11** enables you to send and receive digitally signed and encrypted messages by using Netscape Messenger.
8. **iVEST™ XBrowser** is designed to terminate all activated Internet Browsers when the smart card is being removed from the smart card reader

iVEST™ PKI Architecture



Description:

iVEST™ is an Internet security solution based on Public Key Infrastructure (PKI) – the international standard for secure online transactions. PKI is designed for the Internet and relies on encryption, digital signatures and digital certificates to secure applications, communications and transactions.

Section 3: Using Your Smart Card

Secure access

You can use your smart card for a variety of web-based authentication purposes. Your smart card contains a digital certificate that provides reliable user identification on an open system such as the Internet. When you logon to a website, your digital certificate will be presented, and your identity is authenticated at the server side.

During the authentication process, the iProxy module in iVEST™ Client will establish a 128-bit Secure Socket Layer (SSL) session with the targeted website. Being SSL compliant, you can be sure that every session using smart card is secure and private. Refer to glossary for SSL description. Please refer to **Section 6: iProxy** for more information on iProxy.

Smart card-based authentication is superior user identification for the Internet as compared to username and password.

Digital signature

A digital signature is equivalent to a handwritten signature on a paper. Each signer has a pair of signature keys (a private key and a public key). The private key is used to create signatures and the public key is used to verify these signatures. Under the provisions of the Malaysian Digital Signature Act 1997 and Digital Signature Regulation 1998, a digital signature can be admitted as court evidence if it is issued by a licensed Certification Authority.

You can use your smart card to sign data, message, and document electronically by using iSign module in iVEST™ Client. Please refer to **Section 7: iSign** for more information on iSign.

Secure e-mail

Secure e-mail is an application that you may use with your smart card.

For Outlook Express e-mail application, the iVEST™ CSP module in iVEST™ Client enables you to encrypt/decrypt and sign e-mail messages. Please refer to **Section 8: iVEST™ CSP** for more information on iVEST™ CSP.

For Netscape Messenger e-mail application, the iVEST™ PKCS #11 module in iVEST™ Client enables you to encrypt/decrypt and sign e-mail messages. Please refer to **Section 9: iVEST™ PKCS #11** for more information on iVEST™ PKCS #11.

Recipients of secure e-mail will know that the message comes from the rightful person and the data has not been read or modified by unauthorised third party. In addition, the sender cannot deny sending (non-repudiation) the message if it is signed.

Section 4: Installation

System requirements

- Operating System:
 - Microsoft Windows XP
 - Windows Vista Enterprise/Vista Home Basic

Note: iVEST™ Client 4.1 does not support Window Vista Standard User account type. It will only support account type with Administrator privileges. iVEST™ Client 41R will automatically turn off User Account Control.

More info on User Account Control :

<http://www.microsoft.com/windows/products/windowsvista/features/details/useraccountcontrol.msp>

Important: Whenever 'Check your User Account Control settings' message box pops up, please do not click to fix the problem as this will turn on the User Account Control, which will disrupt the functioning of iVEST™ Client 4.1R

- Web browsers supported :
 - Internet Explorer 6 and above
 - Netscape Navigator (version 7.0, 7.2, 8.0, 9.0.06)
 - Mozilla 1.7 and above
 - Mozilla Firefox 2.0 and above
- Internet access, 1 USB port, PC/SC compliant smart card readers certified by iVEST™
- For office environment that has External Proxy Server, a re-configuration is required. Please refer to page 24.
- E-mail applications:
 - Microsoft Outlook Express (version 5.0, 5.5 and 6.0)
 - Microsoft Outlook
 - Netscape Messenger (version 4.5x, 4.6x, 4.7x and 4.8x)
 - iVESTmail
- Recommended hardware requirements for iVEST Client running on Windows Vista Home Basic :
 - 1 GHz processor
 - 512 MB of RAM
 - 15 GB hard disk free space
- Recommended hardware requirements for iVEST Client running on Windows Vista Enterprise :
 - 1 GHz processor
 - 1 GB of RAM
 - 15 GB hard disk free space
- Recommended hardware requirements for iVEST Client running on Windows XP :
 - A Pentium or higher microprocessor
 - 64 MB of RAM
 - 5 MB hard disk free space
- Smart cards:
 - iVEST™ Card (SETEC16K and MyMS 32K iVCOS smart card)
 - 64K MyKad

Installation instruction

To install, you MUST follow the following steps:-

Step 1: Plug-in the smart card reader

Step 2: Driver installation (USB reader model) under Windows Vista/XP

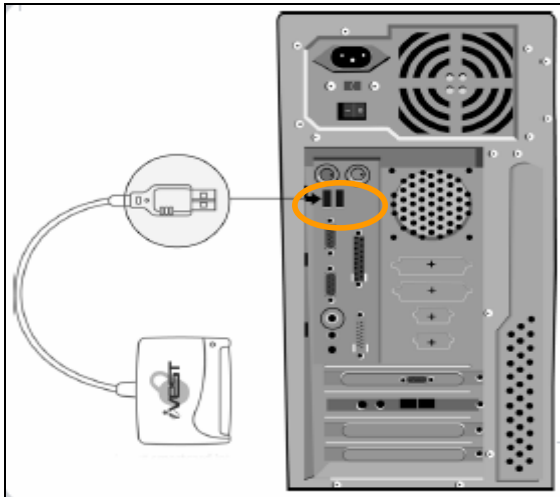
Step 3: iVEST™ Client software installation

Step 4: Configuring Proxy Security Settings in Web Browser.

Step 5: Test your installation and setting at <http://www.igest.com.my>

Refer to **ReleaseNote.txt** for additional information that may not be covered in this user guide.

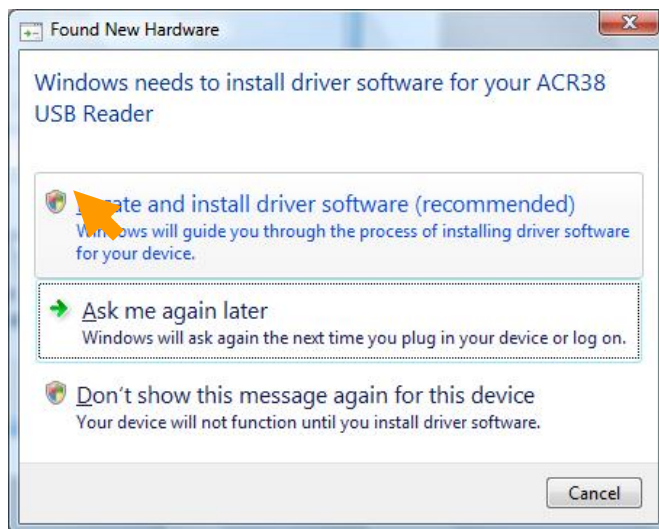
Step 1: Plug-in the smart card reader

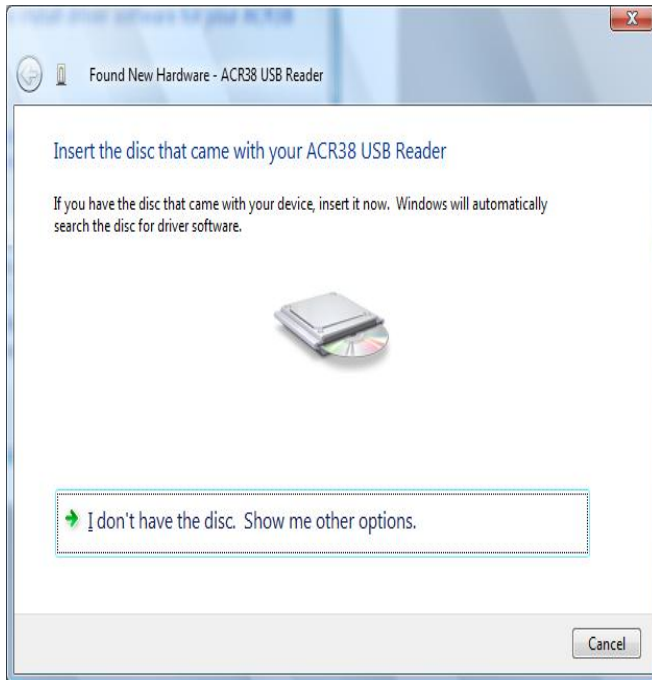


Switch off your PC and connect the smart card reader. Connect the USB cable of the reader to the USB port of the PC. Switch on your PC.

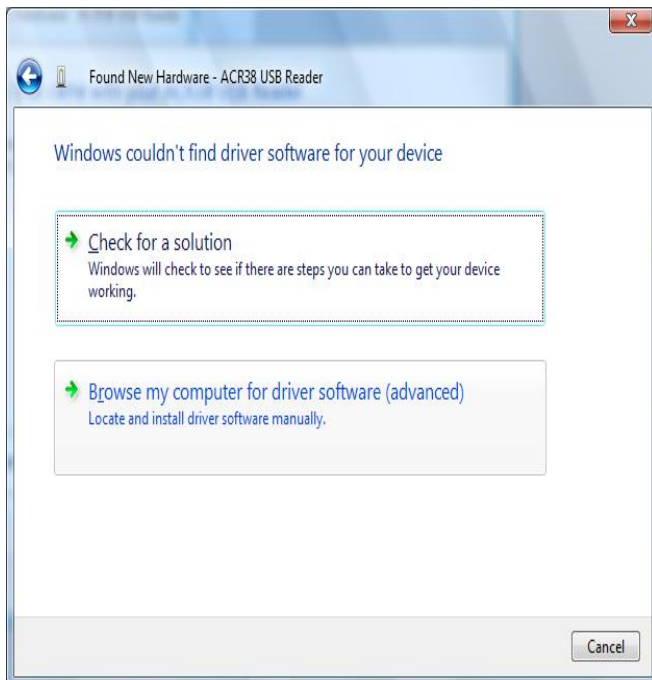
Step 2: Driver installation (USB reader model) under Windows Vista/XP

1. As you logon to Windows, the system tells you there is a new hardware found. Choose **Locate and install driver software (recommended)**.

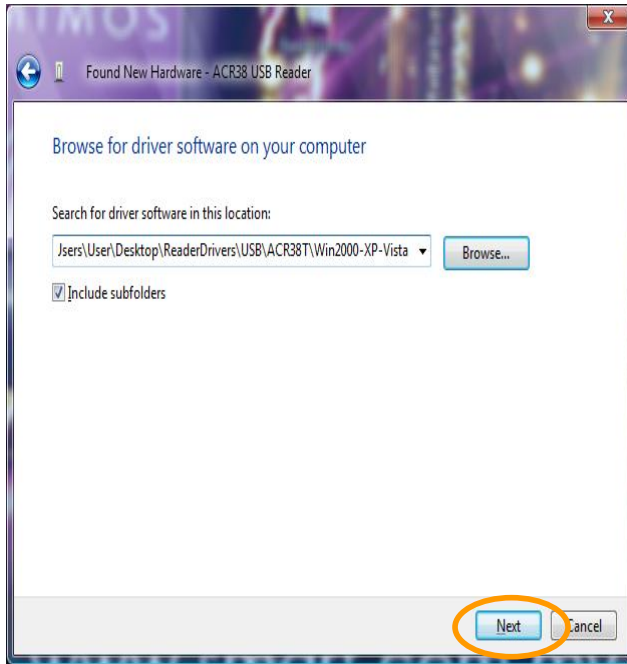




2. **Found New Hardware** screen will appear. Please insert iVEST Client 4.1 **Installation CD** into the CD-ROM drive and the driver will automatically be installed. However, you can also choose to browse to the location that contains the driver by selecting **I don't have the disc. Show me other options.** For this option, continue to Step 3.

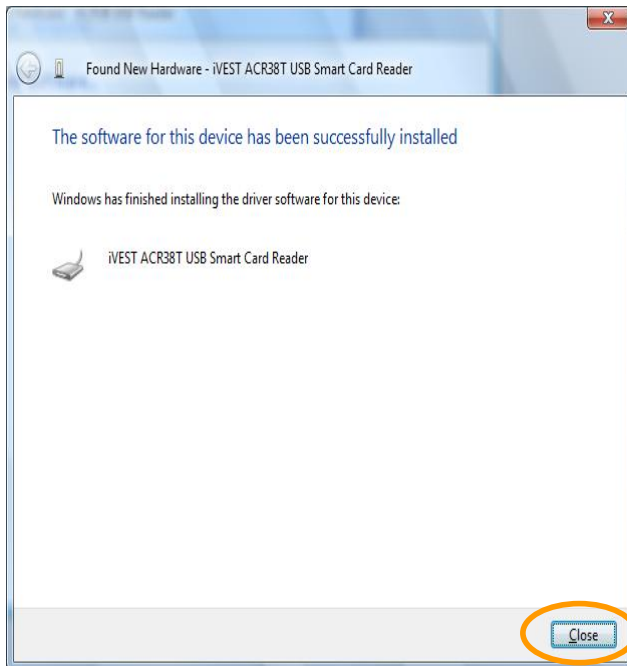


3. Choose **Browse my computer for driver software(advanced).** **Locate and install driver software manually.**



4. Click **Browse** to browse inside the driver folder you wish to install. Then, click **Next**.

Note: The location given is only an example.

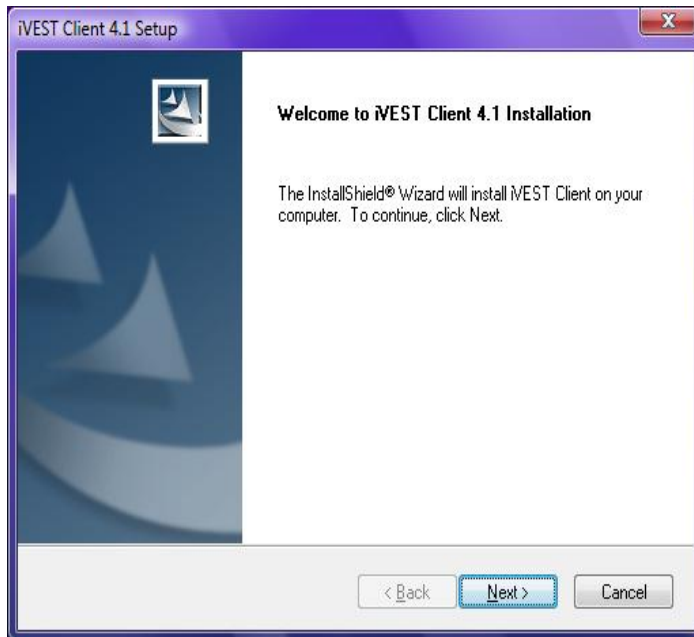
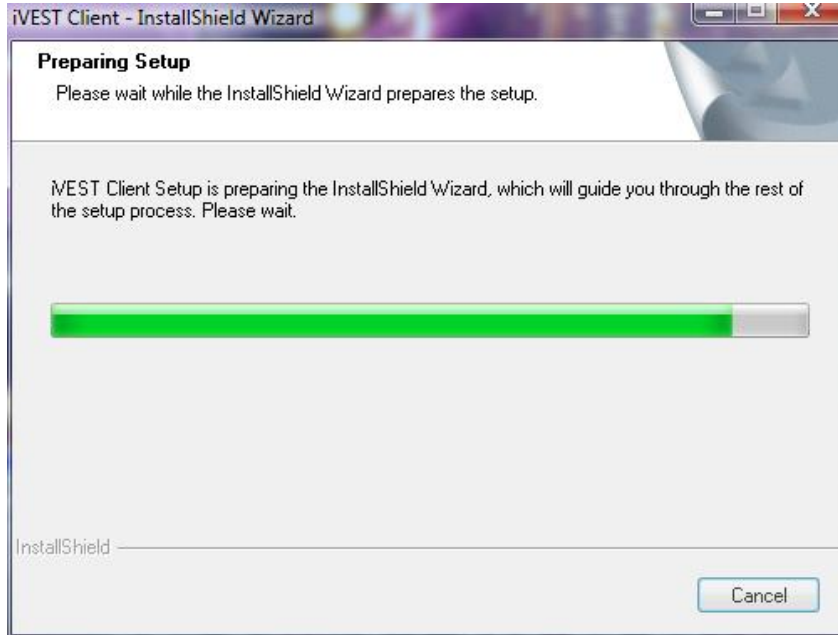


5. A screen will appear to inform that the installation has completed. Click **Close**.

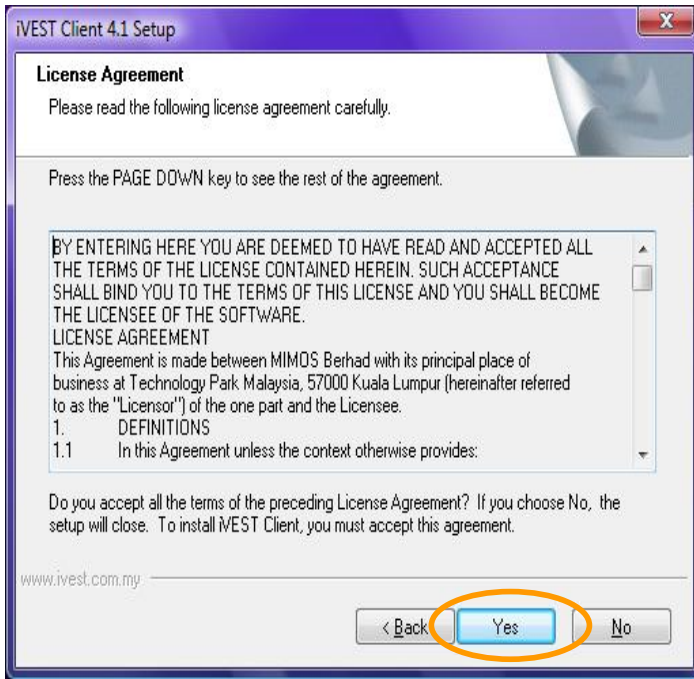
Step 3: iVEST™ Client Software Installation

Note: Please ensure you have the Administrator's rights.

1. Close all web browsers and insert the Installation CD into your CD drive.
2. Double-click **My Computer** on your Desktop and browse to your CD-ROM drive. Double-click iVESTClient 4-1.exe. (assuming 4-1 is the version of iVEST Client inside the Installation CD)
3. There will be some extraction of files being done by the InstallShield Wizard. This will only take a moment.

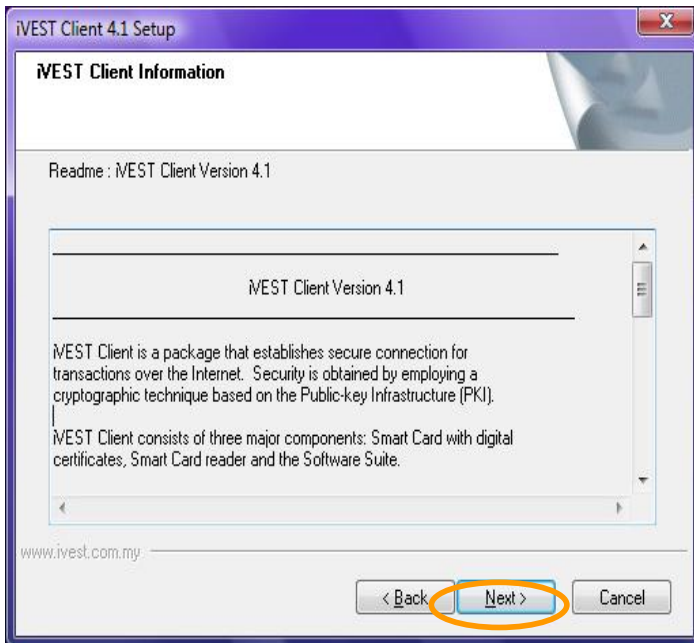


4. Please wait until the **Welcome to iVEST Client 4.1 Installation** dialog box appears. Click **Next**

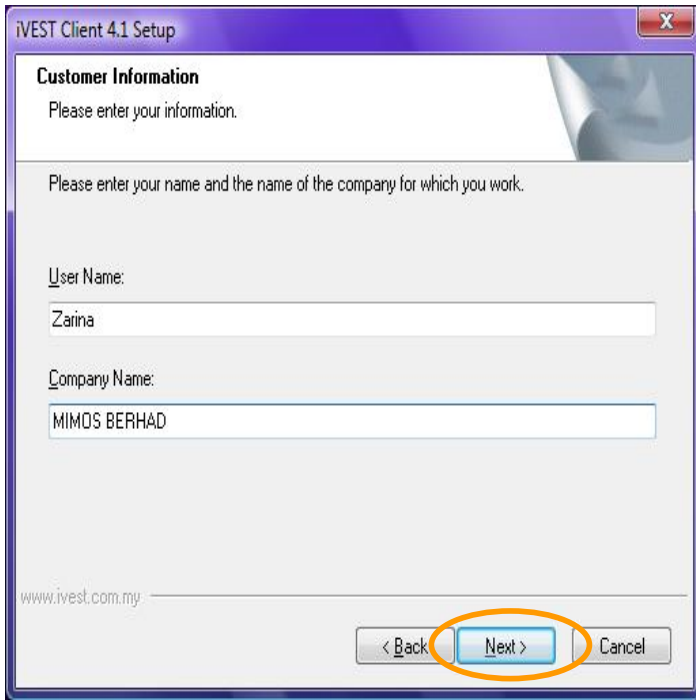


5. The **License Agreement** dialog box will appear. Please read the agreement and click **Yes** to accept.

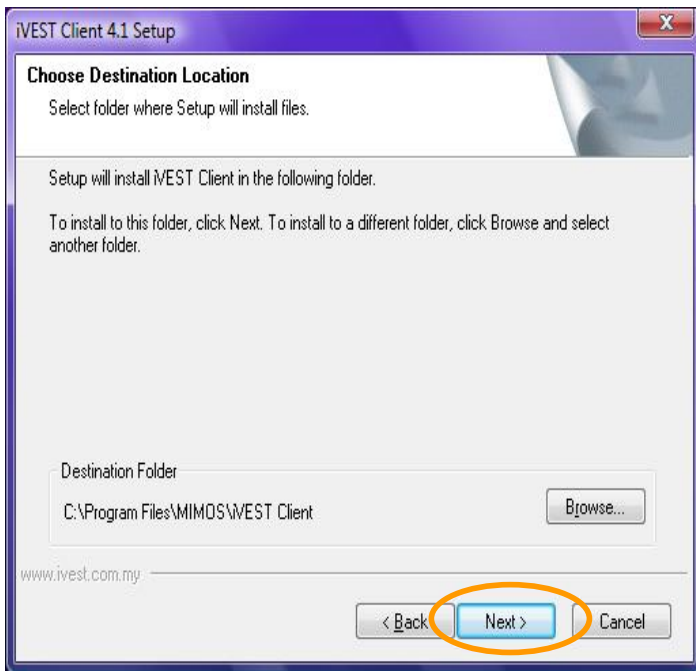
Note: If you click **No**, the whole installation process will be aborted.



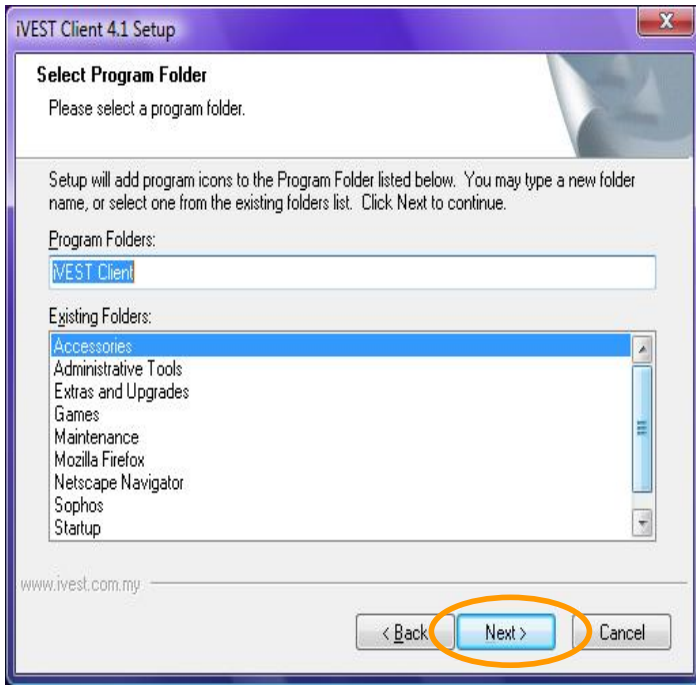
6. The **iVEST Client Information** dialog box will appear. This dialog box explains about iVEST™ Client. Click **Next**



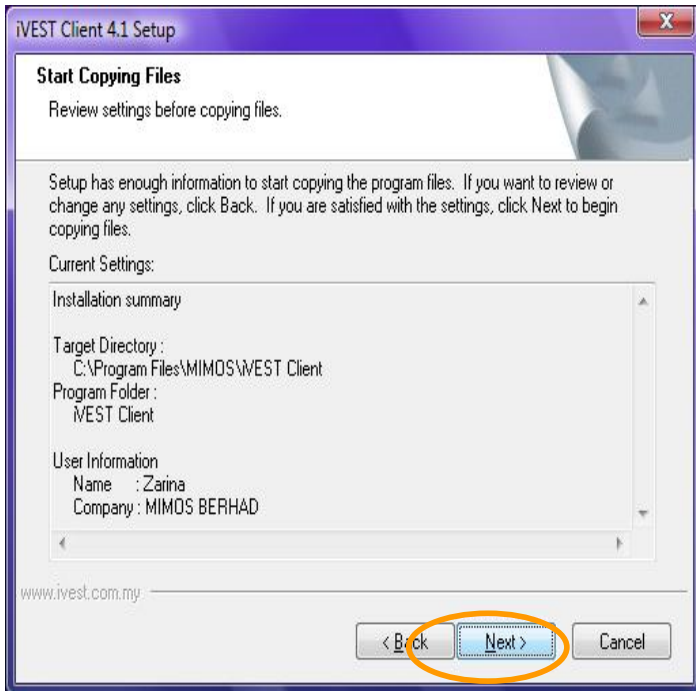
7. The **Customer Information** dialog box appears. Enter the requested information before clicking the **Next >** button. Make sure that it is typed correctly before you continue.



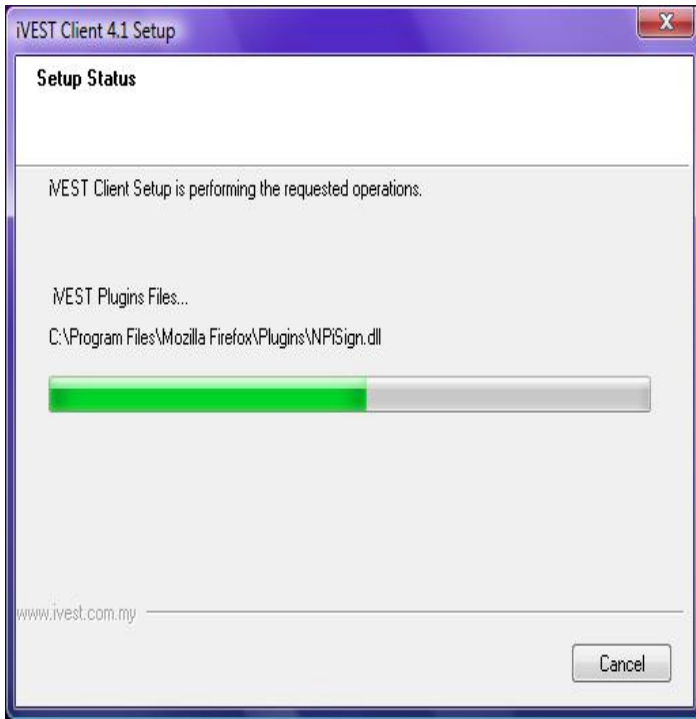
8. The **Choose Destination Location** appears. It is recommended to just accept the default destination folder. Alternatively, you may change the destination folder by clicking **Browse**. Then, click the **Next** button.



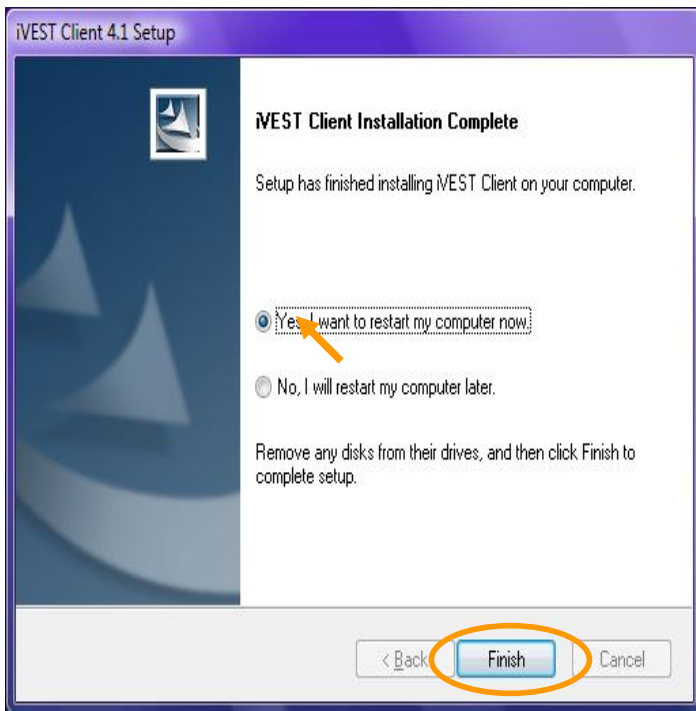
9. The **Select Program Folder** dialog box will appear. Click **Next**



10. The **Start Copying Files** dialog box appears. This will allow you to review your settings before copying files into the folder. Click **Next**



11. Windows now will start installing the software.



12. After installation is completed, the **iVEST Client Installation Complete** dialog box will appear. You will be prompted to restart your PC. Choose, **Yes I want to restart my computer now** and click **Finish** button.

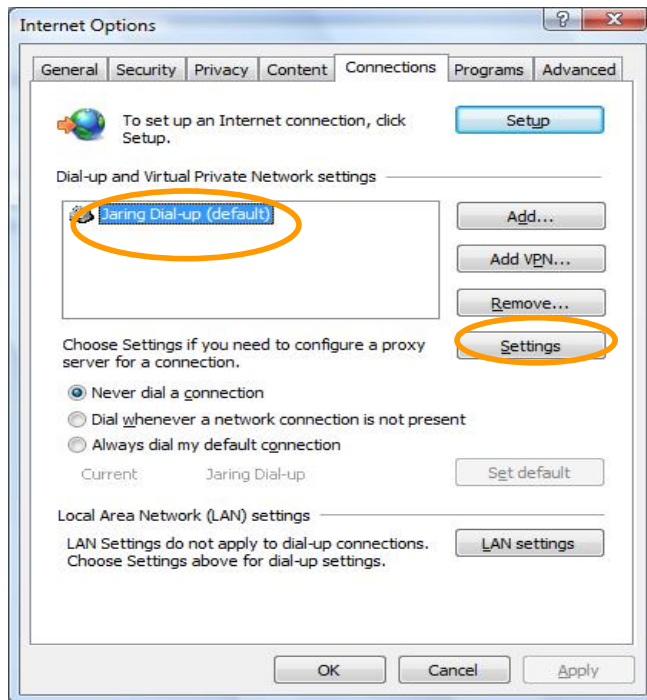
Note Every time you install/re-install any browsers in a machine which already have iVEST Client installed, you need to un-install iVEST Client and re-install it back. Reason being is we need to install all the certificates into the browser's cert store and perform all the settings that are required inside the browsers.

Step 4: Configuring Proxy Security Settings in Web Browser

For secure web access (website address starts with https://...) you need to configure proxy security settings in web browser to enable iProxy. This configuration is done automatically during installation for Internet Explorer(using LAN connection), Netscape Navigator, Mozilla and Mozilla Firefox. For Internet Explorer using Dial-up, you need to configure the settings manually. It is recommended for you to double check the settings configured using the outlined steps for respective browsers:

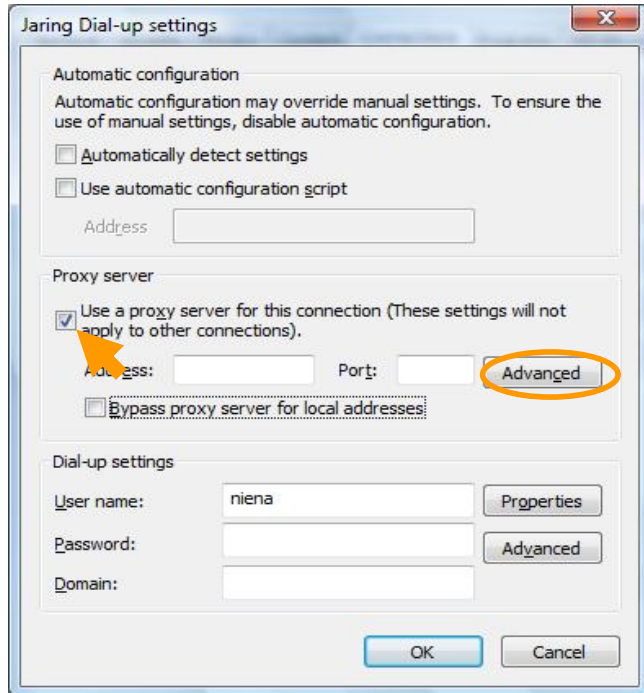
Note For machines with multiple user accounts, browser proxy security setting is only configured for the user(with admin right) who installed iVEST Client. For other users, you need to configure the settings manually.

Internet Explorer on Dial-up Connection



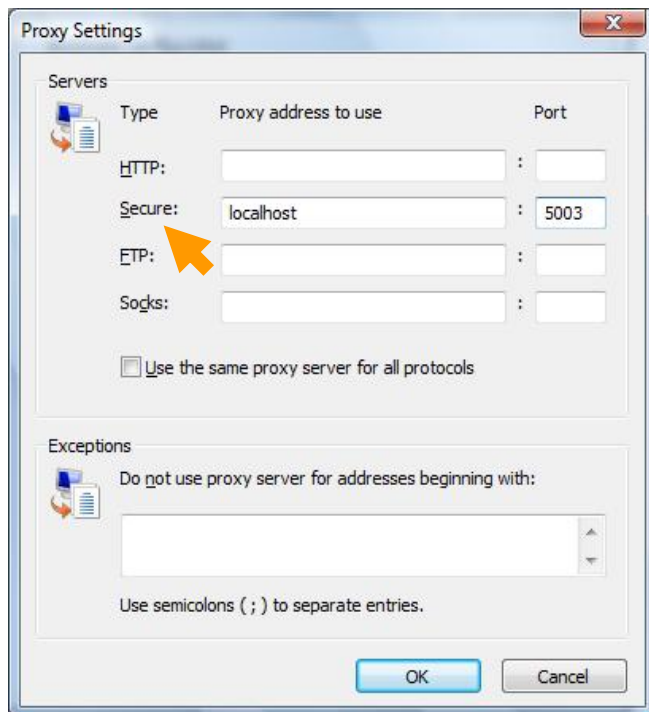
1. Launch web browser
2. Click **Tools** -> **Internet Options** -> **Connections**
3. Highlight your preferred ISP (e.g. Jaring Dial-up as shown) and click the **Settings...** button

Note: If you are using more than one ISP, you should highlight and set the configuration for each setting.



4. Select **Use a proxy server...** DO NOT check **Bypass proxy server for local addresses**.

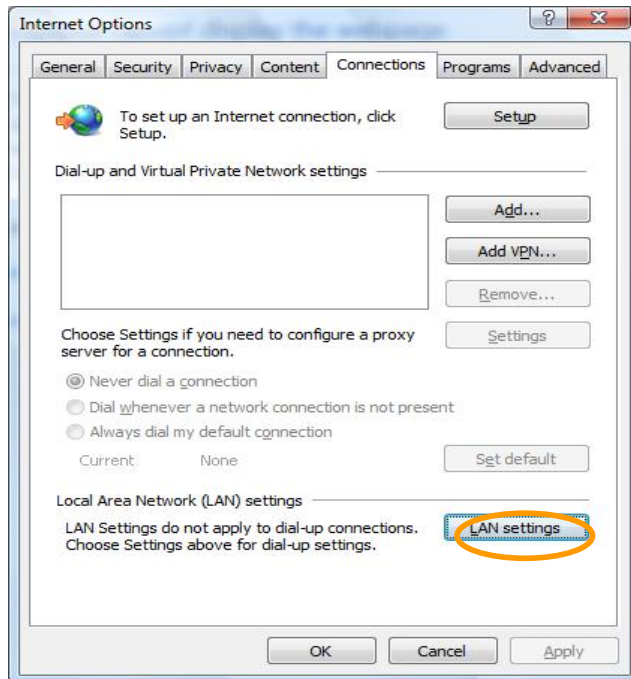
5. Click **Advanced...**



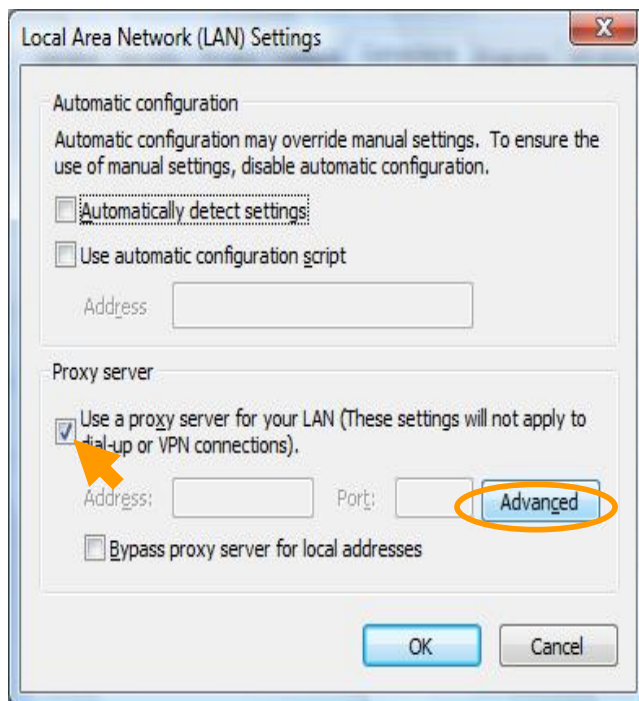
6. The **Proxy Settings** screen will appear. Type in **localhost** and **5003** at the **Secure** field.

7. Click **OK** to close all the windows and re-launch Internet Explorer.

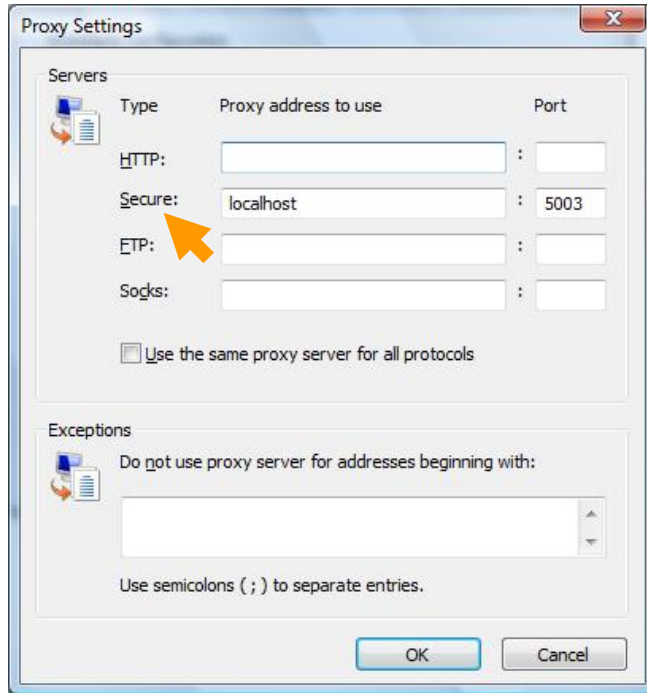
Internet Explorer 7 on LAN Connection



1. Launch Internet Explorer
2. Click **Tools -> Internet Options -> Connections**
3. Click **LAN Settings** button

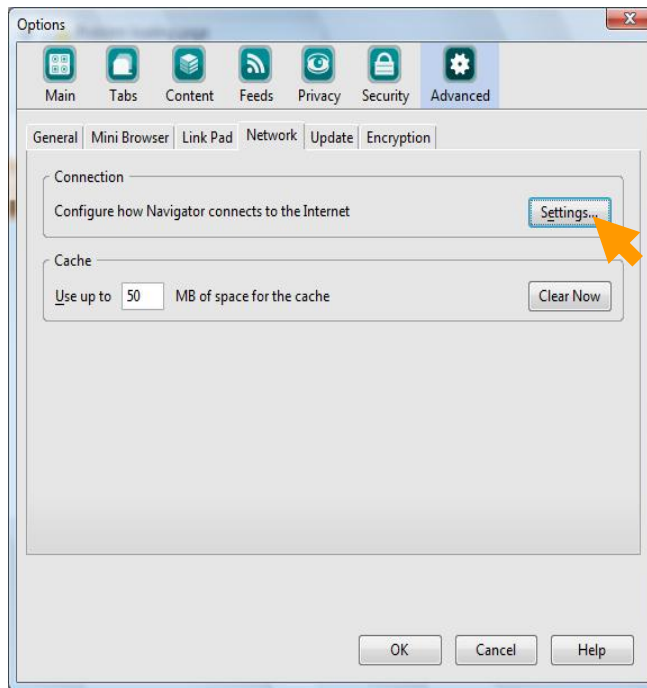


4. **Local Area Network (LAN) Settings** screen will appear. Select **Use a proxy server** under **Proxy server**. **DO NOT** check **Bypass proxy server for local addresses**. Click on **Advanced** button.

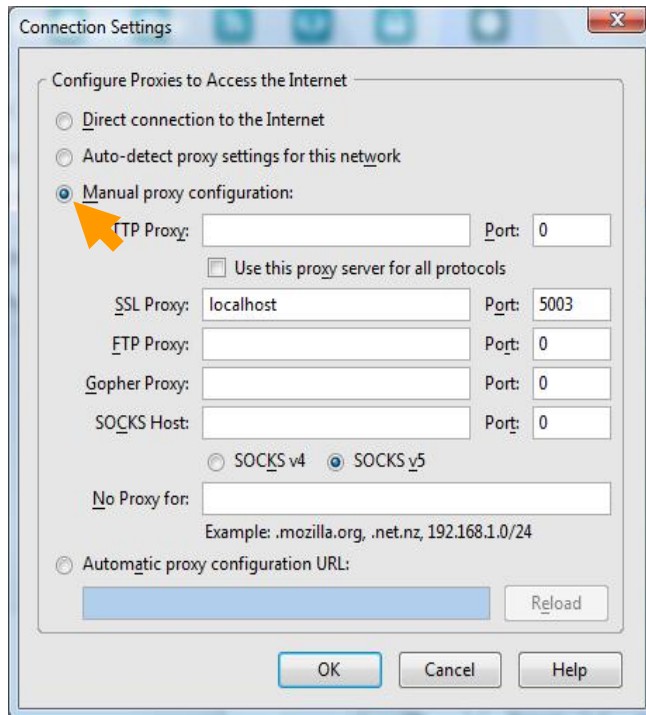


5. The **Proxy Settings** screen will appear. Type in **localhost** and **5003** at the **Secure** field.
6. Click **OK** to close all the windows and re-launch Internet Explorer.

Netscape 9 on Dial-up and LAN Connection



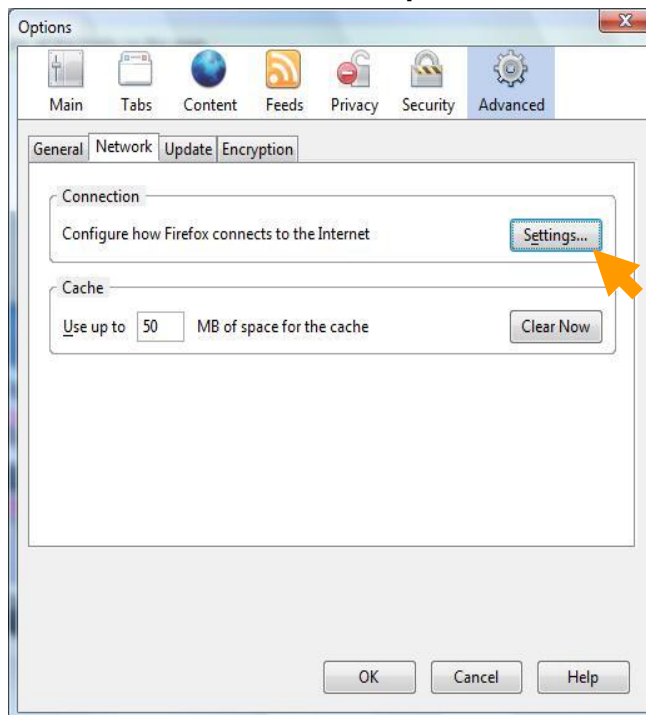
1. Launch Netscape Navigator
2. Click **Tools > Options > Advanced > Network**
3. Click on **Settings** button



3. Choose **Manual proxy Configuration**. Type in **localhost** and **5003** at the **SSL Proxy** field.

4. Click **OK** to close all the screens and re-launch Netscape

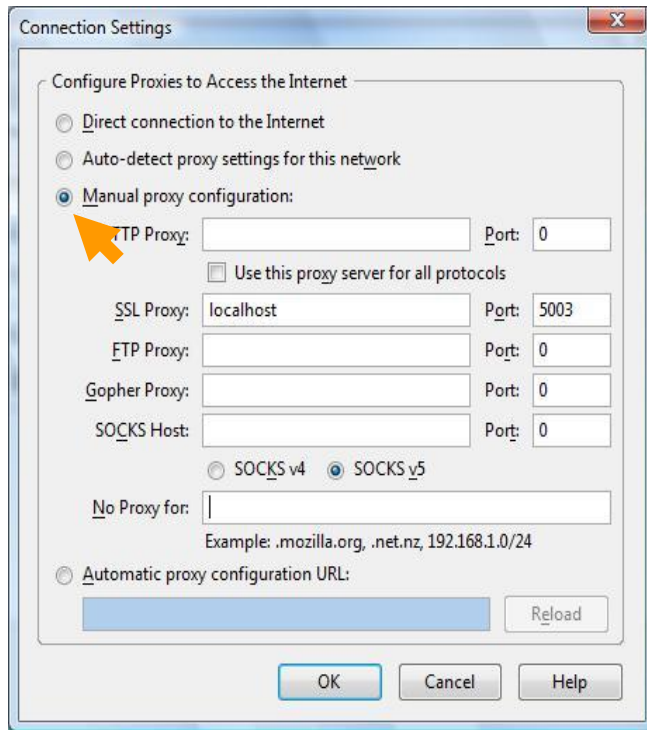
Mozilla Firefox 2.0 on Dial-up an LAN Connection



1. Launch Mozilla Firefox

2. Click **Tools > Options > Advanced > Network**

3. Click on **Settings** button.

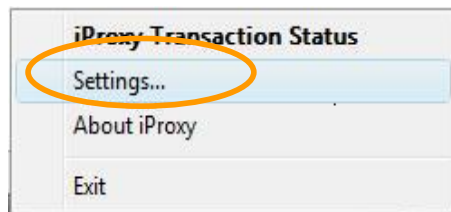



4. Choose **Manual proxy configuration** Type in **localhost** and **5003** at the **SSL Proxy** field
5. Click **OK** to close all the screens and re-launch Mozilla Firefox.

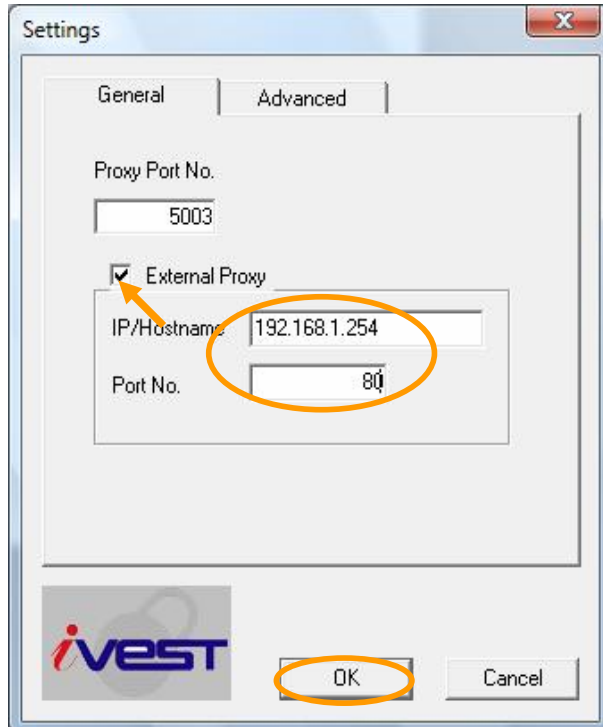
Using External Proxy Server on LAN environment– additional settings required

For LAN environment that utilizes an external proxy server, you need to perform additional settings.

iVEST™ connection only supports *pass-through* proxy server (which means that the proxy will just pass the connections and will not inspect the packet contents). Please check with your system administrator to confirm whether your external proxy server supports *pass-through* feature. You also need to get the IP address and corresponding port of the external proxy server from your system administrator.

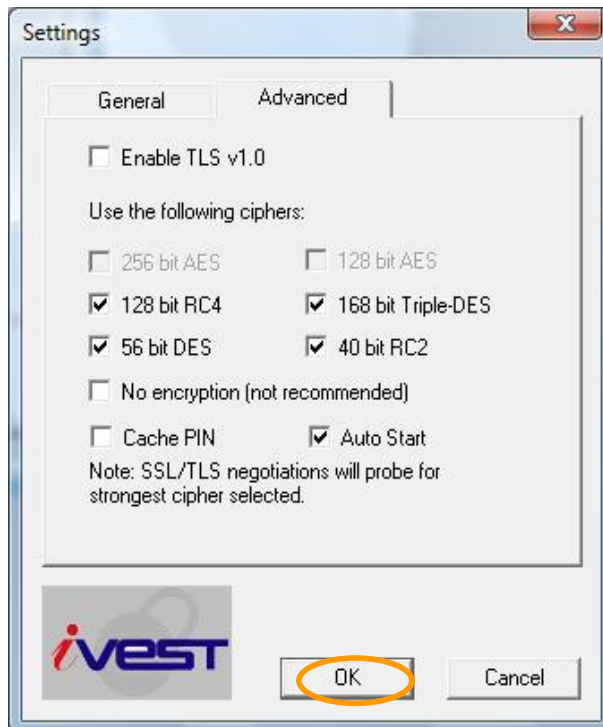


1. At the iProxy icon () at the system tray, right click your mouse and select **Setting...**



2. At **General** tab, the screen displays current iProxy setting. The default **Proxy Port No.** is **5003**. Please **DO NOT** change the **Proxy Port No.**
3. Check the **External Proxy** checkbox
4. Assuming the IP address of external proxy given by your system administrator is **192.168.1.254** and port **80**
5. Type in the IP address at the **IP/Hostname** and its corresponding port number at the **Port No.**. Click **OK**.

Note If Microsoft Proxy Server is used as the External Proxy, you are advised to install the Microsoft Proxy Client on your pc.



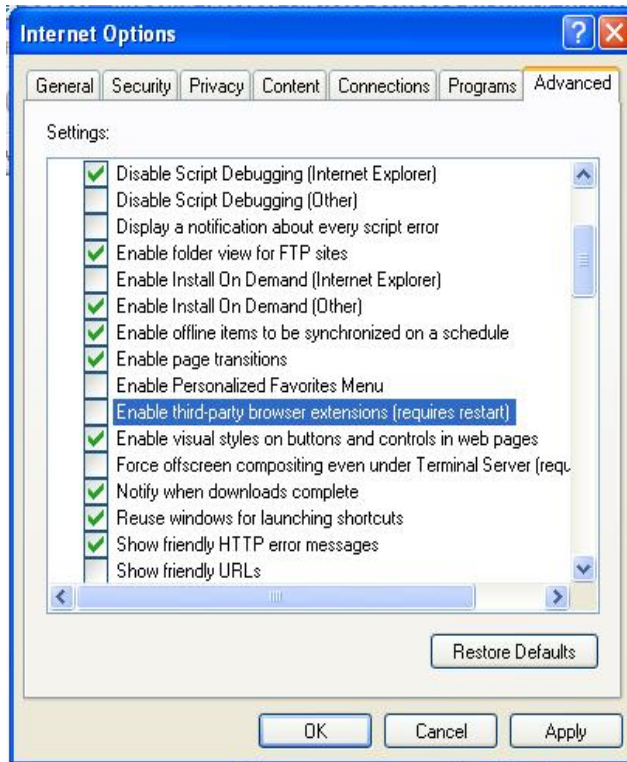
6. If you prefer to cache your PIN, you may select the **Cache PIN** option at the **Advanced** tab. Please reinsert card when accessing another secured site.

Note: **Cache PIN** is not recommended because it compromises security.

7. Auto Start option is where you can control iProxy to start or not to start automatically. By default, iProxy is set to start automatically.
8. Click **OK** to close the screen.

Step 5: Extra Configuration for Internet Explorer

To avoid Internet Explorer from crashing, there is an extra configuration that is done automatically during installation. It is recommended for you to double check the setting configured using the following steps :



1. Open Internet Explorer.
2. Click **Tools -> Internet Options -> Advanced -> Browsing**.
3. Un-check "Enable third-party browser extensions" box.
4. Restart Internet Explorer.

Note: Please make sure that the box is un-checked all the time.

Step 6: Test your installation and settings



1. Go to <http://www.igest.com.my>
2. Click **Test your smartcard & view digital cert** link on the left menu.
3. Then, click on the iVEST™ logo.



4. **iVEST PIN Request** box will appear. Enter your PIN and click **OK**.

iVEST Testing Page

- [Digital Certificate based authentication](#)
- [Digital Signature](#)

5. **iVEST Testing Page** will appear. Click **Digital Certificate based authentication** link.

User Authentication

Verification Result:

Welcome Soo Hoo Kin Hoon

Your Certificate is Valid

Subject	Certificate detail
Name	Soo Hoo Kin Hoon
IC No	701018086001
Email	soohoo@mimos.my
Serial No	0931c1
Certificate Type	DIGISIGN iVEST CA
Certificate Issuer	Digicert Sdn. Bhd.

6. **User Authentication** page will appear. Some of the details of your digital certificate will be displayed.
7. Congratulations! By getting the page with “Your certificate is valid”, this means that the installation and settings were successful.

Note: On the same **iVEST Testing Page**, you can also test the digital signing functionality by clicking the **Digital Signature** link.

Note: For machines with multiple users, if want to change user, need to log off the first user, then log in as the second user. Do not just switch user because the first user will still hold the instances of iVEST Client and thus iVEST client will not be able to function for the second user.

Upgrade Software

Note: Please ensure you have the Administrator's rights

1. Close all web browsers and insert the Installation CD into your CD drive.
2. Double-click **My Computer** on your Desktop and browse to your CD-ROM drive. Double-click iVESTClient-4.1.exe. (assuming 4.1 is the version of iVEST Client inside the Installation CD)
3. You will notice that there will be some extraction of files being done followed by the preparation of the InstallShield Wizard. This will only take a moment.
4. InstallShield will detect if you have a previous or different version of iVEST™ Client installed. The **Remove the program** screen will appear. Click **Next** to continue, else click **Cancel**. Double-click again on iVESTClient-4.1.exe to install iVEST Client 4.1.

Section 5: iVEST™ Gate

Introduction

iVEST™ Gate is the interface between smart card and iVEST™ modules : iProxy, iVEST™ CSP, iVEST™ PKCS#11 and iSign.

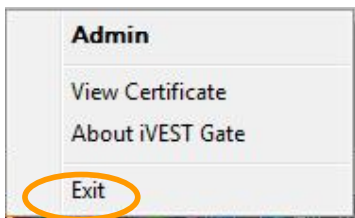
Using **iVEST™ Gate Admin**, users can change their PIN, the smart card reader setting, and view the digital certificate as well.

How to start and exit iVEST™ Gate

1. By default, iVEST™ Gate launches automatically when you switch on your PC. Alternately, you can manually run iVEST™ Gate from Windows **Start -> Programs -> iVEST Client -> iVEST Gate**.
2. The iVEST™ Gate icon will appear as below at your system tray.



3. To exit, right-click iVEST™ Gate icon and select **Exit**.



How to use iVEST™ Gate

1. Insert your smart card into the smart card reader, the iVEST™ Gate icon at system tray will “spin”.

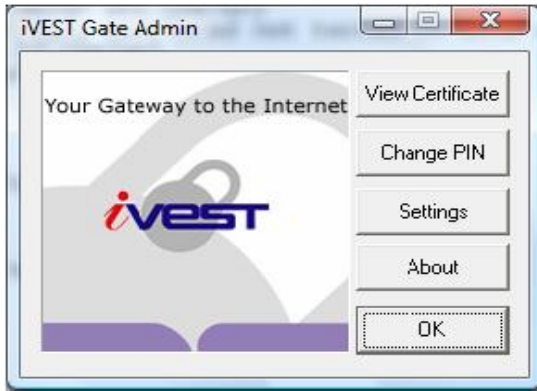


Warning: Do not pull out your smart card while iVEST™ Gate is loading. It may take a few seconds to read the smart card.

2. The iVEST™ Gate icon becomes active once it stops “spinning” as shown below. By default, the web browser will be launched.



3. Double-click iVEST™ Gate icon to access the **iVEST Gate Admin**.



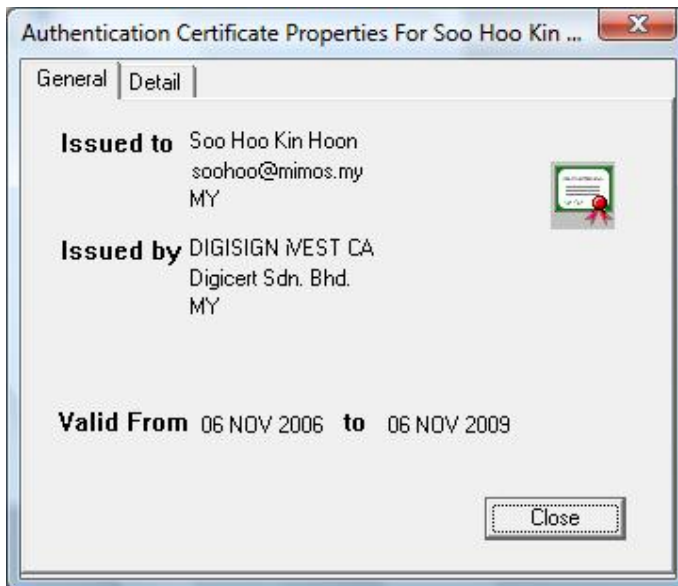
4. At **iVEST Gate Admin** , there are buttons for :
 - i. View certificate
 - ii. Change PIN
 - iii. Change settings
 - iv. About iVEST Gate Admin

View certificate

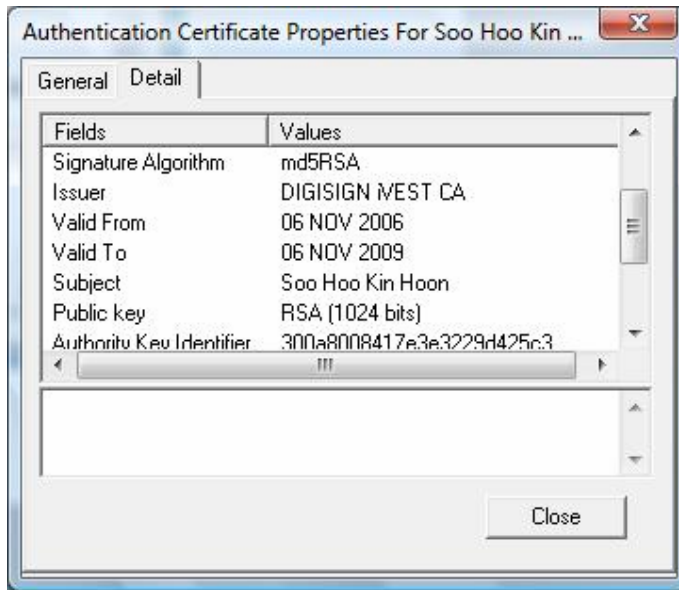
1. To view your Certificate, click **View Certificate** at the **iVEST Gate Admin**.
2. The **Please Select Certificate** window will appear. Select the certificate that you want to view.



3. The certificate properties window will appear, showing the details of **Issued to**, **Issued by** and **Valid From** of your digital certificate.



- To view the detailed contents of the digital certificate, click the **Detail** tab on the Authentication Certificate Properties screen. The iVEST™ Gate Certificate details content screen will appear.



Note: If user overlaps this window with other Window Browsers or folders, when go back to this window, it will not show the certificate details.

Solution : User need to click on 'General' tab, click back on 'Detail' tab, then only all the information will be displayed back as normal.

- Click **Close** when you are done and you will return to the iVEST Gate Admin.

Change PIN

- Please ensure your smart card is inserted into the smart card reader before changing PIN
- Click **Change PIN** at the iVEST Gate Admin
- The iVEST Gate Change PIN dialog box will appear as below



- Please fill in the boxes as required
- Click **OK** to update your PIN

Note: Advisable to use between 6 to 8 alphanumeric characters for your PIN. Avoid using space and tab.

Warning: Your smart card will be blocked if you type in three invalid PINs consecutively. You have to bring your blocked smart card in person to the nearest authorized RA counter to unblock.

- Click **OK** to return to iVEST Gate Admin

Change settings

1. Click **Settings** button on the **iVEST Gate Admin** screen window. The **iVEST Gate - Smart Card Reader Setting** default dialog box appears as below to show the smart card reader in use:



2. Click **Advanced...** button for further start-up options

Note: You need to login with Administrator rights in order to change settings.



3. Uncheck **Browser** if you prefer your default web browser not to be launched upon insertion of your smart card
4. Uncheck **Auto Start** if you prefer not to launch **iVEST™ Gate** upon Windows start-up
5. Click **OK**

About iVEST Gate Admin

1. Click **About** on iVEST Gate Admin screen window to see iVEST Gate Admin version.



About iVEST™ Gate

1. To view the iVEST™ Client version and iVEST™ Gate version, right click iVEST™ Gate icon and select **About iVEST Gate**.



2. iVEST™ Client version and iVEST™ Gate version will be shown.



iVEST™ Gate Sleep Mode

iVEST™ Gate will be placed in sleep mode when the smart card reader is unplugged from the PC/notebook. The **iVEST™ Gate** icon in the taskbar will change to the following:



During this time, viewing certificate, changing settings and changing PIN cannot be done. The icon will change back to normal when the smart card reader is plugged back in.

Section 6: iProxy

Introduction

iProxy is the local secure proxy that authenticates client and server sides via a Secure Socket Layer (SSL) connection. It supports 128-bit cryptography. It supports X.509 digital certificates issued by licensed Certification Authority.

With **iProxy** enabled, your web browser can access any SSL-enabled web sites safely and securely. Please refer to glossary for more information on SSL.

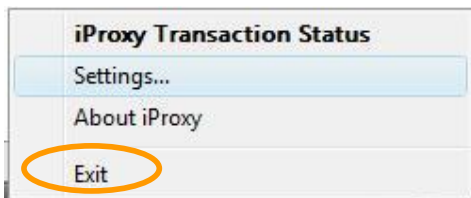
iProxy allows you to change Settings and view SSL connection details.

How to start and exit iProxy

1. By default, **iProxy** launches automatically when you switch on your PC. Alternately, you can manually run **iProxy** from Windows **Start -> Programs -> iVEST Client -> iProxy**.
2. The **iProxy** icon will appear as below at your system tray.



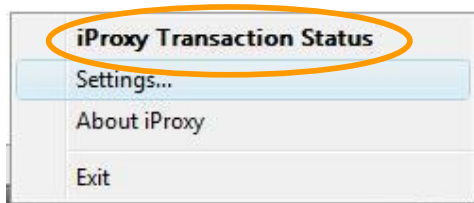
3. To exit, right-click **iProxy** icon and select **Exit**.



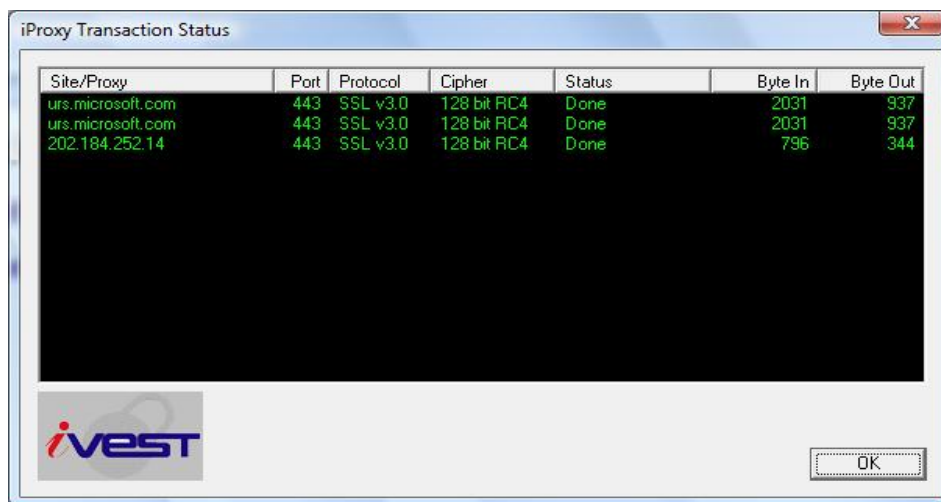
How to use iProxy

SSL connection details

1. Double-click the iProxy icon at the system tray (padlock icon). You can also do this by right clicking and selecting the **iProxy Transaction Status**.



2. The system will display the **iProxy Transaction Status** screen.



3. The window above shows SSL connection details and its status.
4. Click **OK** to close the **iProxy Transaction Status** window.

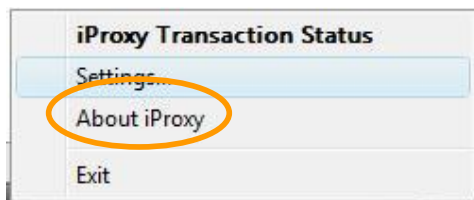
Change setting

1. General Settings (LAN environment using External Proxy Server)
2. Advanced Settings (Ciphers selection, Cache PIN option and Auto Start option)

Note : Please refer to page 25.

About iProxy

1. To view iVEST™ Client version and iProxy version, right-click iProxy icon and select **About iProxy**.



2. iVEST™ Client version and iProxy version will be shown.



Section 7: iSign

Introduction

iSign is a plug-in to perform digital signature. It uses a *private key* from smart card to generate digital signatures on web form data.

This digital signing is done to ensure the integrity and non-repudiation of the signed data. This digital signature is legally binding as it complies with the requirements of the Malaysian Digital Signature Act 1997.

It is important to remember that you need to view the data to be signed to make sure that you are signing the right data. Hence, to ensure proper viewing, it is advisable data size to be signed is around 200 kilobyte. For larger sized data, you can use our iVEST File product which can support file signing.

How to sign data?

Digital signature is only applicable at certain web sites.

1. When you have completed and submitted the web form, your web browser will automatically load the iSign plug-in. The iSign icon will appear.
2. Click the **iSign** icon.



The **iVEST PIN Request** will be displayed. This dialog box displays the data to be signed.

3. Enter your PIN and click **OK**.



4. Please wait for a while until the process is completed.
5. A notification of the signing status will be displayed.

Note: *iSign is designed for web content signing. There are some international standards applied in this component. As iSign is used for web content signing, it signs data that is recognized by the web.*

Signing is not supported for single quote ('), double quotes ("), less than (<), and plus (+). These special characters are handled differently in Web environment as these characters have different meaning. Therefore, the System Integrator who developed the system application at the server side need to change all these characters to the following format in the application before sending data to iSign for signing:

*(') change to %27<space>
(") change to %22<space>
(<) change to %3c<space>
(+) change to %2b<space>*

Section 8: iVEST™ CSP

Introduction

iVEST™ CSP is a Cryptographic Service Provider for Microsoft platform. With iVEST™ CSP implemented, iVEST™ Client allows secure e-mail using Outlook Express and Microsoft Outlook. The following steps will teach you how to:

1. Encrypt e-mail
2. Decrypt e-mail
3. Digital sign e-mail
4. Verify signed e-mail

Note: *iVEST™ CSP is not tested in iVEST™ Client version 4.1.*

Securing e-mail using Outlook Express

Encrypting e-mail

To encrypt e-mail, both sender and recipient must have digital certificate.

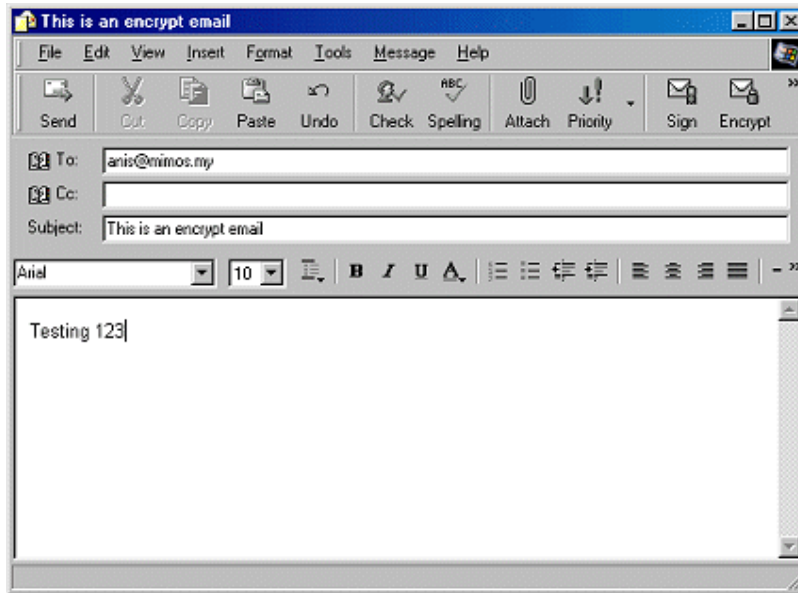
Obtaining the recipient's digital certificate. There are two options:

1. Go to your CA web site to download the recipient's certificate, or
2. Request the recipient to sign an e-mail and send to you. Once received, open the e-mail and your recipient's digital certificate will be automatically stored in your Outlook Certificate Manager.

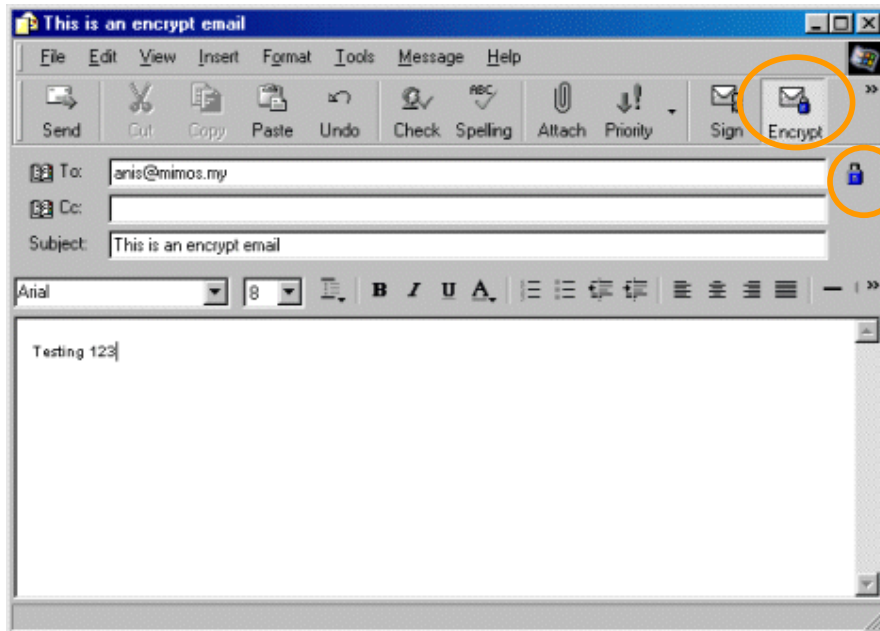
Note: *To check whether your recipient's certificate is in your Certificate Manager, click Tools -> Options > Security tab > Digital IDs ... button > Other People tab*

Steps to encrypt e-mail:

1. Ensure iVEST™ Gate is active (indicated by the key icon in your system tray)
2. Insert smart card into the Smart Card reader
3. Launch Outlook Express
4. Type your recipient e-mail address



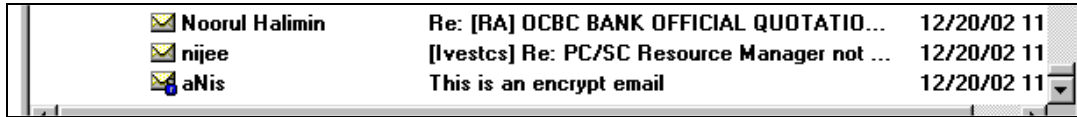
5. Click **Encrypt** button to encrypt your e-mail. You will see a padlock icon on your right of your e-mail to confirm your e-mail is encrypted.



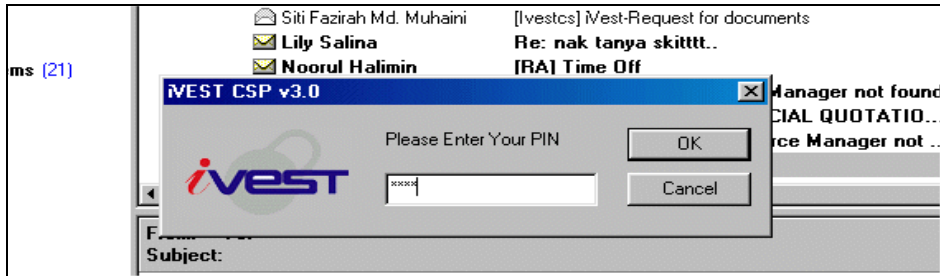
6. Click **Send** button to send the e-mail.

Decrypting e-mail

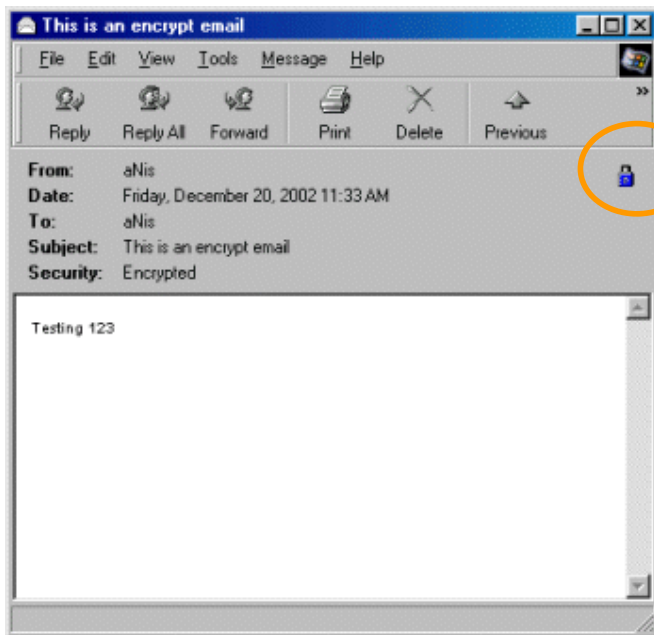
1. Ensure iVEST™ Gate is active (indicated by the key icon in your system tray)
2. Insert smart card into the Smart Card reader
3. Launch Outlook Express
4. Click **Send/ Recv** button to retrieve the encrypted e-mail.
5. Double-click to open the encrypted e-mail (denoted by a padlock icon on the mail).



6. Enter you PIN when prompted. Click **OK**.

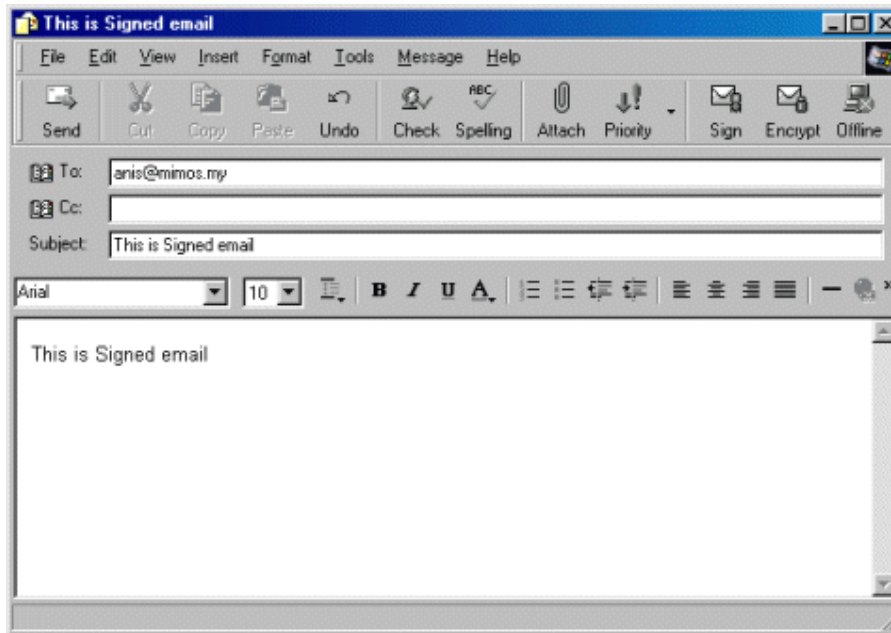


7. Outlook Express will display the following message.

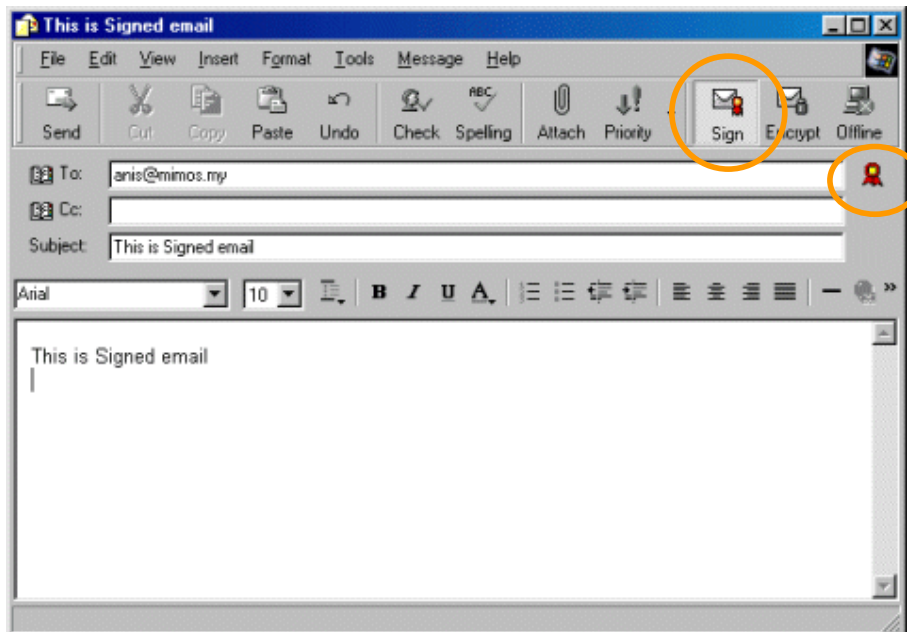


Signing e-mail

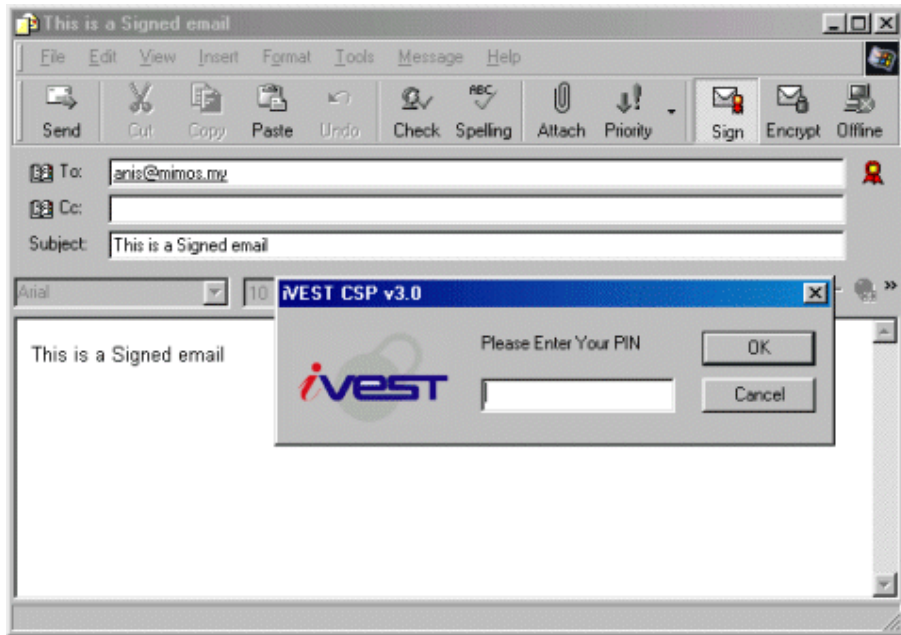
1. Ensure iVEST™ Gate is active (indicated by the key icon in your system tray).
2. Insert smart card into the Smart Card reader.
3. Launch Outlook Express.
4. Type your recipient e-mail address.



5. Click **Sign** button to sign your e-mail. You will see a ribbon icon on your right of your e-mail to confirm your e-mail is signed.



- Click *Send* button. Enter your PIN when prompted. Click *OK*.

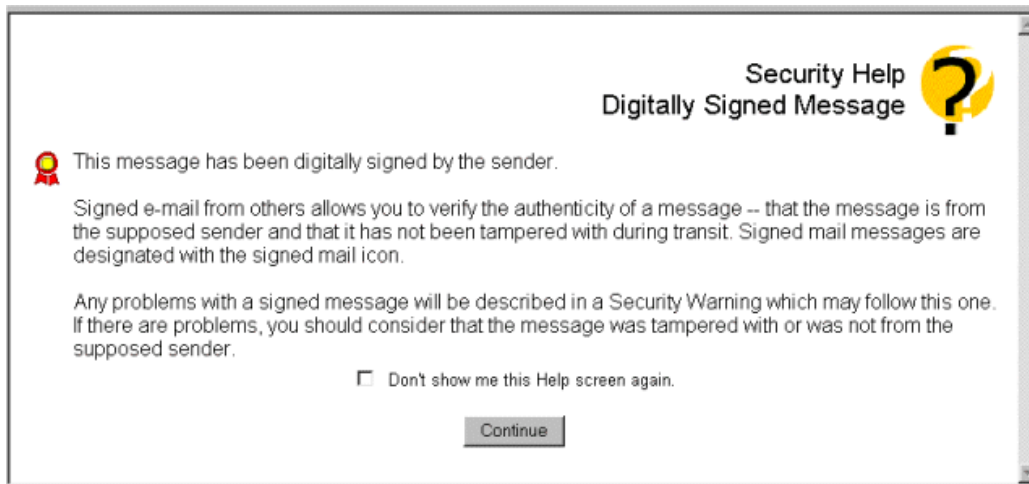


- Your signed e-mail has been sent.

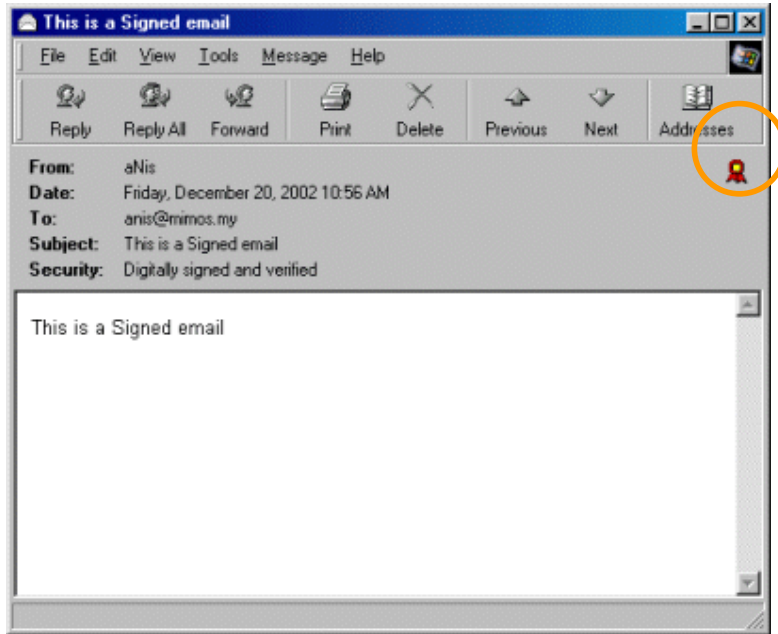
Verifying signed e-mail

- Launch Outlook Express
- Click **Send/Recv** button to retrieve the signed e-mail.
- Double-click to open the signed e-mail (denoted by a ribbon icon on the mail).

0	hairani	[[vestcs] iVEST Client error	12/20/02 10:22
0	george	[RA] OCBC BANK OFFICIAL QUOTATION - PRICING	12/20/02 10:25
	Siti Fazirah Md. Muh...	[[vestcs] iVest-Request for documents	12/20/02 10:10
	aNis	This is a Signed email	12/20/02 10:10



4. Click Continue button to read the encrypted e-mail.
5. Your e-mail will be shown but with a ribbon icon displayed on the right of your e-mail



Microsoft Outlook

To send digitally signed messages and to receive encrypted messages, you need to launch iVEST™ Gate, insert your smart card and launch Microsoft Outlook application.

The instructions are similar as Outlook Express, but in Microsoft Outlook, the encrypt and signature checkboxes are located at **Options... -> Security Settings...**

For further information see the step-by-step Guide to Public Key Feature of Microsoft Outlook at <http://www.microsoft.com> which describes how to configure Microsoft Outlook to send signed and encrypted e-mail messages.

Section 9: iVEST™ PKCS #11

Introduction

iVEST™ PKCS #11 enables you to send and receive digitally signed and encrypted messages by using Netscape Messenger. The following steps will teach you on how to:

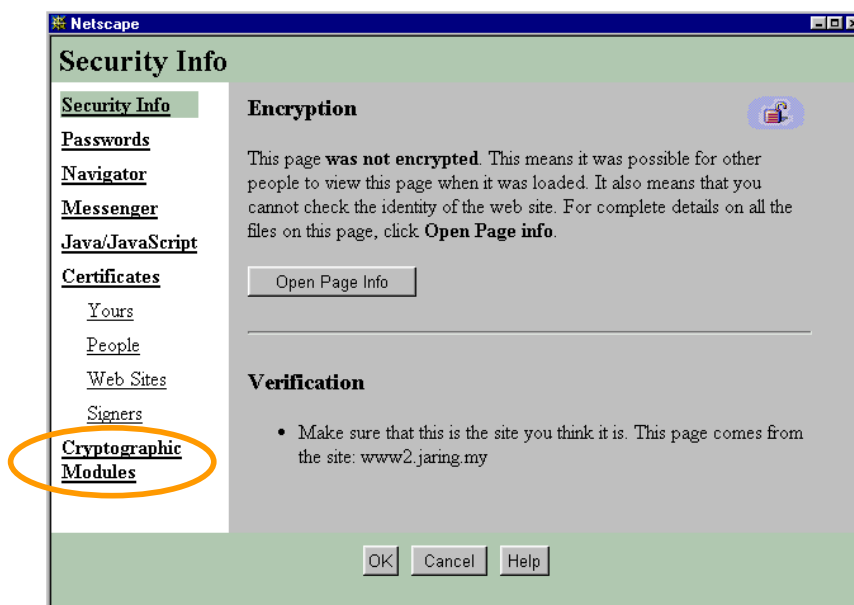
1. Enable Netscape Messenger
2. Log-in to Smart Card Token
3. Encrypt e-mail
4. Decrypt e-mail
5. Digital sign e-mail
6. Verify signed e-mail

Note: iVEST™ PKCS #11 is not tested in iVEST™ Client version 4.1.

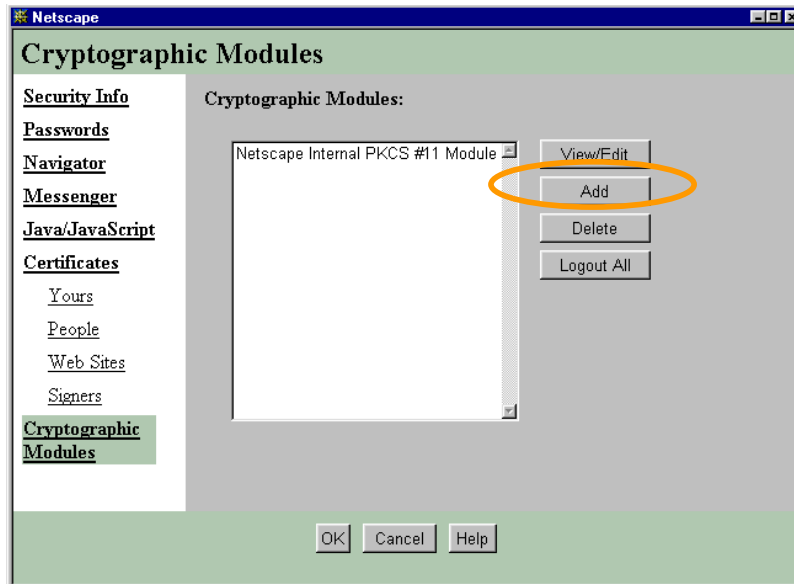
Securing e-mail using Netscape Messenger

Enabling Netscape Messenger

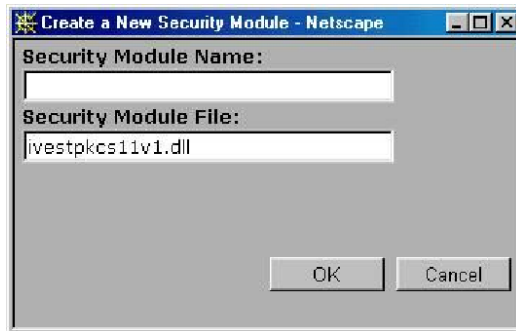
1. Launch your Netscape Navigator.
2. Click the **Security** button at the navigation bar.
3. The **Netscape – Security Info** will appear. Click the **Cryptographic Modules** on the left panel



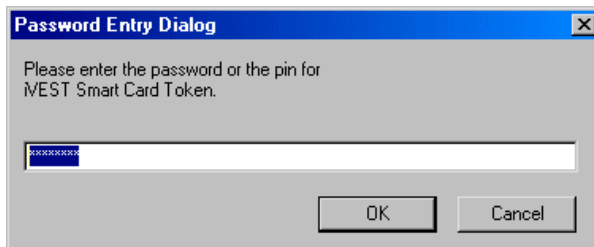
- The **Cryptographic Modules** screen will appear. Click **Add** button.



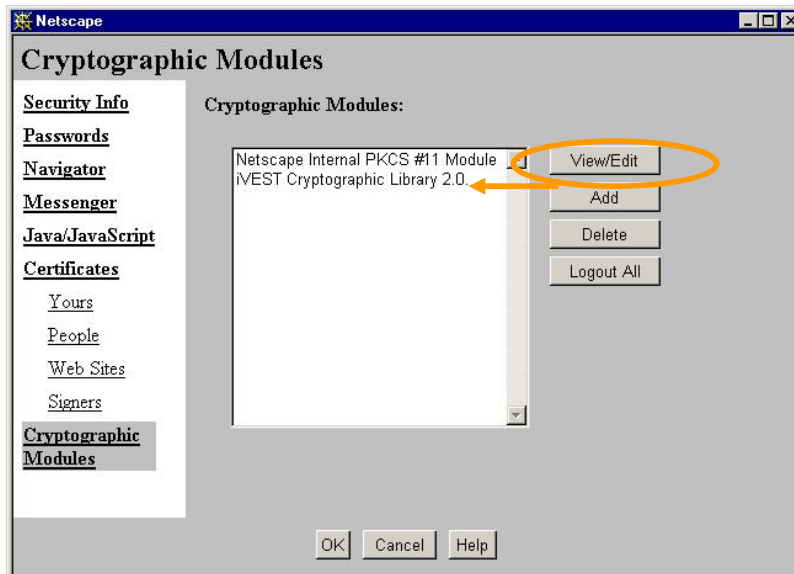
- Create a New Security Modules** screen will appear. Leave the **Security Module Name** blank but fill in the **Security Module File** with "ivestpkcs11v1.dll".



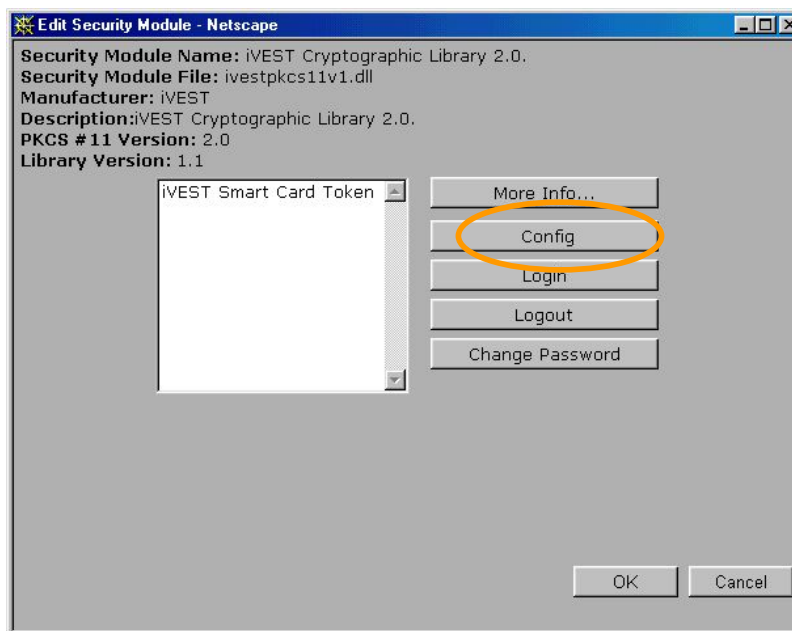
- Netscape Navigator will prompt you to enter your smart card PIN. Click **OK**.



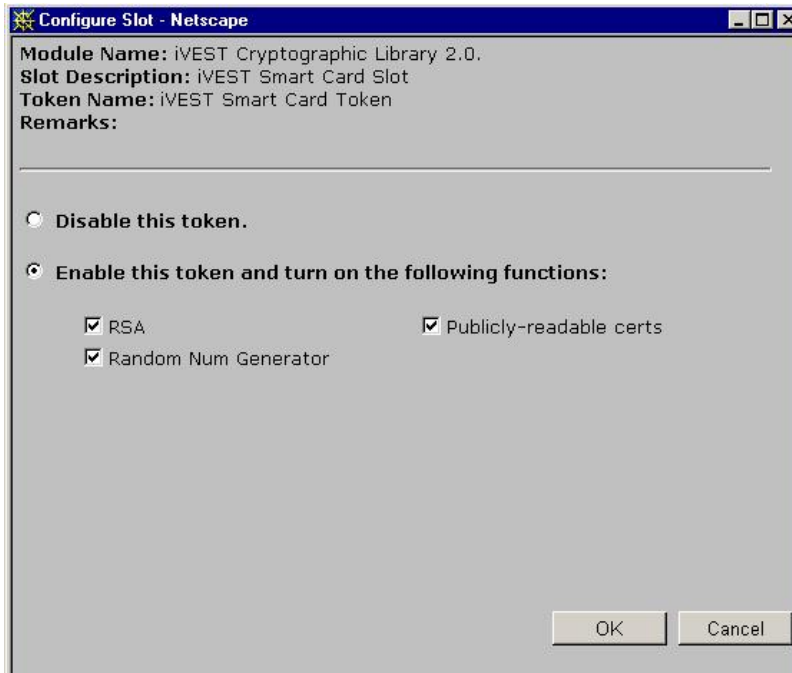
- The **iVEST™ Cryptographic Library 2.0** will be added in the **Cryptographic Modules** screen. Choose **iVEST Cryptographic Library 2.0**. Click **View/Edit** button.



8. The **Edit Security Module** screen appears. Highlight **iVEST Smart Card Token** and click the **Config** button.



9. The **Configure Slot** screen will appear. Select **Enable this token and turn on the following functions**:



10. Check all the listed functions: **RSA**, **Random Number Generator**, and **Publicly-readable certs**. Click **OK**.
11. The **Cryptographic Modules** screen will appear. Choose **Messenger** on the left panel.

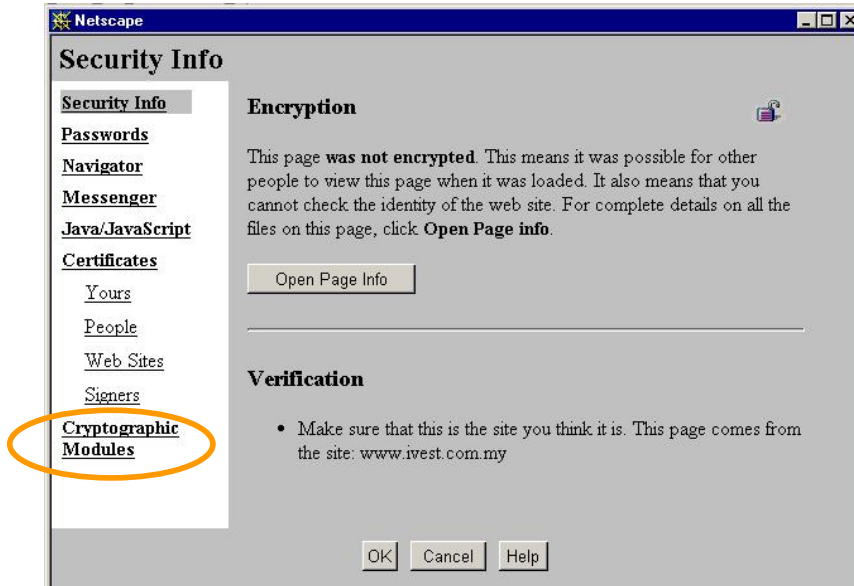


12. You should highlight **iVEST™ Smart Card Token: Authentication Certificate** at the drop-down box **Certificate for your Signed and Encrypted Messages**. Click **OK**.
13. To start using your secure e-mail, re-launch Netscape Messenger.

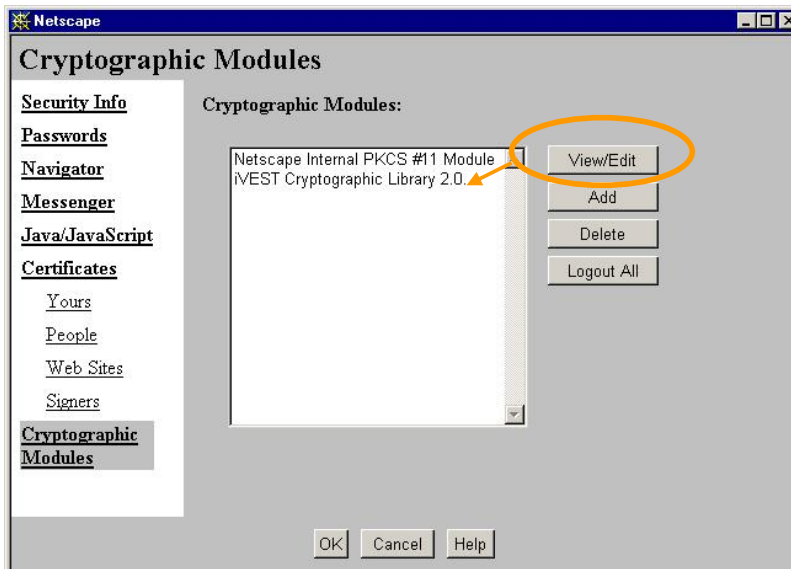
Log-in to Smart Card Token

Note: Perform "Log-in to Smart Card Token" each time you launch Netscape Messenger for secure e-mail purpose

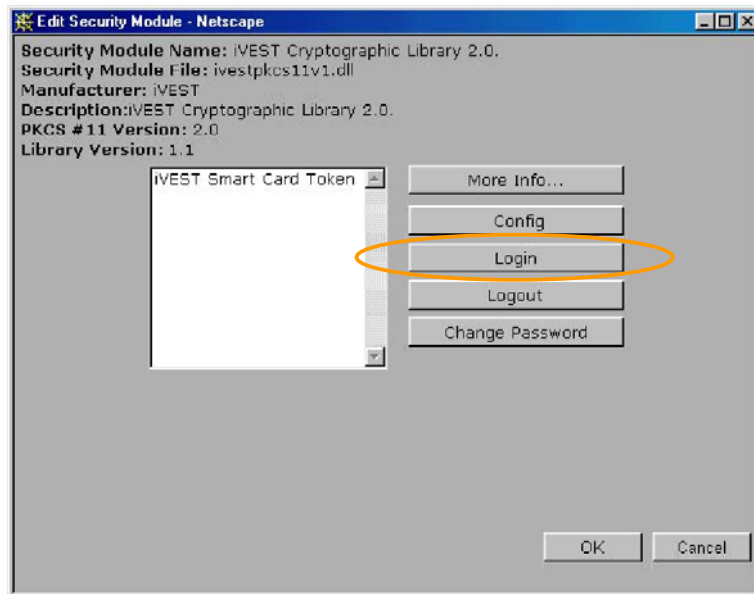
1. At the **Netscape Navigation bar**, Click **Security**.
2. The **Netscape - Security Info** will appear. Click the **Cryptographic Modules** on the left panel.



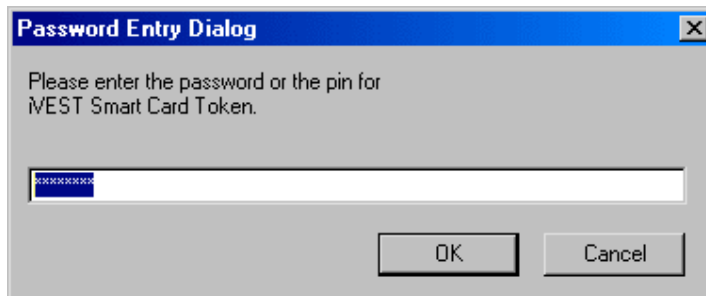
3. The **Cryptographic Modules** screen will appear. Highlight **iVEST Cryptographic Library 2.0**, and click **View/Edit** button.



4. The **Edit Security Module** screen will appear. Highlight **iVEST Smart Card Token** and click **Login**.



5. Netscape Browser will prompt for password. Enter your Smart Card PIN and click **OK**.



6. You have successfully login to Smart Card Token. Click **OK**.

Encrypting e-mail

To encrypt an e-mail, both sender and recipient must have digital certificate.

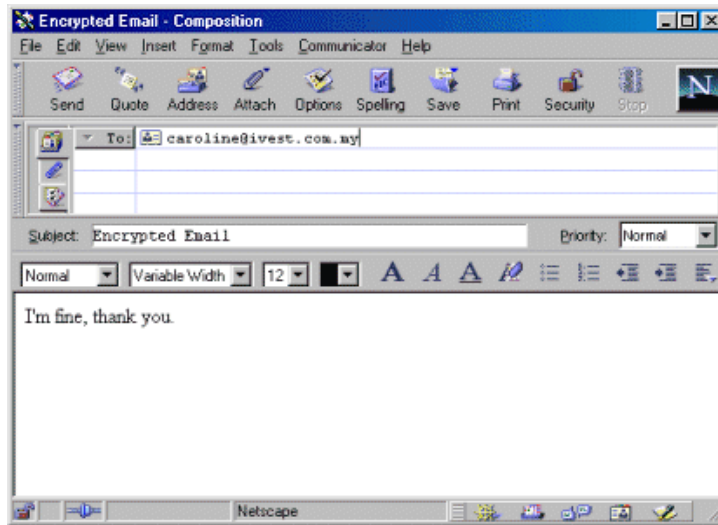
Obtain the recipient's digital certificate. Two options to obtain:

1. Go to your CA web site to download the recipient's certificate, or
2. Request the recipient to sign an e-mail and send to you. Once received, open the e-mail (your recipient's digital certificate will be automatically stored in your Netscape certificate list)

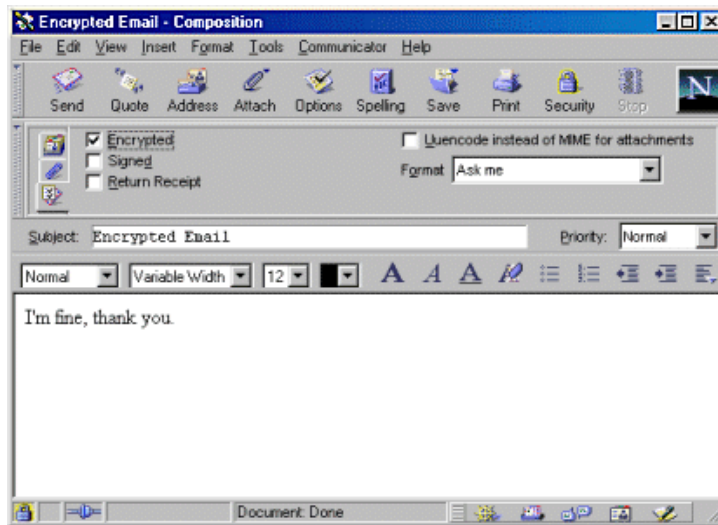
Note: To check whether your recipient's certificate is in your certificate list, click at *People under Certificates* in your Netscape Security pop-up screen.

Steps to encrypt e-mail:

1. Insert smart card into the smart card reader, the iVEST™ Gate icon at system tray will "spin".
2. Launch Netscape Messenger.
3. Login to the Smart Card Token (refer to page 46)
4. Type your recipient e-mail address.



6. Click **Option** button and check **Encrypted** checkbox. Click **Send** button to send the e-mail.



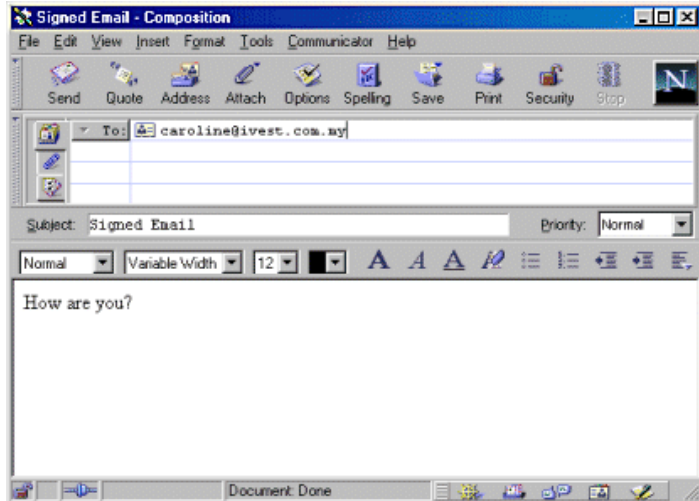
Decrypting e-mail

1. Insert smart card into the smart card reader, the iVEST™ Gate icon at system tray will “spin”.
2. Launch Netscape Messenger.
3. Login to the Smart Card Token (refer to page 46)
4. Click **Get Msg** button to retrieve the encrypted e-mail. When the e-mail is opened with an encrypted icon displayed, it means you have successfully decrypted the e-mail.

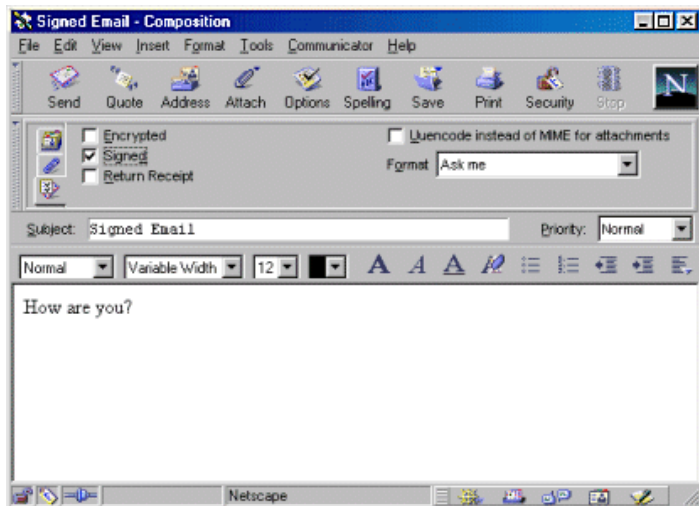


Signing e-mail

1. Insert smart card into the smart card reader, the iVEST™ Gate icon at system tray will “spin”.
2. Launch Netscape Messenger.
3. Login to the Smart Card Token (refer to page 46).
4. Type your recipient e-mail address.



6. Click **Option** button and check **Signed** checkbox. Click **Send** button to send the e-mail.



Verifying signed e-mail

Click **Get Msg** button to retrieve the signed e-mail. When the e-mail is opened with a **Signed** icon displayed, it means you have successfully verified the digital signature.



Section 10: iVEST™ XBrowser

Introduction

iVEST™ XBrowser is designed to terminate all activated Internet Browsers when the smart card is removed from the smart card reader. It provides a solution to the internet session that is not terminated after the smart card is removed from the reader when accessing PKI enabled web application.

iProxy which handles the SSL connection will establish a new SSL session if it detects a different smart card in the reader. However, even without the presence of iProxy, the session will remain until the Internet Browser is closed, and thus creating a non-secured connection to the PKI enabled web application. With iVEST™ XBrowser, the internet session will be terminated by closing the Internet Browser when smart card is removed from the reader.

iVEST™ XBrowser will not be able to function without iVEST™ Client running. This application will always monitor the PC/SC (smart card) events. When it detects any event on the PC/SC (card removed), the behaviour will be based upon the settings of iVEST™ XBrowser. By default, the user will be prompted for browser termination.

iVEST™ XBrowser features:

1. Force to terminate opened SSL sessions by closing respective active Internet Browsers when smart card is removed from the reader.
2. Allow different user to have their own settings.
3. Able to detect changes on the settings (browser type and close type) without re-starting the application.

How to start and exit iVEST™ XBrowser

1. To run iVEST™ XBrowser from Windows, go to **Start -> Programs -> iVEST Client -> iVEST XBrowser**.
2. The iVEST™ XBrowser icon will appear as below at your system tray.

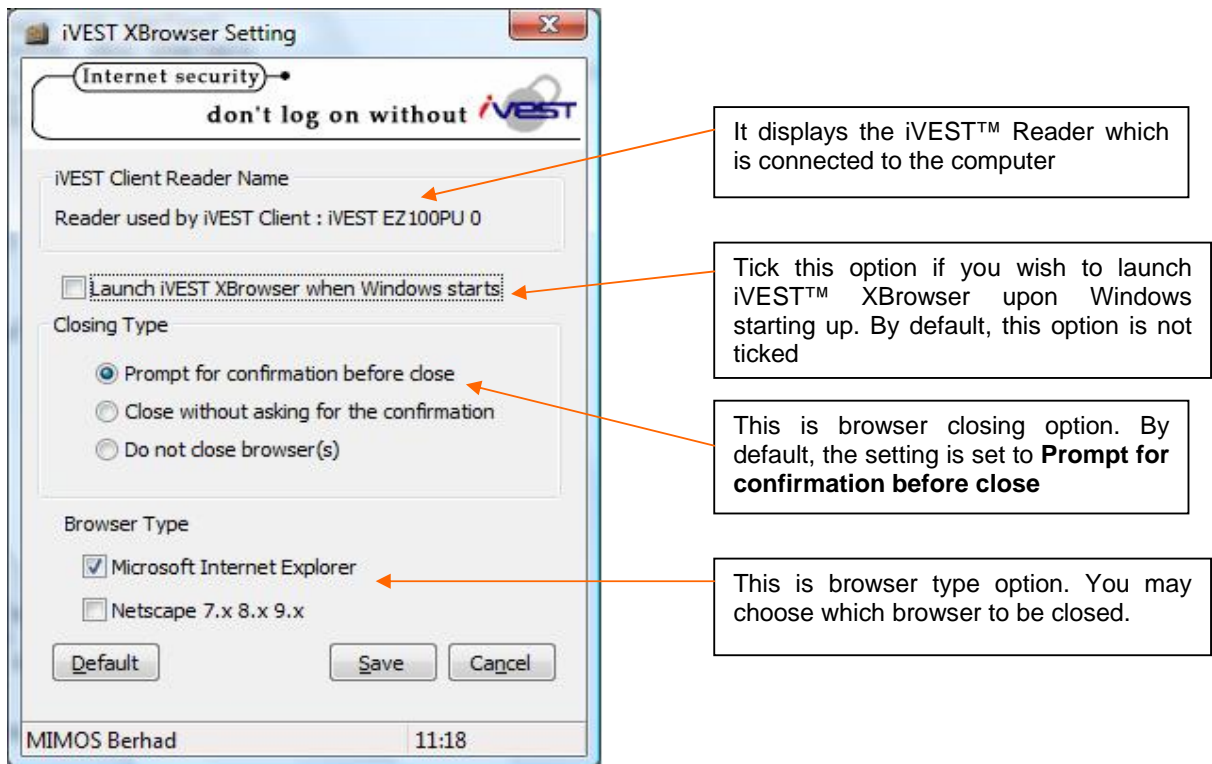


3. To exit, right-click iVEST™ XBrowser icon and select **Exit**.



iVEST™ XBrowser Setting

1. To access iVEST™ XBrowser Setting, double-click the icon on system tray.



2. Clicking the **Default** button will get back all the default setting.
3. Click **Save** to save the new setting or **Cancel** for not accepting the changes.

Section 11: Uninstallation

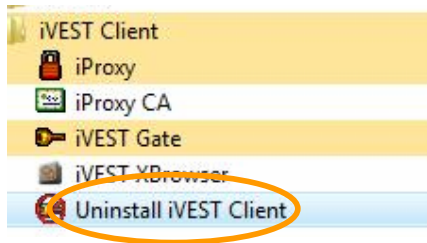
Introduction

There are two methods to uninstall iVEST™ Client software:

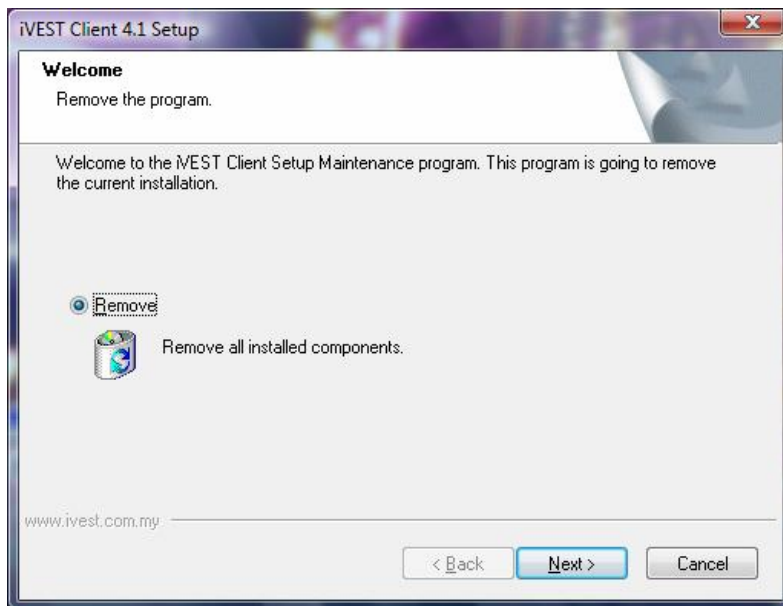
1. Uninstall through “Uninstall iVEST Client”
2. Uninstall through “Add/Remove Program”

Uninstall through “Uninstall iVEST Client”

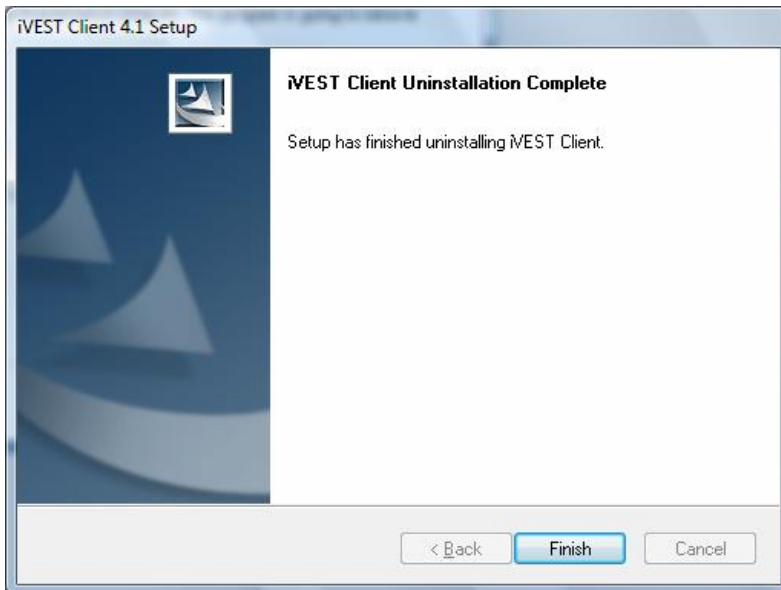
1. Close all web browsers and e-mail applications.
2. Click **Windows** button -> **All Programs** -> **iVEST Client** -> **Uninstall iVEST Client**.



3. Windows is preparing to uninstall iVEST Client.
4. The **Remove the program** screen will appear. Click **Next** to continue, else click **Cancel**.



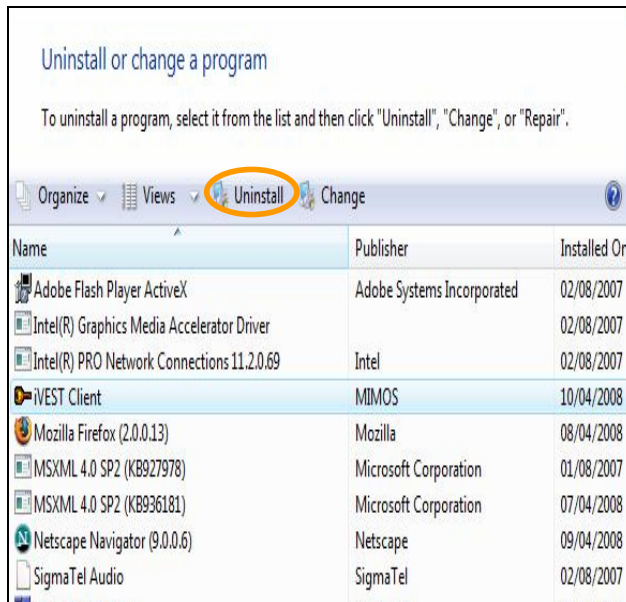
5. The uninstallation process will take place. The **Uninstallation Complete** screen will appear to tell you that the iVEST Client has successfully uninstalled. Click **Finish** to end the process.



Uninstall through “Add/Remove Program”

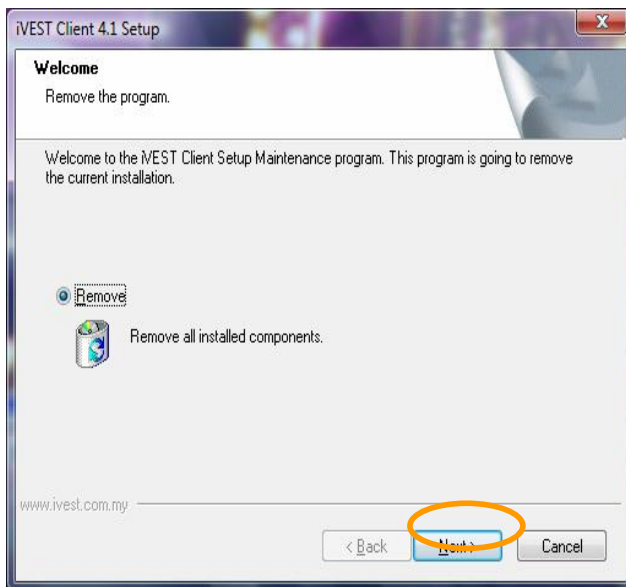


1. Close all web browsers and e-mail applications.
2. Click the Windows button -> **Control Panel -> Programs.**
3. Select **Programs and Features.**

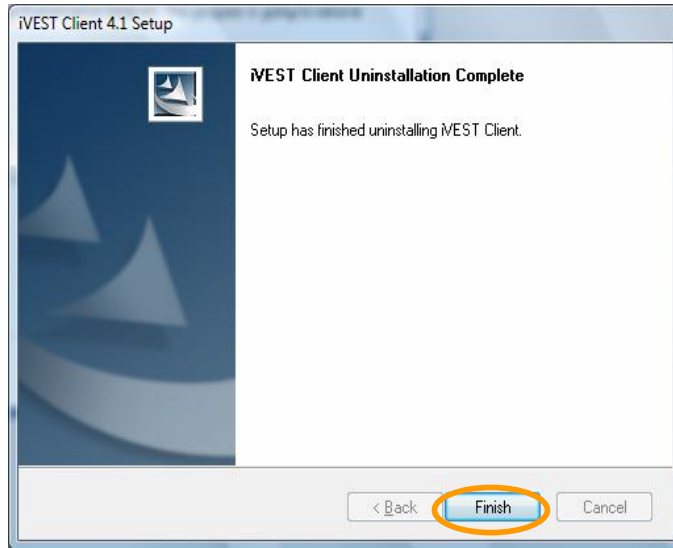


4. The **Uninstall or change a program** dialog box will appear. Highlight **iVEST Client** and click **Uninstall** button.

5. Windows is preparing to uninstall iVEST Client.



6. The **Remove the program** will appear. Click **Next** to continue, else click **Cancel**.



7. The **Uninstallation Complete** screen will appear to inform that iVEST Client has been successfully uninstalled. Click **Finish** to end the process.

Section 12: Software Specifications

iVEST™ Gate

1. Auto Start is enabled by default - only users with administrator right can change the setting.
2. PIN length is between 6 to 8 alphanumeric characters.
3. Allow to view authentication and non-repudiation certificates.
4. Auto configuration and detection of smart card reader.
5. Default browser will be launched when smart card is inserted into the smart card reader.
6. Will be placed in sleep mode when the reader is unplugged. **iVEST™ Gate** icon with exclamation mark is displayed in the taskbar.

iSign

1. Plug-in is used in Netscape browsers.
2. ActiveX technology is used in Internet Explorer.
3. All digital signature is created using non-repudiation certificate.
4. Complies with S/MIME standard.
5. iSign supports Internet Explorer 7, Netscape browser (7.0, 7.2, 8.0, 9.0.06), Mozilla 1.7 and Mozilla Firefox 2.0.

iProxy

1. Uses the authentication certificate for SSL connection.
2. The session timeout is up to 1 hour thus making the SSL connection faster and more efficient.
3. The socket timeout is extended to 20 minutes thus allowing the transfer rate to be improved and the connection timeout with heavy network load to be resolved.
4. Enable file transfers up to 15MB using dial-up.
5. Have an option to cache PIN.
6. Auto Start is enabled by default - only users with administrator right can change the setting.

iVEST™ CSP

1. Supports e-mail signing and encryption for Outlook Express 5.0, 5.5 and 6.0 and Microsoft Outlook 2000 and 2002/XP in older versions of iVEST™ Client, but not tested in iVEST™ Client version 4.1.
2. Does not support Microsoft Outlook 97.
3. Supports on-board RSA key generation and insertion of MyKad Online certificate request via Internet Explorer.

iVEST™ PKCS #11

1. Supports Netscape Messenger (version 4.5x, 4.6x, 4.7x and 4.8x) in older versions of iVEST™ Client, but not tested in iVEST™ Client version 4.1.
2. Does not support Netscape Messenger 6.0 and 7.0.

iVEST™ XBrowser

1. Supports Netscape (7.X, 8.X, 9.X) and Internet Explorer 7.

Section 13: Troubleshooting

If you encounter any problem and no solution can be obtained from the **Section 13: Troubleshooting** and iVEST website, please contact our hotline at 03-89917070 or support@invest.com.my for assistances. Our operation hour is Monday to Friday, 8:30am to 5:30pm.

Installation

Error message/symptom	Cause/Solution
Manual installation of certificate for Netscape 7.2 browser	<p>Follow the following steps for each certificate file in C:\Program Files\MIMOS\iVEST Client\Cert :</p> <ul style="list-style-type: none"> • Open Netscape 7.2 browser. • Click Edit → Preferences • Expand Privacy & Security on left panel. Select Certificates. • Click Manage Certificates... button on right hand side. • Click Authorities on top panel. • Click Import. Select certificate from C:\Program Files\MIMOS\iVEST Client\Cert folder. • Click OK. Certificate will then be installed. • Close screen by clicking OK.
Manual installation of certificate for Netscape 8.0 browser	<p>Follow the following steps for each certificate file in C:\Program Files\MIMOS\iVEST Client\Cert :</p> <ul style="list-style-type: none"> • Open Netscape 8 browser. • Click Tools → Options → Advanced. • Expand Certificates on right-hand side. Click Manage Certificates... button. • Click Authorities on top panel. • Click Import. Select certificate from C:\Program Files\MIMOS\iVEST Client\Cert folder • Click OK. Certificate will then be installed. • Close screen by clicking OK.
Manual installation of certificate for Mozilla browser	<p>Follow the following steps for each certificate file in C:\Program Files\MIMOS\iVEST Client\Cert :</p> <ul style="list-style-type: none"> • Open Mozilla browser. • Click Edit → Preferences • Expand Privacy & Security on left panel. Select Certificates. • Click Manage Certificates... button on right hand side. • Click Authorities on top panel. • Click Import. Select certificate from C:\Program Files\MIMOS\iVEST Client\Cert folder. • Click OK. Certificate will then be installed. • Close screen by clicking OK.
Manual installation of certificate for Mozilla Firefox browser	<p>Follow the following steps for each certificate file in C:\Program Files\MIMOS\iVEST Client\Cert :</p> <ul style="list-style-type: none"> • Open Mozilla Firefox browser. • Click Tools → Options → Advanced → Encryption • Click View Certificates button. Click Authorities • Click Import. Select certificate from C:\Program Files\MIMOS\iVEST Client\Cert folder • Click OK. Certificate will then be installed. • Close screen by clicking OK.

Manual installation of certificate for Internet Explorer 7	<p>Follow the following steps for each certificate file in C:\Program Files\MIMOS\iVEST Client\Cert :</p> <ul style="list-style-type: none"> • Open Internet Explorer. • Click Tools → Internet Options. Click Content on top panel. Click Certificates. • Click Import. Certificate Import Wizard screen will open. Click Next. • Click Browse and select certificate from C:\Program Files\MIMOS\iVEST Client\Cert folder. Click Next. Choose Automatically select the certificate store based on the type of certificate. Click Next → Finish. • Box with message "The import was successful" appears. Click OK.
Installation of iProxy CA	<p>iProxy Certificate valid from 05/12/2005 until 31/12/2010</p> <p>Two options to install: Using shortcut</p> <ul style="list-style-type: none"> • Click window Start button > Programs > iVEST Client -> Click iProxy CA. • Certificate screen will appear. Click Install Certificate... button. • The Welcome to the Certificate Manager Import Wizard screen will appear. Click Next >. • The Select the Certificate Store screen will appear. Choose Automatically select the certificate store based on the type of certificate and click Next >. • The Completing the Certificate Manager Import Wizard screen appears. Click Finish. • The Root Certificate Store screen will appear. Click Yes to add the iProxy CA. • The import was successful screen will appear. Click OK. <p>Manual installation</p> <ul style="list-style-type: none"> • Open Windows Explorer and locate the path of iProxy CA. The default path is C:\Program Files\MIMOS\iVESTClient\Cert. • Double-click iProxyCA.crt. <p>The Certificate screen will appear. For the rest of the steps, please refer to "Using shortcut" installation steps from step 2 until finish.</p>
Error message: iGate.exe unable to locate dll	<p>Cause: Uninstalling iVEST™ Client and without restarting PC, reinstall the iVEST™ Client again</p> <p>Solution: Reboot machine, reinstall iVEST™ Gate and choose "Restart Now".</p>
Power failure during installation or uninstallation.	<p>Solution: Delete the iVEST™ Client folder from your Windows Explorer. Re-install iVEST™ Client</p>

iVEST™ card reader and driver

Error message/symptom	Cause/Solution
"Device error" message.	<p>Solution 1: Ensure that your readers are securely connected to the machine</p> <p>Solution 2: Ensure that the correct driver is installed.</p>
Smart card reader gets disconnected while running the iVEST™ Client	<p>Solution: Reconnect the reader (USB), and Windows will detect it automatically.</p>
Mouse driver not found	<p>Solution: Check your smart card reader and mouse device connections.</p>
iVEST™ Client hang	<p>Cause: If the card reader is disconnected while iVEST™ Client is loading, the task has to be killed.</p> <p>Solution: Reconnect the card reader and re-launch iVEST™ Gate.</p>

iVEST™ card

Error message/symptom	Cause/Solution
Error message," Sorry, access denied. You need and iVEST™ card to login", when trying to access iVEST™ smart card testing page and other iVESTed website	Cause: iVEST™ card has expired Solution: Apply for iVEST™ card renewal
Error message," You are not authorized to view this page", when trying to access iVEST™ smart card testing page and other iVESTed website	Cause 1: iVEST™ card has expired Solution: Apply for iVEST™ card renewal Cause 2: You do not have an authority to access the website Solution 2: Report to website administrator to grant you the access
Smart Card Error: Please restart iVEST™ Gate and iProxy, and reinsert the smart card	Cause: This is an unforeseen problem caused by the smart card OS which fail when verifying the correct PIN. Solution: Re-launch iVEST™ Gate and iProxy, and reinsert the smart card.

iVEST™ Gate

Error message/symptom	Cause/Solution
iVEST PIN Request at every iVEST™ed secure page	Solution 1: Enable cache PIN. How enable:- <ul style="list-style-type: none"> • Right click iProxy > select Settings... • The Settings screen will appear. Select Advanced tab. • check the Cache PIN box. • Click Ok. Solution 2: Disable the TLS option. How to disable:- <ul style="list-style-type: none"> • Launch Internet Explorer • Go to Tools > Internet Options > Click Advanced tab. Look for security and uncheck the box beside "TLS 1.0".
iVEST Gate Error: Error State	Cause: During animation state, iVEST™ Client does not detect the card properly or the card is faulty Solution: Pull card from the reader and re-insert. If problem still persist, return the card to any iVEST™ or Anjung Internet Jaring counter for further testing
iVEST Gate Error: Please click on Settings to configure your smart card reader first!	Cause: More than one reader attached but the first default reader is taken out Solution: Log in to windows again and select the new reader attached
Unable to change setting at iVEST™ Gate Startup setting	Login as administrator to change the setting.
iVEST Gate Warning: iVEST™ is not running.	<ul style="list-style-type: none"> • Ensure smart card is valid • Ensure smart card reader is functioning well • Ensure serial/USB port enabled.
iVEST Gate Warning: You need to restart your iVEST™ Gate for new changes to take effect!	Cause: You have more than one reader attached to the PC. Message box will appear when attempting to change settings. Solution: Exit iVEST™ Gate and re-start iVEST™ Gate.
iVEST Gate Error: Error listing reader. Please ensure you have the readers connected and installed the drivers	Cause: No reader attached to the machine Solution 1: Attach smart card reader to the machine and restart the machine Solution 2: Install the correct and latest driver.
Error message: Can't write startup Key	Cause: No permission to over ride the registry setting. Solution: Logon and install the software as administrator right.

iVEST Gate Error: Error reading certificate. Please make sure iVEST™ Gate is running and smart card is properly inserted	Solution: Ensure to insert your smart card into reader properly. If error still persist, most likely the smart card is faulty. Please return the card to any iVEST™ or Anjung Internet Jaring counter for further testing.
iVEST Gate Error: Smart card may not be present	Cause: Smart card is not slot into the reader properly when trying to change pin Solution: Ensure to insert your smart card into reader properly.
iVEST Gate Error: Smart Card PIN Blocked! Contact your administrator to unblock the PIN	Cause: An attempt to key in the wrong PIN for 3 consecutive times. Solution: Send smart card to iVEST™ or Anjung Internet Jaring ounter for unblocking.
Error reading certificate	Solution: Reinsert card
iVEST Gate not detected	Solution: Unplug and plug again reader
iVEST Gate hang	Solution: Unplug and plug again reader
iVEST Gate changed to gray color	Solution: Reinsert card
iVEST™ Gate will keep reading more than 5 mins and reader remains in red light continuous.	Solution: Restart machine

iProxy

Error message/symptom	Cause/Solution
Connection to https site fail if iVEST™ Gate is left idle for a long period of time i.e. more than two and a half hour.	Solution: Remove the card and reinsert. If still fail, please restart PC.
iProxy icon is not activated/does not exist on the system tray.	Solution: Run iProxy from Windows Start button > Programs > iVESTClient -> Click iProxy
Removing smart card during the following: <ul style="list-style-type: none"> • ongoing SSL browsing session • when iVEST™ Client PIN request is opened • before iVEST™ Gate finish loading. 	Solution: <ul style="list-style-type: none"> • Click at the browser STOP button before remove the smart card from the reader. • If the iVEST™ Client hangs, please close and re-launch iVEST™ Gate and iProxy • If it is still fail, please restart PC then re-launch iVEST™ Gate and iProxy
iProxy error: Unable to update setting in registry.	Does not have the privileges to change the setting when attempted to change the iProxy setting. Logon under administrator to change the setting.
Smart card error 0: Smart card error Code Oe	Cause: MyKad user might experience some problem to access secure site. This error might prompt or the error keep looping Solution: <ul style="list-style-type: none"> • Cancel the pop-up screen by clicking the X button on the top right hand side. • Pull MyKad from the smart card reader • Exit iVEST™ Gate and iProxy • Re-launch iVEST™ Gate and iProxy • Insert MyKad • Re-enter the secure site
".... has received an incorrect or unexpected message. Error code: -12227" error message when trying to access an https site which requires client certificate.	Cause: Localhost proxy setting is not configured in browser. Solution: Configure browser security setting(refer to Web Browser section under Section 13:Troubleshooting).
iProxy crash	Solution: Relaunch iProxy

" failed generating iProxy Cert" error displayed in iProxy Transaction Status and page cannot be displayed in IE browser	Solution: Reinsert card
--	-------------------------

iVEST™ CSP

Error message/symptom	Cause/Solution
Installation of CA Certificate in Internet Explorer (for secure e-mail using Outlook Express)	<p>There are two certificates that need to be installed, which are the trusted root certificate and intermediate certificate.</p> <p>Installing the trusted root certificate</p> <ul style="list-style-type: none"> • Open Windows Explorer and locate the path of trusted root certificate. The default path is C:\Program Files\MIMOS\iVEST Client\Cert. • Double-click the certificate. • Certificate screen will appear. Click Install Certificate... button. • Certificate Manager Import Wizard screen will appear. Click Next >. • Select a Certificate Store screen will appear. Select Place all certificate into the following store and click Browse... button. • Select Certificate Store screen appears. Check Show Physical Stores checkbox and expand the list of Trusted Root Certificate Authorities. • Select Local Computer and click OK. • Click Next > to continue and the Completing the Certificate Manager Import Wizard screen will appear. Click Finish. <p>Installing the intermediate certificate</p> <ul style="list-style-type: none"> • Open Windows Explorer and locate the path of trusted root certificate. The default path is C:\Program Files\MIMOS\iVEST Client\Cert. • Double-click the certificate. • Certificate screen will appear. Click Install Certificate... button. • Certificate Manager Import Wizard screen will appear. Click Next >. • Select a Certificate Store screen will appear. Select Place all certificate into the following store and click Browse... button. • Select Certificate Store screen appears. Check Show Physical Stores checkbox and expand the list of Intermediate Certificate Authorities. • Select Local Computer and click OK. • Click Next > to continue and the Completing the Certificate Manager Import Wizard screen will appear. Click Finish.
Checking the installed certificate in Internet Explorer	<ul style="list-style-type: none"> • Launch Internet Explorer • Click Tools > Internet Options > Content. • Click Certificates... button. • The Certificate Manager screen will appear. <p>Locate the installed certificates at the respective column.</p>
Fail to decrypt e-mail/message.	<p>Solution: Ensure to sign the message using the correct Digital ID hence the recipient would be able to grab the right public key. The right public key will then be used to encrypt message to you and later to be decrypted with the matching private key in your smart card.</p>
When sending encrypted e-mail, you will receive a warning, "Security warning: This message is being sent with 40 bit encryption. Your advanced security options are set to warn on less than 168 bit encryption. Would you like to send this message anyway? Click [Yes] or [No] to continue."	<p>Cause: User has set (or set by default) to encrypt using 40bit encryption and at the same time user has set (or set by default) to warn when sending any message below 168 bit encryption.</p> <p>Solution: If confirmed prefer to use the encryption level, just click YES to continue. Otherwise, increase the encryption strength or decrease the strength to warn.</p>

Smart card general access error	<p>Cause: MyKad user might experience some problem to access secure site. This error might prompted or the error keep looping</p> <p>Solution:</p> <ul style="list-style-type: none"> • Cancel the pop-up screen by clicking the X button on the top right side. • Pull card from the smart card reader • Exit iVEST™ Gate and iProxy • Re-launch iVEST™ Gate and iProxy • Insert MyKad • Re-enter the secure site
<p>When accessing a secure site, a screen appears;</p> <p>Client Authentication: Identification. The web site you want to view requests identification. Select the certificate to use when connecting. (There are 2 certificates under the registered user name). Click [More info], [View Certificate], [OK] or [Cancel]. “ If the first certificate is selected, iVEST™ CSP PIN request box will pop up. After entering the PIN. The “page cannot be displayed” is displayed on the screen. If the second certificate is selected, the transaction is successful but you might get a frequent request for PIN.</p>	<p>Cause: This message appears because you are not accessing the secure sites thru iVEST™ CSP instead of iProxy. The listed certificates are Non-repudiation certificate and Authentication certificate, respectively. You have selected non-repudiation certificate when prompted.</p> <p>Solution:</p> <ul style="list-style-type: none"> • You are not encouraged to access using iVEST™ CSP. To access secure site using iProxy, configure the browser security accordingly. • If you have to access using iVEST™ CSP for a certain reason, select Authentication Certificate.

iVEST™ PKCS #11

Error message/symptom	Cause/Solution
<p>Installation of CA Certificate in Netscape (for secure e-mail using Netscape Messenger)</p>	<p>Before installation, you need to identify who is your certificate's issuer. View your certificate to find out. Based on your certificate's issuer, install the respective trusted root and intermediate CA certificate.</p> <ul style="list-style-type: none"> • Launch Netscape Navigator. • Launch Windows Explorer and locate the path of CA certificate. The default path is C:\Program Files\MIMOS\iVEST Client\Cert. • Drag the certificate from the Windows Explorer into Netscape Navigator screen. • The New Certificate Authority screen appears. Click Next button for the next three screens. • New Certificate Authority screen will ask you to accept the certificate authority. Check Accept this Certificate Authority for Certifying e-mail users. Click Next>. • A screen appears which will give you an option whether to be prompted with a warning message before sending any information. Check the box if you wish to and click Next>. • You will be asked to enter a short name for the certificate authority. Enter any suitable name to identify the certificate authority. Click Finish button.
<p>Netscape: The certificate issuer for this server is not recognized by Netscape. The security certificate may or may not be valid. Netscape refuses to</p>	<p>Solution:</p> <p>Send signed e-mail, ensure the following:</p> <ul style="list-style-type: none"> • log-in to Smart Card Token • PKCS #11 has been installed successfully (one time installation). • Install the root and intermediate certificate (one time installation)

connect to this server.	<p>Send encrypted e-mail:</p> <ul style="list-style-type: none"> Your recipient's certificate is marked as not trusted. To trust the certificate, open Netscape Navigator, click Security > People > highlight your recipient's e-mail address and click View/Edit button > Choose to trust this certificate. The root and intermediate certificate has not been installed (one time installation).
Invalid Signature statement when receiving e-mail, check whether the smart card is your own smart card.	<p>Solution: Double-click iVEST™ Gate icon and select "View Certificate". Ensure that the e-mail in your smart card is the same as registered at your Netscape Messenger.</p>
Netscape may give an error message when you try to sign, encrypt or decrypt messages.	<p>Cause: You have removed your smart card and insert another smart card without closing all Netscape browser and Messengers screens. Solution: Exit Netscape and Messenger whenever you change your smart card and log-in to Smart Card Token.</p>

Web Browser

Error message/symptom	Cause/Solution
Configuring proxy security setting in Internet Explorer (version 5.0 and 6.0) for LAN environment	<ul style="list-style-type: none"> Launch Internet Explorer Click Tools > Internet Options > Connections. Click LAN Settings... button. The Local Area Network (LAN) Settings screen will appear. Select Use a proxy server under Proxy server and click Advanced... button. The Proxy Settings screen will appear. Type in localhost and 5003 at the Secure field. Click OK to close all the screens and re-launch Internet Explorer.
Program not Found detected when you want to start iVEST™ Client for the first time.	<p>Solution: Set IE as the default browser</p> <ul style="list-style-type: none"> Launch IE 5.0 Click Tools > Internet Options > click Programs tab > Select Internet Explorer should check to see whether it is the default browser. Re-launch IE. Click YES when a screen appears asking you to make IE as the default browser
Not able to set the browser security at Proxy Setting menu on IE because the security field cannot be edited	<p>Solution: Uncheck the User the same proxy server for all protocols checkbox at Proxy Settings.</p>
Fail to connect to secure sites, with or without iProxy.	<p>Solution:</p> <ul style="list-style-type: none"> Launch IE Click Tools > Internet Options > click Advanced tab > click Restore defaults button. Re-launch IE
Security Alert: Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate. The security certificate is from a trusted certifying authority. The security certificate is valid. The name on the security certificate is invalid or does not match the name of the site. Do you want to proceed? Click [Yes], [No] or [View Certificate].	<p>Solution: Click Yes</p>

<p>Error message: New site cert. Click next, next, next, next & Finish. No user cert. Security info. Click Continue button. Sorry, you are not authorized to view this page.</p>	<p>Cause: Error message appears when trying to access secure site which require smart card Solution: Configure web browser security setting</p>
<p>Error message: Client Authentication. Click OK, Security Alert screen appears. Click yes. Http 403 (forbidden), you are not authorized to view this page appears.</p>	<p>Solution: Configure web browser security setting</p>
<p>Error message: Your Certificate Is Invalid and CRL not found.</p>	<p>Cause: The server at Digicert is not available and fails to retrieve CRL. Solution: Try again later</p>
<p>Error message: Your Digital Signature is invalid</p>	<p>Solution 1: Your smart card has expired. Renew your smart card. Solution 2: Double confirm by trying to use with other smart cards or other machines. If all machines and cards produce the same result, there might be a server connection error. Report to iVEST™ Customer Service and try again later.</p>
<p>During installation, iVEST Client, will turn off caching in browsers. However, for machines with multiple users, it will only be turned off for the user who installed iVEST Client. For other users, need to manually turn off caching. (For Netscape 7.2, Netscape 8 and Mozilla).</p> <p>Note: Cache PIN functionality is not recommended by iVEST.</p>	<p>Solution: Need to manually turn off caching in browser.</p> <p>Step:</p> <ol style="list-style-type: none"> 1. Open the Netscape or Mozilla browser. 2. Type about:config at the address. 3. Select network.http.proxy.keep-alive, right-click, choose Modify. <p>Change Boolean value to false. Click OK. The values for network.http.proxy.keep-alive will then be as the following:</p> <ol style="list-style-type: none"> a) Status : user set b) Type : Boolean c) Value : false

Operating system

Error message/symptom	Cause/Solution
<p>Error message: Unsafe Removal of Device. Click OK to continue.</p>	<p>Cause: Attempt to remove USB smart card reader during an ongoing SSL session or iVEST™ Gate is spinning. Solution:</p> <ul style="list-style-type: none"> • Close all web browsers • Exit iVEST™ Gate • Click Windows Start button > Settings > Click Control Panel • Click Add/Remove Hardware and follow the instructions provided to safely unplug the device. • The Unplug or Eject Hardware icon is displayed.

Networking / Internet connection / External proxy

Error message/symptom	Cause/Solution
How to troubleshoot the problem of whether you can establish SSL connection with the server using your certificate.	<ul style="list-style-type: none"> • Remove security settings at browser (localhost and 5003). • Remove the external proxy setting at iProxy setting. • Re-launch browser. • Go to http://www.igest.com.my/smcardtesting to test your certificate. • For Netscape, if No User Certificate. Forbidden appears, then your network configuration allows and supports SSL connection with user certificate. Hence, iVEST™ can be used in your LAN connection. • For IE, if The web site you want to view requests identification. Select the certificate to use when connecting appears, then your network configuration allows and supports SSL connection with user certificate. Hence iVEST™ can be used in your LAN connection. • If you do NOT see any of the above, your network does NOT support SSL connection with user certificate. You may use Dial Up or ADSL connection or refer to your System Administrator.
Error message: Page Cannot be displayed	<p>Solution 1: Ensure that without going through iProxy, user is able to go to SSL sites. Your system administrator should be able to ensure this by opening port 443 and ensure that your browser is not blocked from accessing the required sites.</p> <p>Solution 2: Test your smart card at http://www.igest.com.my. If you fail to test, check your browser security and external proxy setting.</p> <p>Solution 3: Ensure that your smart card testing at http://www.igest.com.my is successful</p> <p>Right-click iProxy icon and select iProxy Transaction Status. Under the Site/Proxy column, look for the site that you are accessing. State the corresponding connection Status. If the status is connecting for a long time, it could be due to proxy server.</p> <p>If connection is not going through proxy server - Ensure that users do not tick the external proxy box at iProxy Setting.</p> <p>If connection is going through proxy server - Ensure that it is a pass-through type and the external proxy setting is set accordingly.</p> <p>If going through proxy server for sites except for the required sites, do not set the external proxy. At the iProxy Transaction Status (double click iProxy), ensure that the connection status for the required site is done. If the status is connecting for a long time, double-check the proxy server settings.</p>

Error code (while downloading certificates)

Error	Description
0	Successful
1	Operation cancelled
2	No certificate found in smart card when iVEST™ Gate Launch
3	Challenge response failed once (counter = 1)
4	Challenge response failed twice (counter = 2)
5	General Error
6	Challenge response failed thrice, card will be blocked (counter = 3)
7	Card is blocked.
8	Verify pin error.
9	RSA key exists in smart card. (not an error code)
10	No pin exists in smart card.
11	Certificate exists in smart card.
12	URL exists in smart card.
13	No RSA key exists in smart card.
14	Conditions not satisfied, i.e.: try to insert certificate while there is no key in smart card.

15	No PKI application in smart card.
17	No memory in smart card.
18	Invalid command set or invalid card.
19	Invalid command set or invalid card.
20	No certificate in smart card.
50	Key generation fail at PC/SC
60	Insert Certificate fail at PC/SC
70	Public key not matched
80	Read public key fail at PC/SC
32	Invalid data.
48	Device error (reader, driver)
164	Pin blocked, can't perform RSA operation, but still able to read certificate.
224	Token not present.

Section 14: Glossary of Terms

Certificate

The digital ID of a user issued by a Certification Authority.

Certification Authority (CA)

A trusted body that issues certificate to user.

Cryptography

The science of writing in secret. It is a way of transforming information into a form unreadable by anyone without a secret decryption key.

Dialog Box

The small window, which prompted user to key in data. Some do not allow the user to go back to the main window before they are closed.

Dial-up

Internet connection between machines established over a telephone line using a modem.

Digital Certificate

The digital equivalent of a paper certificate (i.e. passport, driver's license or identity card). The file contains the individual's public key and a signature made by a Certification Authority. It serves to prove the individual's identity or right to access information or services on the Internet.

Digital Signature

A digital code that can be attached to an electronically transmitted message to uniquely identify the sender. The signature can be used to verify whether the data actually came from the sender.

Gateway

A network point that acts as an entrance to another network. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.

iVEST™ Proxy

A piece of software located on the Client side. (see Proxy)

iVEST™ CSP

iVEST™ CSP is a Cryptographic Service Provider (CSP) for Microsoft platform. With iVEST™ CSP implemented, iVEST™ Client allows secure e-mail using Outlook Express and Microsoft Outlook.

In general, CSP contains implementations of cryptographic standards and algorithms. At a minimum, a CSP consists of a dynamic-link library (DLL) that implements the functions in CryptoSPI.

Internet Service Provider (ISP)

Company, which provides other companies or individuals with access to the Internet.

Local Area Network (LAN)

A group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). It may also serve for home network (home users) to connect a few computers.

Local Proxy

A piece of software located in the user's machine. (see Proxy)

Pass-Through Proxy Server

A proxy that masquerades as the server it is proxying for, such that the proxy appears to hold a mirror image of whatever is on the proxy server

Personal Identification Number (PIN)

A secret code used for identification purposes.

Plug-in

A software program that extends the capabilities of your browser in a specific way - giving you, for example, the ability to play audio samples or view video movies from within your browser.

Proxy

A proxy is used to provide additional security between your computer and the Internet (usually with a firewall) and/or to increase performance between networks by reducing redundant traffic via caching.

Public-key cryptography

A form of cryptography that makes use of a key-pair: a public key and a private key. Each user will have his/her own key pair. The private key is kept secret and known only to the owner; the public key is published yet cannot be modified by anyone. A message that is encrypted using the public key can only be decrypted using the corresponding private key and vice versa. This infrastructure enables the use of digital signatures.

Private key

One of the keys in a public-key cryptography key-pair. This one is kept by the owner and should be used only by him/her. See *public-key cryptography*.

Public key

One of the keys in a public-key cryptography key-pair. This one is published and used by anyone to encrypt a message that is to be sent to the owner of the key. The owner then decrypts the message using his/her private key. See *public-key cryptography*.

Public-key infrastructure (PKI)

A set of security services that enables the use of public key cryptography and certificates in a distributed computing environment. The services include certificate management (certificate generation and revocation, CRL creation and maintenance and CA management) and secure administration of key pairs (key generation, back-up, recovery and update).

Reader

The component that extracts data (the digital certificate and private key) from a token.

Reader and smart card

A pair that consists of a smart card and its reader. Since every token must have a reader, this pair is treated as one object. (See *reader, smart card*).

Secure Socket Layer (SSL)

SSL is located between the TCP/IP layer and the application layer. It guarantees secure communication through server authentication, data encryption, message integrity and client authentication for a TCP/IP connection.

SSL comes in two strengths, 40-bit and 128-bit, which refer to the length of the "session key" generated by every encrypted transaction. The longer the key, the more difficult it is to break the encryption code. iVEST™ always uses 128-bit key length encryption.

Smart card

A card, the size of a credit card, that has memory and a processor.

Smart card reader

Hardware which is used to read the smart card. It can be external to a computer (using a cable connection) or internal. You insert your smart card into this component so that information can be extracted from it.

Web browser

The application you use to access the Internet. Examples : Netscape Navigator, Internet Explorer, Mozilla, etc.

Web server

This is where web content is served. When you connect to a site, you are actually connecting to a server for the contents of a site.

Window's system tray

This is only available in a Windows environment. It is the box at the right end of your task bar where you can see icons of running applications.

APPENDIX

Recommended Configuration Steps at Server Side For Signing Large Data

In order to enable signing of large data, there are a few configuration steps that can be done by the server administrator at iVEST Server and web sever/application server. It is also recommended that the server have a mininum of 1GB RAM.

iVEST Server

Set the following in iVEST Server configuration file, which is wrapper.config
Wrapper.java.maxmemory = 512

Web/Application Server

Here we give configuration examples for web/application server 1)Apache-Tomcat and 2)JBoss
Other web/application servers may have similar or different configuration steps.

Apache-Tomcat

- a) In catalina.sh file which is under /usr/local/tomcat/bin directory, set
`CATALINA_OPTS= -Xms64m -Xmx512m`

(as in the code below):

```
if [ "$1" = "jpda" ]; then
  if [ -z "$JPDA_TRANSPORT" ]; then
    JPDA_TRANSPORT="dt_socket"
  fi
  if [ -z "$JPDA_ADDRESS" ]; then
    JPDA_ADDRESS="8000"
  fi
  if [ -z "$JPDA_OPTS" ]; then
    JPDA_OPTS="-Xdebug -Xrunjdp:transport=$JPDA_TRANSPORT,
              address=$JPDA_ADDRESS,server=y,suspend=n"
  fi
  CATALINA_OPTS= -Xms64m -Xmx512m
  Shift
fi
```

- b) In server.xml file which is under /usr/local/tomcat/conf directory, add in `-maxPostSize="0"`

(as in the code below):

```
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009" enableLookups="false"
  redirectPort="8443" protocol="AJP/1.3" maxPostSize="0"/>
```

JBoss

Set the following in server.xml which is under /jboss-4.0.4.GA/server/default/deploy/jbossweb-tomcat55.sar directory :

- 1) add `-maxPostSize="0"`
- 2) add `maxSavePostSize="- 1"`
- 3) set `connectionTimeout="40000"`

(as in the code below):

```
<Connector port="443" address="{jboss.bind.address}"
  maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
  emptySessionPath="true" connectionTimeout="40000" disableUploadTimeout="true"
  maxPostSize="0" maxSavePostSize="- 1"
  scheme="https" secure="true" clientAuth="true"
  keystoreFile="conf/jks/tomcat70.jks"
  keystorePass="xxxxxxx" sslProtocol = "TLS"
  truststoreFile="conf/jks/tomcat70truststore.jks"
  truststorePass="xxxxxxx"
/>
```