

■ 申請個人數位憑證

➤ 以「Global Trust」為電子郵件用之數位安全憑證服務為例 (<http://www.globaltrust.com.tw/>)

進階安全選項

請選擇您的進階選項：

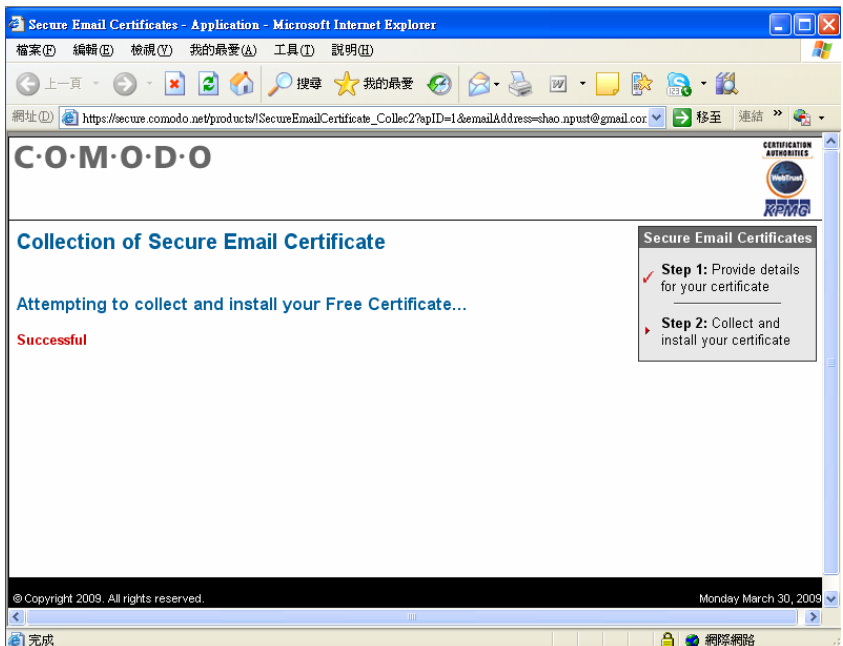
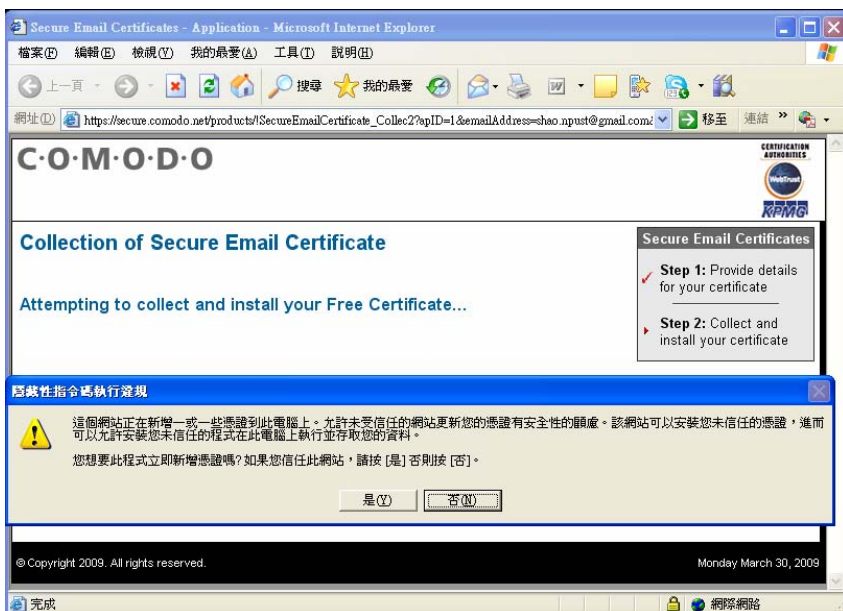
Cryptographic Service Provider: **Microsoft Enhanced Cryptographic Provider v1.0**

Key Size (bits): **1024**

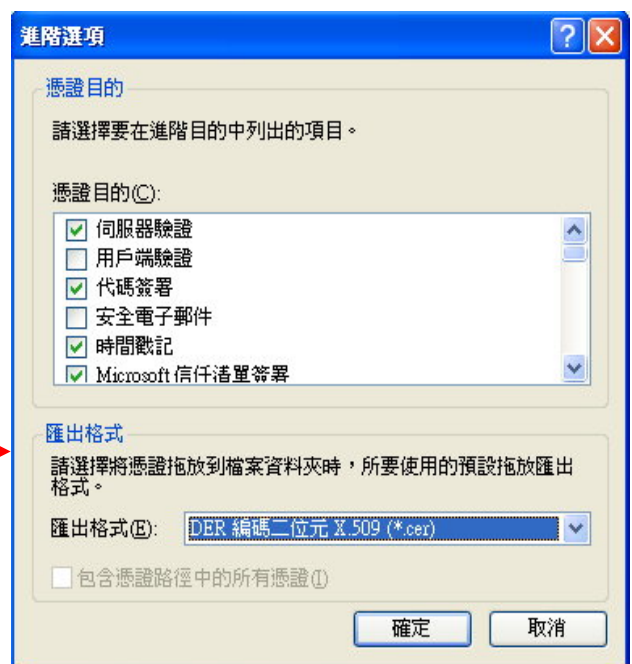
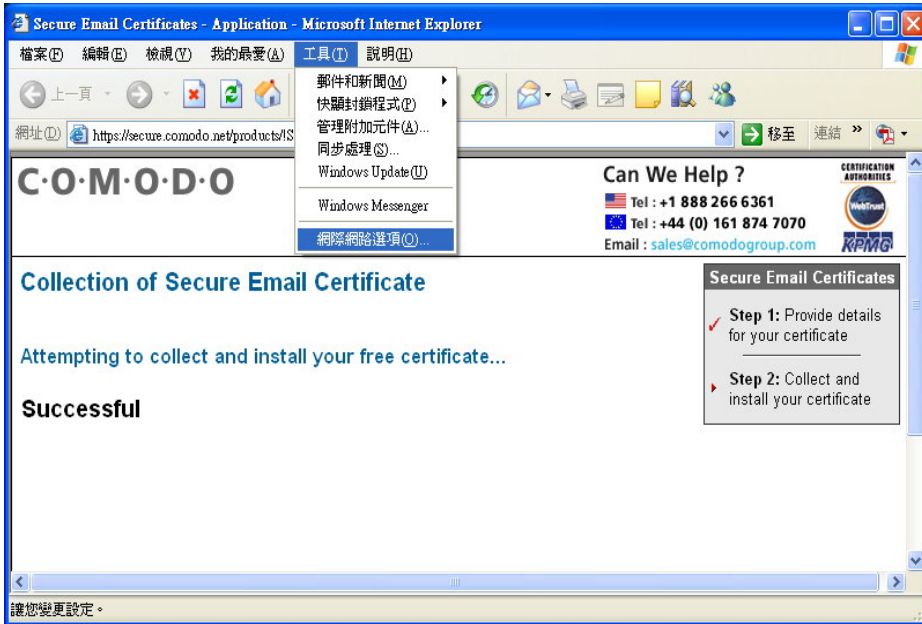
Is Private Key 'User-Protected?': ☒

Is Private Key 'Exportable?': ☒

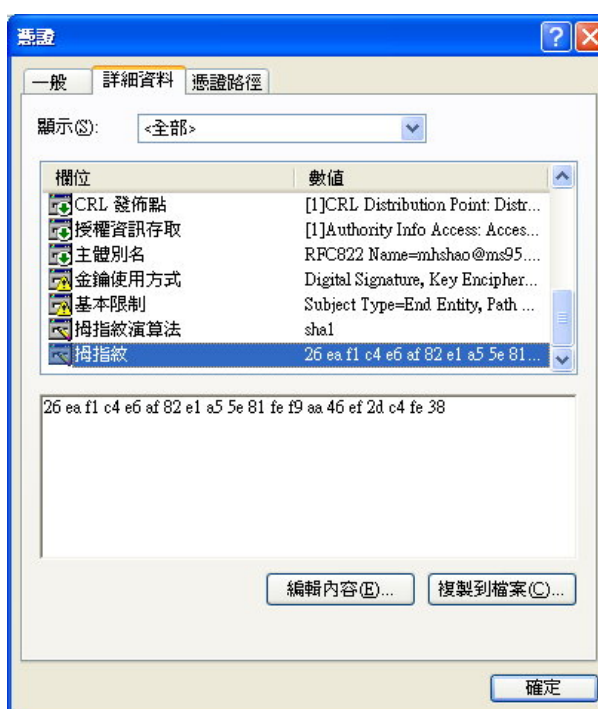
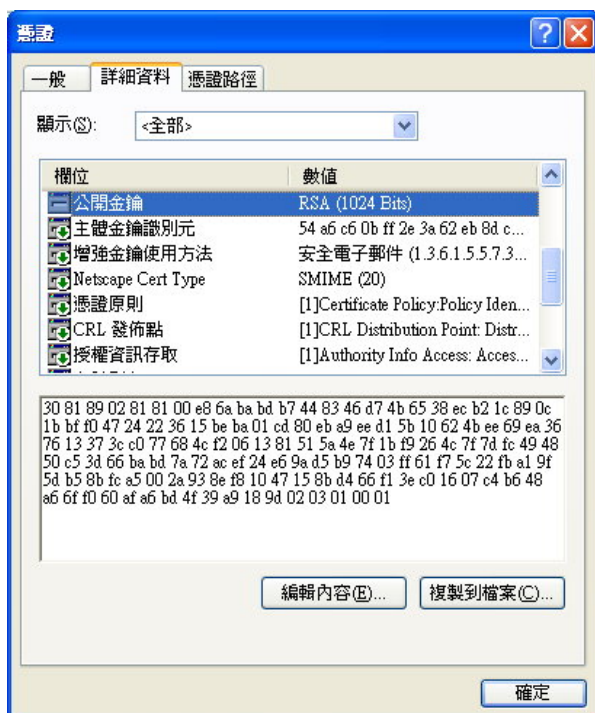
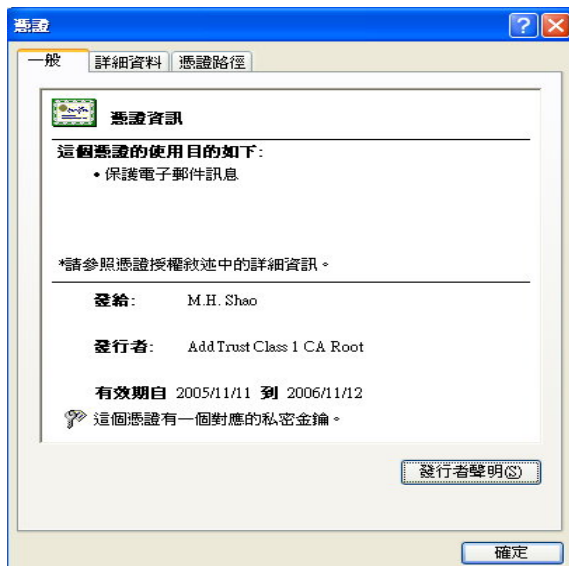
使用預設的安全選項



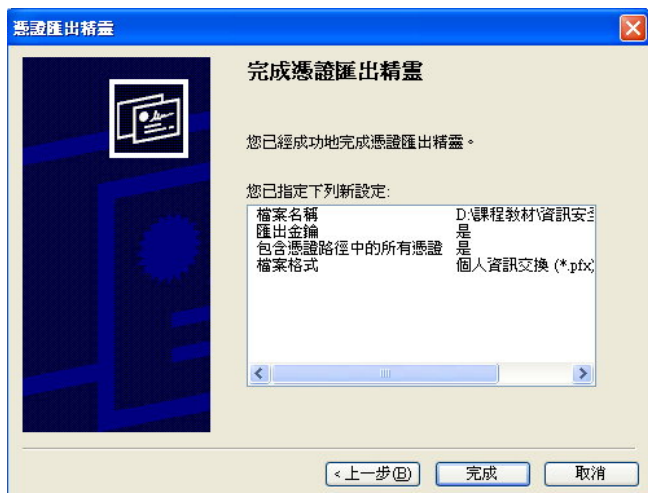
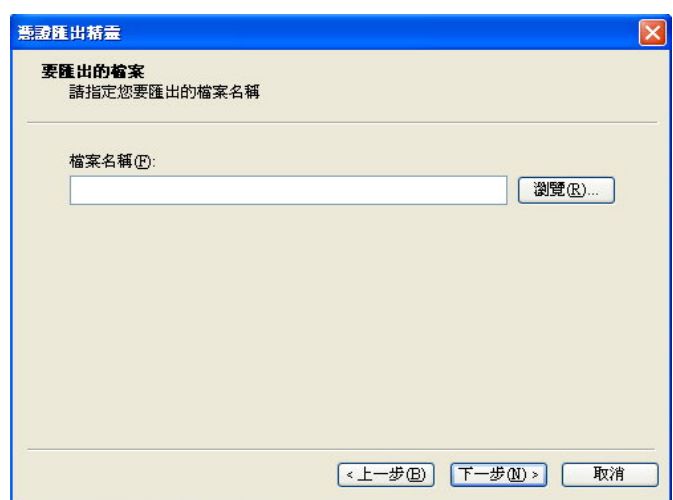
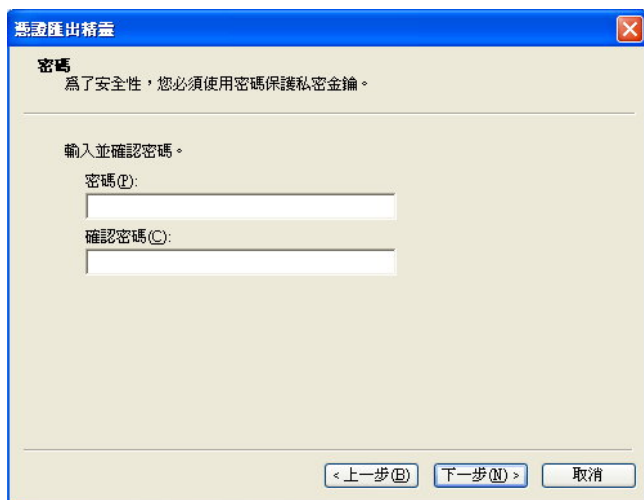
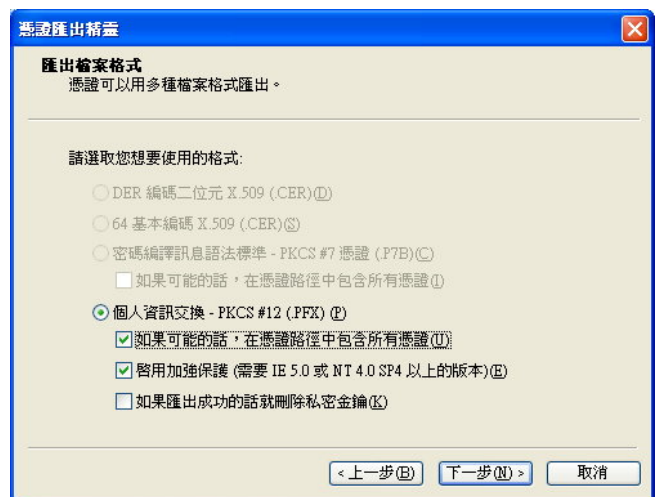
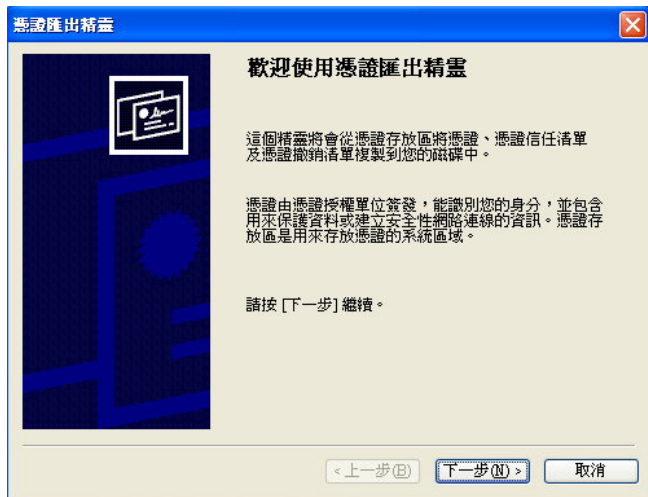
➤ Internet Explorer：功能表【工具】→「網際網路選項」→「內容」標籤



> 檢視

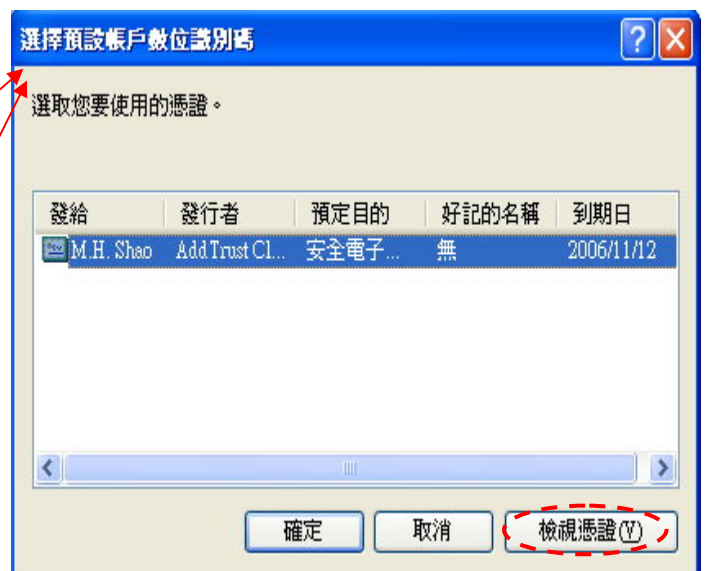
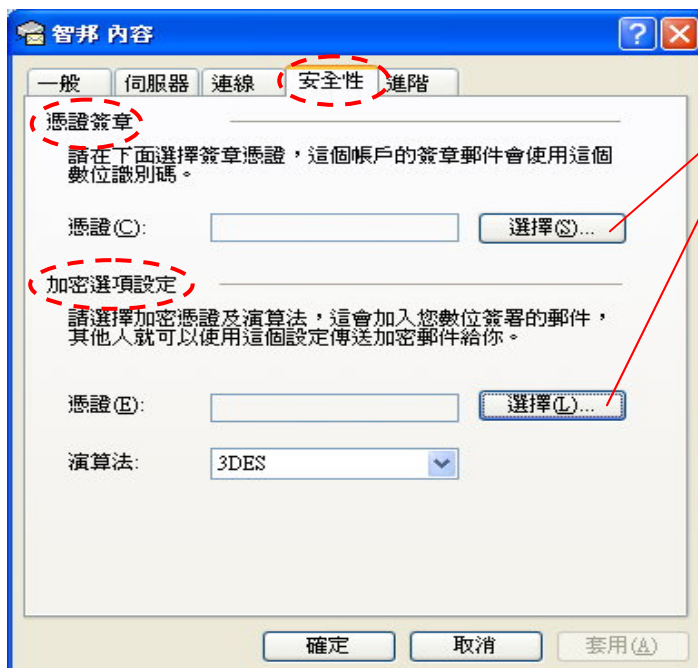
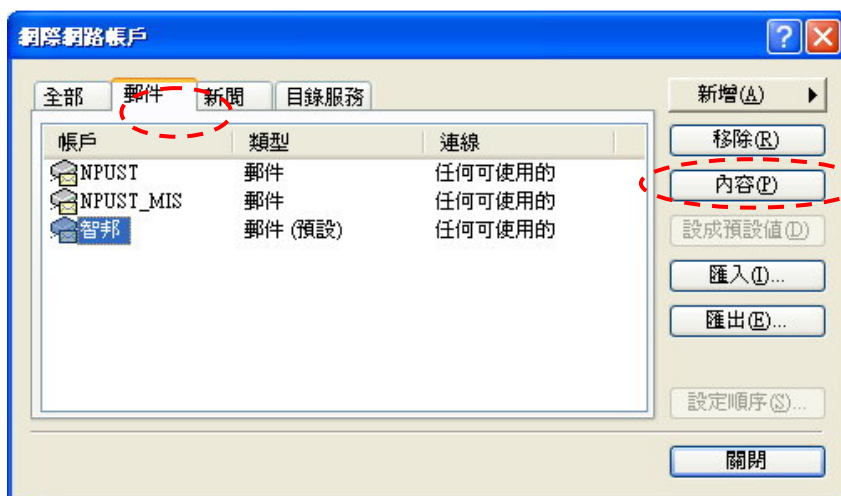
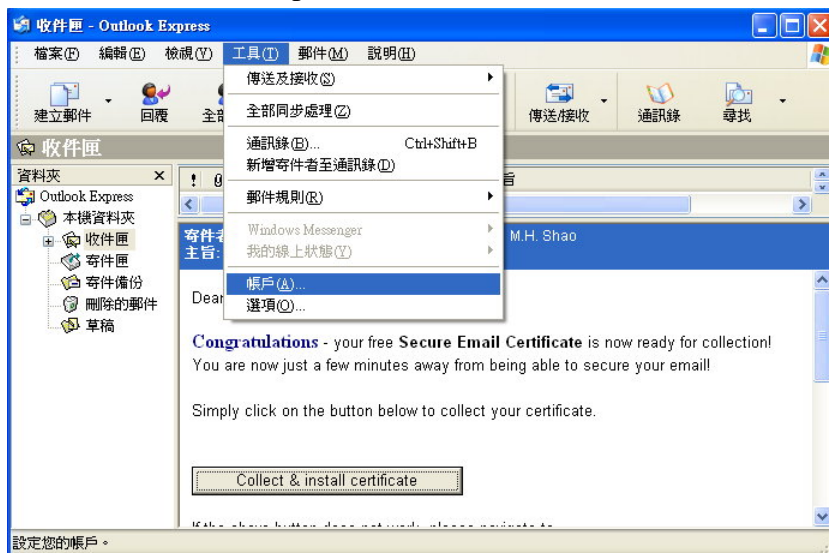


> 匯出



■ 設定「加密用憑證」、「簽章用憑證」

➤ 開啟 Outlook Express → 「工具」→ 「帳戶」



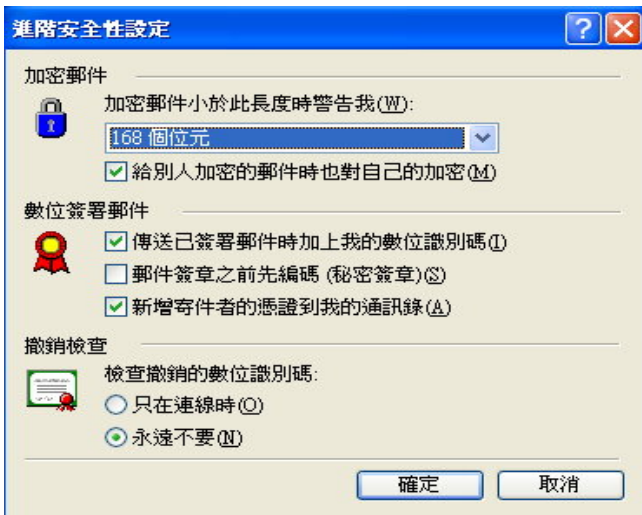
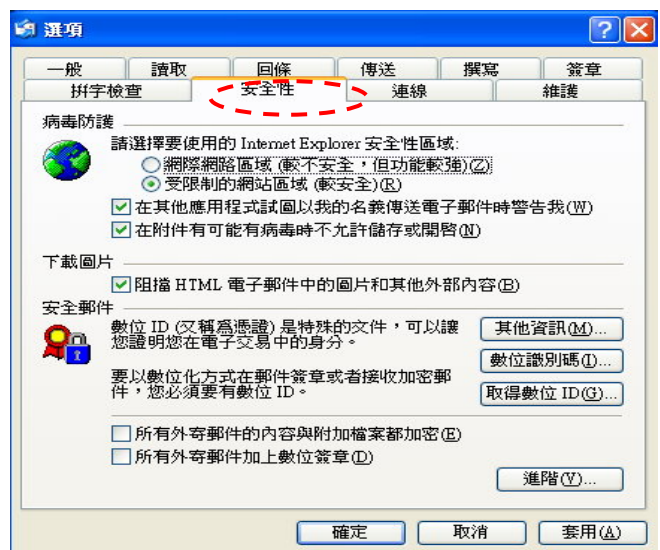
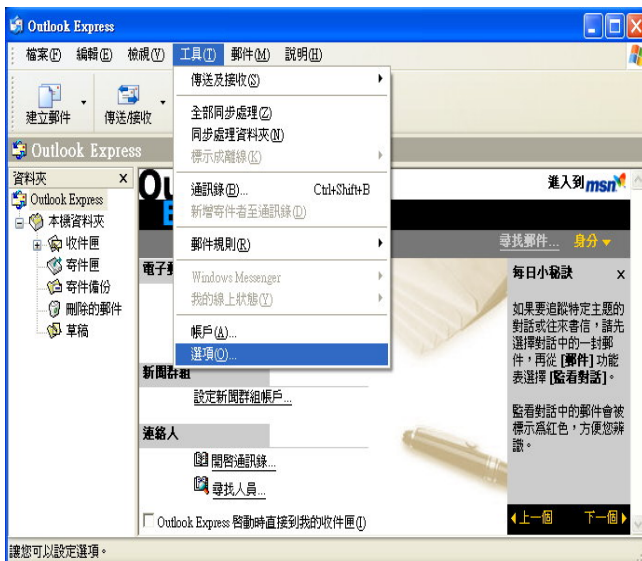


■ 取得他人的數位憑證

1. 自他人傳送具有數位簽名的電子郵件
2. 搜尋簽證中心網站上的數位憑證資料庫
3. 找尋提供數位憑證等內容的 Internet 目錄服務

1. 自他人傳送具有數位簽名的電子郵件

➢ 開啟 Outlook Express → 「工具」→ 「選項」



2. 搜尋簽證中心網站上的數位憑證資料庫 (以 VeriSign 為例)

The first screenshot shows the VeriSign website's search interface. It includes a search bar for email addresses and a section for searching by name. The second screenshot shows the search results for 'SUSY SHEN (Yadd)', displaying the certificate details and a 'Download' button. The third screenshot shows the 'Install Your Digital ID' screen, which displays the certificate information and a button to install the certificate.

Internet Explorer window: Digital ID Services - Microsoft Internet Explorer 是以下列提供 資訊人

網址: <http://www.hitrust.com.tw/landid/verisign/landidindex.html>

首頁 此頁說明

搜尋數位憑證

可以利用姓名、電子郵件地址、序號或憑證者資料搜尋數位憑證。在下列欄位中輸入搜尋資料，然後點選【尋找】鍵便可以查詢到數位憑證。

如果您無法利用姓名或電子郵件地址搜尋到您要的數位憑證，那麼可能數位憑證擁有者在申請時選擇不列名，此時您若要取得該憑證的序號及數位憑證發證者之資料才能搜尋。

請不要輸入特殊字元(wordcard characters)，當您點選【尋找】鍵時，表示您已接受協議之一方合約(Privacy Party Agreement)。

用電子郵件地址搜尋 (建議使用):

輸入電子郵件地址:
(例如: john_doe@verisign.com)

搜尋範圍:

☐ 有效 ☐ 過期 ☒ 全部

☐ 廢止 ☐ 未定

用姓名搜尋:

輸入正確英文姓名:
姓名(包括應附行號在內)必須與數位憑證相符。

搜尋範圍:

☐ 有效 ☐ 過期 ☒ 全部

Internet

Internet Explorer window: Results - Microsoft Internet Explorer 是以下列提供 資訊人

網址: <http://www.hitrust.com.tw/landid/gp-hua/huaola.asp>

數位憑證服務

此頁說明

以下所列之數位憑證符合您搜尋的條件，您可點選某名字以詳細檢視該憑證的相關資訊，或執行其他指令。如：下載、廢止、更新、更換等。

此圖中表列該數位憑證是某擁有者較常用來加密其訊息的憑證。

SUSY SHEN (Yadd)
www@nctu.edu.tw
Digital ID Class 1 - Class Authentication Full Service
Validity period from Dec-10-1999(GMT) to Dec-29-2000(GMT)

重新搜尋

返回

Copyright © 1999, VeriSign, Inc. All Rights Reserved

Internet

Internet Explorer window: Download Certificate - Microsoft Internet Explorer 是以下列提供 資訊人

網址: http://www.hitrust.com.tw/landid/gp-hua/huaola.asp?YHURL_FILE=#2Pbndtcc#2Pquery#2PDownload_Mbndmcc#end=0b10913cd4566a205d565b476f6d5c_https%3Fadd=55&w=1

數位憑證服務

請先選擇所需的格式再下載數位憑證

您已在數位憑證ID格式ID格式ID上使用的數位憑證

下載此數位憑證

當您提出此申請，即表示您同意接受
依此一方合約的規範。

返回

Copyright © 1999, VeriSign, Inc. All Rights Reserved

VeriSign VeriSign Network

Internet

Internet Explorer window: Certificate Download - Microsoft Internet Explorer 是以下列提供 資訊人

網址: <http://www.verisign.com/gp-hua/huaola.asp>

VeriSign

Install Your Digital ID

Your Digital ID

Organization = VeriSign, Inc.
Organizational Unit = www.hitrust.com.tw/RPA, Incorp. by Ref., LIAB.LTD(c)98
Organizational Unit = Authenticated by HITRUST, Inc.
Organizational Unit = Member, VeriSign Trust Network
Organizational Unit = Person Not Validated
Organizational Unit = Digital ID Class 1 - Microsoft Full Service
Common Name = Susy Shen
Email Address = susy@lim.nctu.edu.tw

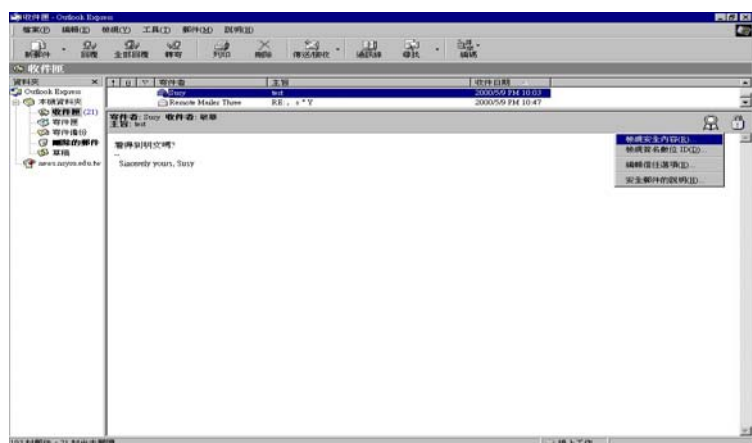
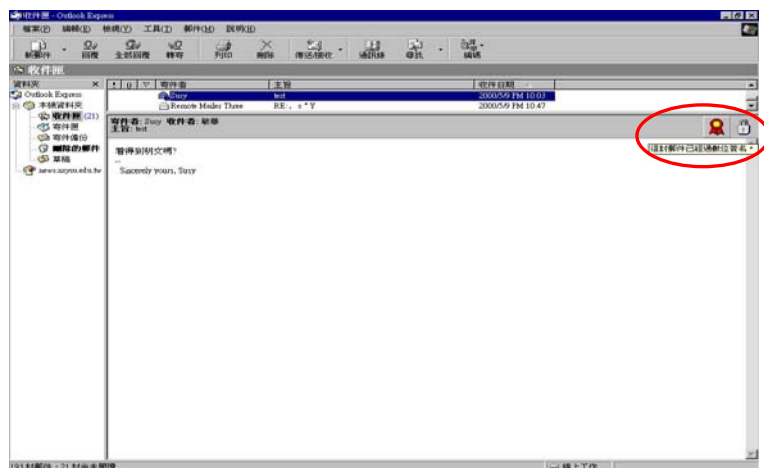
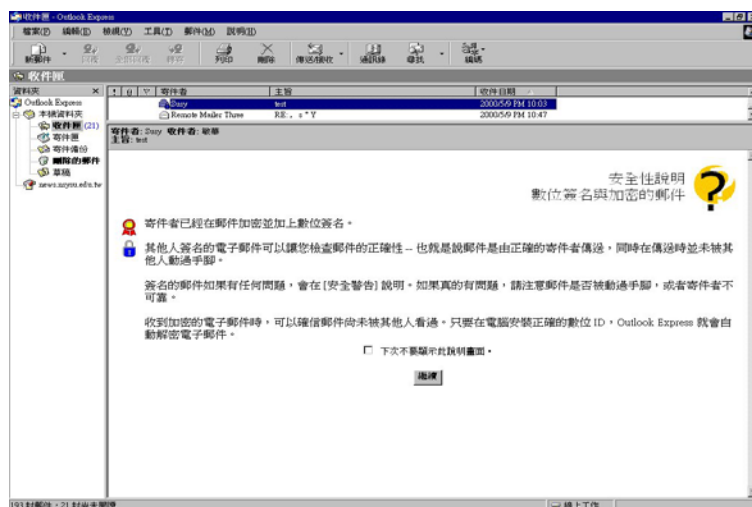
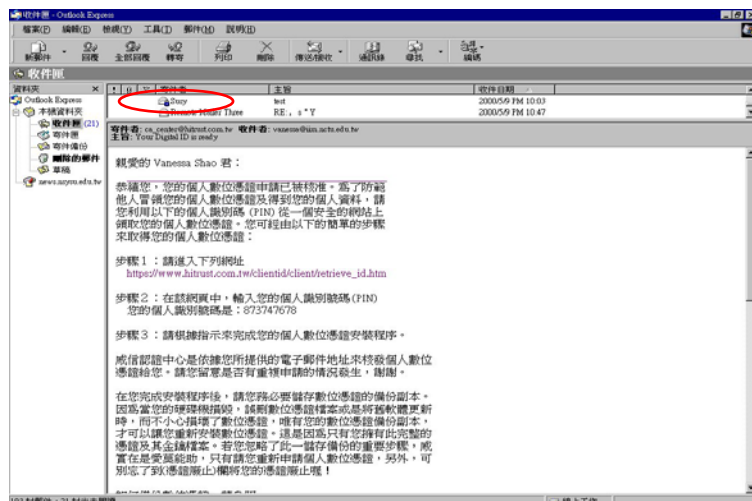
Your Digital ID has been generated successfully.

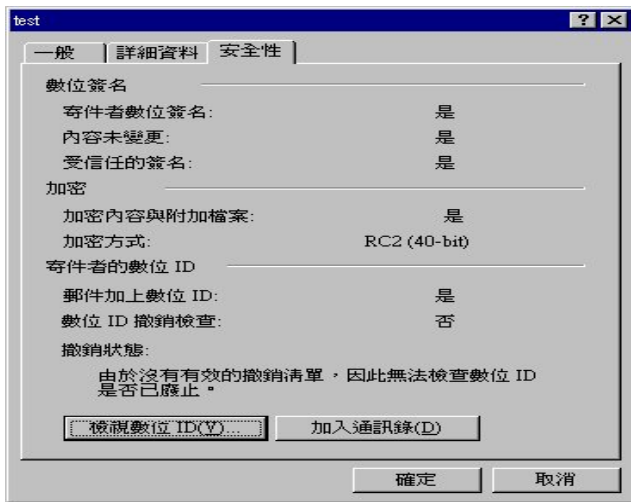
Please select the "Install" button to install.

INSTALL

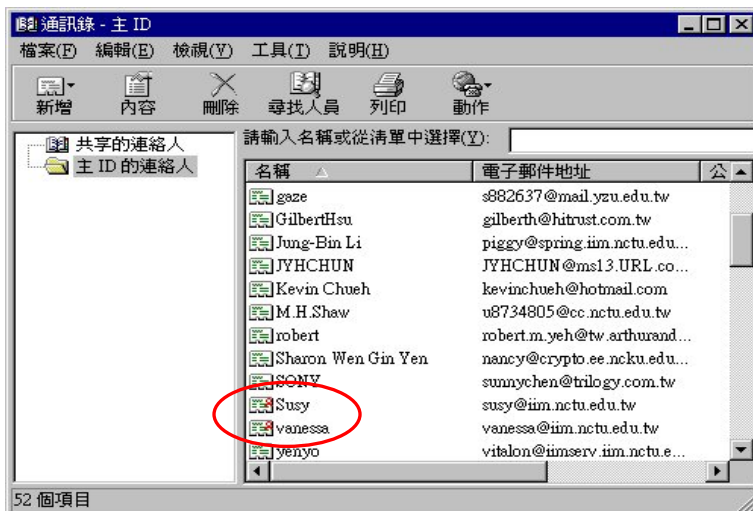
Internet

3. 自他人傳送具有數位簽名的電子郵件

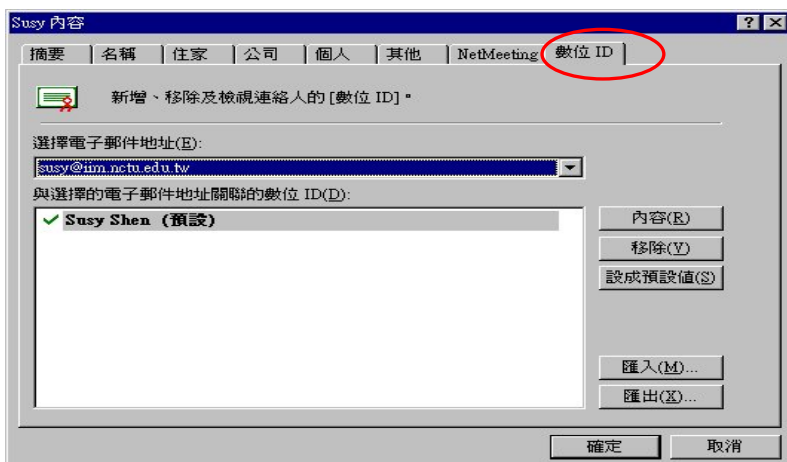




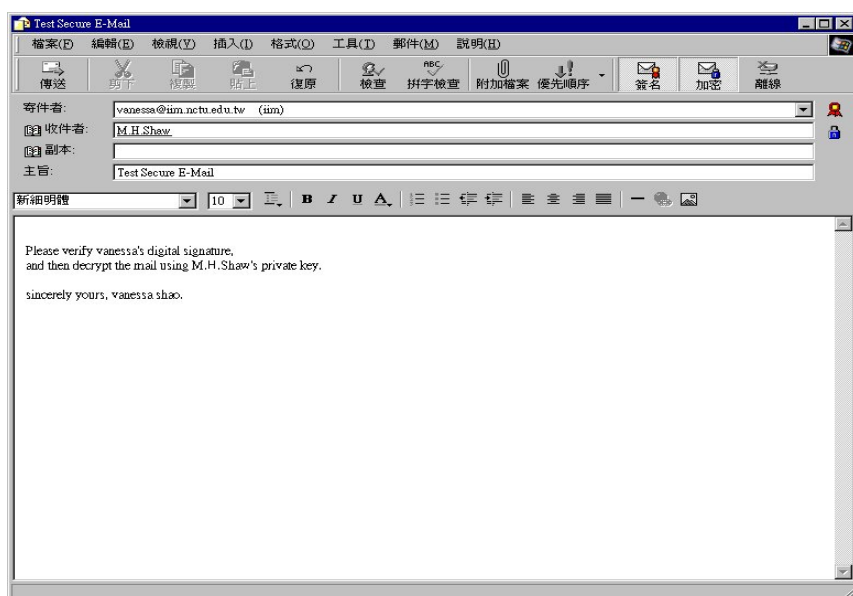
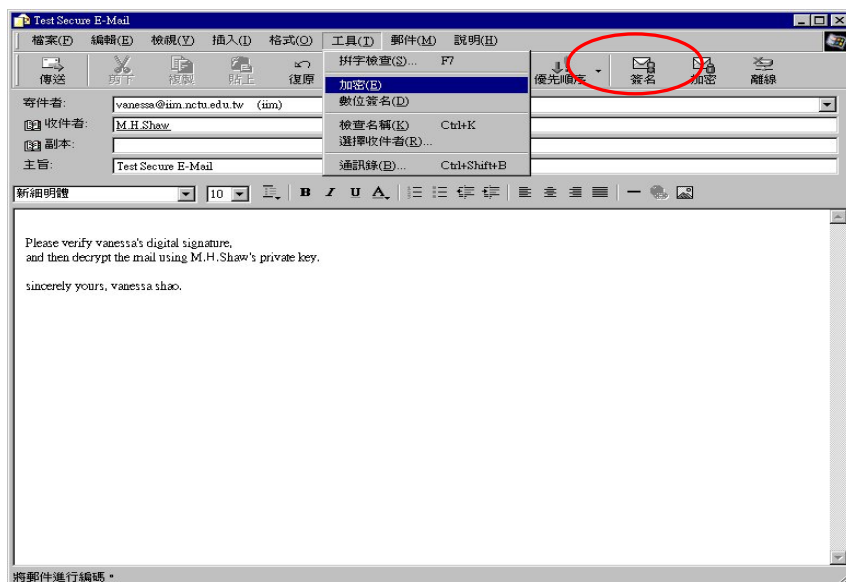
➤ 快捷列「通訊錄」



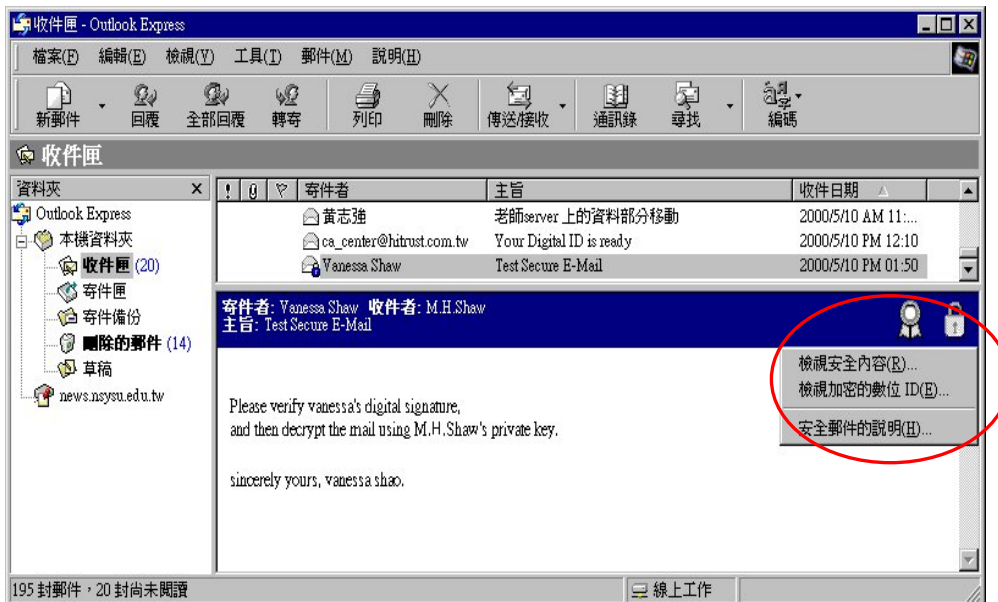
➤ 快捷列「內容」



■ 傳送具有數位簽名/加密的郵件



■ 檢驗具有數位簽名的電子郵件/解密





➤ 安全郵件原始檔

郵件原始檔

Return-Path: <vanessa@iim.serv.iim.nctu.edu.tw>
Received: from newsgate.nctu.edu.tw (newsgate.herc.edu.tw [163.28.64.246])
by cc.nctu.edu.tw (8.10.1/8.10.1) with ESMTP id e4A5obT09062
for <n8734805@cc.nctu.edu.tw>; Wed, 10 May 2000 13:50:37 +0800 (CST)
Received: from iim.serv.iim.nctu.edu.tw (iim.serv.iim.nctu.edu.tw [140.113.73.1])
by newsgate.nctu.edu.tw (8.10.1/8.10.1) with ESMTP id e4A5Yim34452
for <n8734805@cc.nctu.edu.tw>; Wed, 10 May 2000 13:34:44 +0800 (CST)
Received: from essence.essence.iim.nctu.edu.tw [140.113.73.35]
by iim.serv.iim.nctu.edu.tw (8.9.1b+Sun/8.9.1) with SMTP id NAA28829
for <n8734805@cc.nctu.edu.tw>; Wed, 10 May 2000 13:40:25 +0800 (CST)
Message-ID: <002501bfba3f3cd5096e052349718c@iim.nctu.edu.tw>
From: "Vanessa Shaw" <vanessa@iim.serv.iim.nctu.edu.tw>
To: "M.H.Shaw" <n8734805@cc.nctu.edu.tw>
Subject: Test Secure E-Mail
Date: Wed, 10 May 2000 13:21:42 +0800
MIME-Version: 1.0
Content-Type: application/x-pkcs7-mime;
smime-type=enveloped-data;
boundary="-----_NextPart_000_0022_01BFBA82.AE5516B0";
name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="smime.p7m"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2014.211
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2014.211
X-UIDL: 2bnd9#N!!Aeod9L_#"

MIAGCSqGSIb3DQEHA6CAMAIAQAQAggLMQIIBZAIADCBzDCBtzEWMBQGA1UEChMNSGIIUUVIVCwg
SW5JLjEhMBOGA1UECxMwVWVYVWVpNzQ2ZG9VHj1c3QgTmV0d29yazFHEUEGA1UECxM+d3d3LnZlcm1z
aWduLnVybS9yZXZBc2l0b3JlSL1UQSBjbmVucnAuIGJ5IFJlZ4sTElBQ15MVEQ1KGMpOTgxMzAx
BgNVBAUwTKkhpVFJlVU1QgQ2xhc3MgMSBDQSA1EhU2ZGI2aWR1YWwU3Vic2NyaWJlcgIQSFNP18FW
MzTslv2lNK1ezANBgkqhkiG9w0BAQEFAASBgIC4CwNCRAlDouOwLmcyEhCBAxV7CFOnNu5Zk
TFjw02ElbLx3B3U+raFuMCKJrFryUQqUgQ6gef6taElOPIf/R+WJk6FV8Xomc5yZzRnM6tq
u0gaZKL7DumAQm5XOMbrBmv8bVdRfUHEdSQR3SLJ0wg4p5QnN6yQMIIIBZAIADCBzDCBtzEW
MBQGA1UEChMNSGIIUUVIVCwgSW5JLjEhMBOGA1UECxMwVWVYVWVpNzQ2ZG9VHj1c3QgTmV0d29yazFHEUEGA1UECxM+d3d3LnZlcm1z
aWduLnVybS9yZXZBc2l0b3JlSL1UQSBjbmVucnAuIGJ5IFJlZ4sTElBQ15MVEQ1KGMpOTgxMzAx
BgNVBAUwTKkhpVFJlVU1QgQ2xhc3MgMSBDQSA1EhU2ZGI2aWR1YWwU3Vic2NyaWJlcgIQSFNP18FW
MzTslv2lNK1ezANBgkqhkiG9w0BAQEFAASBgBwZAE+zVkmRDAJl
56ebixX8fyV59nS+ArAO7DKFt5Qv84daJyn6hJwbrx28+0mzCb6CO1InsVvJ4kHAc4BfrXWcJh
PTdu8EFQbQqVamNfwkzh5YiOO/hU51StOcr1x9rtaRuPpNlmoPmXNPBtveuGvqQleEu5hNRYs
iMGKMA GCSqGSIb3DQEHA6CMAIAQAQAggLMQIIBZAIADCBzDCBtzEWMBQGA1UEChMNSGIIUUVIVCwg
SW5JLjEhMBOGA1UECxMwVWVYVWVpNzQ2ZG9VHj1c3QgTmV0d29yazFHEUEGA1UECxM+d3d3LnZlcm1z
aWduLnVybS9yZXZBc2l0b3JlSL1UQSBjbmVucnAuIGJ5IFJlZ4sTElBQ15MVEQ1KGMpOTgxMzAx
BgNVBAUwTKkhpVFJlVU1QgQ2xhc3MgMSBDQSA1EhU2ZGI2aWR1YWwU3Vic2NyaWJlcgIQSFNP18FW
MzTslv2lNK1ezANBgkqhkiG9w0BAQEFAASBgBwZAE+zVkmRDAJl

➤ 郵件原始檔

郵件原始檔

From: "Vanessa Shaw" <vanessa@iim.serv.iim.nctu.edu.tw>
To: "M.H.Shaw" <n8734805@cc.nctu.edu.tw>
Subject: Test Secure E-Mail
Date: Wed, 10 May 2000 13:21:42 +0800
Content-Type: multipart/alternative;
boundary="-----_NextPart_000_0022_01BFBA82.AE5516B0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2014.211

This is a multi-part message in MIME format.

-----_NextPart_000_0022_01BFBA82.AE5516B0
Content-Type: text/plain;
charset="big5"
Content-Transfer-Encoding: quoted-printable

Please verify vanessa's digital signature,
and then decrypt the mail using M.H.Shaw's private key.

sincerely yours, vanessa shao.

-----_NextPart_000_0022_01BFBA82.AE5516B0
Content-Type: text/html;
charset="big5"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content=3D"text/html; charset=3Dbig5" http-equiv=3DContent-Type>
<META content=3D"MSHTML 5.00.2014.210" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV> </DIV>
<DIV>Please verify vanessa's digital =
signature.</DIV>
<DIV>and then decrypt the mail using M.H.Shaw's private=20
key.</DIV>
<DIV> </DIV>
<DIV>sincerely yours, vanessa =
shao.</DIV></BODY></HTML>

-----_NextPart_000_0022_01BFBA82.AE5516B0--