The Secure Mail Guide

Version 1.0

Introduction

This document will help users to sign personal mail contents. The technique is based on the user certificate issued by Academia Sinica Grid Computing Certification Authority (ASGCCA). All certificates comply with "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework " [RFC3647], "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC3280] and Grid Certificate Profile. Users could follow the document to write mails by secure communication and receivers could trust the Certification Authority's certificate in the signed mail. This document provides two methods for users to sign the secure mails. There are Microsoft Outlook and Outlook Express.

Microsoft Outlook

1.1 Get personal certificate

Users must get personal certificate first. If you do not have any certificate, please contact ASGCCA.
ASGCCA website http://ca.grid.sinica.edu.tw/index.html
ASGCCA contact asgcca@grid.sinica.edu.tw

1.2 SubjectAlternativeName

Please check the SubjectAlternativeName of the user certificate. When users send secure mails, its certificate must have an rfc822EmailAddress in the SubjectAlternativeName X.509v3 extension. Users could execute the following command to check this issue. (See Figure1) If there is no SubjectAlternativeName on your certificate, please contact ASGCCA manager.

#openssl x509 –in usercert.pem –noout –text | less

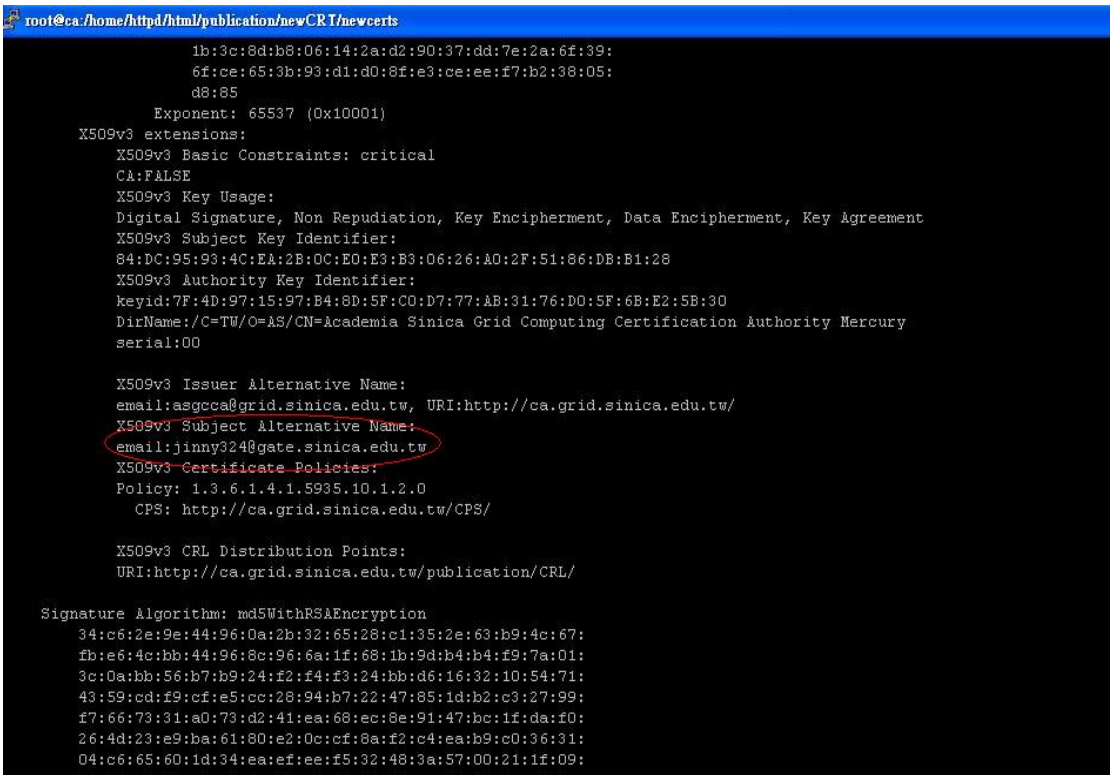


Figure1.

1.3 Import the certificate into the browser

Please make sure the user certificate is already imported into the Internet Explorer. (See Figure 2)

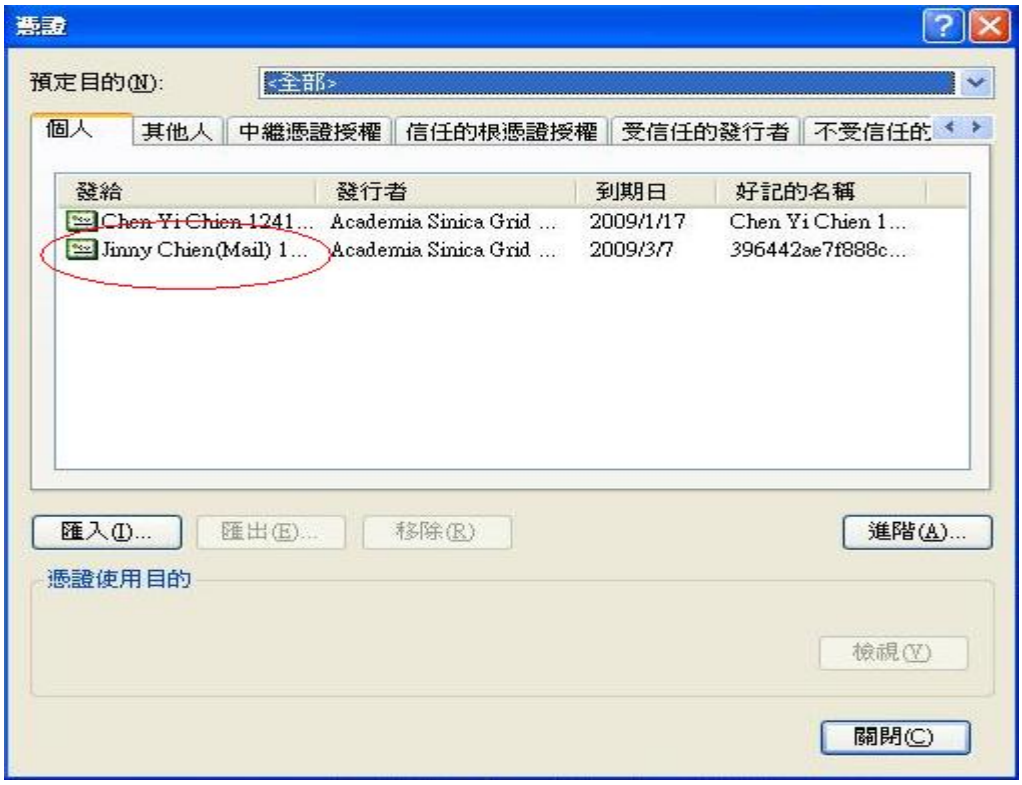


Figure 2

1.4 Create an email account

You must have an email account and it complied with the SubjectAlternativeName of personal certificate. (See figure 3)

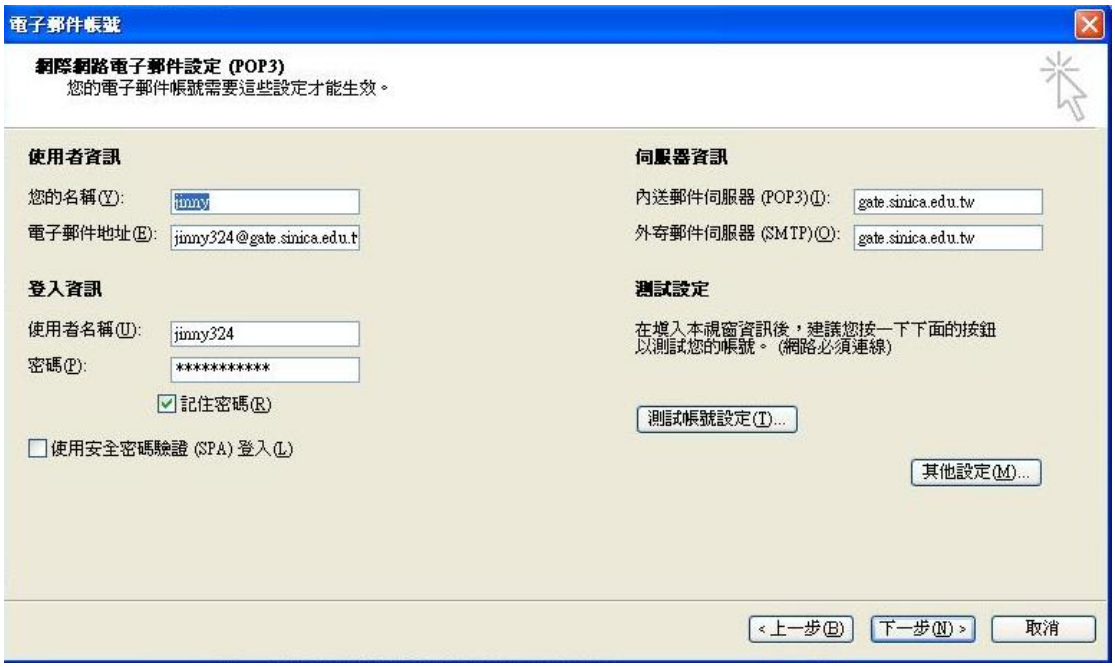


Figure 3

1.5 Export the certificate

Before users set the client mail, they must export the certificates to the PKS12 files from the browser. The PKS12 files included private keys must save in the secure place. The method could be found http://ca.grid.sinica.edu.tw/certificate/request/certificate_management.html

1.6 The configuration of Microsoft Outlook

User must follow the following steps to import the certificate into the Microsoft Outlook. Open Microsoft Outlook -> Tool -> Option -> Security -> Import / Export and select the personal PKS12 file -> Complete the import. (See figure 4 and figure 5)


選項
偏好
郵件設定
郵件格式
拼字檢查
安全性
其他
加密的電子郵件
外寄郵件的內容及附件加密(E)
在外寄郵件加入數位簽章(D)
當傳送簽名郵件時傳送純文字簽名郵件(T)
爲所有 S/MIME 簽名郵件索取 S/MIME 回條(R)
預設設定(F):
jinny
設定(S)...
安全性區域
安全性區域供您自訂是否可在 HTML 郵件中執行指令碼和主動式內容。
區域
限制的網站
區域設定值(N)...
下載圖片
變更自動下載設定(C)...
數位 ID (憑證)
數位 ID 或憑證是在電子交易中供您證明身份的文件。
匯入/匯出(I)...
取得數位 ID(G)...
確定
取消
套用(A)

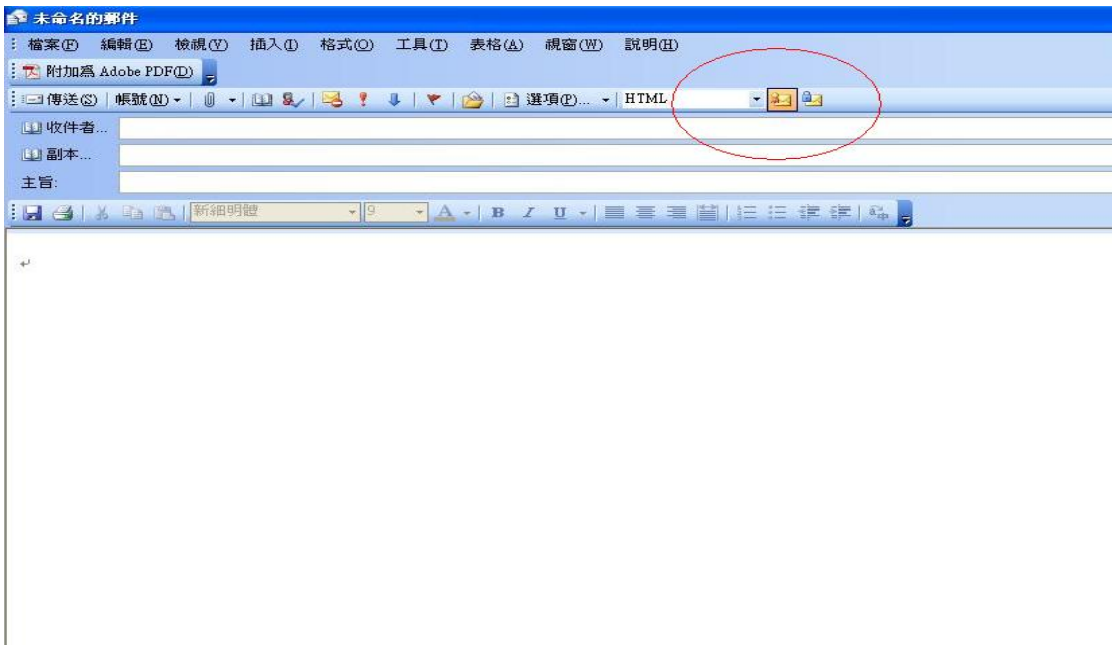
Figure 4


匯入/匯出數位 ID
從檔案匯入現有的數位 ID (I)
從該檔案匯入數位 ID 到您的電腦。您必須使用與匯出該憑證到這個檔案時相同的密碼。
匯入檔案(F):
瀏覽(B)...
密碼(P):
數位 ID 名稱(D):
將數位 ID 匯出至檔案(E)
匯出該數位 ID 資訊到一個檔案中。鍵入密碼以協助保護該資訊。
數位 ID:
選取(S)...
檔案名稱(F):
瀏覽(W)...
密碼(R):
確認(C):
Microsoft Internet Explorer 4.0 相容 (低-安全性)(M)
從系統刪除數位 ID(L)
確定
取消

Figure 5

1.7 Sign the mail

Create a mail and select the digital signature.



Outlook Express

2.1 Get personal certificate

Users must get personal certificate first. If you do not have any certificate, please contact ASGCCA.
ASGCCA website http://ca.grid.sinica.edu.tw/index.html
ASGCCA contact asgcca@grid.sinica.edu.tw

2.2 SubjectAlternativeName

Please check the SubjectAlternativeName of the user certificate. When users send secure mails, its certificate must have an rfc822EmailAddress in the SubjectAlternativeName X.509v3 extension. Users could execute the following command to check this issue. (See Figure1) If there is no SubjectAlternativeName on your certificate, please contact ASGCCA manager.

#openssl x509 –in usercert.pem –noout –text | less

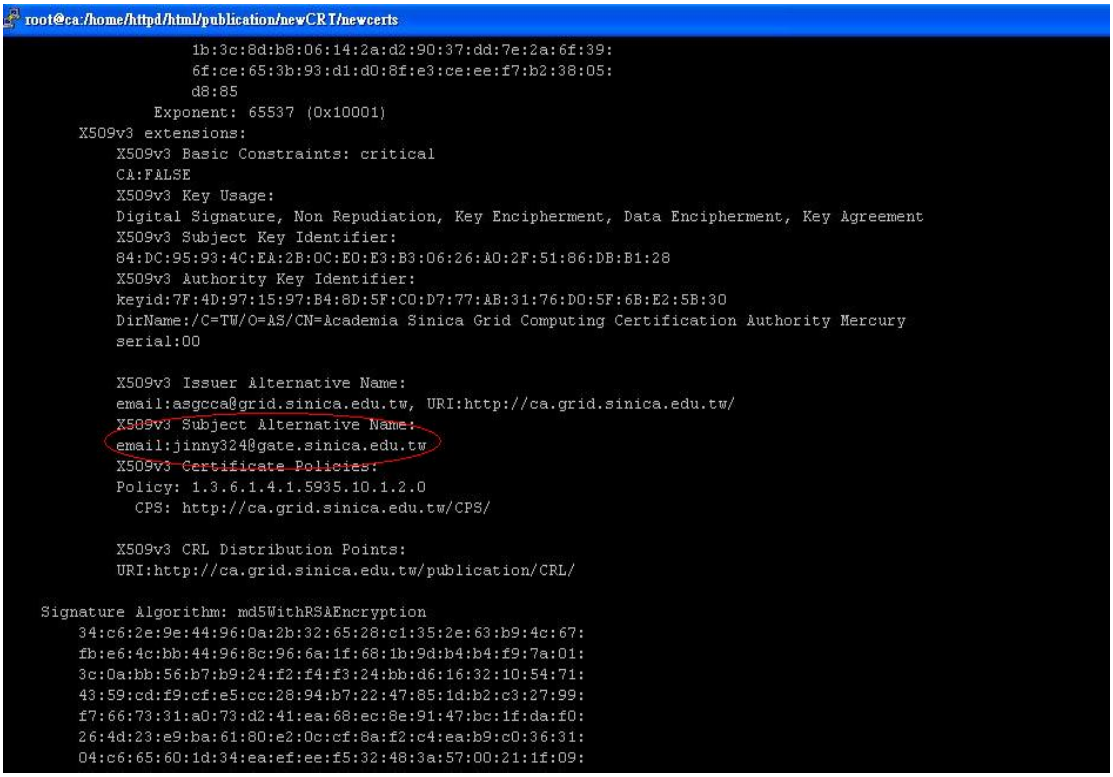


Figure1.

2.3 Import the certificate into the browser

Please make sure the user certificate is already imported into the Internet Explorer. (See Figure 2)

Figure 2

2.4 Create an email account

You must have an email account and it complied with the SubjectAlternativeName of personal certificate. User must send a secure mail with the specific mail address and receiver will trust the user certificate signed by the production CA. The detailed process is Open Outlook Express -> Tool -> Account -> Mail -> Create a new account. (see Figure 3)

Figure 3

2.5 Import the certificate into specific accounts

Please make sure the personal mail account is already existed first, modify the user account and import the user certificate. You could follow the procedure to execute it. The detailed procedure is open Outlook Express -> Tool -> Account (See Figure 4) -> Select mail field -> Select the account that you want to send secure mail (See Figure 5) -> Contents -> Security (See Figure 6) -> Please follow the instructions to click your certificate (See Figure 7) -> Complete the setting and try to send a secure mail (See Figure 8 and 9).

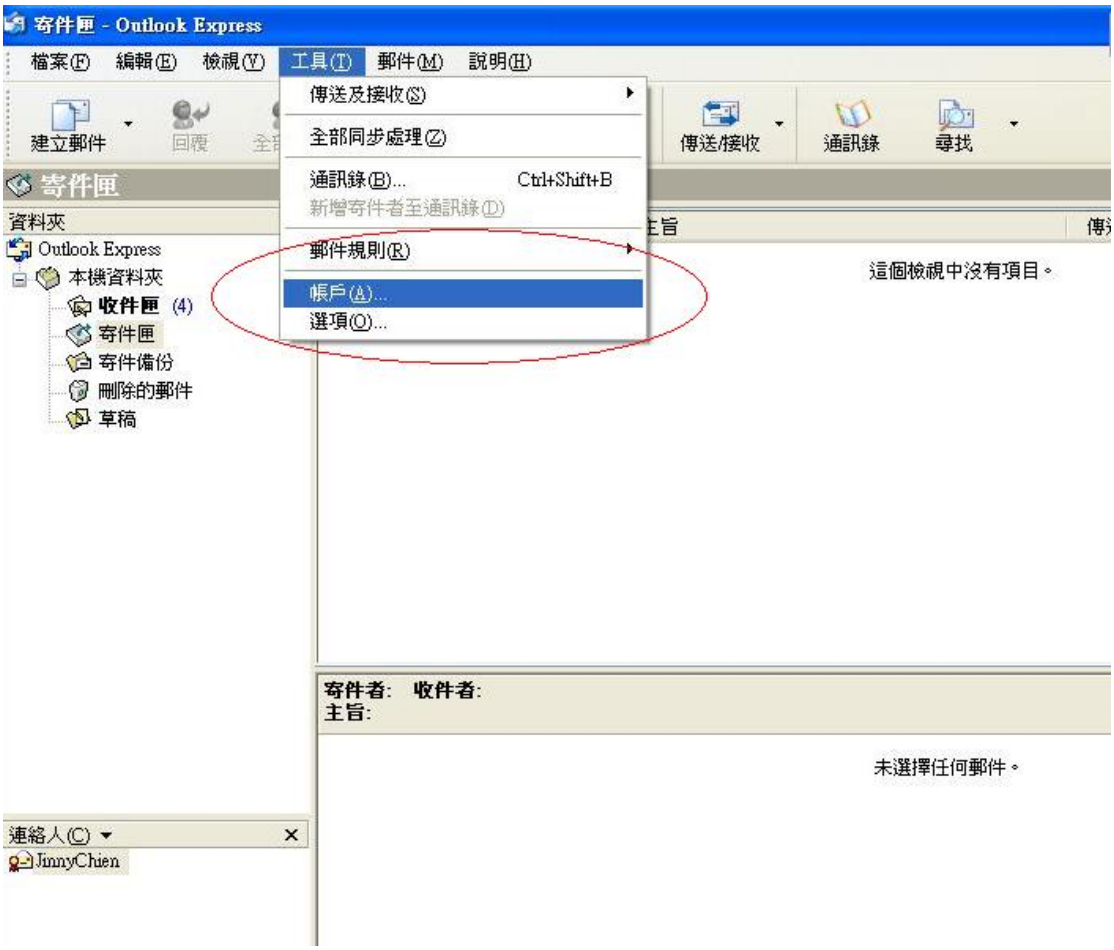


Figure 4

Figure 5

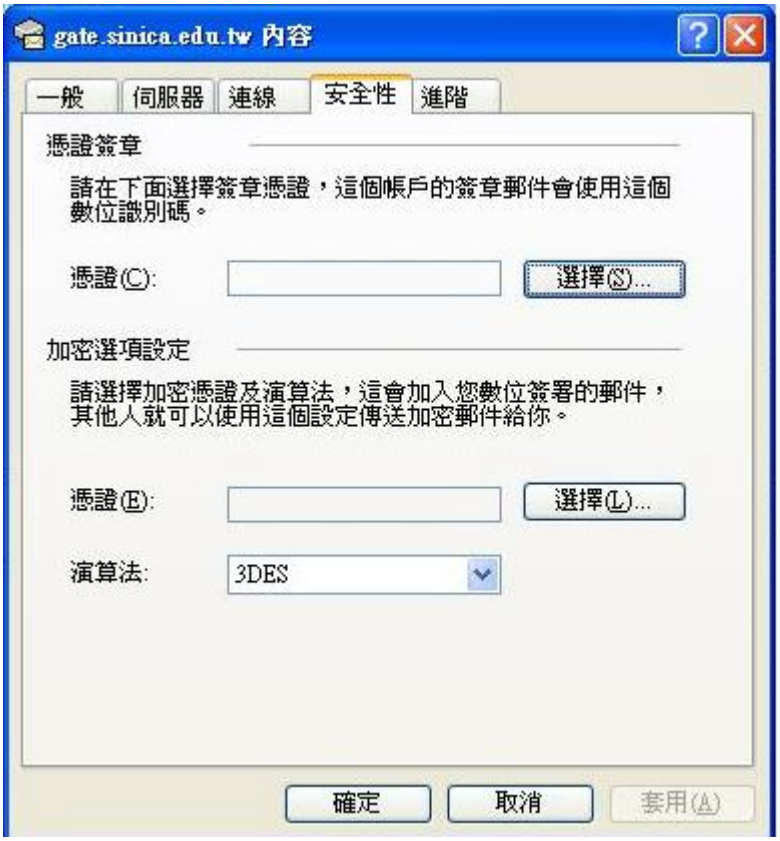


Figure 6

Figure 7

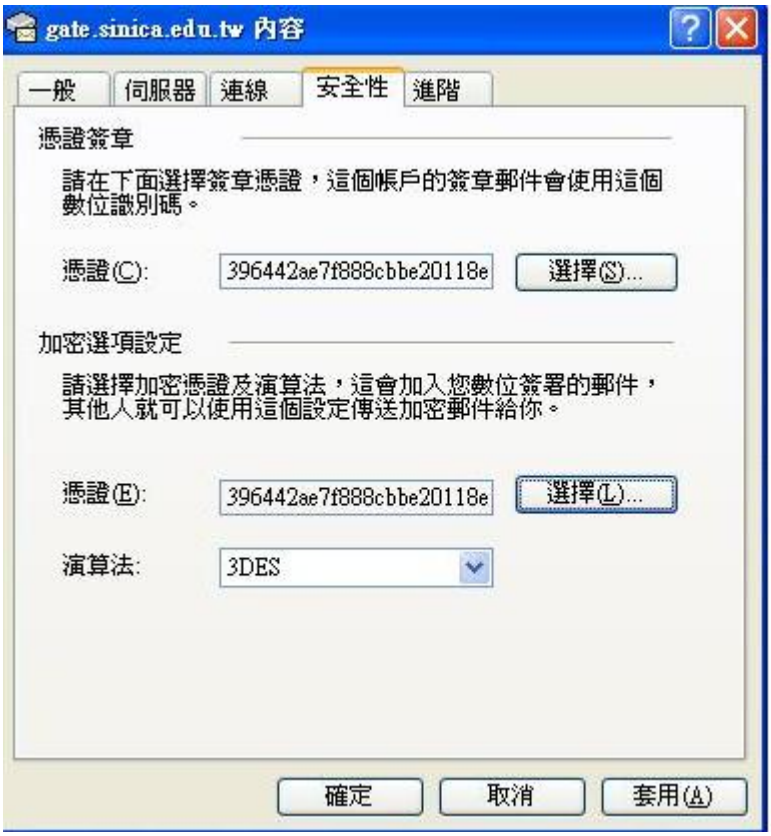


Figure 8

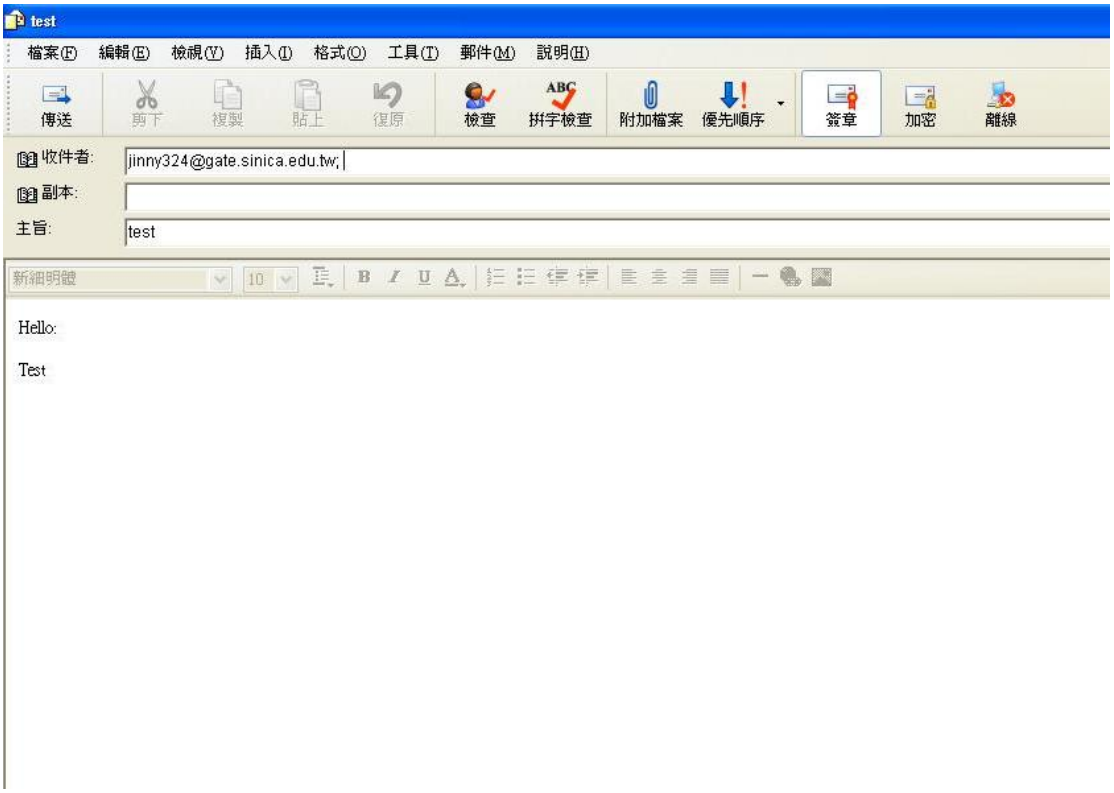


Figure 9