

The Secure Mail Guide

Version 1.0

Introduction	3
Microsoft Outlook	3
1.1 Get personal certificate	3
1.2 SubjectAlternativeName	3
1.3 Import the certificate into the browser	4
1.4 Create an email account.....	5
1.5 Export the certificate.....	6
1.6 The configuration of Microsoft Outlook.....	6
1.7 Sign the mail.....	8
Outlook Express	8
2.1 Get personal certificate	8
2.2 SubjectAlternativeName	8
2.3 Import the certificate into the browser	9
2.4 Create an email account.....	10
2.5 Import the certificate into specific accounts.....	11

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
```

```
root@ca:/home/httpd/html/publication/newCRT/newcerts
1b:3c:8d:b8:06:14:2a:d2:90:37:dd:7e:2a:6f:99:
6f:ce:65:3b:93:d1:d0:8f:e3:ce:ee:f7:b2:38:05:
d8:85
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Key Usage:
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
X509v3 Subject Key Identifier:
84:DC:95:93:4C:EA:2B:0C:E0:E3:B3:06:26:AD:2F:51:86:DB:B1:28
X509v3 Authority Key Identifier:
keyid:7F:4D:97:15:97:B4:8D:5F:CO:D7:77:AB:31:76:D0:5F:6B:E2:5B:30
DirName:/C=TW/O=AS/CN=Academia Sinica Grid Computing Certification Authority Mercury
serial:00

X509v3 Issuer Alternative Name:
email:asgcca@grid.sinica.edu.tw, URI:http://ca.grid.sinica.edu.tw/
X509v3 Subject Alternative Name:
email:jinny324@gate.sinica.edu.tw
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.5935.10.1.2.0
CPS: http://ca.grid.sinica.edu.tw/CPS/

X509v3 CRL Distribution Points:
URI:http://ca.grid.sinica.edu.tw/publication/CRL/

Signature Algorithm: md5WithRSAAEncryption
34:c6:2e:9e:44:96:0a:2b:32:65:28:c1:35:2e:63:b9:4c:67:
fb:e6:4c:bb:44:96:8c:96:6a:1f:68:1b:9d:b4:b4:f9:7a:01:
3c:0a:bb:56:b7:b9:24:f2:f4:f3:24:bb:d6:16:32:10:54:71:
43:59:cd:f9:cf:e5:cc:28:94:b7:22:47:85:1d:b2:c3:27:99:
f7:66:73:31:a0:73:d2:41:ea:68:ec:8e:91:47:bc:1f:da:f0:
26:4d:23:e9:ba:61:80:e2:0c:cf:8a:f2:c4:ea:b9:c0:36:31:
04:c6:65:60:1d:34:ea:ef:ee:f5:32:48:3a:57:00:21:1f:09:
```

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)

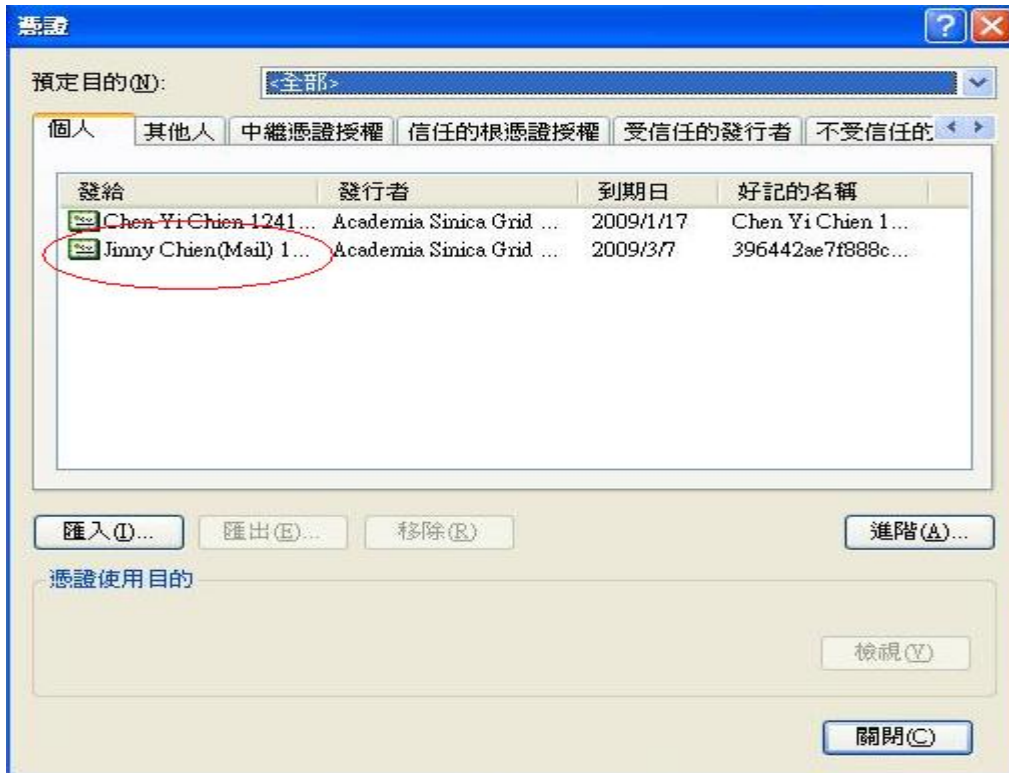
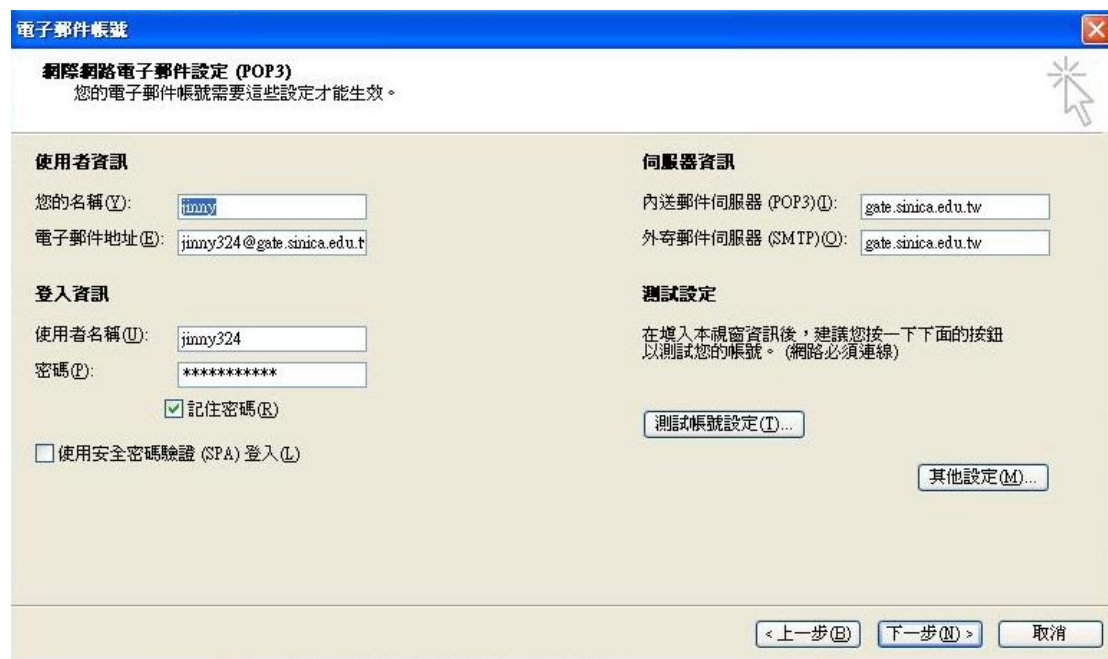


Figure 2

1.4 Create an email account

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



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)



Figure 4

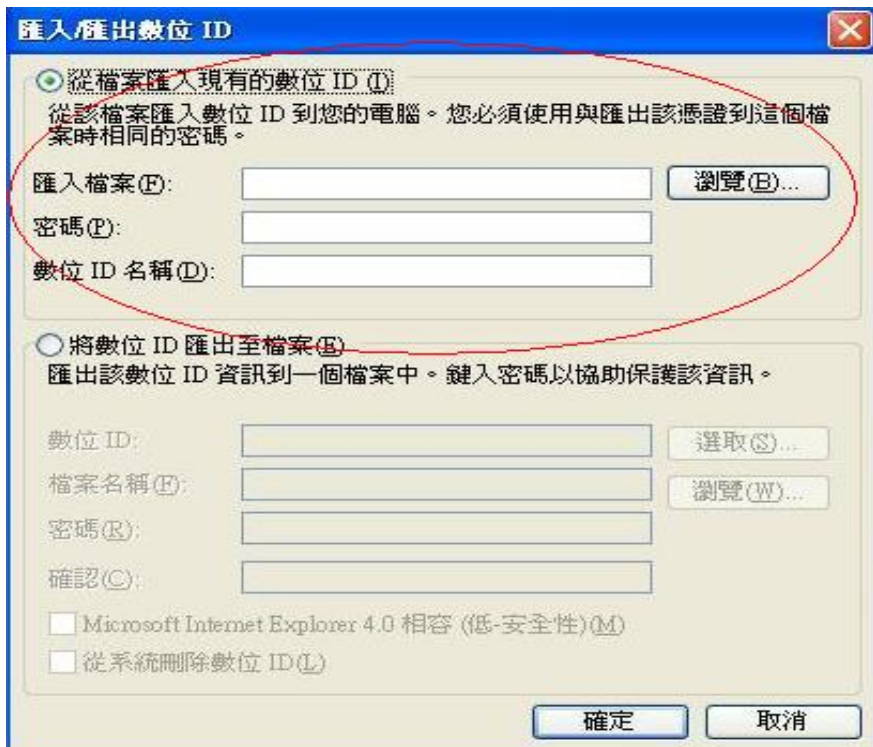
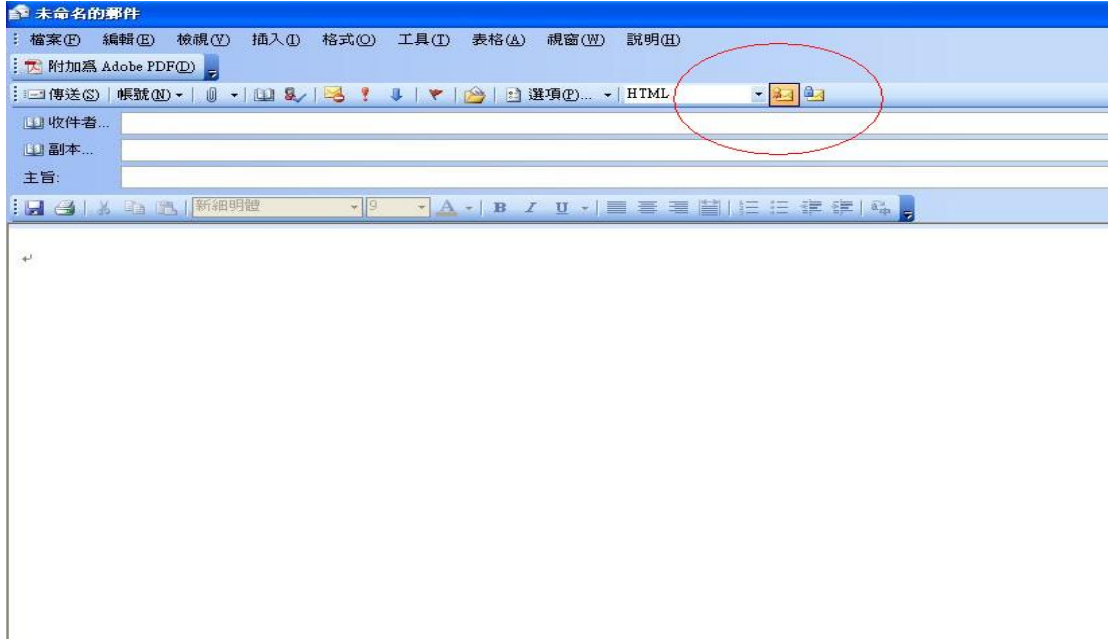


Figure 5

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.

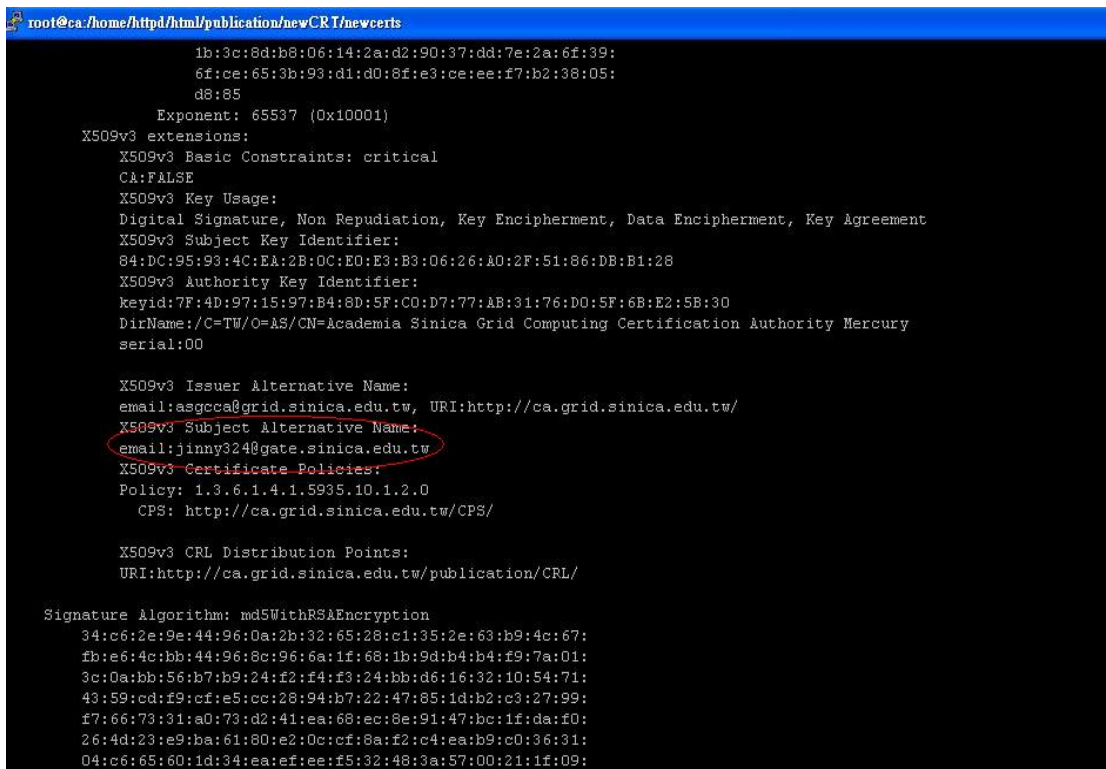
ASGCCA website <http://ca.grid.sinica.edu.tw/index.html>

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
```



```
root@ca:/home/httpd/html/publication/newCRT/newcerts
1b:3c:8d:b8:06:14:2a:d2:90:37:dd:7e:2a:6f:99:
6f:ce:65:3b:93:d1:d0:8f:e3:ce:ee:f7:b2:38:05:
d8:85
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Key Usage:
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
X509v3 Subject Key Identifier:
84:DC:95:93:4C:EA:2B:0C:E0:E3:B3:06:26:AD:2F:51:86:DB:B1:28
X509v3 Authority Key Identifier:
keyid:7F:4D:97:15:97:B4:8D:5F:CD:D7:77:AB:31:76:D0:5F:6B:E2:5B:30
DirName:/C=TW/O=AS/CN=Academia Sinica Grid Computing Certification Authority Mercury
serial:00

X509v3 Issuer Alternative Name:
email:asgcca@grid.sinica.edu.tw, URI:http://ca.grid.sinica.edu.tw/
X509v3 Subject Alternative Name:
email:jimmy324@gate.sinica.edu.tw
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.5935.10.1.2.0
CPS: http://ca.grid.sinica.edu.tw/CPS/

X509v3 CRL Distribution Points:
URI:http://ca.grid.sinica.edu.tw/publication/CRL/

Signature Algorithm: md5WithRSAAEncryption
34:c6:2e:9e:44:96:0a:2b:32:65:28:c1:35:2e:63:b9:4c:67:
fb:e6:4c:bb:44:96:8c:96:6a:1f:68:1b:9d:b4:b4:f9:7a:01:
3c:0a:bb:56:b7:b9:24:f2:f4:f3:24:bb:d6:16:32:10:54:71:
43:59:cd:f9:cf:e5:cc:28:94:b7:22:47:85:1d:b2:c3:27:99:
f7:66:73:31:a0:73:d2:41:ea:68:ec:8e:91:47:bc:1f:da:f0:
26:4d:23:e9:ba:61:80:e2:0c:cf:8a:f2:c4:ea:b9:c0:36:31:
04:c6:65:60:1d:34:ea:ef:ee:f5:32:48:3a:57:00:21:1f:09:
```

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).

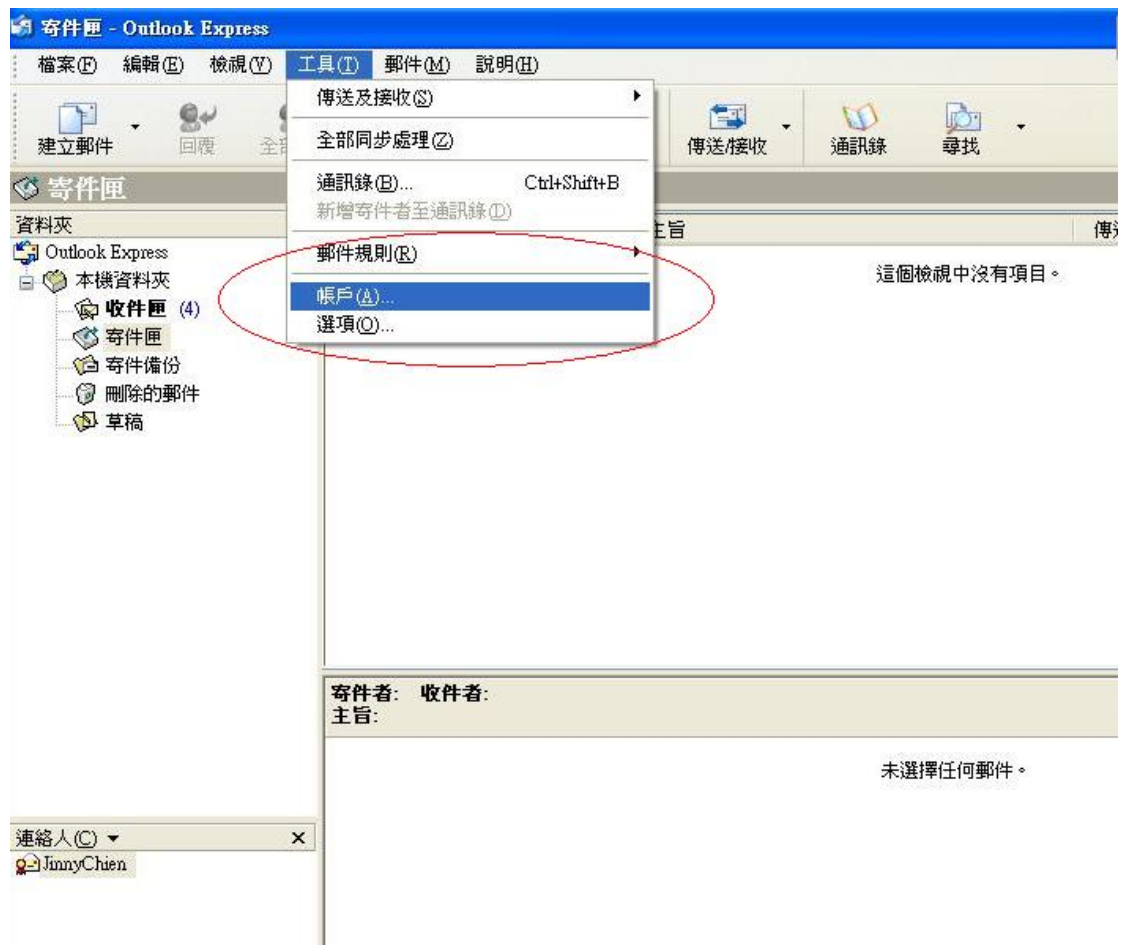


Figure 4



Figure 5

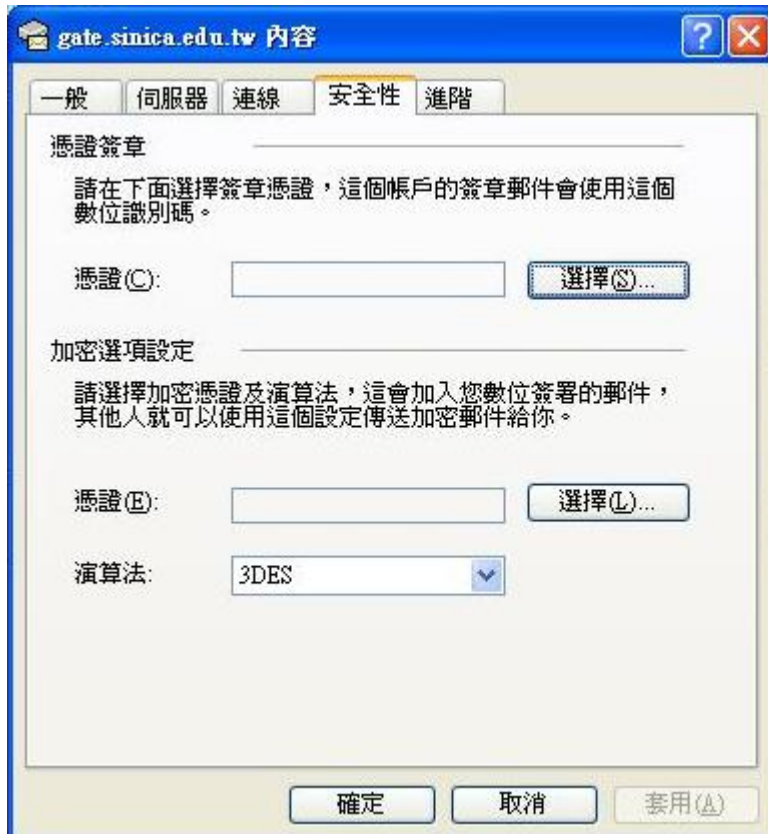


Figure 6



Figure 7



Figure 8

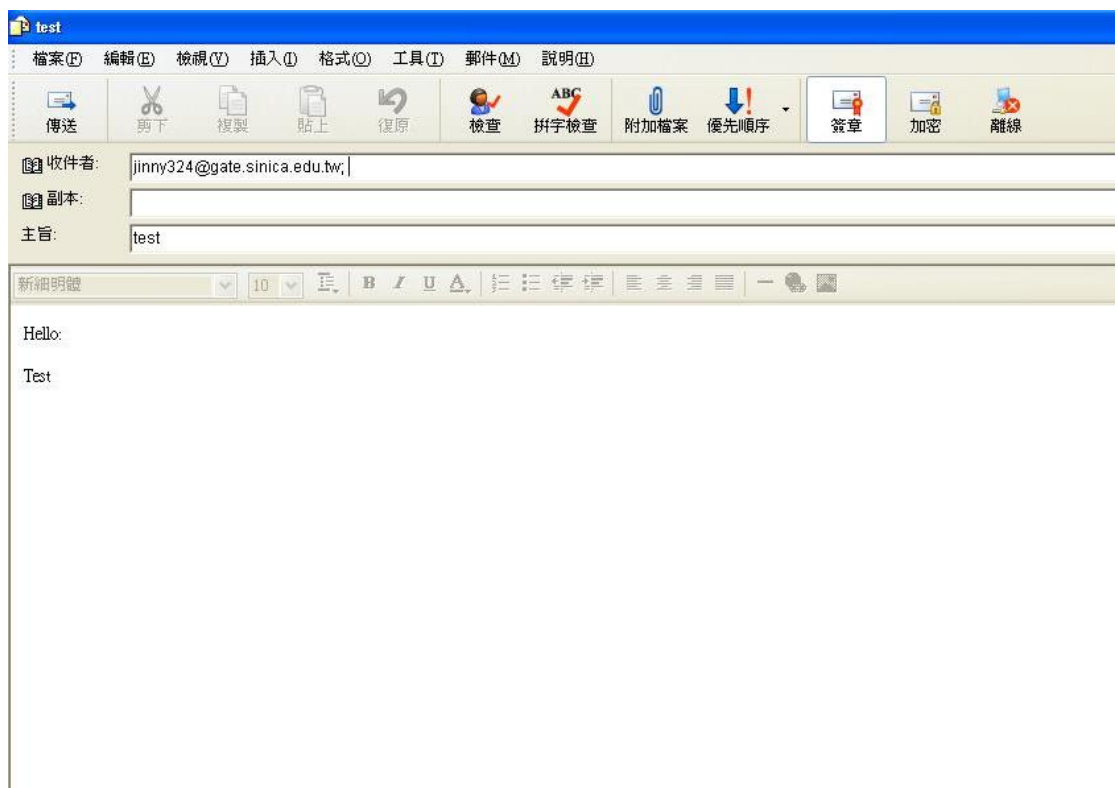


Figure 9