ELEC-C7420 Basic Principles in Networking
Part II: Security

Assignment IV: PGP

Members: Beatriz Glaser
Thuy Määttä

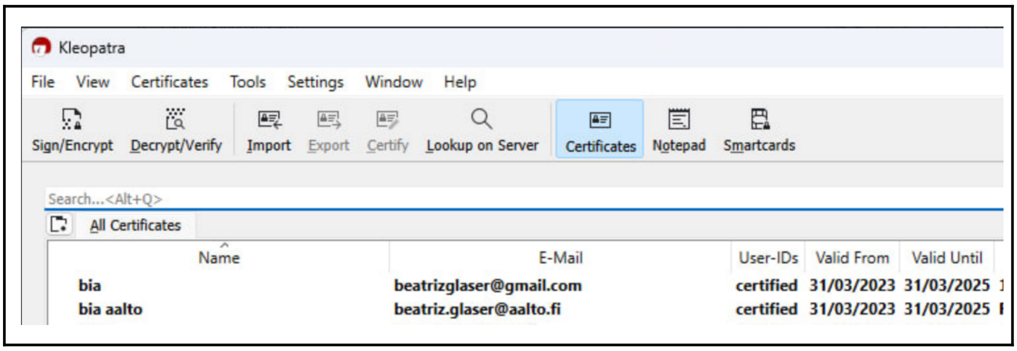
1. Goals of the experiment

The goal of this experiment is to create a secure email communication with particular privacy layers using a certificate manager Kleopatra, including digital signatures from the sender and receiver, encrypting and decrypting the plaintext and attachments at the sender and receiver end.

In general, the learning goals of this topic are understanding public-key cryptography, managing keys, using PGP software (such as Kleopatra) to encrypt and decrypt messages, verify digital signatures, and secure email communication in various email clients and operating systems. Using PGP can enhance online security and protect sensitive information from unauthorised access.

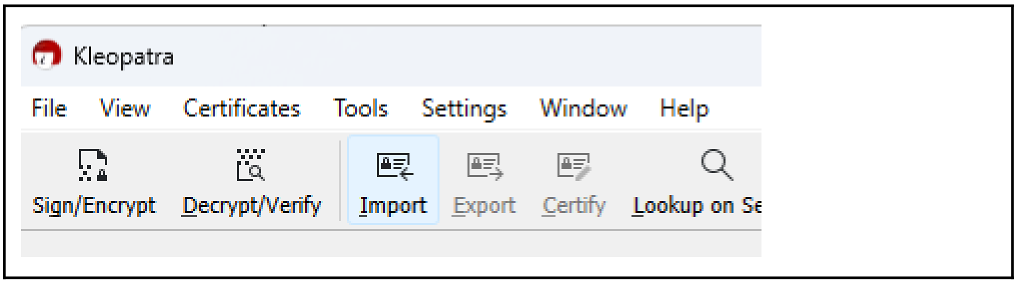
2. Experimental setup

a. Download and install Gpg4win
b. Launch Kleopatra app
c. Create a pair key (set name, email and passphrase)

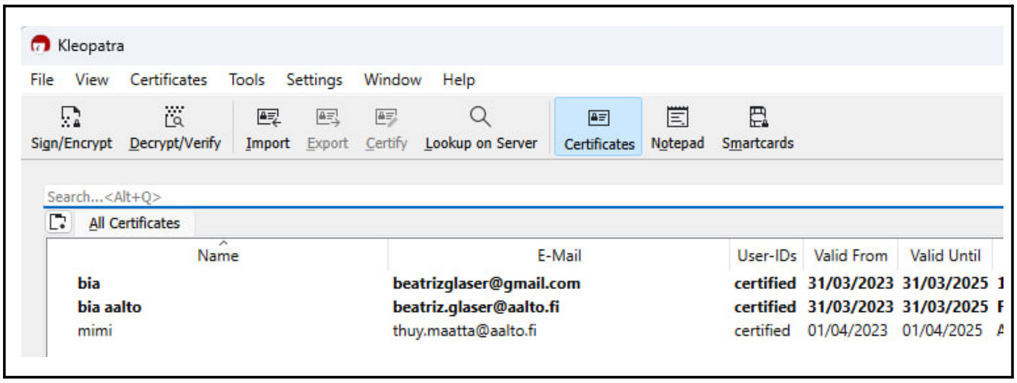


Name	E-Mail	User-IDs	Valid From	Valid Until
bia	beatrizglaser@gmail.com	certified	31/03/2023	31/03/2025
bia aalto	beatriz.glaser@aalto.fi	certified	31/03/2023	31/03/2025

d. You can save a backup of your key to your computer. And use export your public key in order to share it with others.
e. Import the recipient's key using "import".

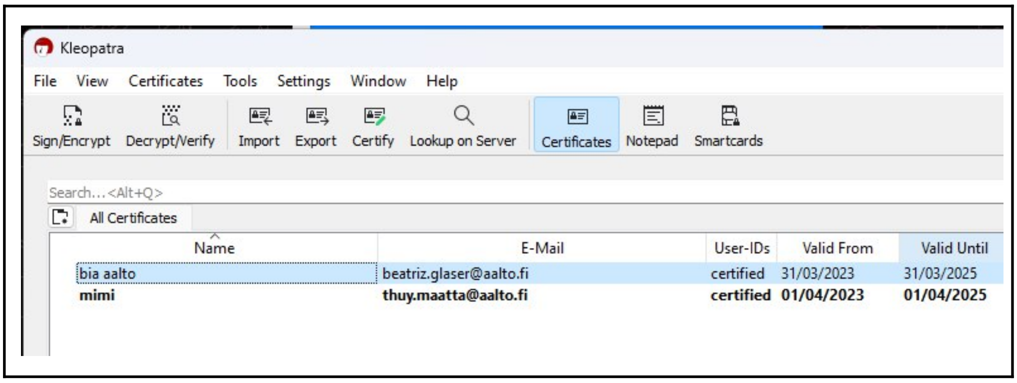


f. After verifying their certificate, you can see their certificate.



Name	E-Mail	User-IDs	Valid From	Valid Until	
bia	**beatrizglaser@gmail.com**	**certified**	**31/03/2023**	**31/03/2025**	**1**
bia aalto	**beatriz.glaser@aalto.fi**	**certified**	**31/03/2023**	**31/03/2025**	**F**
mimi	thuy.maatta@aalto.fi	certified	01/04/2023	01/04/2025	A

g. The recipient should also add the sender's key to their certificates in Kleopatra.



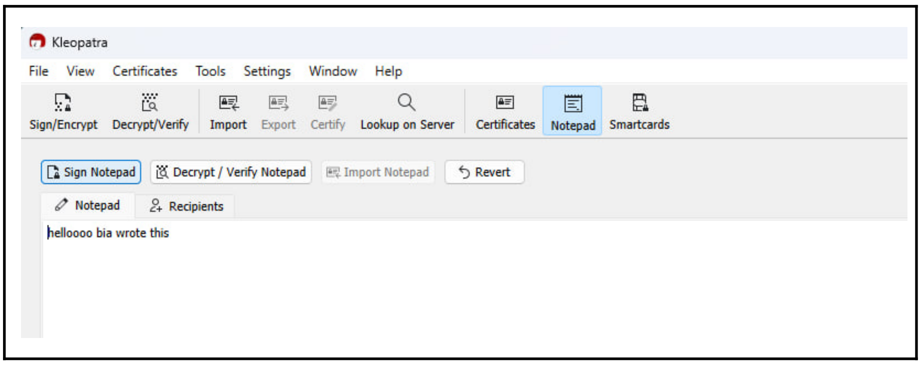
Name	E-Mail	User-IDs	Valid From	Valid Until
bia aalto	beatriz.glaser@aalto.fi	certified	31/03/2023	31/03/2025
mimi	**thuy.maatta@aalto.fi**	**certified**	**01/04/2023**	**01/04/2025**

NOTE: For this experiment, "bia" is the sender and "mimi" the recipient.

3. Results

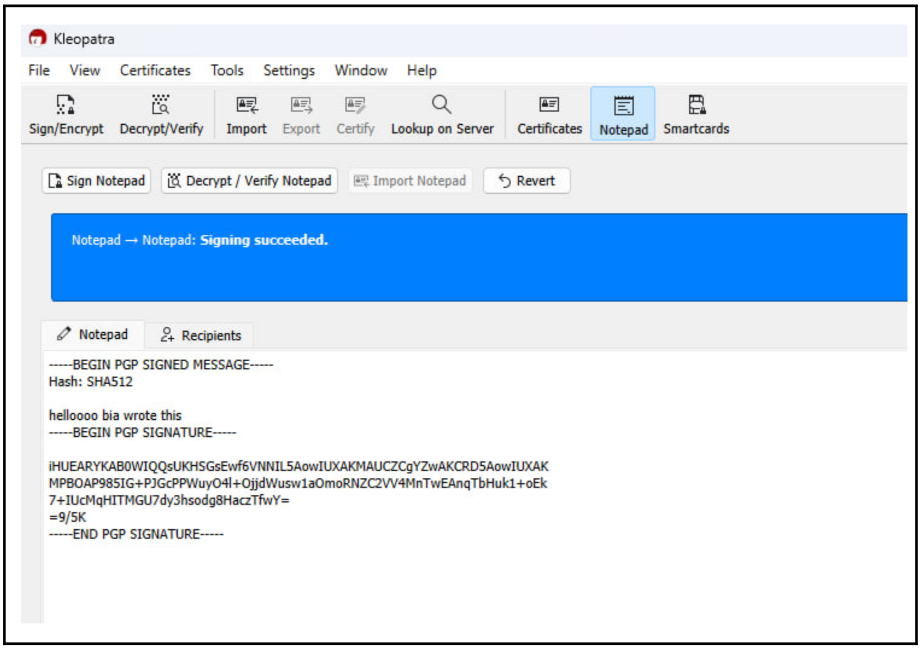
a. <u>Digital signature implementation (without encryption)</u>

i. Write a message to be signed and press "sign notepad"



helloooo bia wrote this

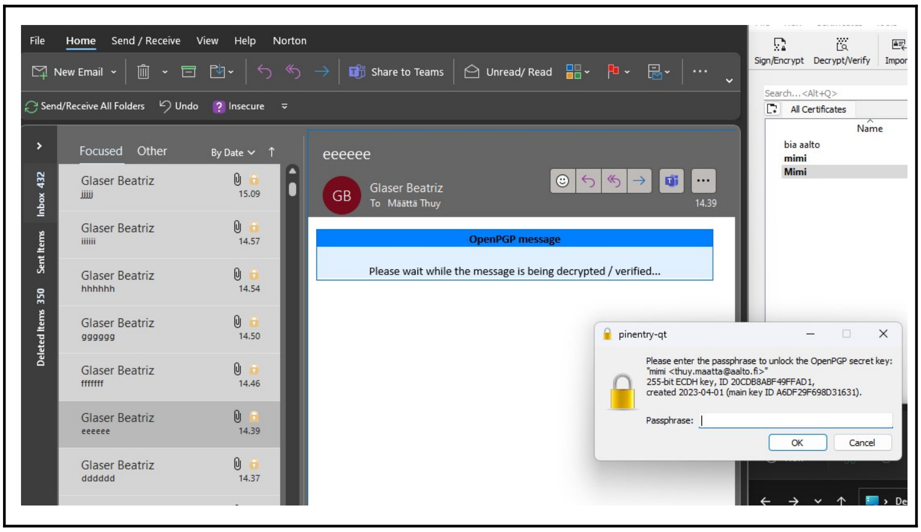
ii. After signing, you can see the signature on the message



Notepad → Notepad: **Signing succeeded.**

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

helloooo bia wrote this
-----BEGIN PGP SIGNATURE-----

iHUEARYKAB0WIQQsUKHSGsEwf6VNNIL5AowIUXAKMAUCZCgYZwAKCRD5AowIUXAK
MPBOAP985IG+PJGcPPWuyO4l+OjjdWusw1aOmoRNZC2VV4MnTwEAnqTbHuk1+oEk
7+IUcMqHITMGU7dy3hsodg8HaczTfwY=
=9/5K
-----END PGP SIGNATURE-----
```

iii. Send the message through email to the recipient, who has to confirm their own identity before opening the email



Glaser Beatriz jjjjjj	15.09
Glaser Beatriz iiiiii	14.57
Glaser Beatriz hhhhhh	14.54
Glaser Beatriz gggggg	14.50
Glaser Beatriz ffffff	14.46
Glaser Beatriz eeeeee	14.39
Glaser Beatriz dddddd	14.37

eeeeee

GB Glaser Beatriz
To Määttä Thuy
14.39

OpenPGP message

Please wait while the message is being decrypted / verified...

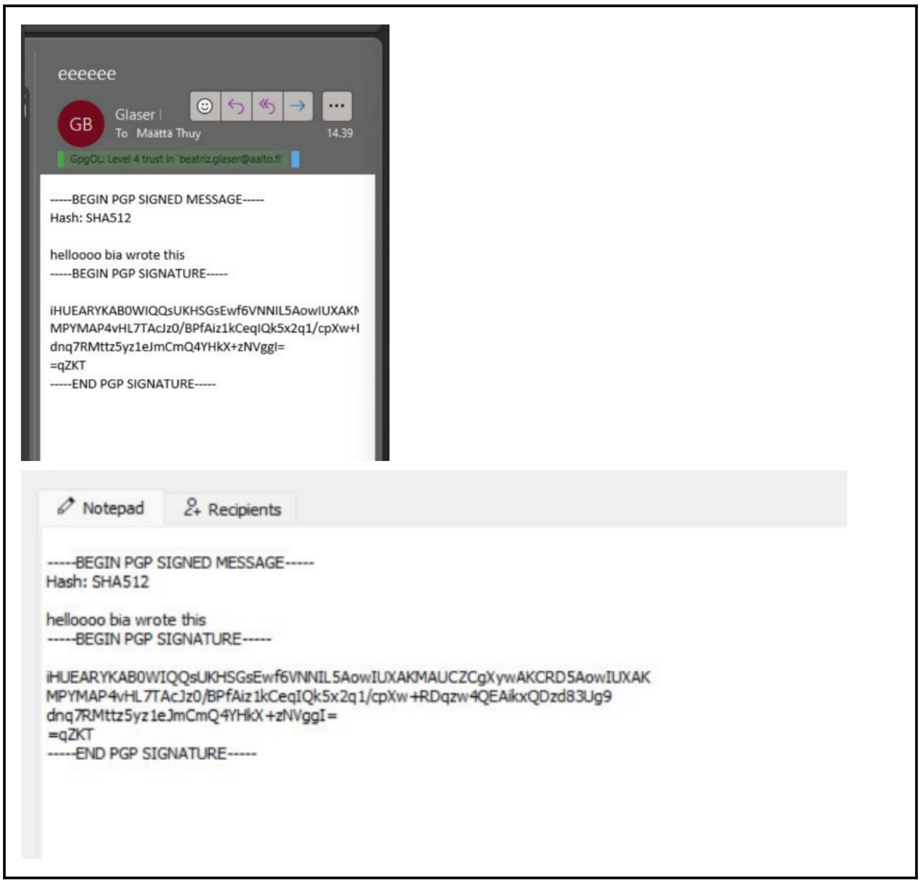
pinentry-qt

Please enter the passphrase to unlock the OpenPGP secret key:
"mimi <thuy.maatta@aalto.fi>"
255-bit ECDH key, ID 20CDB8ABF49FFAD1,
created 2023-04-01 (main key ID A6DF29F698D31631).

Passphrase:

OK Cancel

iv. The recipient can then copy-paste the message into their notepad for verification



eeeeee

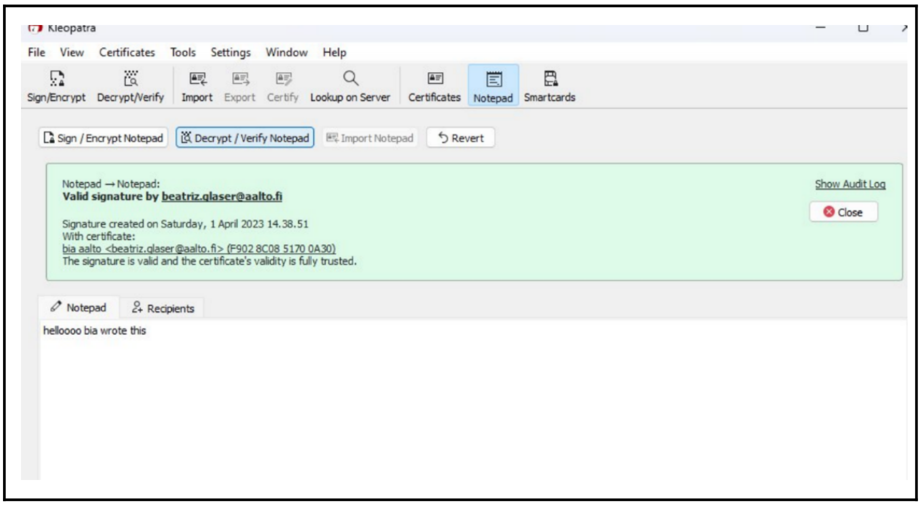
GB Glaser | To Määttä Thuy 14.39

GpgOL: Level 4 trust in 'beatriz.glaser@aalto.fi'

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

helloooo bia wrote this
-----BEGIN PGP SIGNATURE-----

iHUEARYKAB0WIQQsUKHSGsEwf6VNNIL5AowIUXAKM
MPYMAP4vHL7TAcJz0/BPfAiz1kCeqIQk5x2q1/cpXw+I
dnq7RMttz5yz1eJmCmQ4YHkX+zNVggI=
=qZKT
-----END PGP SIGNATURE-----
```

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

helloooo bia wrote this
-----BEGIN PGP SIGNATURE-----

iHUEARYKAB0WIQQsUKHSGsEwf6VNNIL5AowIUXAKMAUCZCgXywAKCRD5AowIUXAK
MPYMAP4vHL7TAcJz0/BPfAiz1kCeqIQk5x2q1/cpXw+RDqzw4QEAikxQDzd83Ug9
dnq7RMttz5yz1eJmCmQ4YHkX+zNVggI=
=qZKT
-----END PGP SIGNATURE-----
```

v. After verifying, you can see the validity of the signature



Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Sign / Encrypt Notepad
Decrypt / Verify Notepad
Import Notepad
Revert
Show Audit Log
Close
Notepad
Recipients

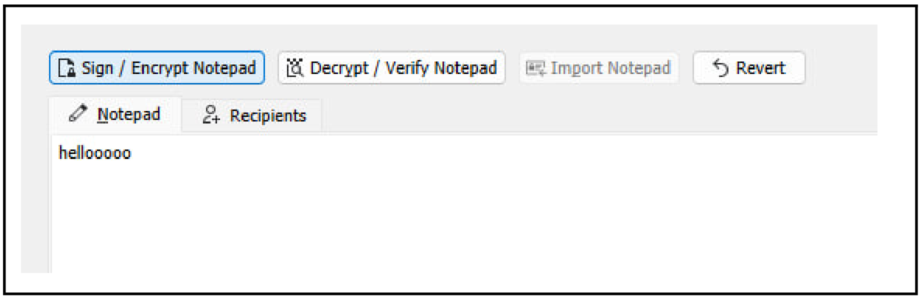
Notepad → Notepad:
Valid signature by beatriz.glaser@aalto.fi

Signature created on Saturday, 1 April 2023 14.38.51
With certificate:
bia aalto <beatriz.glaser@aalto.fi> (F902 8C08 5170 0A30)
The signature is valid and the certificate's validity is fully trusted.

helloooo bia wrote this

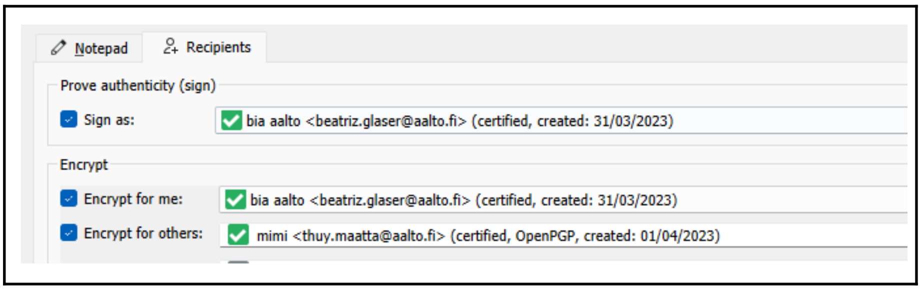
b. Plain text encryption

i. Write down text to encrypt and press “sign / encrypt notepad”



hellooooo

ii. When encrypting, make sure you encrypt it for the public key of your recipient



Prove authenticity (sign)

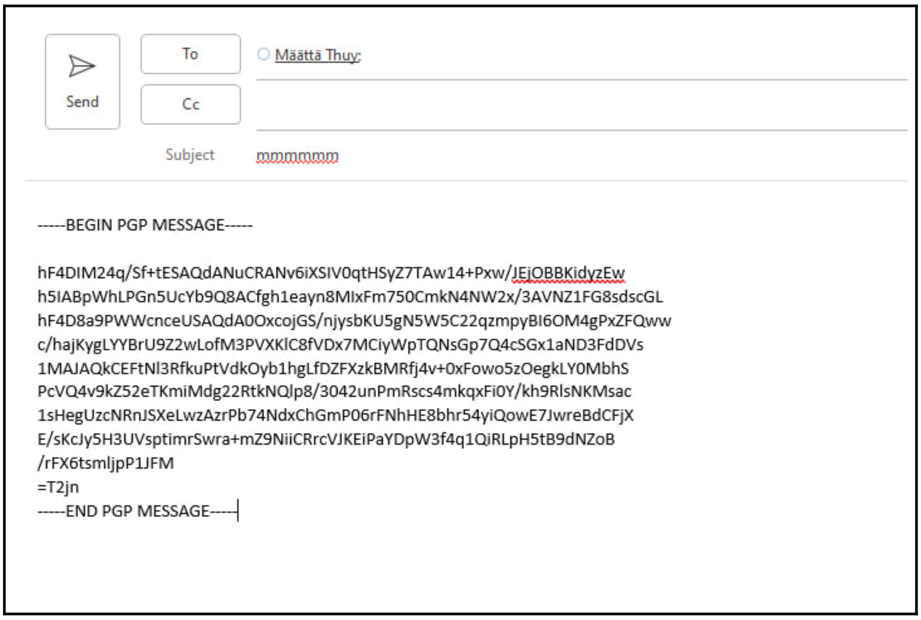
☑ Sign as: ✓ bia aalto <beatriz.glaser@aalto.fi> (certified, created: 31/03/2023)

Encrypt

☑ Encrypt for me: ✓ bia aalto <beatriz.glaser@aalto.fi> (certified, created: 31/03/2023)

☑ Encrypt for others: ✓ mimi <thuy.maatta@aalto.fi> (certified, OpenPGP, created: 01/04/2023)

iii. After encrypting you get the encrypt message, copy paste the it into an email for the recipient



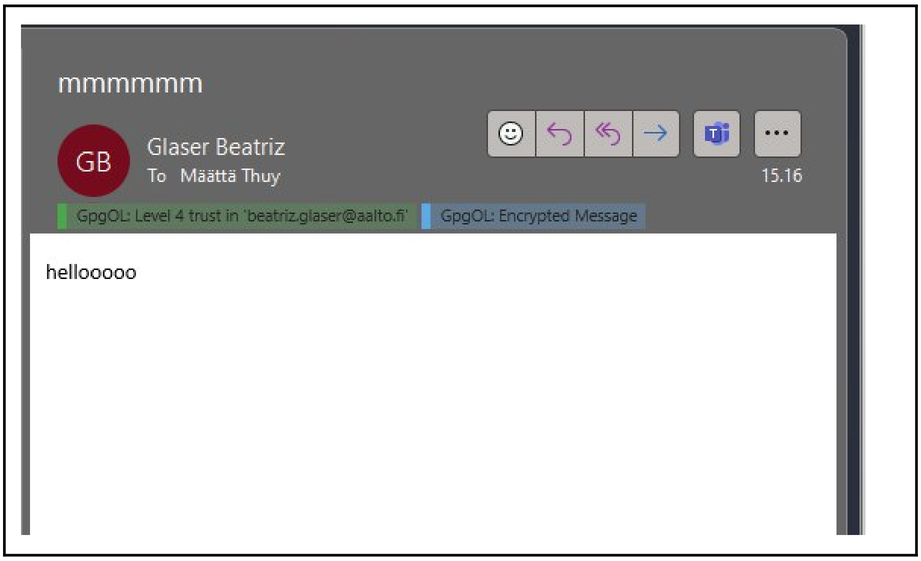
To: ○ Määttä Thuy;

Subject: mmmmmm

```
-----BEGIN PGP MESSAGE-----

hF4DIM24q/Sf+tESAQdANuCRANv6iXSIV0qtHSyZ7TAw14+Pxw/JEjOBBKidyzEw
h5IABpWhLPGn5UcYb9Q8ACfgh1eayn8MIxFm750CmkN4NW2x/3AVNZ1FG8sdscGL
hF4D8a9PWWcnceUSAQdA0OxcojGS/njysbKU5gN5W5C22qzmpyBI6OM4gPxZFQww
c/hajKygLYYBrU9Z2wLofM3PVXKlC8fVDx7MCiyWpTQNsGp7Q4cSGx1aND3FdDVs
1MAJAQkCEFtNl3RfkuPtVdkOyb1hgLfDZFXzkBMRfj4v+0xFowo5zOegkLY0MbhS
PcVQ4v9kZ52eTKmiMdg22RtkNQlp8/3042unPmRscs4mkqxFi0Y/kh9RlsNKMsac
1sHegUzcNRnJSXeLwzAzrPb74NdxChGmP06rFNhHE8bhr54yiQowE7JwreBdCFjX
E/sKcJy5H3UVsptimrSwra+mZ9NiiCRrcVJKEiPaYDpW3f4q1QiRLpH5tB9dNZoB
/rFX6tsmljpP1JFM
=T2jn
-----END PGP MESSAGE-----
```

c. <u>Plain text decryption</u>

i. The recipient receives the encrypted message, and Outlook automatically decrypts it. As you can see from the green bar on the email, it uses GpgOL and is protected.



mmmmmm

Glaser Beatriz
To Määttä Thuy

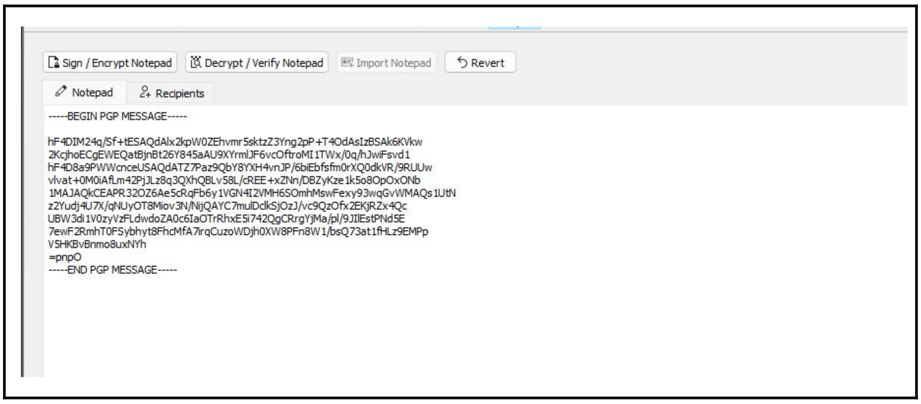
15.16

GpgOL: Level 4 trust in 'beatriz.glaser@aalto.fi'

GpgOL: Encrypted Message

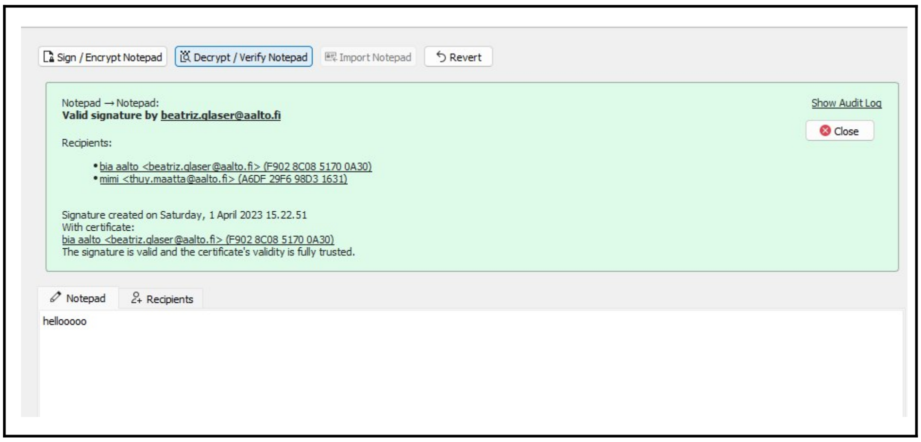
hellooooo

ii. If the message is not automatically decrypted, it can also be done manually. The recipient only has to paste the encrypted message onto their notepad on their Kleopatra



```
-----BEGIN PGP MESSAGE-----

hF4DIM24q/Sf+tESAQdAlx2kpW0ZEhvmr5sktzZ3Yng2pP+T4OdAsIzBSAk6KVkw
2KcjhoECgEWEQatBjnBt26Y845aAU9XYrmlJF6vcOftroMI1TWx/0q/hJwiFsvd1
hF4D8a9PWWcnceUSAQdATZ7Paz9QbY8YXH4vnJP/6biEbfsfm0rXQ0dkVR/9RUUw
vlvat+0M0iAfLm42PjJLz8q3QXhQBLv58L/cREE+xZNn/DBZyKze1k5o8OpOxONb
1MAJAQkCEAPR32OZ6Ae5cRqFb6y1VGN4I2VMH6SOmhMswFexy93wqGvWMAQs1UtN
z2Yudj4U7X/qNUyOT8Miov3N/NijQAYC7mulDclkSjOzJ/vc9QzOfx2EKjRZx4Qc
UBW3di1V0zyVzFLdwdoZA0c6IaOTrRhxE5i742QgCRrgYjMa/pl/9JIlEstPNd5E
7ewF2RmhT0FSybhyt8FhcMfA7irqCuzoWDjh0XW8PFn8W1/bsQ73at1fHLz9EMPp
V5HKBvBnmo8uxNYh
=pnpO
-----END PGP MESSAGE-----
```

iii. And decrypt it. They can also see the digital signature of the sender.



Notepad → Notepad:
Valid signature by beatriz.glaser@aalto.fi

Recipients:

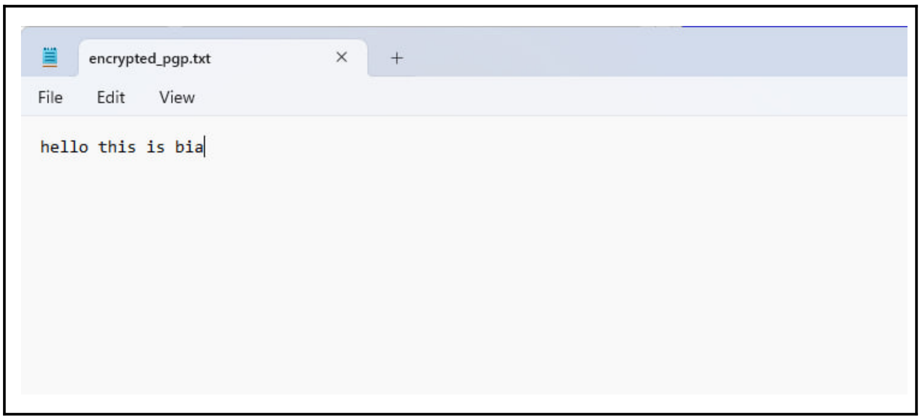
- bia aalto <beatriz.glaser@aalto.fi> (F902 8C08 5170 0A30)
- mimi <thuy.maatta@aalto.fi> (A6DF 29F6 98D3 1631)

Signature created on Saturday, 1 April 2023 15.22.51
With certificate:
bia aalto <beatriz.glaser@aalto.fi> (F902 8C08 5170 0A30)
The signature is valid and the certificate's validity is fully trusted.

hellooooo

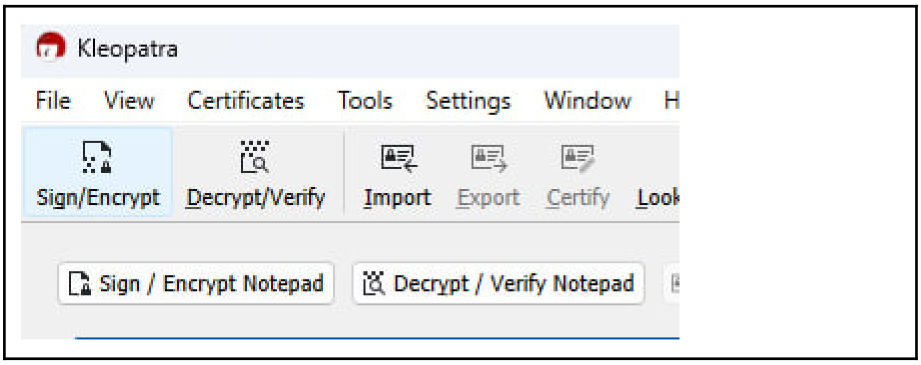
d. Attachment encryption

i. Choose a file to encrypt

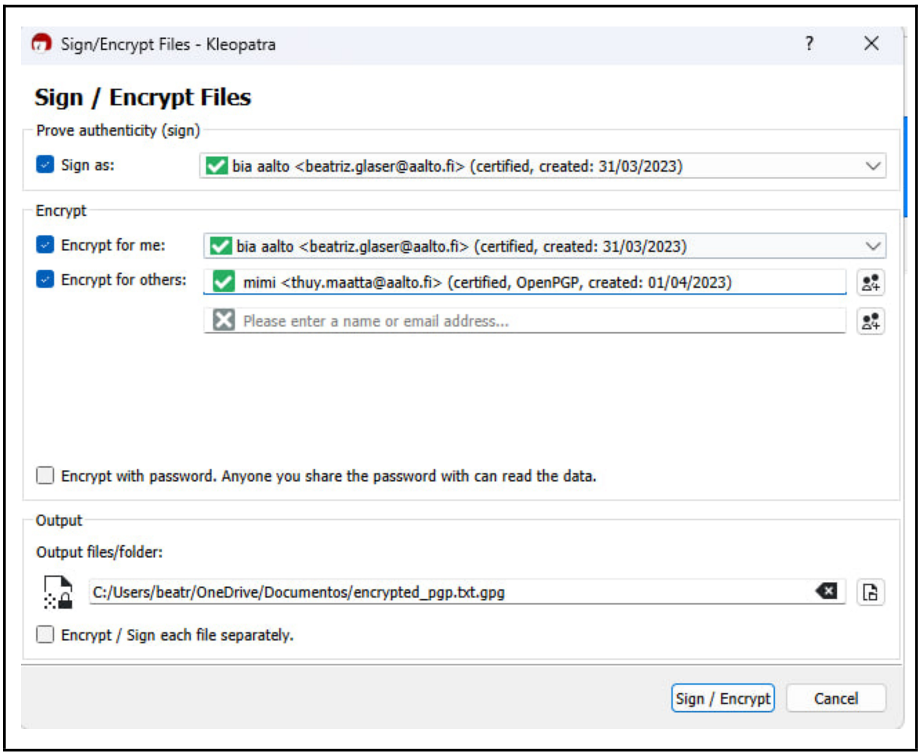


```
hello this is bia
```

ii. Encrypt it by pressing the “Sign/Encrypt” button in Kleopatra



iii. After choosing the file, you need to choose the public key of your recipient



Sign / Encrypt Files

Prove authenticity (sign)

☑ Sign as: bia aalto <beatriz.glaser@aalto.fi> (certified, created: 31/03/2023)

Encrypt

☑ Encrypt for me: bia aalto <beatriz.glaser@aalto.fi> (certified, created: 31/03/2023)

☑ Encrypt for others: mimi <thuy.maatta@aalto.fi> (certified, OpenPGP, created: 01/04/2023)

Please enter a name or email address...

☐ Encrypt with password. Anyone you share the password with can read the data.

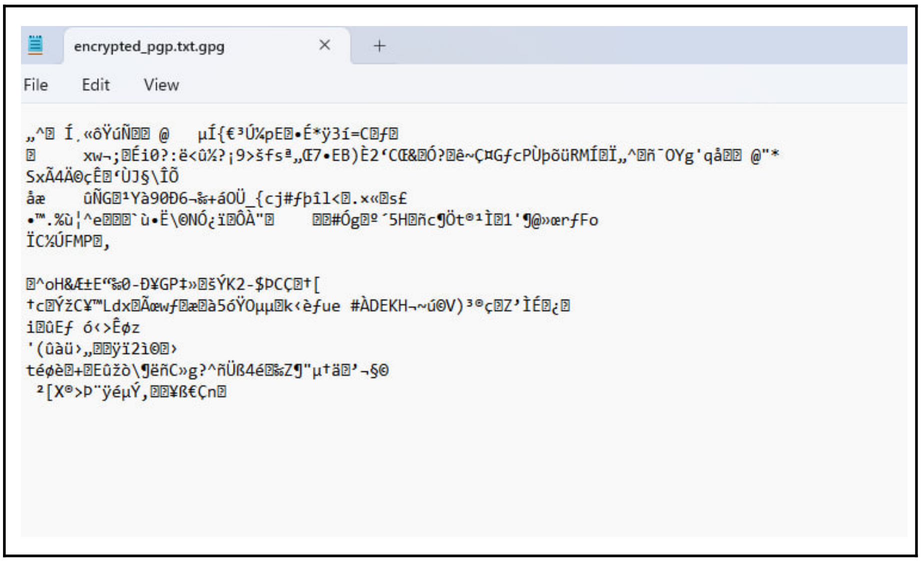
Output

Output files/folder:

C:/Users/beatr/OneDrive/Documentos/encrypted_pgp.txt.gpg

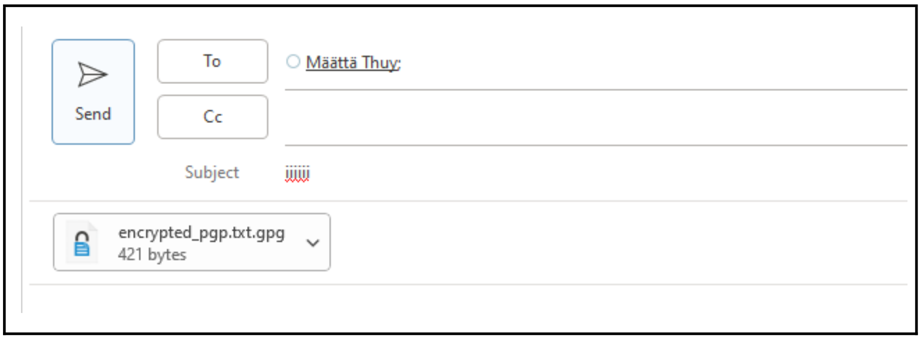
☐ Encrypt / Sign each file separately.

iv. Once the content is encrypted into a gpg file, you can check the encryption by opening in on a notepad, for example.



```
„^□ Í˛«ôŸúÑ□□ @   µÍ{€³Ú¼pE□•É*ÿ3í=C□ƒ□
□     xw¬;□Éi0?:ë<û½?¡9>šfsª„Œ7•EB)È2‘CŒ&□Ó?□ê~Ç¤GƒcPÙþõüRMÍ□Ï„^□ñ¯OYg'qå□□ @"*
SxÃ4Ä©çÊ□‘ÙJ§\ÎÕ
åæ    ûÑG□¹Yà90Ð6¬‰+áOÜ_{cj#ƒþîl<□.×«□s£
•™.%ù¦^e□□□`ù•Ë\©NÓ¿ï□ÔÀ"□    □□#Óg□º´5H□ñc¶Öt®¹Ì□1'¶@»œrƒFo
ÏC½ÚFMP□,

□^oH&Æ±E“‰0-Ð¥GP‡»□šÝK2-$ÞCÇ□†[
†c□ÝžC¥™Ldx□Ãœwƒ□æ□à5óŸOµµ□k‹èƒue #ÀDEKH¬~ú©V)³®ç□Z’ÌÉ□¿□
i□ûEƒ ó‹>Êøz
'(ûàü›„□□ÿï2ì©□›
téøè□+□Eûžò\¶ëñC»g?^ñÜß4é□‰Z¶"µ†ä□’¬§©
 ²[X®>Þ¨ÿéµÝ,□□¥ß€Çn□
```

v. Send the file as an attachment to the recipient’s email. Enter your passphrase if prompted.



To: Määttä Thuy;

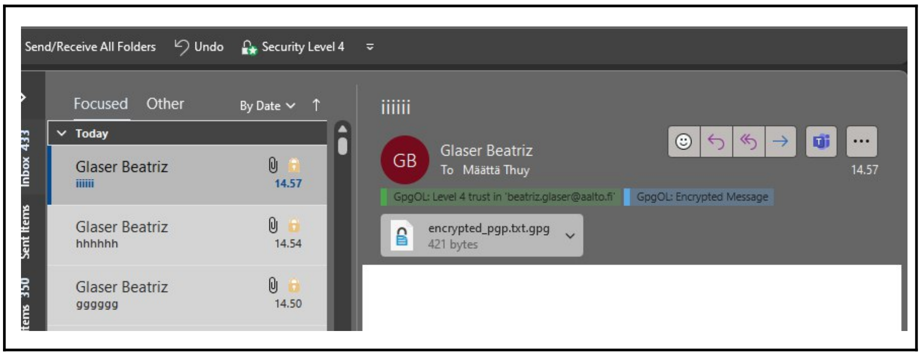
Cc:

Subject: iiiiii

encrypted_pgp.txt.gpg
421 bytes

e. Attachment decryption

i. The recipient receives the secure email and downloads the gpg file.



Glaser Beatriz
iiiiii
14.57

Glaser Beatriz
hhhhhh
14.54

Glaser Beatriz
gggggg
14.50

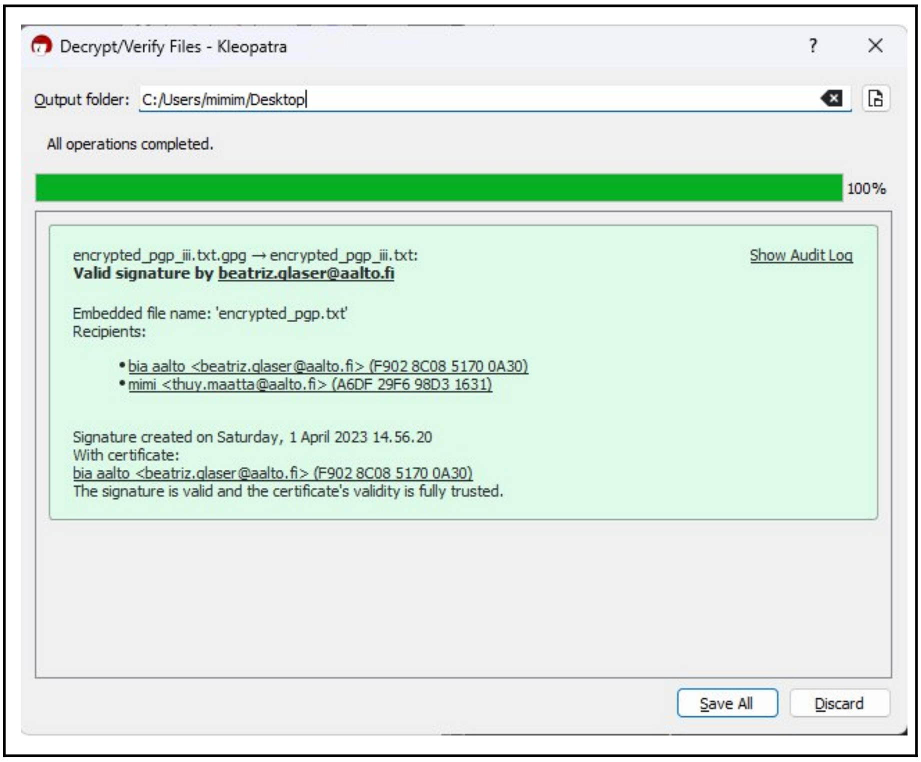
iiiiii

Glaser Beatriz
To Määttä Thuy
14.57

GpgOL: Level 4 trust in 'beatriz.glaser@aalto.fi'
GpgOL: Encrypted Message

encrypted_pgp.txt.gpg
421 bytes

ii. When opening the gpg file Kleopatra checks the digital signature and decrypts the file, saving it into a new txt file.



Output folder: C:/Users/mimim/Desktop

All operations completed.

100%

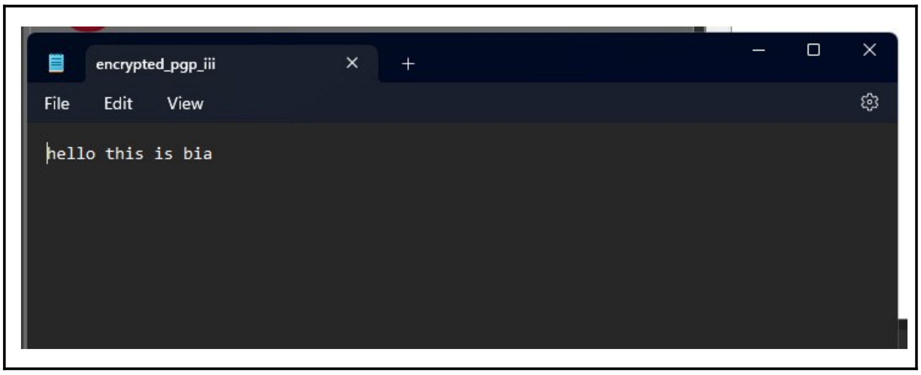
encrypted_pgp_iii.txt.gpg → encrypted_pgp_iii.txt:
Valid signature by beatriz.glaser@aalto.fi

Embedded file name: 'encrypted_pgp.txt'
Recipients:

- bia aalto <beatriz.glaser@aalto.fi> (F902 8C08 5170 0A30)
- mimi <thuy.maatta@aalto.fi> (A6DF 29F6 98D3 1631)

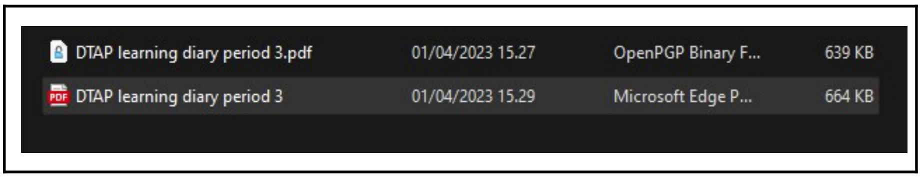
Signature created on Saturday, 1 April 2023 14.56.20
With certificate:
bia aalto <beatriz.glaser@aalto.fi> (F902 8C08 5170 0A30)
The signature is valid and the certificate's validity is fully trusted.

iii. The decrypted file can then be opened and read



```
hello this is bia
```

iv. We also tried sending other types of file, for example pdf. The process and results are the same.



DTAP learning diary period 3.pdf	01/04/2023 15.27	OpenPGP Binary F...	639 KB
DTAP learning diary period 3	01/04/2023 15.29	Microsoft Edge P...	664 KB

4. Conclusion

In conclusion, creating a secure email communication system using PGP encryption is essential to safeguard sensitive information from unauthorised access, as well as to protect sensitive information from cyber-attacks. Therefore, it is important to understand private/public-key cryptography and know how to use PGP softwares to secure email communication.