A7010E Homework 3

Nico Ferrari (nicfer-0@student.ltu.se)

November 2, 2020

1.

Assumptions:

- Each employee will have his own workstation in the office.
- the company has at least a server for VPN and access control
- each employee has its own workstation in the office/desk connected to the company's network.

Access control
In order to access to the working files from remote, i suggest a VPN connection to the main server, and from there, each employee will have access to a personal workstation through remote connection (in case of Windows as OS, otherwise there are the variants for Unix systems and macOS). To access to the VPN the following type of access will be established, depending on the LoA.

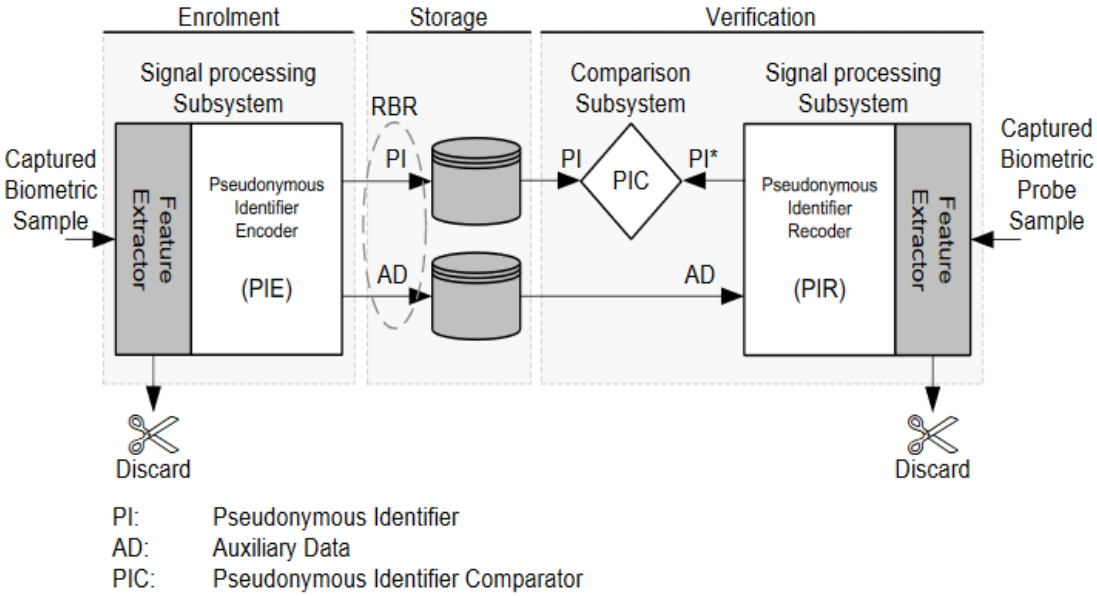
- **Level 2 assurance:** According to NIST, Level 2 provides single factor remote network authentication. A person will be successfully authenticated after proving its entity through a secure authentication protocol,showing that the entity has control of an agreed credential. Level 2 of assurance allows:
  - Look-up Secret Tokens, storing a set of secrets and is used to look up the secret based on a prompt.
  - Out of Band Tokens, received over a separate channel and presented to the authentication protocol.

  I propose an Out of Band authentication protocol, where a one-time PIN will be sent secretly by SMS to the phone number registred during enrollment when the employee wants to access the online platform. Then, the PIN code has to be entered in the platform in order to perform the authentication, as described in the following steps:
  - Enrollment phase: the employee register a phone number. During this phase it is necessary to make sure that the number is correct and available. Moreover a email address or username is set.
  - Employee start the login phase when starting the VPN connection: In this phase, the employee which wants to authenticate himself goes to the platform and tries to login with his username or email. The central server will send a SMS to the registered number with a PIN code.
  - Authentication phase: after sending the SMS, a popup window will appear asking for the PIN code. The employee enters the PIN code in the platform and, if accepted will be authenticated otherwise a new PIN will be requested. The PIN code will be sent for a prestablished maximum of times, and after that the account will be blocked. To reactivate the account, the employee must contact the IT Department of the company and Identify himself in person.

  the size of the PIN code and the number of ttimes that the user can enter the wrong PIN code must be set in an "*Encryption Policy*".

- **Level 3 assurance:** In LoA 3, multifactor authentication is enabled. in order to access to the VPN another factor used to authenticate the user must be used. Usually passwords are used, but as described in previous assignments, they are getting weaker and weaker. Biometrics will be then used, especially a techniques called BioHashing, which doesn't store any detail related to the biometric feature, but only a sort of hash. The process will be describe in LoA 4, where an external devices (USB crypto token) will be used for the generation of this sort of HASH of biometric feautres. in this case, the registration will be done during enrollment time, when also the phone number will be registred. The user will generate a biohash and there will be an exchange through secure channel of the digital certificate of the server. His public key will be used to initialize the authentication, by encrypting the bioHash that the the user will generate during login phase. if the bioHash is decrypted by the server and equals to the one registred during enrollment time, he will send the PIN code to the user, which must then been entered in order to conclude the authentication (as described previously).
- **Level 4 assurance:** LoA 4 is used when a high risk is associated with erroneous authentication. LoA 4 provides the highest level of entity authentication assurance defined . In order to authenticate itself, a user must proof the possession of a key through a cryptographic protocol. This level requires a physical token and strong cryptographic authentication of all parties and all sensitive data transfers between the parties.For this purpose, cryptographic USB keys are being developed since only "hard" cryptographic tokens which cannot readily be copied are allowed. the usb device needs to have an integrated biometric fingerprint's features reader. internally, the device willas described in the schema in Fig. 1 to authenticate the users using their biometrics data. As described in BioHASH, PIE

Figure 1: BioHASH protocol used in : *https://www.genkey.com*



introduces random seed and salting, plus redundancy to enable the use of error-correcting codes later on in the verification process. The template consists of two parts, the PI and the AD, without revealing any information about the biometric features that were used in creating them. During verification, error correction takes care of any finger placement differences, and this produces a candidate PI*. This creates a binary match with the PI from the template, if the template and the probe came from the same finger. In this process of generating PI*, the randomness that was introduced in PIE cancels out. This is the same process used also for fuzzy generator schemes, which are nowdays often used for IoT devices authentication using data form the environment like sounds and light. this process doesn't

store any biometric key. PI and AD will be stored in a secured server encrypted using asymmetric key algorithms. An enrollment phase will be established the firs day of each employee, where the cryptographic USB stick will be handled to the employee and used to generate the PI and AD with the biometrics features of the employee's fingerprint. the features extraction function has to be unique for each USB and kept secret. The main server will send its own digital certificate to the user's device used as BYOD and encrypted using AES algorithm and as a password PI*.

The resources in the network will then have an ABAC access mode. in this way, each user will have certain attributes and will have access only to the resources allowed by those attributes. For example, documents shared among the HR should not be accessible by developers, which will not have those kind of attributes. **Secure emails** each mailbox must have a spam filter and a list of trusted email addresses/ domains (such as the domain used by the company). in order to add new trusted email, the user must contact the IT department and ask to allow to send emails the following email address. Each email must be encrypted using GPG protocol. The keys must be created by each employee in the beginning and they will follow the guidelines explained in the 'encryption policy'.

Malware analysis in case of malware analysis, a separate workstation, disconnected from the network must be enabled. VMs can be detected by malwares and they will not run anymore in order to stay hidden. moreover, they can be exploited and infect the system anyway. therefore it is better to have a workstation just for malware analysis .

Trainings in order to make the users aware of security threats, training must be organized for the new employees. During this courses, the employees will learn how to detect suspicious emails and attachments, moreover they will learn the security policies and guidelines.

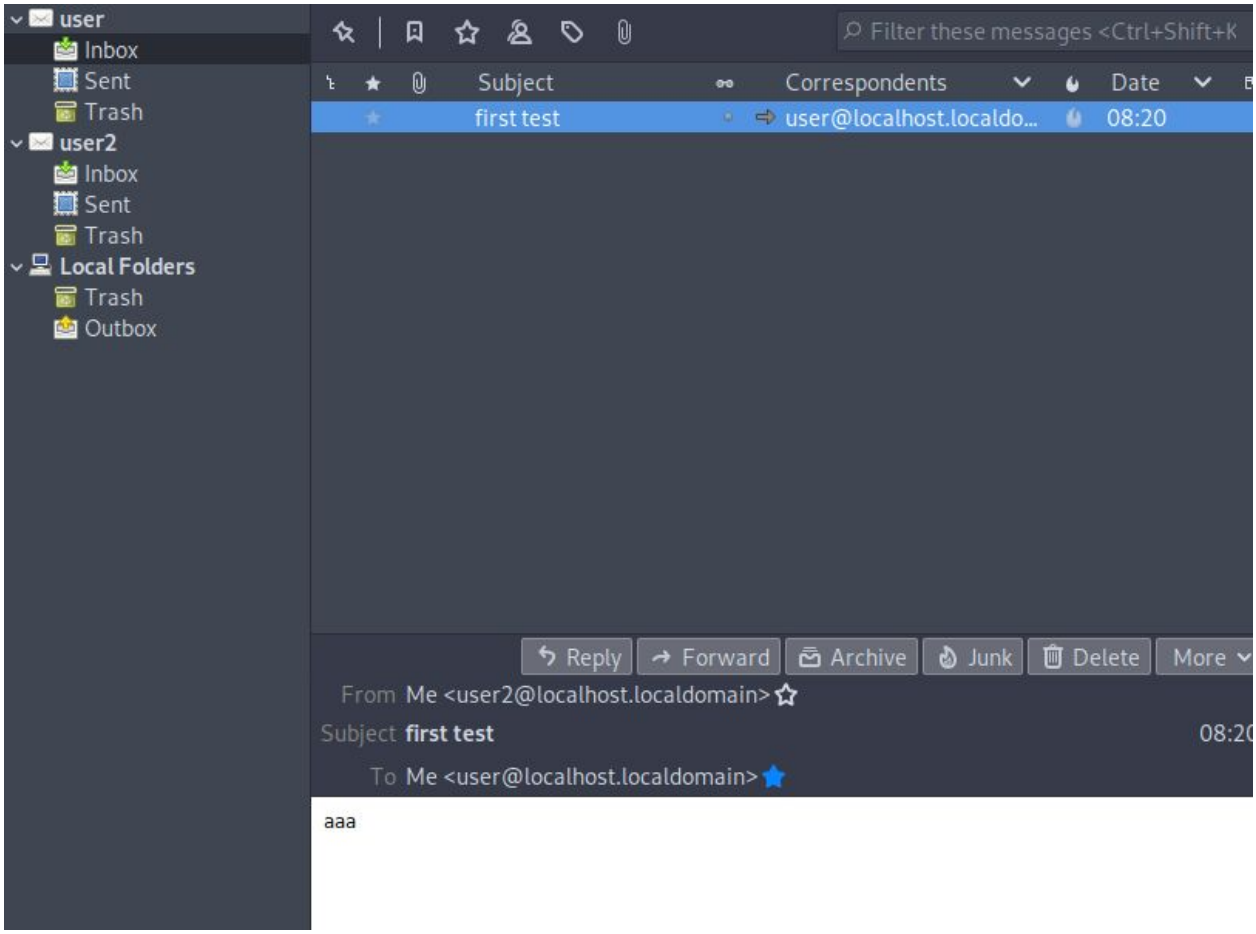
Policies some policies must be created, especially:

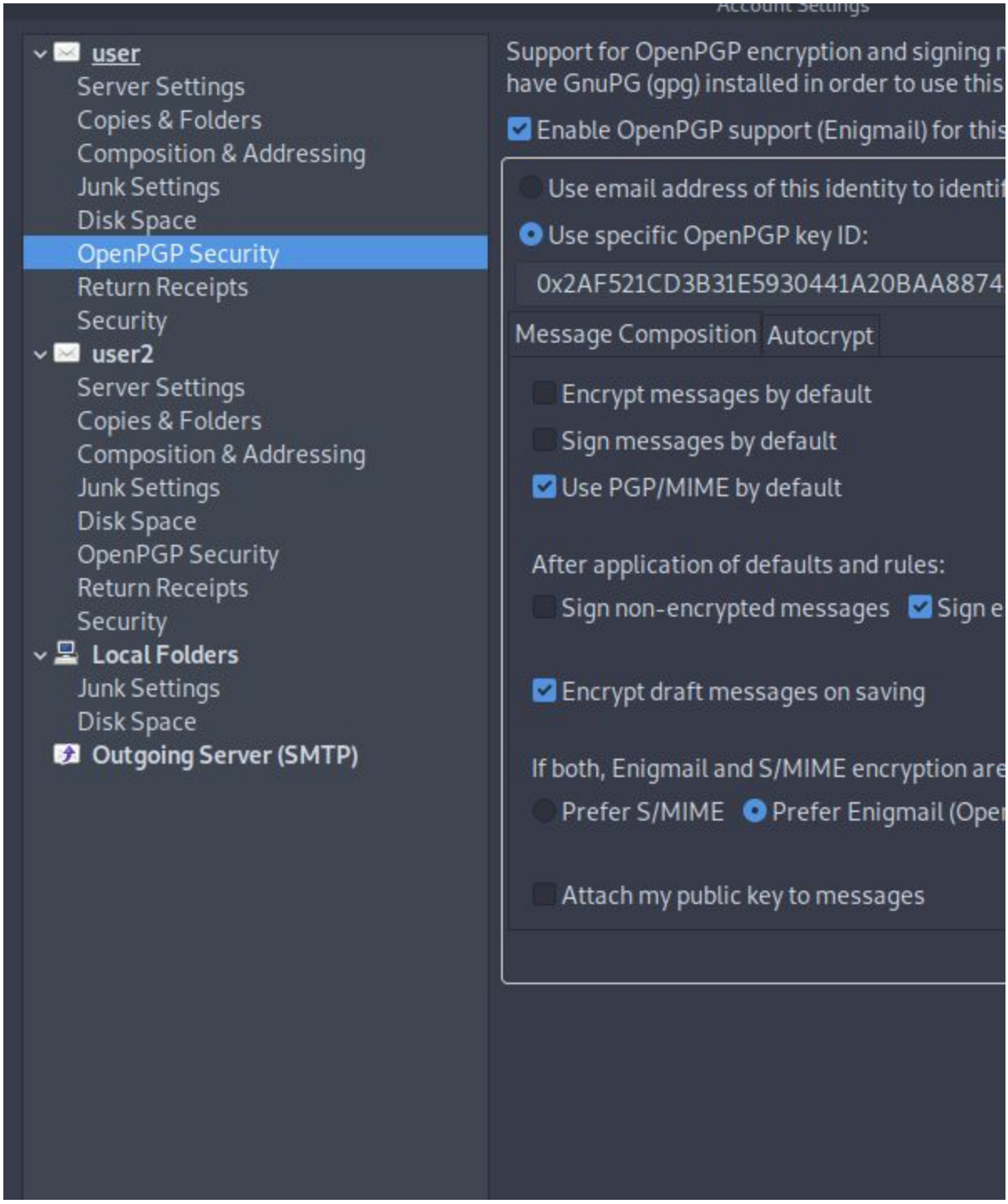
- Encryption policy: this policy must set the guidelines to create a random PIN, such as length and maximum number of wrong attempts. Moreover, must set the key length for the AES protocol and the length of the bioHash. In this policy will also established the length of the keypair generated with tools such as gnuPG and the expiration time og those. In order to use smaller keys, Elliptic Curve cryptography must be used. This policy must state also that the personal files in the workstations must be encrypted with a public key of the employee, and they must not be stored on personal devices.
- software policy: this policy must ensure that the software must be installed by an IT department, which also will take take of fixing patches and ensure that updates and patches do not 'block' the workflow of the employees. In fact, the IT department must constantly check for security issues in the software installed and look for patches. when a patch or updates are available, they must been checked first and then , if they are selected to be implemented, they will be installed in the employees computers.
- system protection: each computer must have an antivirus software installed and a firewall enabled on each workstation.
- email policy: this policy must ensure that employees do not send executables files by email. moreover, spam filter must be enabled and constantly updated. Each email communication must be securing used GPG protocol and a white list of contacts must be used in order to send emails only to those which are known. In case of suspicious emails, they must be reported to the InfoSec team of the company. the mailbox must not be used for personal user.

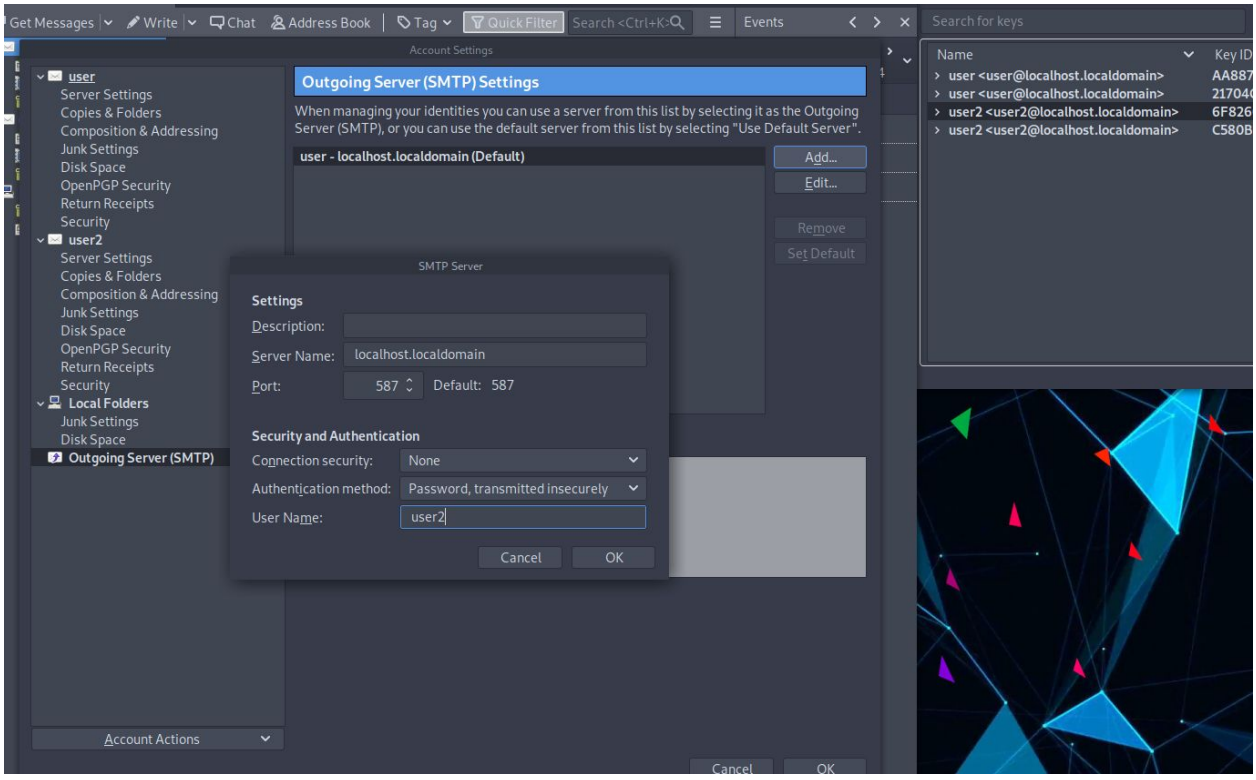
2. What is your own reflection on the entire week of the course?

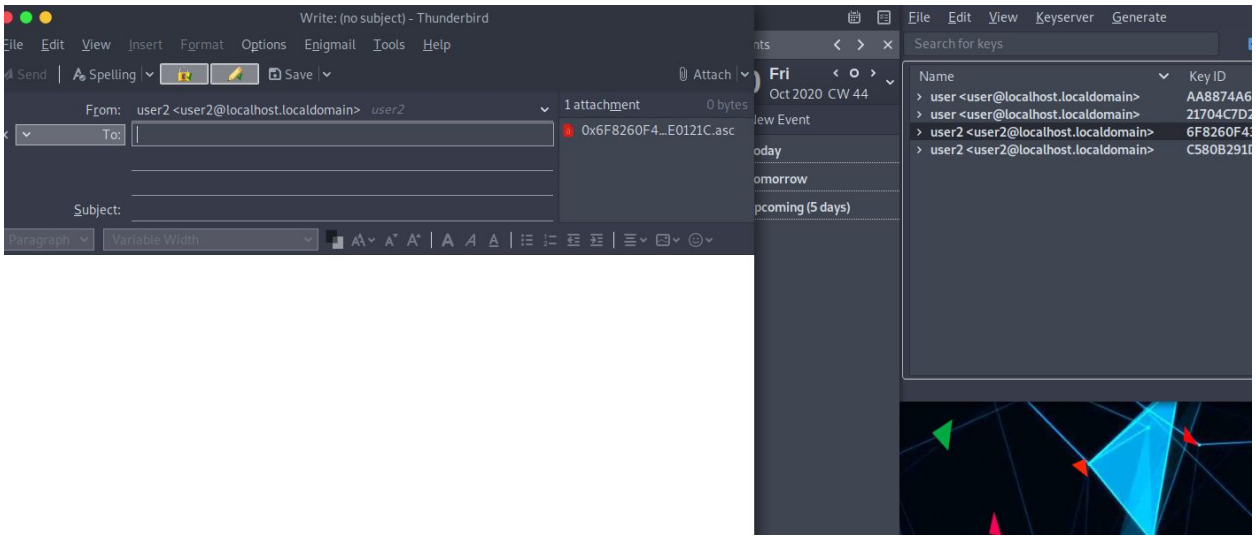
busy week, studying for the exam and then the assignment. asymmetric key is really a fun topic, and creating 'secure' channels among users is very interesting.

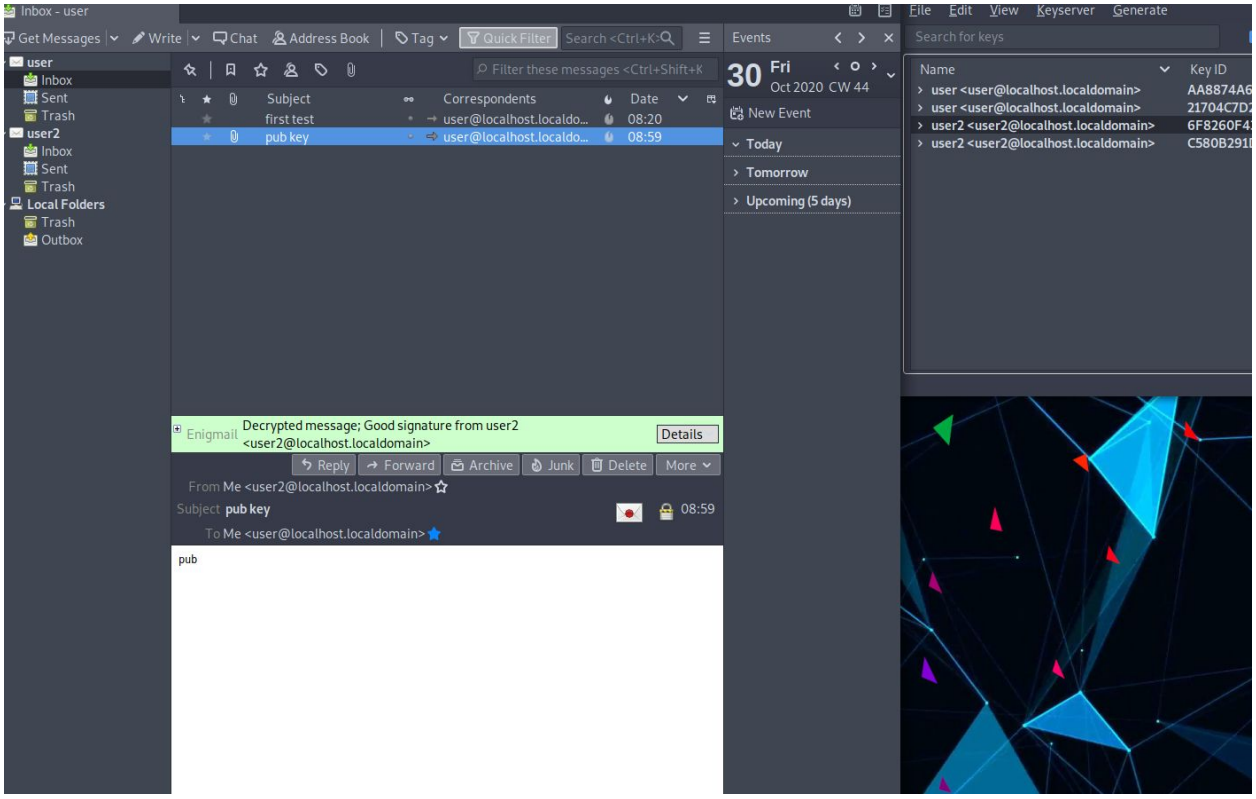
The first parts of the lab are a bit different compared to the one shown in the slides. Instead of login with root user, i will use the current user *user.* The users created will then be user and user2. Enigmail doesn't have the checkbox *Force using S/MIME and Enigmail.*




Account Settings
user
Server Settings
Copies & Folders
Composition & Addressing
Junk Settings
Disk Space
OpenPGP Security
Return Receipts
Security
user2
Server Settings
Copies & Folders
Composition & Addressing
Junk Settings
Disk Space
OpenPGP Security
Return Receipts
Security
Local Folders
Junk Settings
Disk Space
Outgoing Server (SMTP)
Support for OpenPGP encryption and signing r
have GnuPG (gpg) installed in order to use this
Enable OpenPGP support (Enigmail) for this
Use email address of this identity to identi
Use specific OpenPGP key ID:
0x2AF521CD3B31E5930441A20BAA8874
Message Composition
Autocrypt
Encrypt messages by default
Sign messages by default
Use PGP/MIME by default
After application of defaults and rules:
Sign non-encrypted messages
Sign e
Encrypt draft messages on saving
If both, Enigmail and S/MIME encryption are
Prefer S/MIME
Prefer Enigmail (Oper
Attach my public key to messages


Get Messages
Write
Chat
Address Book
Tag
Quick Filter
Search <Ctrl+K>
Events
Account Settings
user
Server Settings
Copies & Folders
Composition & Addressing
Junk Settings
Disk Space
OpenPGP Security
Return Receipts
Security
user2
Server Settings
Copies & Folders
Composition & Addressing
Junk Settings
Disk Space
OpenPGP Security
Return Receipts
Security
Local Folders
Junk Settings
Disk Space
Outgoing Server (SMTP)
Account Actions
Outgoing Server (SMTP) Settings
When managing your identities you can use a server from this list by selecting it as the Outgoing Server (SMTP), or you can use the default server from this list by selecting "Use Default Server".
user - localhost.localdomain (Default)
Add...
Edit...
Remove
Set Default
SMTP Server
Settings
Description:
Server Name: localhost.localdomain
Port: 587 Default: 587
Security and Authentication
Connection security: None
Authentication method: Password, transmitted insecurely
User Name: user2
Cancel
OK
Cancel
OK
Search for keys
Name
Key ID
user <user@localhost.localdomain>
user <user@localhost.localdomain>
user2 <user2@localhost.localdomain>
user2 <user2@localhost.localdomain>


Write: (no subject) - Thunderbird
File Edit View Insert Format Options Enigmail Tools Help
Send
Spelling
Save
Attach
From: user2 <user2@localhost.localdomain> user2
To:
Subject:
1 attachment 0 bytes
0x6F8260F4...E0121C.asc
Paragraph
Variable Width
File Edit View Keyserver Generate
Search for keys
Name
Key ID
user <user@localhost.localdomain>
user <user@localhost.localdomain>
user2 <user2@localhost.localdomain>
user2 <user2@localhost.localdomain>
Fri
Oct 2020 CW 44
New Event
Today
Tomorrow
Upcoming (5 days)



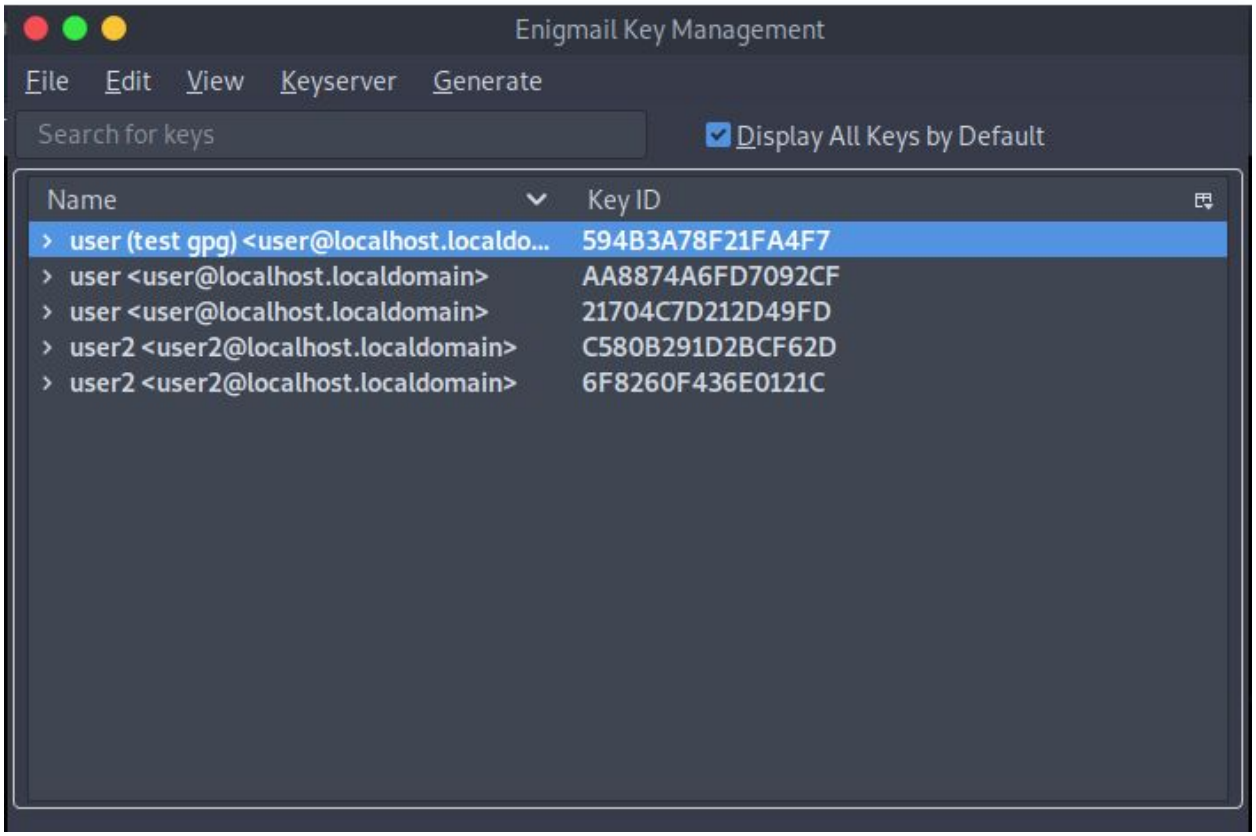
Challenge

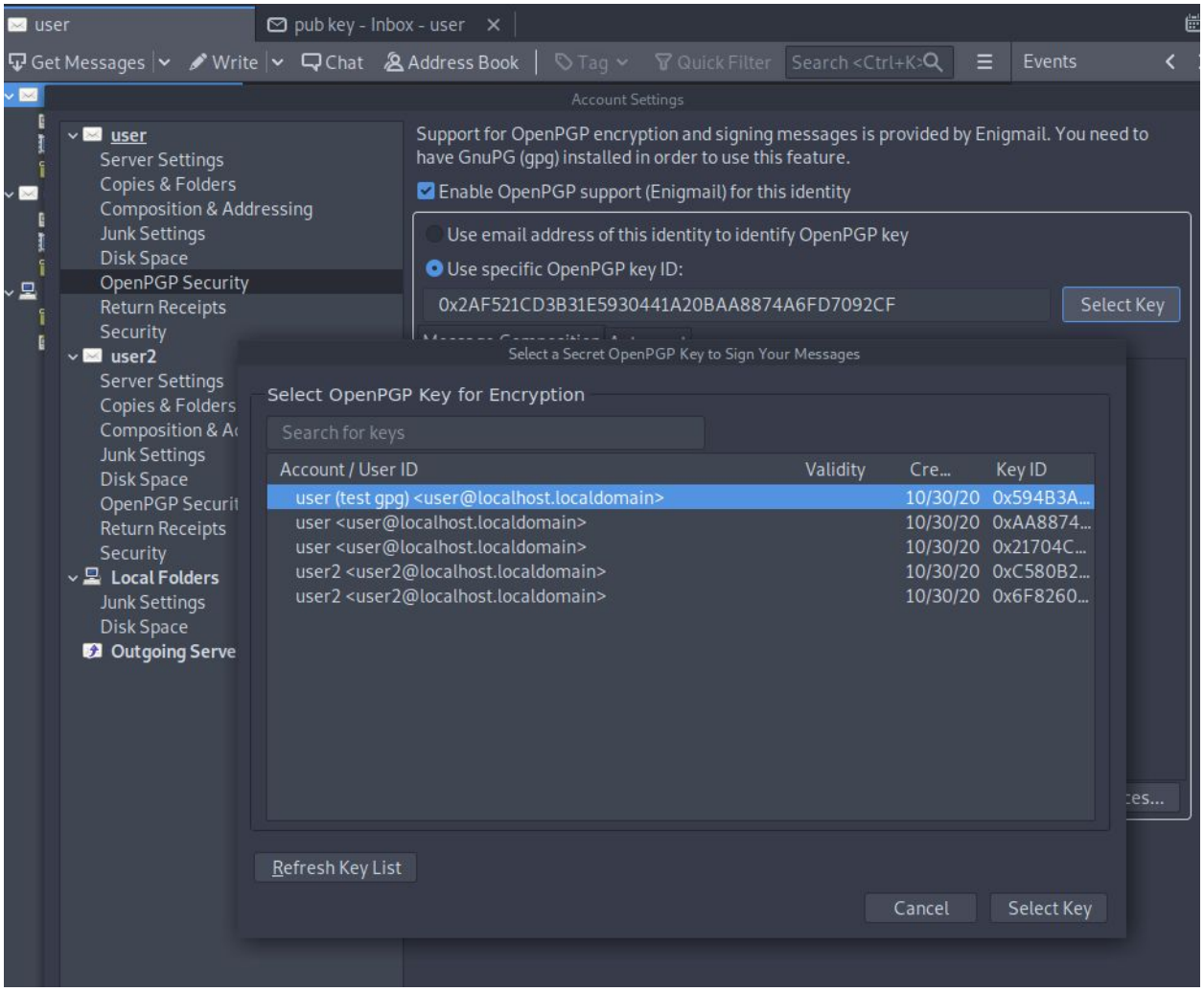
In order to create my keyset with GnuPG, i execute the command *gpg --full-generate-key* . this will create a pub key and private key associated to a specific user name and email. To create the keyset i used the default parameters (RSA 4096 bit long).

```
┌─[user@parrot-virtual]─[~]
└──╼ $gpg --full-generate-key
pg (GnuPG) 2.2.20; Copyright (C) 2020 Free Software Foundation, Inc.
his is free software: you are free to change and redistribute it.
here is NO WARRANTY, to the extent permitted by law.

lease select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
our selection? 1
SA keys may be between 1024 and 4096 bits long.
hat keysize do you want? (4096)
equested keysize is 4096 bits
lease specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
ey is valid for? (0) 10
ey expires at Mon 09 Nov 2020 09:06:47 GMT
s this correct? (y/N) y

nuPG needs to construct a user ID to identify your key.

eal name: user
mail address: user@localhost.localdomain
omment: test gpg
ou selected this USER-ID:
    "user (test gpg) <user@localhost.localdomain>"

hange (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

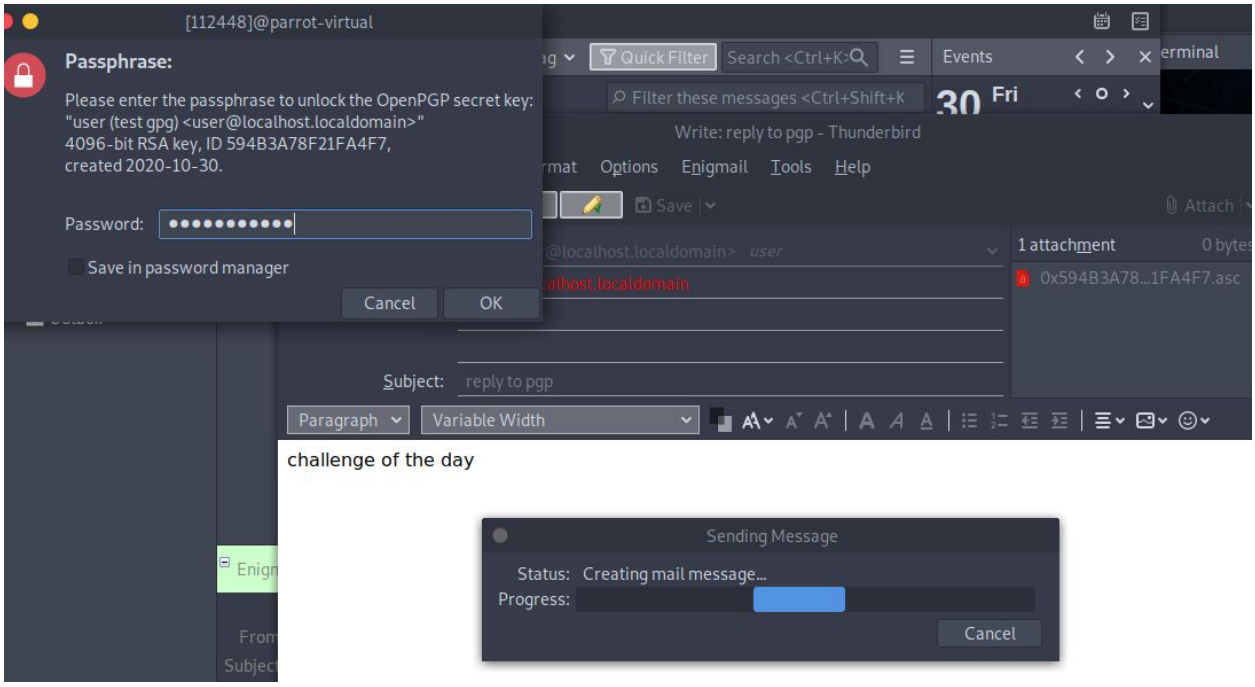
```
You selected this USER-ID:
    "user (test gpg) <user@localhost.localdomain>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key 594B3A78F21FA4F7 marked as ultimately trusted
gpg: revocation certificate stored as '/home/user/.gnupg/openpgp-revocs.d/8C658ABAE08D351B391EC1D5594B3A78F21FA4F7.rev'
public and secret key created and signed.

pub   rsa4096 2020-10-30 [SC] [expires: 2020-11-09]
      8C658ABAE08D351B391EC1D5594B3A78F21FA4F7
uid                      user (test gpg) <user@localhost.localdomain>
sub   rsa4096 2020-10-30 [E] [expires: 2020-11-09]

┌─[user@parrot-virtual]─[~]
└──╼ $
```

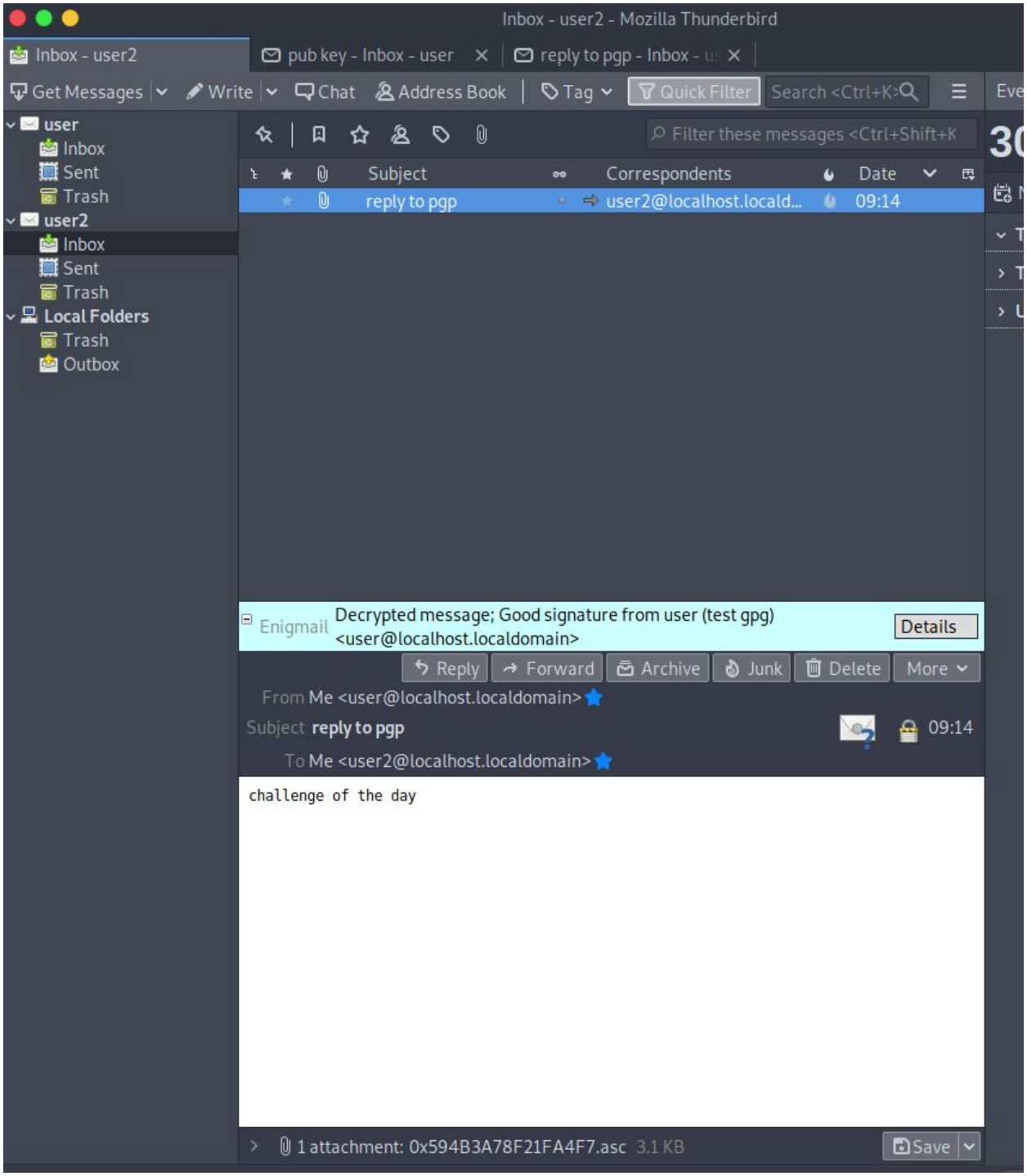
when i open the key management tool of enigmail, the keyset is already recognized and i can select that key to encrypt the future messages as shown in the screenshots below.





When i want to attach the pub key in the message, i will choose the newly created public key instead of the one used earlier.


[112448]@parrot-virtual
Passphrase:
Please enter the passphrase to unlock the OpenPGP secret key:
"user (test gpg) <user@localhost.localdomain>"
4096-bit RSA key, ID 594B3A78F21FA4F7,
created 2020-10-30.
Password:
Save in password manager
Cancel
OK
Quick Filter
Search <Ctrl+K>
Events
Filter these messages <Ctrl+Shift+K
30 Fri
Write: reply to pgp - Thunderbird
Options
Enigmail
Tools
Help
Save
Attach
1 attachment
0x594B3A78...1FA4F7.asc
Subject:
reply to pgp
Paragraph
Variable Width
challenge of the day
Sending Message
Status: Creating mail message...
Progress:
Cancel


Inbox - user2 - Mozilla Thunderbird
Inbox - user2
pub key - Inbox - user
reply to pgp - Inbox - us
Get Messages
Write
Chat
Address Book
Tag
Quick Filter
Search <Ctrl+K>
user
Inbox
Sent
Trash
user2
Inbox
Sent
Trash
Local Folders
Trash
Outbox
Filter these messages <Ctrl+Shift+K
Subject
Correspondents
Date
reply to pgp
user2@localhost.locald...
09:14
Enigmail
Decrypted message; Good signature from user (test gpg) <user@localhost.localdomain>
Details
Reply
Forward
Archive
Junk
Delete
More
From Me <user@localhost.localdomain>
Subject reply to pgp
09:14
To Me <user2@localhost.localdomain>
challenge of the day
1 attachment: 0x594B3A78F21FA4F7.asc 3.1 KB
Save