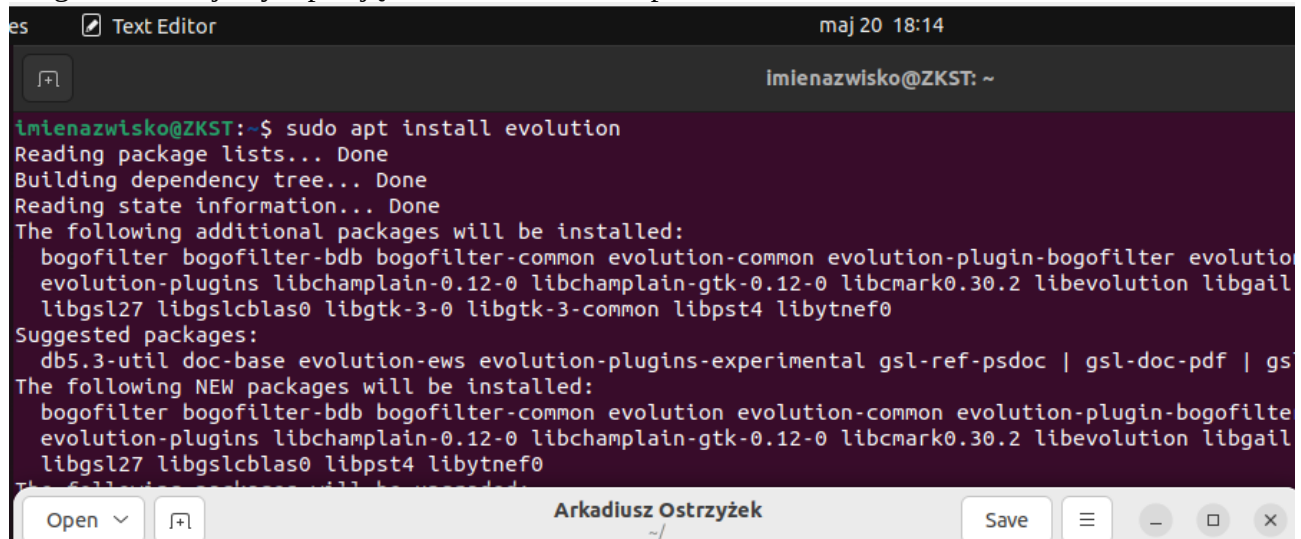


Zadanie 1

1. Zainstalować program do poczty elektronicznej np. Evolution;

Program instalujemy wpisując w terminalu `sudo apt install evolution`.



```
es Text Editor maj 20 18:14
imienazwisko@ZKST: ~
imienazwisko@ZKST:~$ sudo apt install evolution
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bogofilter bogofilter-bdb bogofilter-common evolution-common evolution-plugin-bogofilter evolution-plugins libchamplain-0.12-0 libchamplain-gtk-0.12-0 libcmack0.30.2 libevolution libgail
  libgsl27 libgslcblas0 libgtk-3-0 libgtk-3-common libpst4 libytnef0
Suggested packages:
  db5.3-util doc-base evolution-ews evolution-plugins-experimental gsl-ref-psdoc | gsl-doc-pdf | gs
The following NEW packages will be installed:
  bogofilter bogofilter-bdb bogofilter-common evolution evolution-common evolution-plugin-bogofilter evolution-plugins libchamplain-0.12-0 libchamplain-gtk-0.12-0 libcmack0.30.2 libevolution libgail
  libgsl27 libgslcblas0 libpst4 libytnef0
The following packages will be upgraded:
```

2. Skonfigurować obsługę dowolnego konta poczty elektronicznej;

W gui wpisujemy dane do konta, po czym program sam rozpoznaje potrzebne protokoły do nawiązania połączenia. Podajemy login i hasło i uwierzytelniamy się na platformie.

Identity



Welcome

Restore from Backup

Identity

Receiving Email

Sending Email

Account Summary

Done

Please enter your name and email address below. The "optional" fields below do not need to be filled in, unless you wish to include this information in email you send.

Required Information

Full Name: Arkadiusz Ostrzyżek

Email Address: arkadiusz.ostrzyzek@gmail.com|

Optional Information

Reply-To:

Organization:

Aliases:

Add

Edit

Remove

☒ Look up mail server details based on the entered e-mail address

Cancel

Back

Next

Evolutionmaj 20 18:15

Account Summary

Welcome

Restore from Backup

Identity

Receiving Email

Receiving Options

Sending Email

Account Summary

Done

This is a summary of the settings which will be used to access your mail.

Account Information

Name:

The above name will be used to identify this account.
Use for example, "Work" or "Personal".

Personal Details

Full Name: Arkadiusz Ostrzyżek
Email Address: arkadiusz.ostrzyzek@gmail.com

Receiving	Sending
Server Type: imapx	smtp
Server: imap.gmail.com	smtp.gmail.com
Username: arkadiusz.ostrzyzek@gmail.com	arkadiusz.ostrzyzek@gmail.com
Security: TLS	TLS

Google Features

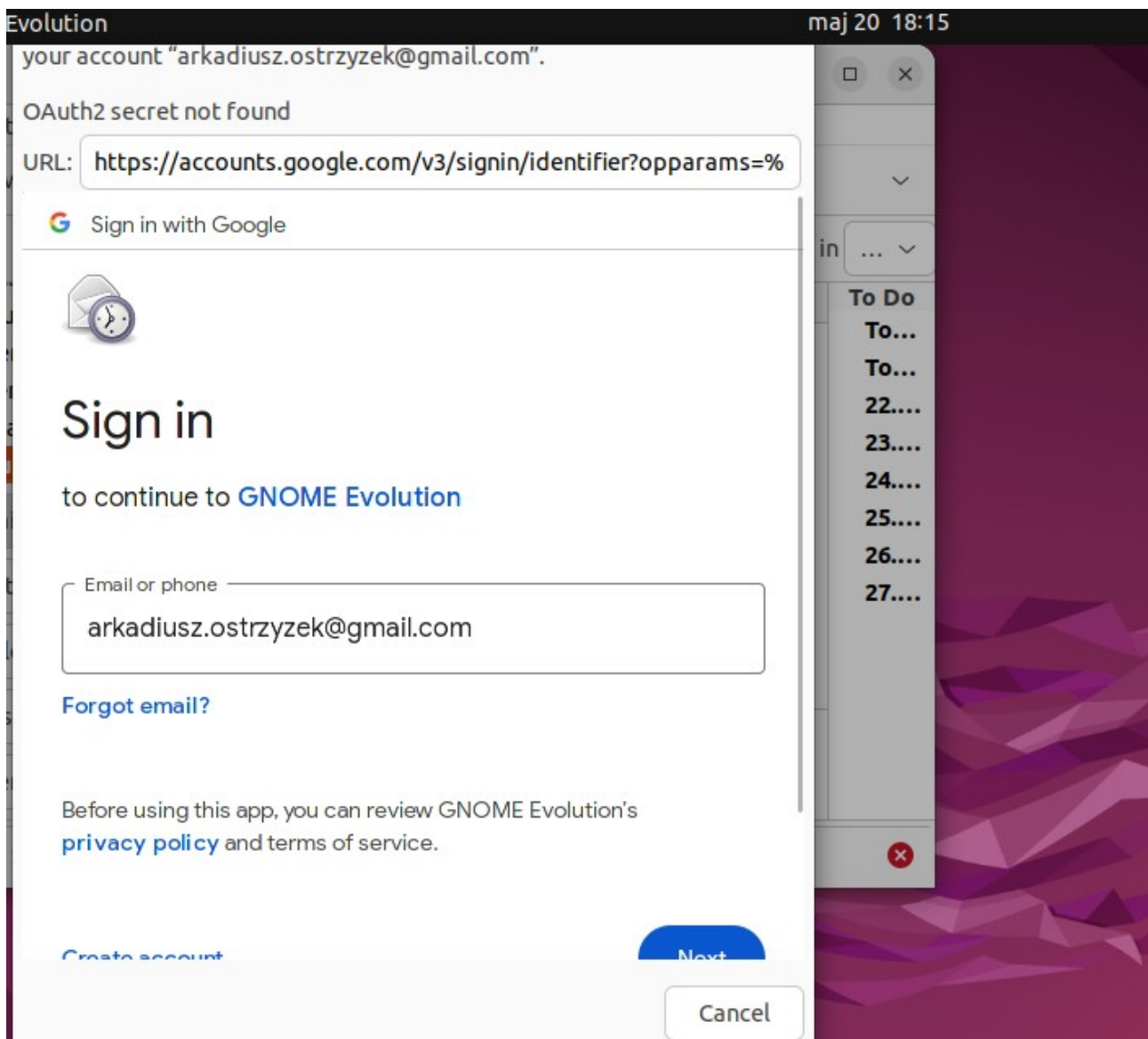
☒ Add Calendar to this account
☒ Add Contacts to this account

You may need to enable [IMAP access](#) and [Calendars to synchronize](#)

Cancel

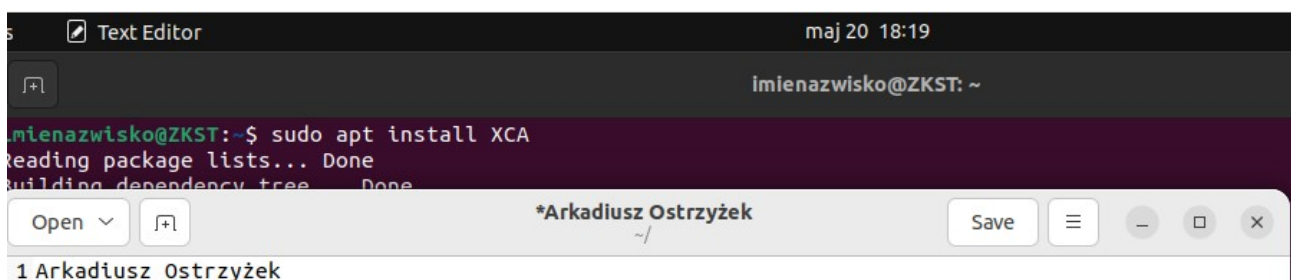
Back

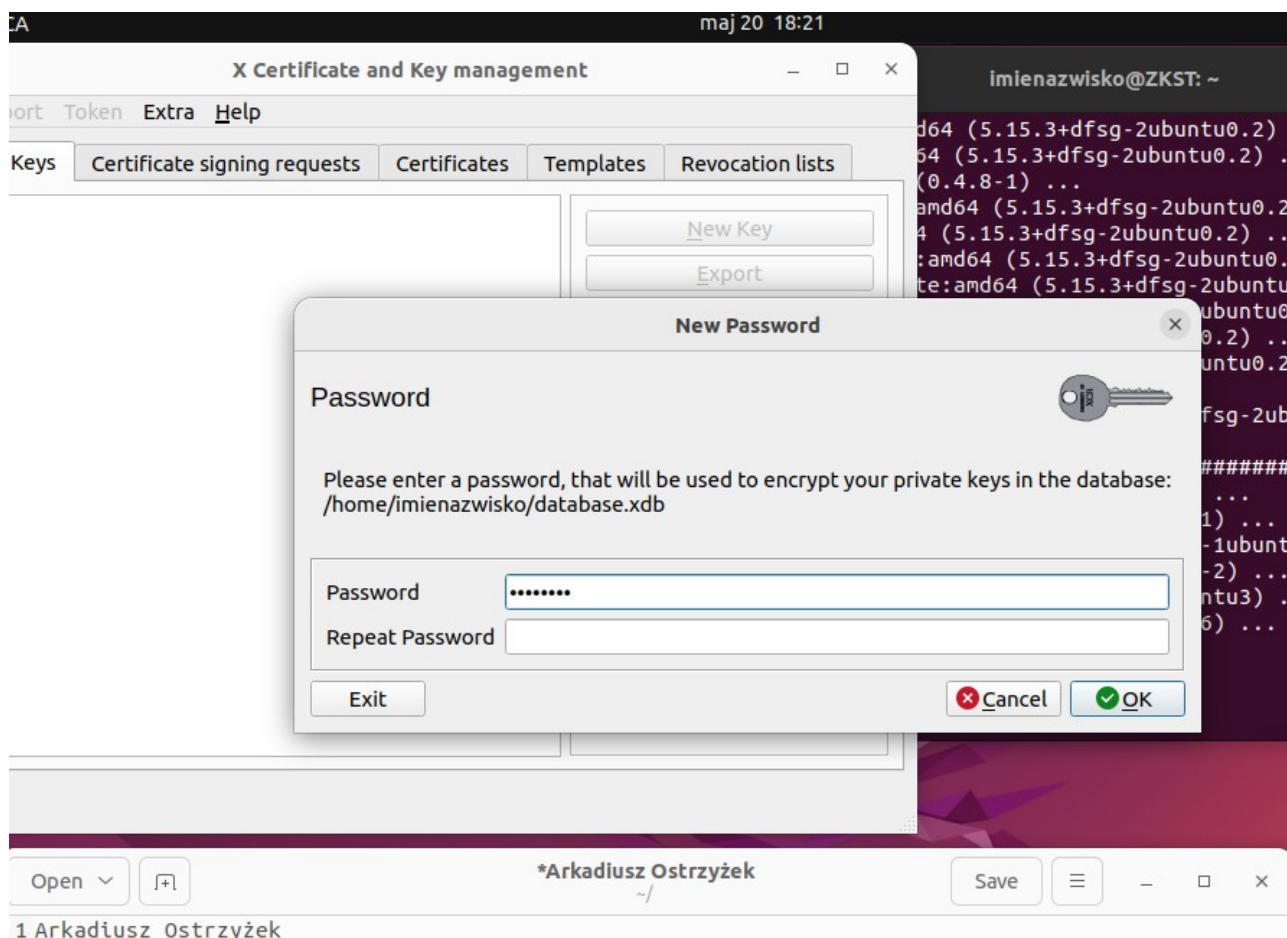
Next

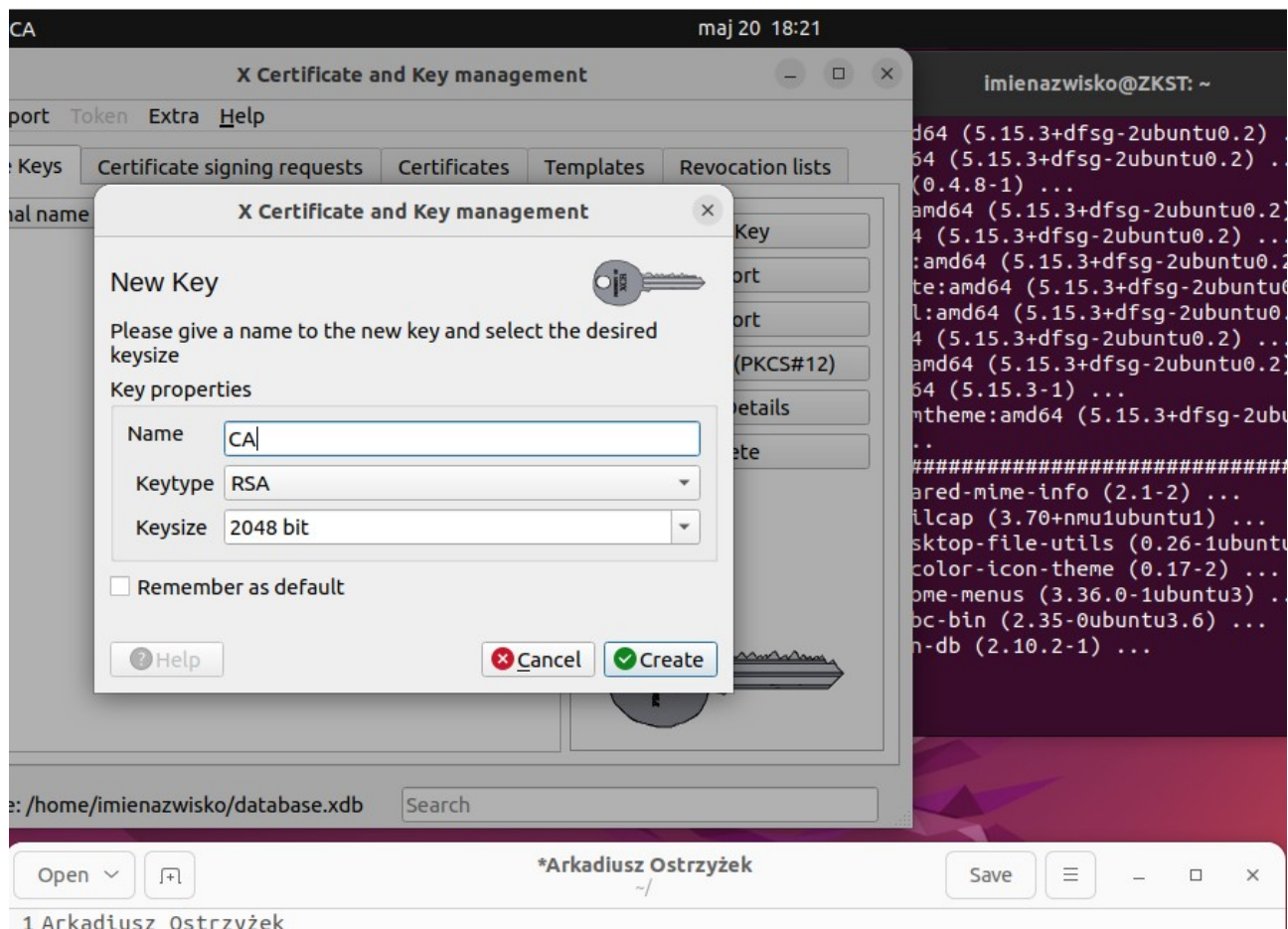


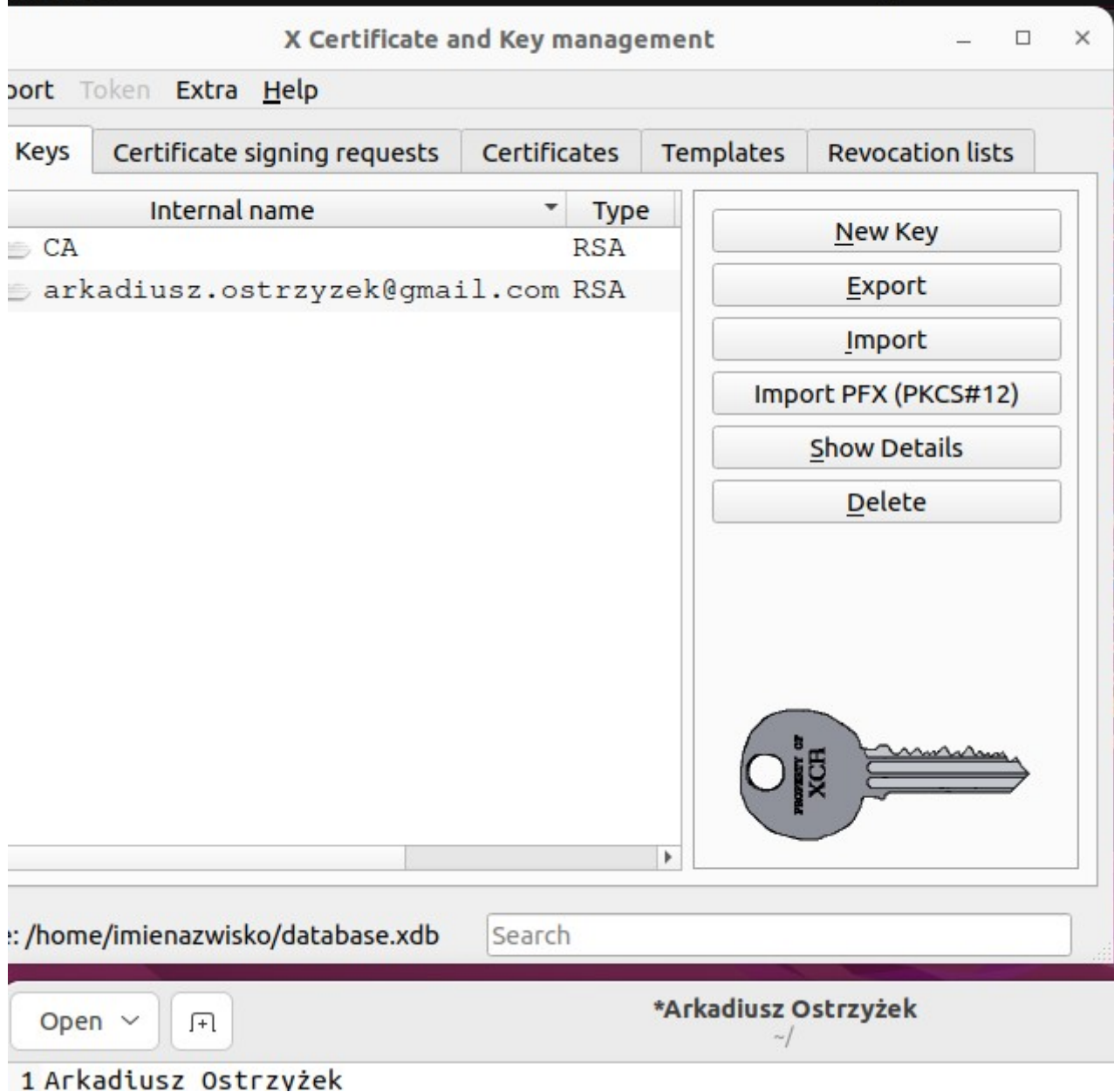
3. Wygenerować certyfikat dla tożsamości zgodnej ze skonfigurowanym adresem poczty elektronicznej

W aplikacji XCA tworzymy najpierw klucze prywatne dla użytkownika i CA, po czym ich certyfikaty z odpowiednimi uprawnieniami









Tworzenie certyfikatów:
Do CA używamy template CA.

XCA maj 20 18:23

X Certificate and Key management

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced Comment

Internal Name [CA]

Distinguished name

countryName organizationalUnitName

stateOrProvinceName commonName

localityName emailAddress

organizationName

Type	Content
------	---------

Add

Delete

Private key

CA (RSA:2048 bit)

☐ Used keys too

Generate a new key

Help Cancel OK

Open [+] *Arkadiusz Ostrzyżek Save

1 Arkadiusz Ostrzyżek

XCA maj 20 18:24

X Certificate and Key management

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced Comment

Signing request

☐ Sign this Certificate signing request

☒ Copy extensions from the request

☐ Modify subject of the request

Signing

☒ Create a self signed certificate

☐ Use this Certificate for signing

Signature algorithm

SHA 256

Template for the new certificate

[default] CA

Apply extensions Apply subject Apply all

Help Cancel OK

Open [+] *Arkadiusz Ostrzyżek Save

1 Arkadiusz Ostrzyżek

Dla użytkownika:

5 XCA maj 20 18:25

X Certificate and Key management

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced Comment

Internal Name

Distinguished name

countryName	<input type="text"/>	organizationalUnitName	<input type="text"/>
stateOrProvinceName	<input type="text"/>	commonName	<input type="text" value="us.ostrzyzek@gmail.com"/>
localityName	<input type="text"/>	emailAddress	<input type="text" value="us.ostrzyzek@gmail.com"/>
organizationName	<input type="text"/>		

Type	Content	
		Add
		Delete

Private key

☐ Used keys too


Open Save

XCA

maj 20 18:25

X Certificate and Key management

Create x509 Certificate



Source

Subject

Extensions

Key usage

Netscape

Advanced

Comment

09v3 Basic Constraints

Type

End Entity

Path length

☐ Critical

Key identifier

☐ X509v3 Subject Key Identifier

☐ X509v3 Authority Key Identifier

Validity

Not before

2024-05-20 16:24 GMT

Not after

2025-05-20 16:24 GMT

Time range

365

Days

Apply

☐ Midnight☐ Local time☐ No well-defined expiration

09v3 Subject Alternative Name

Edit

09v3 Issuer Alternative Name

Edit

09v3 CRL Distribution Points

Edit

Authority Information Access

Edit

☐ OCSP Must Staple

Help

Cancel

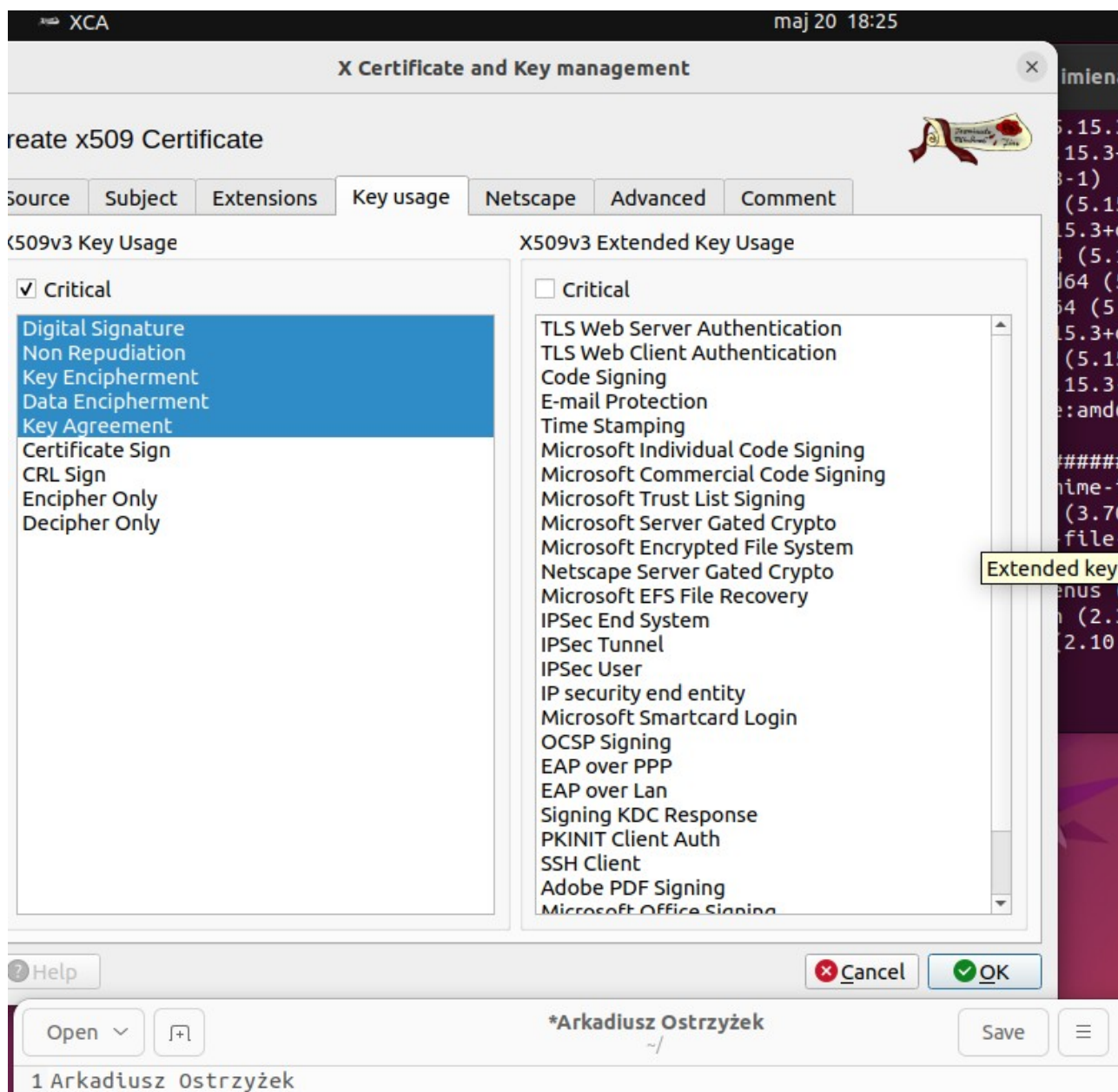
OK

Open

*Arkadiusz Ostrzyżek

Save

1 Arkadiusz Ostrzyżek



Text Editor

maj 20 18:26

X Certificate and Key management

FileImportTokenExtraHelp

Private KeysCertificate signing requestsCertificatesTemplatesRevocation lists

Internal name

CA

arkadiusz.ostrzyzek@gmail.com arkadi

New Certificate

Export

Import


Show Details

Delete

Import PKCS#12

Import PKCS#7

Plain View



Database: /home/imienazwisko/database.xdbSearch

Open

+l

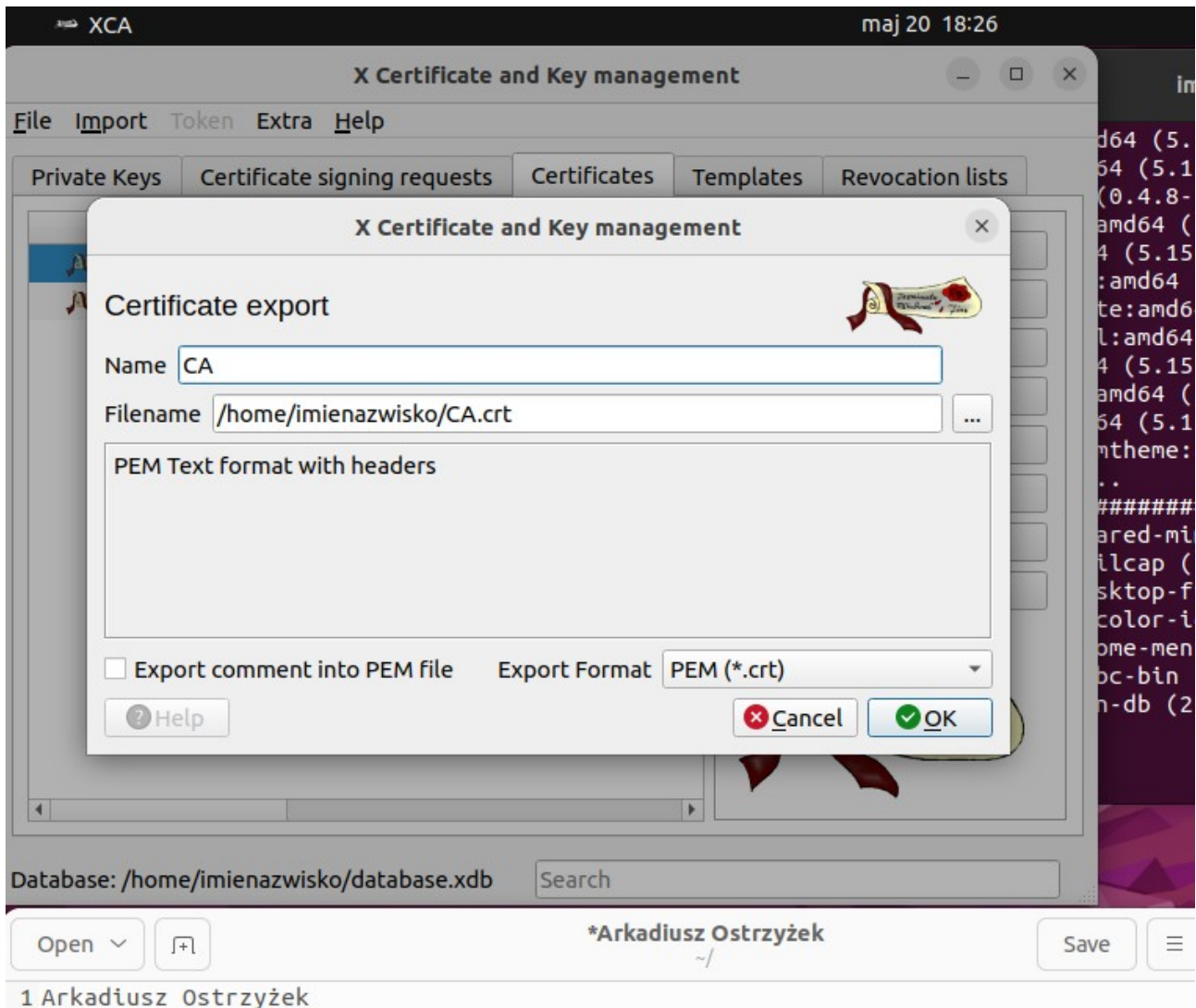
*Arkadiusz Ostrzyżek

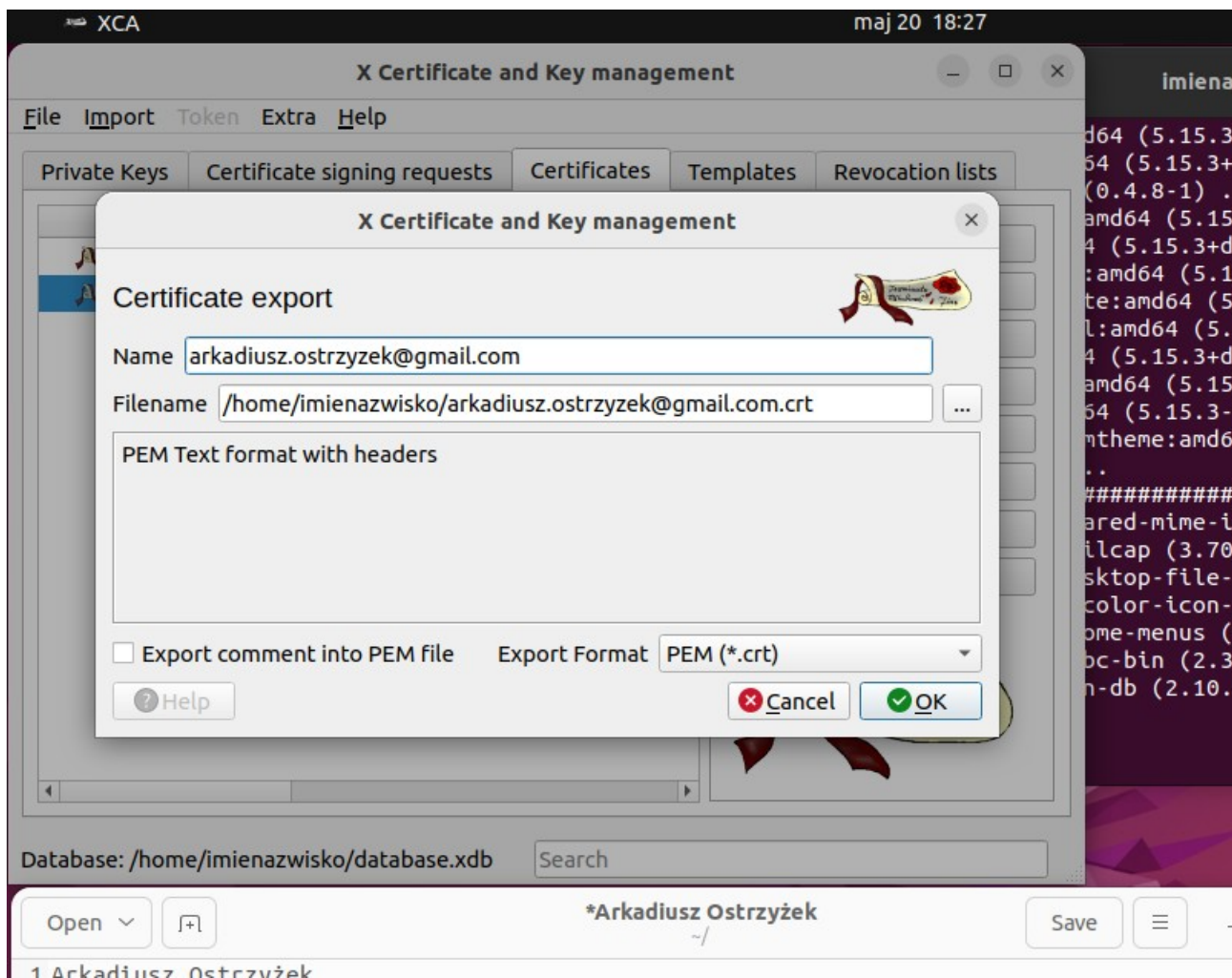
Save

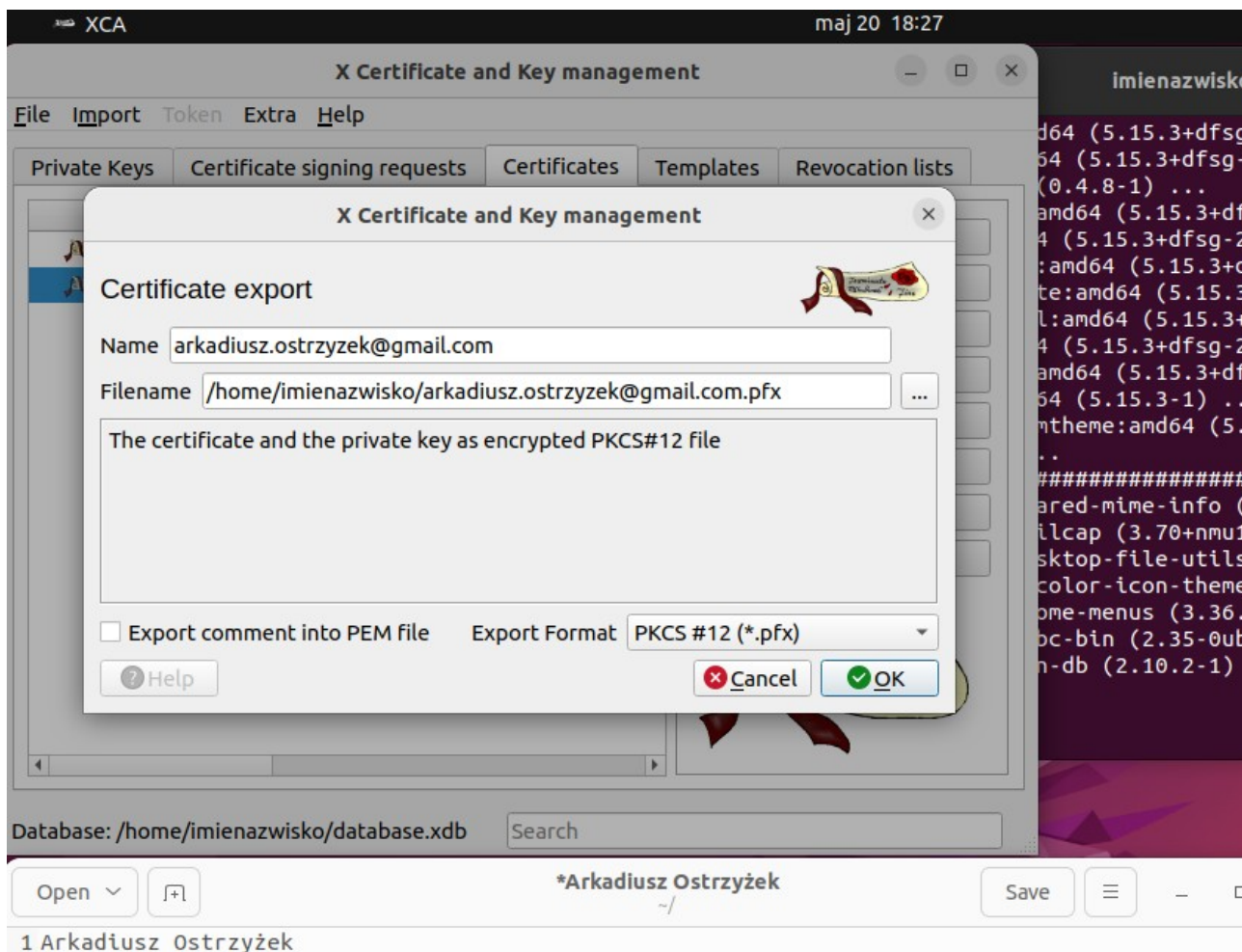
≡

1 Arkadiusz Ostrzyżek

Następnie eksportujemy klucze dla CA i usr.







4. Wysłać wiadomość podpisaną, zaszyfrowaną oraz podpisaną i zaszyfrowaną do siebie;

Najpierw musimy dodać certyfikat nasz i CA. Następnie wiadomość wysyłamy tak jak zazwyczaj, tylko z zaznaczonymi opcjami szyfrowania i podpisu S/MIME.

maj 20 18:28

Evolution Preferences

Your Certificates

Contact Certificates

Authorities

Mail

You have certificates from these organizations that identify you:

Select a certificate to import...

Recent

Home

Documents

Downloads

Music

Pictures

Videos

Other Locations

< imienazwisko >

Name	Size	Type	Modified
Desktop			12 lut
Documents			12 lut
Downloads			12 lut
Music			12 lut
Pictures			12 lut
Public			12 lut
snap			12 lut
Templates			12 lut
Videos			12 lut
arkadiusz.ostrzyzek@gmail.com.crt	1,2 kB	X.509 Certificate	18:27
arkadiusz.ostrzyzek@gmail.com.pfx	2,7 kB	PKCS#12 certificate bundle	18:27
CA.crt	1,1 kB	X.509 Certificate	18:26

maj 20 18:29

Evolution Preferences

Your Certificates

Contact Certificates

Authorities

Mail

You have certificates on file that identify these certificate authorities:

Select a certificate to import...

Recent

Home

Documents

Downloads

Music

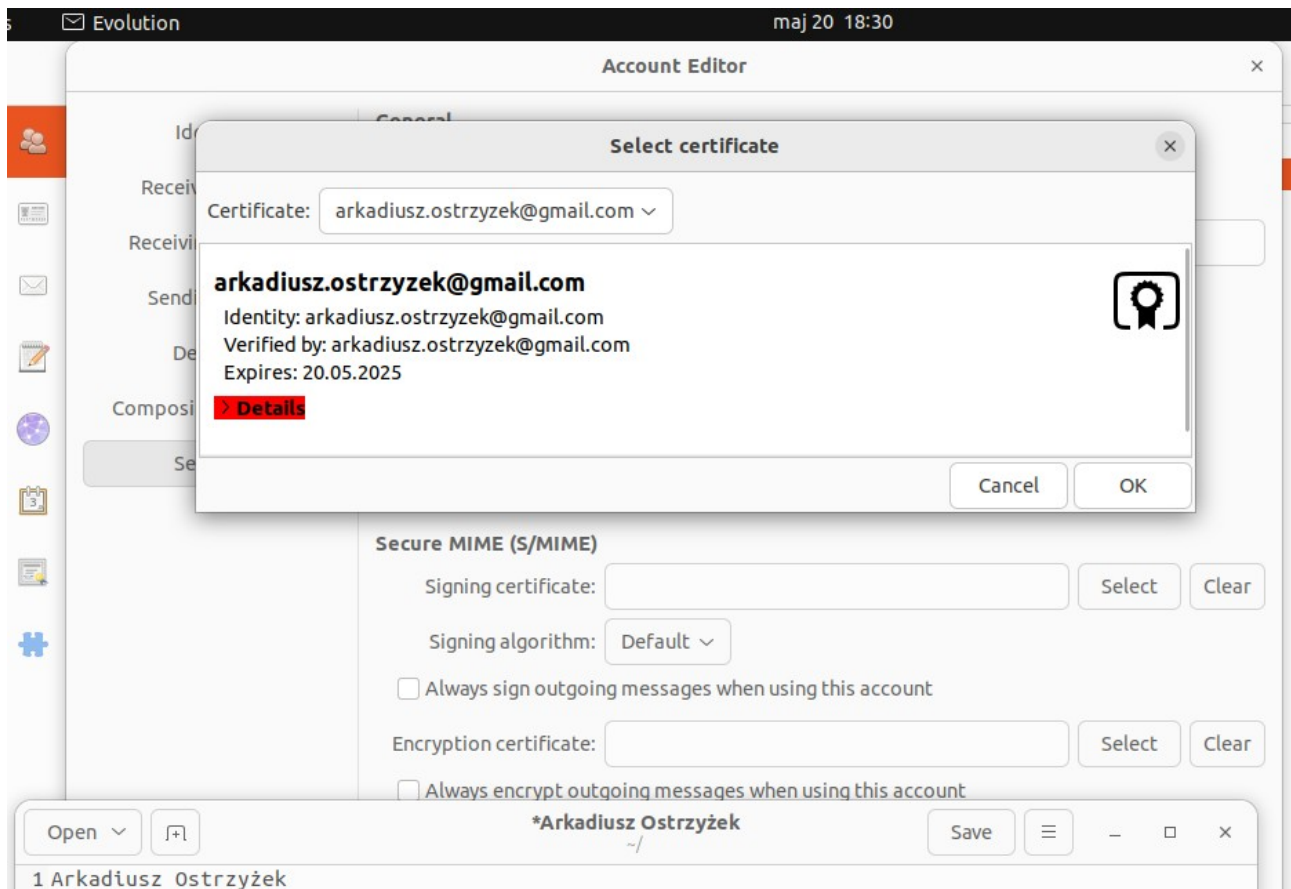
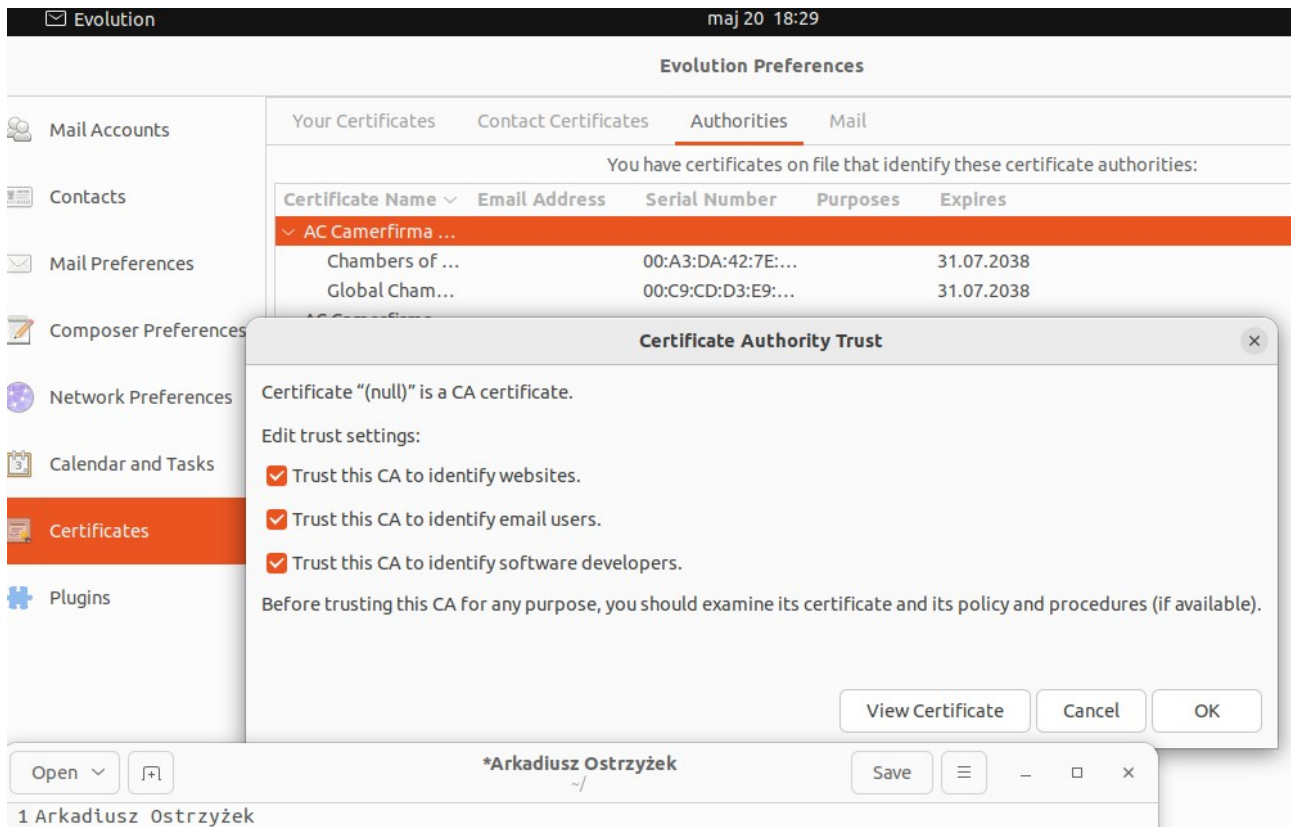
Pictures

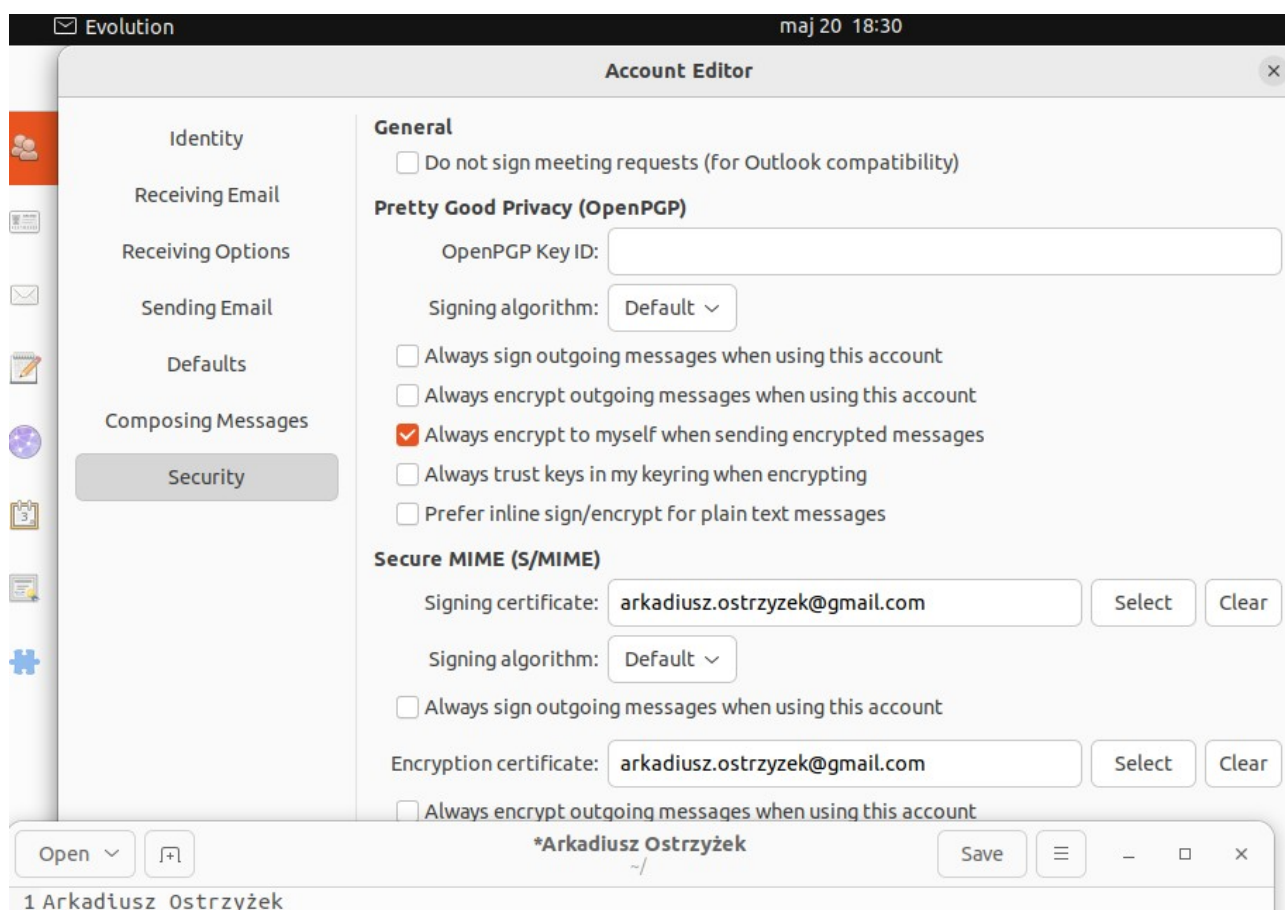
Videos

Other Locations

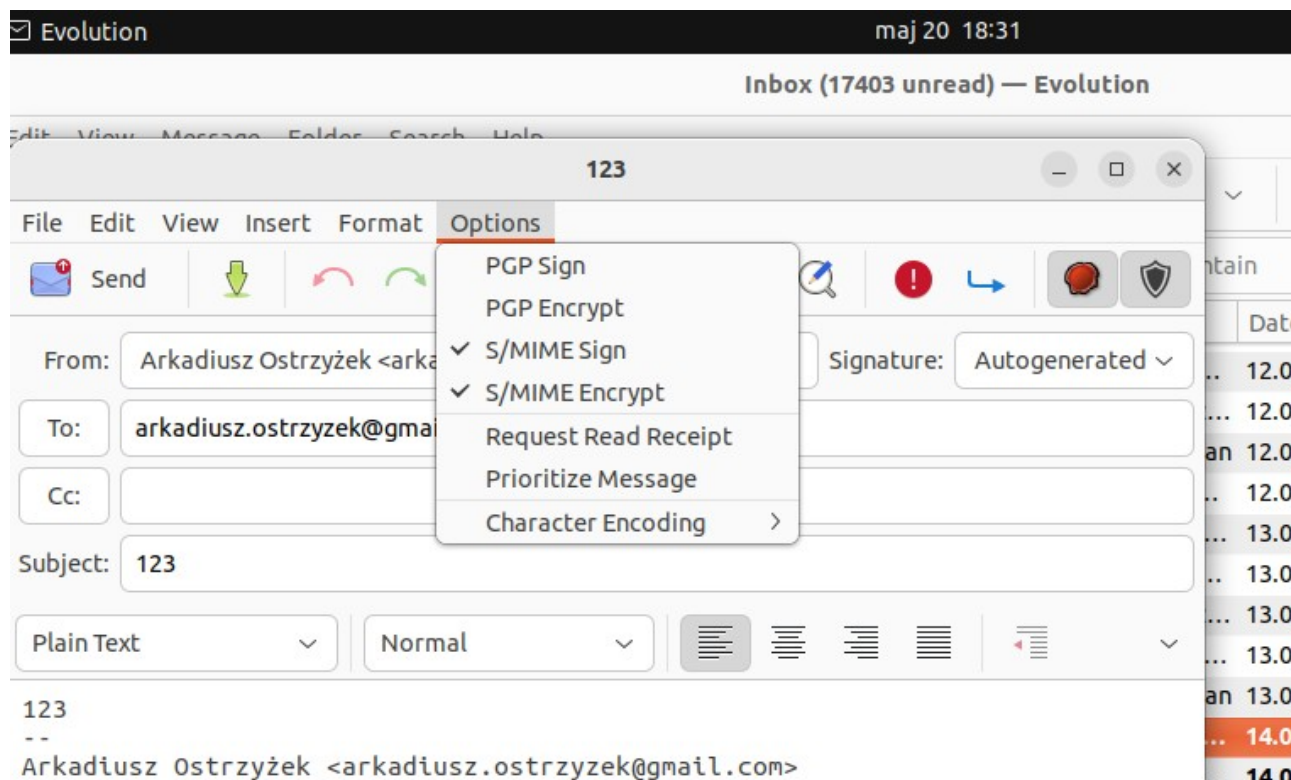
< imienazwisko >

Name	Size	Type	Modified
Desktop			12 lut
Documents			12 lut
Downloads			12 lut
Music			12 lut
Pictures			12 lut
Public			12 lut
snap			12 lut
Templates			12 lut
Videos			12 lut
arkadiusz.ostrzyzek@gmail.com.crt	1,2 kB	X.509 Certificate	18:27
CA.crt	1,1 kB	X.509 Certificate	18:26

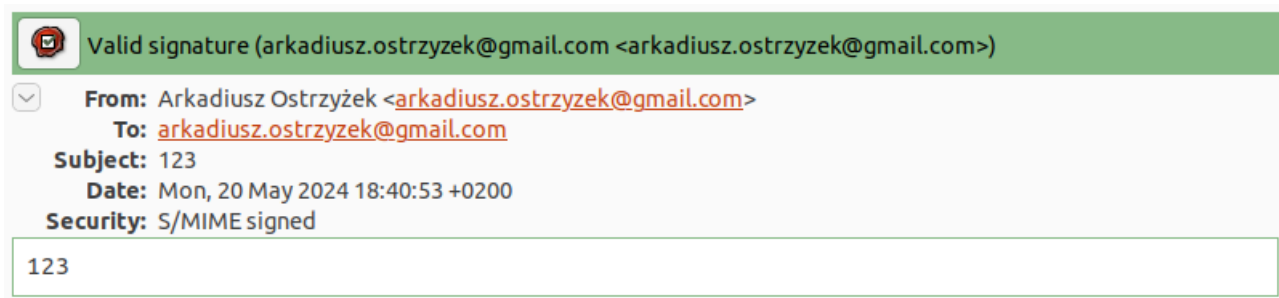




Po dodatniu, wysłałyśmy wiadomości:



W tym momencie pojawia się błąd -8190, który nie jest udokumentowany i nie występował w trakcie przygotowywania się do zajęć. Możliwe jest tylko wysłanie podpisanej wiadomości.



5. Wymienić się certyfikatami wymaganymi do szyfrowanej komunikacji z inną osobą realizującą zajęcia;

Wymieniamy się certyfikatami wymaganymi do szyfrowanej komunikacji wysyłając je sobie emailiem.

6. Wymienić się wiadomościami podpisanymi, zaszyfrowanymi oraz podpisanymi i zaszyfrowanymi z tą osobą i zweryfikować podpis;

Najpierw dodajemy certyfikat osoby, do której chcemy wysłać zaszyfrowaną wiadomość. Następnie wysyłamy sobie wiadomości tak samo jak w podpunkcie 4.

7. Zweryfikować zawartość wiadomości zaszyfrowanych lub podpisanych dostępnych na serwerze poczty poprzez interfejs www.

Logujemy się do poczty w przeglądarce, gdzie możemy zobaczyć, że wiadomości nie da się odczytać. Widoczne są jako zaszyfrowane pliki.

Zadanie 2

1. Zainstalować inny program do poczty elektronicznej np. Thunderbird;

Program instalujemy wpisując w terminalu `sudo apt install thunderbird`.


```
maj 20 19:00

mienazwisko@ZKST:~$ arkadiusz ostrzyzek
arkadiusz: command not found
mienazwisko@ZKST:~$ sudo apt install thunderbird
[sudo] password for imienazwisko:
Reading package lists... Done
Building dependency tree... Done
```

2. Skonfigurować obsługę tego samego konta poczty elektronicznej i certyfikatu jak dla programu np. Thunderbird;

Najpierw musimy dodać certyfikat nasz i CA. Następnie wiadomość wysyłamy tak jak zazwyczaj, tylko z zaznaczonymi opcjami szyfrowania i podpisu S/MIME.

Thunderbird Mail maj 20 19:01

Account Setup × Thunderbird Privacy Notice - ×

Set Up Your Existing Email Address


To use your current email address fill in your credentials.
Thunderbird will automatically search for a working and recommended server configuration.

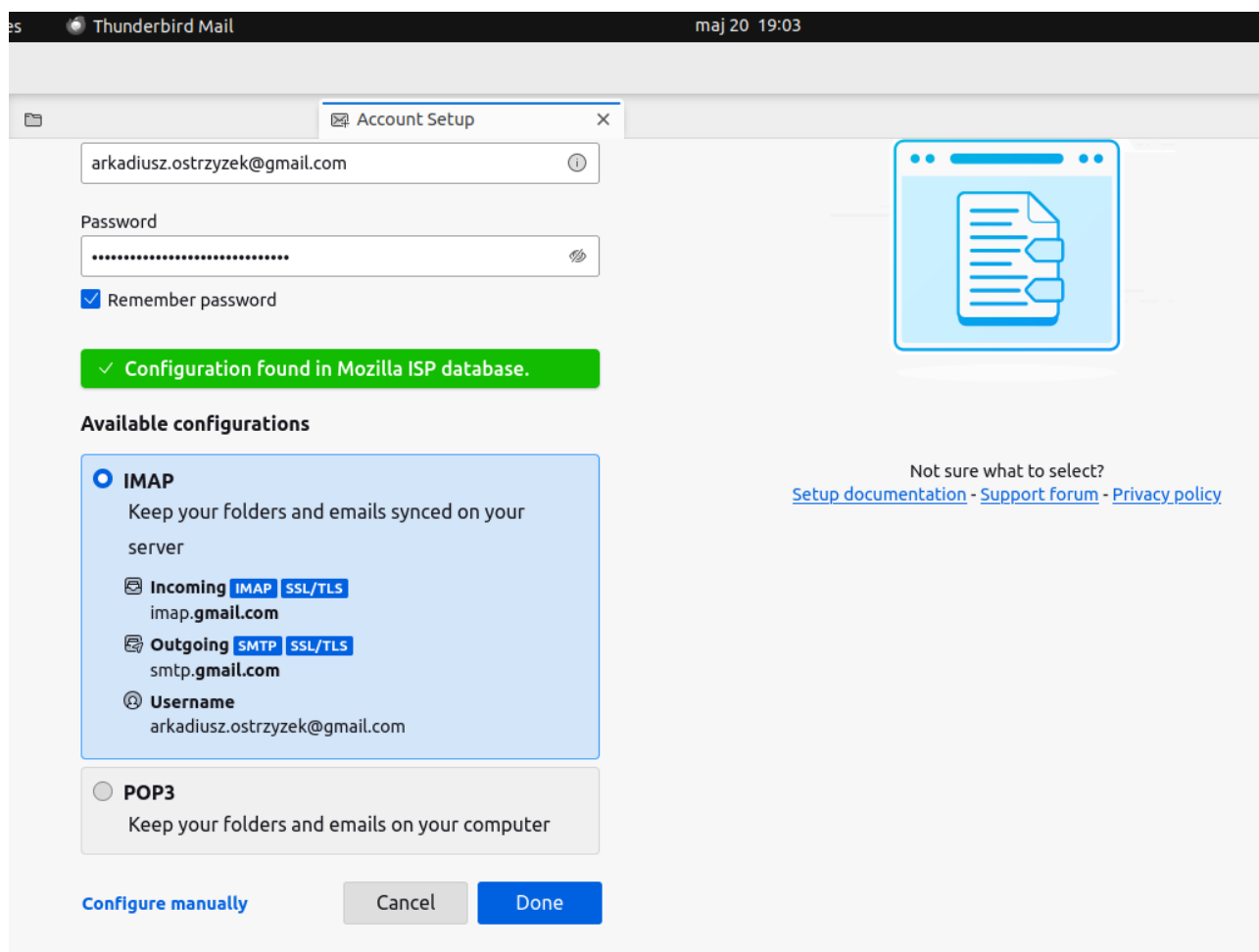
Your full name

Email address

Password

☒ Remember password





3. Wymienić się wiadomościami podpisanymi, zaszyfrowanymi oraz podpisanymi i zaszyfrowanymi z inną osobą i zweryfikować podpis;

Najpierw dodajemy certyfikat osoby, do której chcemy wysłać zaszyfrowaną wiadomość. Następnie wysyłamy sobie wiadomości z zaznaczeniem opcji szyfrowania i podpisu S/MIME.

4. Zweryfikować interoperacyjność standardu pomiędzy różnymi programami obsługującymi pocztę elektroniczną.

Wiadomości widoczne są w obu programach, ze sprawdzonym podpisem i zdeszyfrowane.