

ZKST

WEB OF TRUST

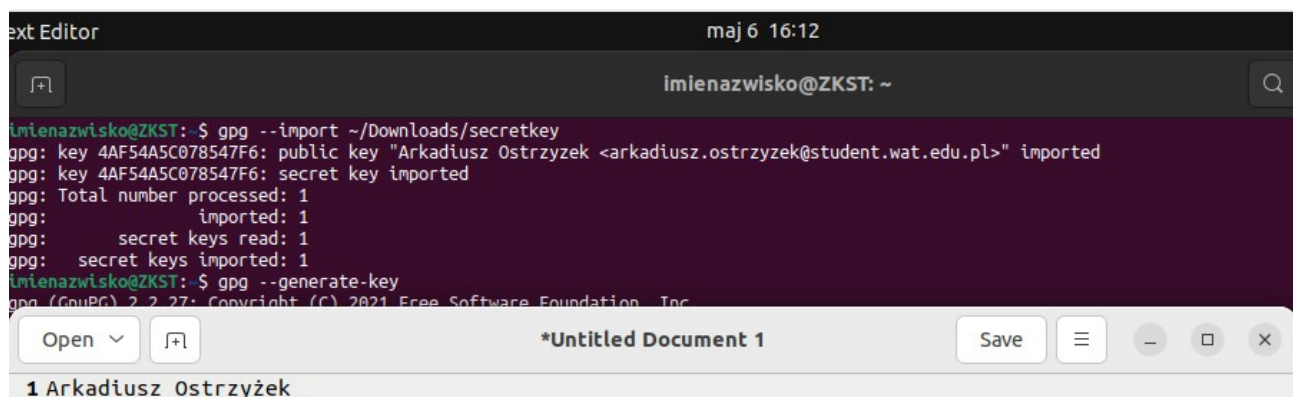
Arkadiusz Ostrzyżek

Zadanie 1

1.1

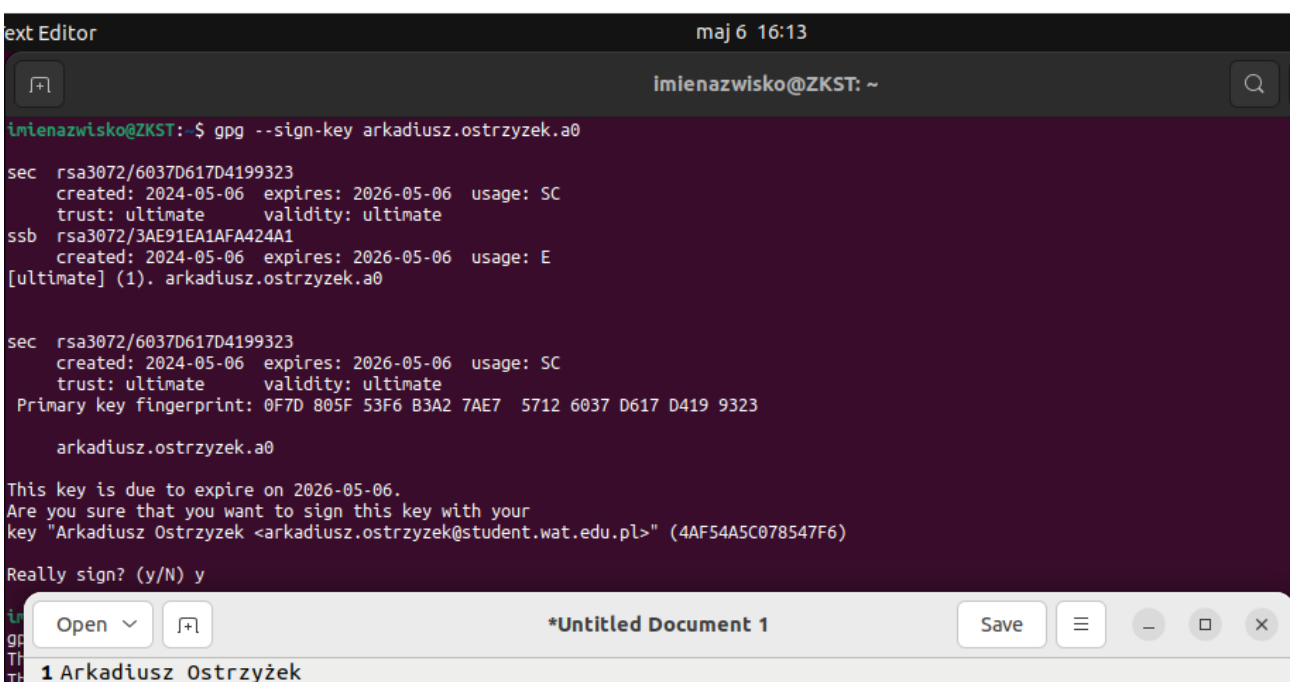
1.1.1

Najpierw importujemy klucz. Następnie tworzymy podpisany przez klucz użytkownika utworzony w trakcie ZKST-LAB-05. Wykorzystujemy `gpg --generate-key` oraz `--sign-key`, aby stworzyć i podpisać klucz.



The screenshot shows a terminal window titled "maj 6 16:12" with the prompt "imienazwisko@ZKST: ~". The user enters the command `gpg --import ~/Downloads/secretkey`. The output shows that a public key for "Arkadiusz Ostrzyżek" and a corresponding secret key were imported successfully. Then, the user enters `gpg --generate-key`, which generates a new key pair. The terminal output shows the details of the generated keys: a primary RSA key (rsa3072/6037D617D4199323) and a subkey (rsa3072/3AE91EA1AFA424A1), both with ultimate trust and validity.

```
imienazwisko@ZKST:~$ gpg --import ~/Downloads/secretkey
gpg: key 4AF54A5C078547F6: public key "Arkadiusz Ostrzyżek <arkadiusz.ostrzyzek@student.wat.edu.pl>" imported
gpg: key 4AF54A5C078547F6: secret key imported
gpg: Total number processed: 1
gpg:      imported: 1
gpg:      secret keys read: 1
gpg:      secret keys imported: 1
imienazwisko@ZKST:~$ gpg --generate-key
gpg (GnuPG) 2.2.27: Copyright (C) 2021 Free Software Foundation, Inc.
```



The screenshot shows a terminal window titled "maj 6 16:13" with the prompt "imienazwisko@ZKST: ~". The user enters the command `gpg --sign-key arkadiusz.ostrzyzek.a0`. The output shows the details of the key being signed: a primary RSA key (rsa3072/6037D617D4199323) and a subkey (rsa3072/3AE91EA1AFA424A1). The user is prompted to confirm the signing, and they respond with 'y'. The terminal output shows the key being signed and the resulting signature file `arkadiusz.ostrzyzek.a0`.

```
imienazwisko@ZKST:~$ gpg --sign-key arkadiusz.ostrzyzek.a0
sec  rsa3072/6037D617D4199323
    created: 2024-05-06  expires: 2026-05-06  usage: SC
    trust: ultimate      validity: ultimate
ssb  rsa3072/3AE91EA1AFA424A1
    created: 2024-05-06  expires: 2026-05-06  usage: E
[ultimate] (1). arkadiusz.ostrzyzek.a0

sec  rsa3072/6037D617D4199323
    created: 2024-05-06  expires: 2026-05-06  usage: SC
    trust: ultimate      validity: ultimate
Primary key fingerprint: 0F7D 805F 53F6 B3A2 7AE7  5712 6037 D617 D419 9323

    arkadiusz.ostrzyzek.a0

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "Arkadiusz Ostrzyżek <arkadiusz.ostrzyzek@student.wat.edu.pl>" (4AF54A5C078547F6)
Really sign? (y/N) y
```

```
Text Editor                                maj 6 16:14
[+]                                       imienazwisko@ZKST: ~

imienazwisko@ZKST:~$ gpg --generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

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

Real name: arkadiusz.ostrzyzek.a0
Email address: arkadiusz.ostrzyzek.a0
Not a valid email address
Email address:
You selected this USER-ID:
    "arkadiusz.ostrzyzek.a0"

Change (N)ame, (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 6037D617D4199323 marked as ultimately trusted
gpg: directory '/home/imienazwisko/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/0F7D805F53F6B3A27AE757126037D617D4199323.rev'
public and secret key created and signed.

pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     0F7D805F53F6B3A27AE757126037D617D4199323
uid                               arkadiusz.ostrzyzek.a0
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]

Open  ▾  [+]                                *Untitled Document 1                                Save  ≡  −  □  ×

1 Arkadiusz Ostrzyzek|
```

1.1.2

Tak samo jak w 1.1 tworzymy i podpisujemy klucz używając klucza użytkownika utworzonego w trakcie ZKST-LAB-05;

```
Text Editor                                maj 6 16:12
[+]                                       imienazwisko@ZKST: ~

arkadiusz.ostrzyzek.a0

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>" (4AF54A5C078547F6)

Really sign? (y/N) y

imienazwisko@ZKST:~$ gpg --generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

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

Real name: arkadiusz.ostrzyzek.a1
Email address:
You selected this USER-ID:
"arkadiusz.ostrzyzek.a1"

Change (N)ame, (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 7C7B63A434AC19C9 marked as ultimately trusted
gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/42C75184A8553426BC1F70B67C7B63A434AC19C9.rev'
public and secret key created and signed.

pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     42C75184A8553426BC1F70B67C7B63A434AC19C9
uid                               arkadiusz.ostrzyzek.a1
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]

imienazwisko@ZKST:~$
```

Open [v] [F1] *Untitled Document 1 Save [≡] [–] [□] [×]

L Arkadiusz Ostrzyzek

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 7C7B63A434AC19C9 marked as ultimately trusted
gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/42C75184A8553426BC1F70B67C7B63A434AC19C9.rev'
public and secret key created and signed.

```
pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     42C75184A8553426BC1F70B67C7B63A434AC19C9
uid                arkadiusz.ostrzyzek.a1
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]
```

imienazwisko@ZKST:~\$ gpg --sign-key arkadiusz.ostrzyzek.a1

```
sec  rsa3072/7C7B63A434AC19C9
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate    validity: ultimate
ssb  rsa3072/8E65EA0C25DA66CB
     created: 2024-05-06  expires: 2026-05-06  usage: E
[ultimate] (1). arkadiusz.ostrzyzek.a1
```

```
sec  rsa3072/7C7B63A434AC19C9
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate    validity: ultimate
Primary key fingerprint: 42C7 5184 A855 3426 BC1F 70B6 7C7B 63A4 34AC 19C9

     arkadiusz.ostrzyzek.a1
```

This key is due to expire on 2026-05-06.

Are you sure that you want to sign this key with your
key "Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>" (4AF54A5C078547F6)

Really sign? (y/N) y

imienazwisko@ZKST:~\$

Open



*Untitled Document 1

Save



1 Arkadiusz Ostrzyzek

1.1.3

Wykonujemy to samo co w 1.2.

```
Text Editor                                maj 6 16:17
imienazwisko@ZKST: ~

Are you sure that you want to sign this key with your
key "Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>" (4AF54A5C078547F6)

Really sign? (y/N) y

imienazwisko@ZKST:~$ gpg --generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

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

Real name: arkadiusz.ostrzyzek.a2
Email address:
You selected this USER-ID:
"arkadiusz.ostrzyzek.a2"

Change (N)ame, (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 F1A92EEA161150C6 marked as ultimately trusted
gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/F09DCCCA3456CF0492F6816AF1A92EEA161150C6.rev'
public and secret key created and signed.

pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     F09DCCCA3456CF0492F6816AF1A92EEA161150C6
uid                               arkadiusz.ostrzyzek.a2
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]
```

```
Text Editor                                maj 6 16:19
imienazwisko@ZKST: ~

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 F1A92EEA161150C6 marked as ultimately trusted
gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/F09DCCCA3456CF0492F6816AF1A92EEA161150C6.rev'
public and secret key created and signed.

pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     F09DCCCA3456CF0492F6816AF1A92EEA161150C6
uid                               arkadiusz.ostrzyzek.a2
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]

imienazwisko@ZKST:~$ gpg --sign-key arkadiusz.ostrzyzek.a2

sec  rsa3072/F1A92EEA161150C6
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/FADADB362AEE678F
     created: 2024-05-06  expires: 2026-05-06  usage: E
[ultimate] (1). arkadiusz.ostrzyzek.a2

sec  rsa3072/F1A92EEA161150C6
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
Primary key fingerprint: F09D CCA3 456C F049 2F68 16AF 1A92 EEA1 6115 0C6

     arkadiusz.ostrzyzek.a2

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>" (4AF54A5C078547F6)

Really sign? (y/N) y

Open  [icon] *Untitled Document 1 Save [icon] [icon] [icon] [icon]
1 Arkadiusz Ostrzyzek
```

1.1.4

Tworzymy klucz podpisany przez imie.nazwisko.a0 i imie.nazwisko.a1;

```
Text Editor                                maj 6 16:22
imienazwisko@ZKST: ~

Really sign? (y/N) y

imienazwisko@ZKST:~$ gpg --generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

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

Real name: arkadiusz.ostrzyzek.b0
Email address:
You selected this USER-ID:
    "arkadiusz.ostrzyzek.b0"

Change (N)ame, (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 5C3C91222A6E20E4 marked as ultimately trusted
gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/4880064668BF3F028201A17A5C3C91222A6E20E4.rev'
public and secret key created and signed.

pub   rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
      4880064668BF3F028201A17A5C3C91222A6E20E4
uid           arkadiusz.ostrzyzek.b0
sub   rsa3072 2024-05-06 [E] [expires: 2026-05-06]
```

```
Text Editor                                maj 6 16:23
imienazwisko@ZKST: ~

uid           4880064668BF3F028201A17A5C3C91222A6E20E4
uid           arkadiusz.ostrzyzek.b0
sub   rsa3072 2024-05-06 [E] [expires: 2026-05-06]

imienazwisko@ZKST:~$ gpg --default-key arkadiusz.ostrzyzek.a0 --sign-key arkadiusz.ostrzyzek.b0

sec   rsa3072/5C3C91222A6E20E4
      created: 2024-05-06  expires: 2026-05-06  usage: SC
      trust: ultimate      validity: ultimate
ssb   rsa3072/5347B87716F18AE5
      created: 2024-05-06  expires: 2026-05-06  usage: E
[ultimate] (1). arkadiusz.ostrzyzek.b0

gpg: using "arkadiusz.ostrzyzek.a0" as default secret key for signing

sec   rsa3072/5C3C91222A6E20E4
      created: 2024-05-06  expires: 2026-05-06  usage: SC
      trust: ultimate      validity: ultimate
Primary key fingerprint: 4880 0646 68BF 3F02 8201  A17A 5C3C 9122 2A6E 20E4

      arkadiusz.ostrzyzek.b0

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.a0" (6037D617D4199323)

Really sign? (y/N) y
```



```
imienazwisko@ZKST:~$ gpg --default-key arkadiusz.ostrzyzek.a1 --sign-key arkadiusz.ostrzyzek.b0
```

```
sec  rsa3072/5C3C91222A6E20E4
    created: 2024-05-06  expires: 2026-05-06  usage: SC
    trust: ultimate      validity: ultimate
ssb  rsa3072/5347B87716F18AE5
    created: 2024-05-06  expires: 2026-05-06  usage: E
[ultimate] (1). arkadiusz.ostrzyzek.b0

gpg: using "arkadiusz.ostrzyzek.a1" as default secret key for signing

sec  rsa3072/5C3C91222A6E20E4
    created: 2024-05-06  expires: 2026-05-06  usage: SC
    trust: ultimate      validity: ultimate
Primary key fingerprint: 4880 0646 68BF 3F02 8201  A17A 5C3C 9122 2A6E 20E4

    arkadiusz.ostrzyzek.b0

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.a1" (7C7B63A434AC19C9)

Really sign? (y/N) y
```

Open ▾



*Untitled Document 1

Save



1 Arkadiusz Ostrzyżek

1.1.5

Tworzymy klucz podpisany przez imie.nazwisko.a0 i imie.nazwisko.a1 i imię.nazwisko.a2.

Text Editor

maj 6 16:26



imienazwisko@ZKST: ~



Change (N)ame, (E)mail, or (O)key/(Q)uit? 0

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: agent_genkey failed: Operation cancelled

Key generation failed: Operation cancelled

```
imienazwisko@ZKST:~$ gpg --generate-key
```

gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.

This is free software: you are free to change and redistribute it.

There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

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

Real name: arkadiusz.ostrzyzek.b1

Email address:

You selected this USER-ID:

"arkadiusz.ostrzyzek.b1"

Change (N)ame, (E)mail, or (O)key/(Q)uit? 0

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 9BA84A1C5DCA2945 marked as ultimately trusted

gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/B68DE37055363E027DD173B39BA84A1C5DCA2945.rev'

public and secret key created and signed.

```
pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     B68DE37055363E027DD173B39BA84A1C5DCA2945
uid                               arkadiusz.ostrzyzek.b1
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]
```

```
imienazwisko@ZKST:~$
```

Open ▾



*Untitled Document 1

Save



1 Arkadiusz Ostrzyżek

```
Text Editor                                maj 6 16:28
imienazwisko@ZKST: ~

uid          arkadiusz.ostrzyzek.b1
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]

imienazwisko@ZKST:~$ gpg --default-key arkadiusz.ostrzyzek.a0 --sign-key arkadiusz.ostrzyzek.b1

sec  rsa3072/9BA84A1C5DCA2945
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/27E28FC82173B12B
     created: 2024-05-06  expires: 2026-05-06  usage: E
[ultimate] (1). arkadiusz.ostrzyzek.b1

gpg: using "arkadiusz.ostrzyzek.a0" as default secret key for signing

sec  rsa3072/9BA84A1C5DCA2945
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
Primary key fingerprint: B68D E370 5536 3E02 7DD1  73B3 9BA8 4A1C 5DCA 2945

     arkadiusz.ostrzyzek.b1

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.a0" (6037D617D4199323)

Really sign? (y/N) y

Open  [icon] *Untitled Document 1 Save [icon] [icon] [icon] [icon]
1 Arkadiusz Ostrzyzek
```

```
Text Editor                                maj 6 16:29
imienazwisko@ZKST: ~

Really sign? (y/N) y

imienazwisko@ZKST:~$ gpg --default-key arkadiusz.ostrzyzek.a1 --sign-key arkadiusz.ostrzyzek.b1

sec  rsa3072/9BA84A1C5DCA2945
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/27E28FC82173B12B
     created: 2024-05-06  expires: 2026-05-06  usage: E
[ultimate] (1). arkadiusz.ostrzyzek.b1

gpg: using "arkadiusz.ostrzyzek.a1" as default secret key for signing

sec  rsa3072/9BA84A1C5DCA2945
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
Primary key fingerprint: B68D E370 5536 3E02 7DD1  73B3 9BA8 4A1C 5DCA 2945

     arkadiusz.ostrzyzek.b1

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.a1" (7C7B63A434AC19C9)

Really sign? (y/N) y

Open  [icon] *Untitled Document 1 Save [icon] [icon] [icon] [icon]
1 Arkadiusz Ostrzyzek
```




```
gpg: using "arkadiusz.ostrzyzek.a1" as default secret key for signing

sec  rsa3072/9BA84A1C5DCA2945
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
Primary key fingerprint: B68D E370 5536 3E02 7DD1  73B3 9BA8 4A1C 5DCA 2945

     arkadiusz.ostrzyzek.b1

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.a1" (7C7B63A434AC19C9)

Really sign? (y/N) y

imienazwisko@ZKST:~$ gpg --default-key arkadiusz.ostrzyzek.a2 --sign-key arkadiusz.ostrzyzek.b1

sec  rsa3072/9BA84A1C5DCA2945
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/27E28FC82173B12B
     created: 2024-05-06  expires: 2026-05-06  usage: E
[ultimate] (1). arkadiusz.ostrzyzek.b1

gpg: using "arkadiusz.ostrzyzek.a2" as default secret key for signing

sec  rsa3072/9BA84A1C5DCA2945
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
Primary key fingerprint: B68D E370 5536 3E02 7DD1  73B3 9BA8 4A1C 5DCA 2945

     arkadiusz.ostrzyzek.b1

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.a2" (F1A92EEA161150C6)

Really sign? (y/N) y
```

Open ▾



*Untitled Document 1

Save



1 Arkadiusz Ostrzyżek

1.1.6

Tworzymy imie.nazwisko.c0 - podpisany przez imie.nazwisko.b0 i imie.nazwisko.b1;

```
Text Editor                                maj 6 16:30
imienazwisko@ZKST: ~
arkadiusz.ostrzyzek.b1
This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.a2" (F1A92EEA161150C6)
Really sign? (y/N) y
imienazwisko@ZKST:~$ gpg --generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Note: Use "gpg --full-generate-key" for a full featured key generation dialog.
GnuPG needs to construct a user ID to identify your key.
Real name: arkadiusz.ostrzyzek.c0
Email address:
You selected this USER-ID:
"arkadiusz.ostrzyzek.c0"
Change (N)ame, (E)mail, or (O)key/(Q)uit? 0
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 A18FA6E03EDB9B89 marked as ultimately trusted
gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/6C883DF36AD06EEFFE472D61A18FA6E03EDB9B89.rev'
public and secret key created and signed.

pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     6C883DF36AD06EEFFE472D61A18FA6E03EDB9B89
uid                arkadiusz.ostrzyzek.c0
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]

imienazwisko@ZKST:~$
```

```
Text Editor                                maj 6 16:32
imienazwisko@ZKST: ~
public and secret key created and signed.

pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     6C883DF36AD06EEFFE472D61A18FA6E03EDB9B89
uid                arkadiusz.ostrzyzek.c0
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]

imienazwisko@ZKST:~$ gpg --default-key arkadiusz.ostrzyzek.b0 --sign-key arkadiusz.ostrzyzek.c0

sec  rsa3072/A18FA6E03EDB9B89
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/3A69836B385FB512
     created: 2024-05-06  expires: 2026-05-06  usage: E
[ultimate] (1). arkadiusz.ostrzyzek.c0

gpg: using "arkadiusz.ostrzyzek.b0" as default secret key for signing

sec  rsa3072/A18FA6E03EDB9B89
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
Primary key fingerprint: 6C88 3DF3 6AD0 6EEF FE47 2D61 A18F A6E0 3EDB 9B89
arkadiusz.ostrzyzek.c0

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.b0" (5C3C91222A6E20E4)
Really sign? (y/N) y
```

gpg: using "arkadiusz.ostrzyzek.b0" as default secret key for signing

```
sec  rsa3072/A18FA6E03EDB9B89
    created: 2024-05-06  expires: 2026-05-06  usage: SC
    trust: ultimate      validity: ultimate
Primary key fingerprint: 6C88 3DF3 6AD0 6EEF FE47  2D61 A18F A6E0 3EDB 9B89
```

arkadiusz.ostrzyzek.c0

This key is due to expire on 2026-05-06.

Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.b0" (5C3C91222A6E20E4)

Really sign? (y/N) y

```
Imienazwisko@ZKST:~$ gpg --default-key arkadiusz.ostrzyzek.b1 --sign-key arkadiusz.ostrzyzek.c0
```

```
sec  rsa3072/A18FA6E03EDB9B89
    created: 2024-05-06  expires: 2026-05-06  usage: SC
    trust: ultimate      validity: ultimate
ssb  rsa3072/3A69836B385FB512
    created: 2024-05-06  expires: 2026-05-06  usage: E
[ultimate] (1). arkadiusz.ostrzyzek.c0
```

gpg: using "arkadiusz.ostrzyzek.b1" as default secret key for signing

```
sec  rsa3072/A18FA6E03EDB9B89
    created: 2024-05-06  expires: 2026-05-06  usage: SC
    trust: ultimate      validity: ultimate
Primary key fingerprint: 6C88 3DF3 6AD0 6EEF FE47  2D61 A18F A6E0 3EDB 9B89
```

arkadiusz.ostrzyzek.c0

This key is due to expire on 2026-05-06.

Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.b1" (9BA84A1C5DCA2945)

Really sign? (y/N) y

Open



*Untitled Document 1

Save



1 Arkadiusz Ostrzyżek

1.1.7 Tworzymy imie.nazwisko.d0 - podpisany przez imie.nazwisko.c0;

```
Terminal maj 6 16:34
imienazwisko@ZKST: ~
arkadiusz.ostrzyzek.c0

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.b1" (9BA84A1C5DCA2945)

Really sign? (y/N) y

imienazwisko@ZKST:~$ gpg --generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

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

Real name: arkadiusz.ostrzyzek.d0
Email address:
You selected this USER-ID:
"arkadiusz.ostrzyzek.d0"

Change (N)ame, (E)mail, or (O)key/(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 1D29E0B88B102FF2 marked as ultimately trusted
gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/58043BD1B4C5917A0F87FF091D29E0B88B102FF2.rev'
public and secret key created and signed.

pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     58043BD1B4C5917A0F87FF091D29E0B88B102FF2
uid                arkadiusz.ostrzyzek.d0
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]

imienazwisko@ZKST:~$
```

Open ▾ [🔍] *Untitled Document 1 Save [≡] - □ ×

1 Arkadiusz Ostrzyżek

```
Terminal maj 6 16:35
imienazwisko@ZKST: ~
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 1D29E0B88B102FF2 marked as ultimately trusted
gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/58043BD1B4C5917A0F87FF091D29E0B88B102FF2.rev'
public and secret key created and signed.

pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     58043BD1B4C5917A0F87FF091D29E0B88B102FF2
uid                arkadiusz.ostrzyzek.d0
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]

imienazwisko@ZKST:~$ gpg --default-key arkadiusz.ostrzyzek.c0 --sign-key arkadiusz.ostrzyzek.d0

sec  rsa3072/1D29E0B88B102FF2
     created: 2024-05-06 expires: 2026-05-06 usage: SC
     trust: ultimate validity: ultimate
ssb  rsa3072/ABFC1EA0D1AD933F
     created: 2024-05-06 expires: 2026-05-06 usage: E
[ultimate] (1). arkadiusz.ostrzyzek.d0

gpg: using "arkadiusz.ostrzyzek.c0" as default secret key for signing

sec  rsa3072/1D29E0B88B102FF2
     created: 2024-05-06 expires: 2026-05-06 usage: SC
     trust: ultimate validity: ultimate
Primary key fingerprint: 5804 3BD1 B4C5 917A 0F87 FF09 1D29 E0B8 8B10 2FF2

     arkadiusz.ostrzyzek.d0

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.c0" (A18FA6E03EDB9B89)

Really sign? (y/N) y

imienazwisko@ZKST:~$
```

Open ▾ [🔍] *Untitled Document 1 Save [≡] - □ ×

1 Arkadiusz Ostrzyżek

1.1.8

Tworzymy imie.nazwisko.e0 - podpisany przez imie.nazwisko.d0;

```
Terminal maj 6 16:37
imienazwisko@ZKST: ~

key "arkadiusz.ostrzyzek.c0" (A18FA6E03EDB9B89)

Really sign? (y/N) y

imienazwisko@ZKST:~$ gpg --generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

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

Real name: arkadiusz.ostrzyzek.e0
Email address:
You selected this USER-ID:
"arkadiusz.ostrzyzek.e0"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? 0
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 A7AD3F1CB54949BB marked as ultimately trusted
gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/14D7D7DC7AFF8F9DB3ADFEF6A7AD3F1CB54949BB.rev'
public and secret key created and signed.

pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     14D7D7DC7AFF8F9DB3ADFEF6A7AD3F1CB54949BB
uid          arkadiusz.ostrzyzek.e0
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]

imienazwisko@ZKST:~$ gpg --default-key arkadiusz.ostrzyzek.d0 --sign-key arkadiusz.ostrzyzek.e0

sec  rsa3072/A7AD3F1CB54949BB
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
```

1 Arkadiusz Ostrzyżek

```
Terminal maj 6 16:37
imienazwisko@ZKST: ~

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 A7AD3F1CB54949BB marked as ultimately trusted
gpg: revocation certificate stored as '/home/imienazwisko/.gnupg/openpgp-revocs.d/14D7D7DC7AFF8F9DB3ADFEF6A7AD3F1CB54949BB.rev'
public and secret key created and signed.

pub  rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
     14D7D7DC7AFF8F9DB3ADFEF6A7AD3F1CB54949BB
uid          arkadiusz.ostrzyzek.e0
sub  rsa3072 2024-05-06 [E] [expires: 2026-05-06]

imienazwisko@ZKST:~$ gpg --default-key arkadiusz.ostrzyzek.d0 --sign-key arkadiusz.ostrzyzek.e0

sec  rsa3072/A7AD3F1CB54949BB
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/8435C1363F02188E
     created: 2024-05-06  expires: 2026-05-06  usage: E
[ultimate] (1). arkadiusz.ostrzyzek.e0

gpg: using "arkadiusz.ostrzyzek.d0" as default secret key for signing

sec  rsa3072/A7AD3F1CB54949BB
     created: 2024-05-06  expires: 2026-05-06  usage: SC
     trust: ultimate      validity: ultimate
Primary key fingerprint: 14D7 D7DC 7AFF 8F9D B3AD FEF6 A7AD 3F1C B549 49BB

arkadiusz.ostrzyzek.e0

This key is due to expire on 2026-05-06.
Are you sure that you want to sign this key with your
key "arkadiusz.ostrzyzek.d0" (1D29E0B88B102FF2)

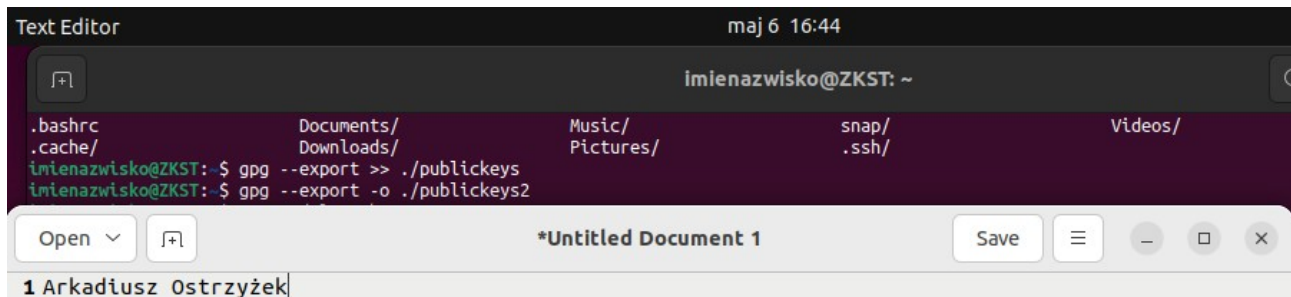
Really sign? (y/N) y

imienazwisko@ZKST:~$
```

1 Arkadiusz Ostrzyżek

1.2

Exportujemy wszystkie klucze.



The screenshot shows a terminal window titled "Text Editor" with the username "imienazwisko@ZKST: ~". The terminal displays the following commands and output:

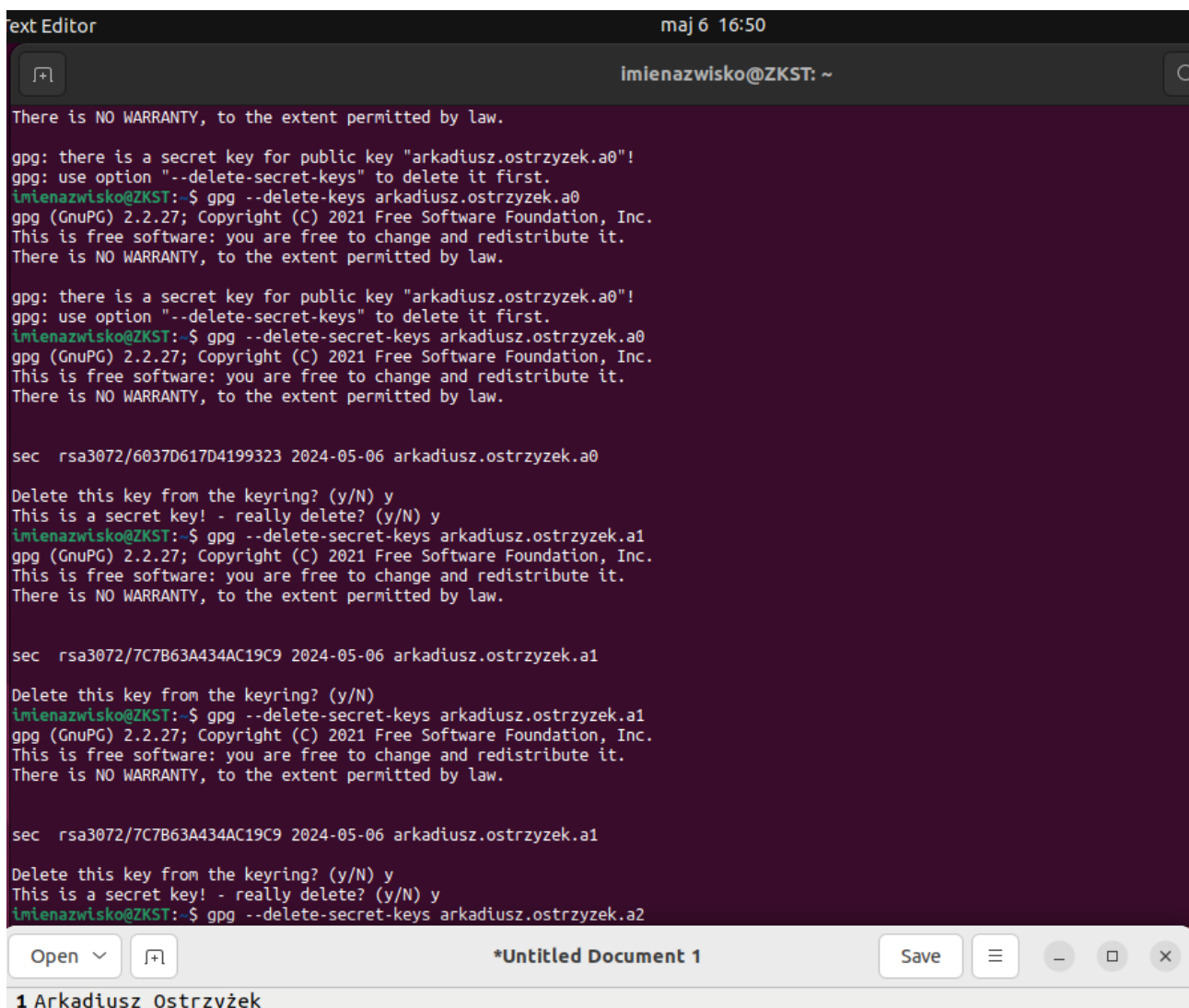
```
.bashrc Documents/ Music/ snap/ Videos/
.cache/ Downloads/ Pictures/ .ssh/
imienazwisko@ZKST:~$ gpg --export >> ./publickeys
imienazwisko@ZKST:~$ gpg --export -o ./publickeys2
```

Below the terminal window, there is a file editor interface for "Untitled Document 1". The file content is:

```
1 Arkadiusz Ostrzyżek
```

1.3

Usuwanie wszystkich kluczy



The screenshot shows a terminal window titled "Text Editor" with the username "imienazwisko@ZKST: ~". The terminal displays the following commands and output:

```
There is NO WARRANTY, to the extent permitted by law.

gpg: there is a secret key for public key "arkadiusz.ostrzyzek.a0"!
gpg: use option "--delete-secret-keys" to delete it first.
imienazwisko@ZKST:~$ gpg --delete-keys arkadiusz.ostrzyzek.a0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: there is a secret key for public key "arkadiusz.ostrzyzek.a0"!
gpg: use option "--delete-secret-keys" to delete it first.
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.a0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  rsa3072/6037D617D4199323 2024-05-06 arkadiusz.ostrzyzek.a0

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.a1
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  rsa3072/7C7B63A434AC19C9 2024-05-06 arkadiusz.ostrzyzek.a1

Delete this key from the keyring? (y/N)
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.a1
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  rsa3072/7C7B63A434AC19C9 2024-05-06 arkadiusz.ostrzyzek.a1

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.a2
```

Below the terminal window, there is a file editor interface for "Untitled Document 1". The file content is:

```
1 Arkadiusz Ostrzyżek
```



```
ext Editor                                maj 6 16:51
imienazwisko@ZKST: ~

imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.a1
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  rsa3072/7C7B63A434AC19C9 2024-05-06 arkadiusz.ostrzyzek.a1

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.a2
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  rsa3072/F1A92EEA161150C6 2024-05-06 arkadiusz.ostrzyzek.a2






Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.b0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  rsa3072/5C3C91222A6E20E4 2024-05-06 arkadiusz.ostrzyzek.b0

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.b1
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  rsa3072/9BA84A1C5DCA2945 2024-05-06 arkadiusz.ostrzyzek.b1

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.c0
```

Open ▾  *Untitled Document 1 Save    

1 Arkadiusz Ostrzyżek

```
terminal                                maj 6 16:51
imienazwisko@ZKST: ~

imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.c0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  rsa3072/A18FA6E03EDB9B89 2024-05-06 arkadiusz.ostrzyzek.c0

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.d0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  rsa3072/1D29E0B88B102FF2 2024-05-06 arkadiusz.ostrzyzek.d0






Delete this key from the keyring? (y/N)
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.d0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  rsa3072/1D29E0B88B102FF2 2024-05-06 arkadiusz.ostrzyzek.d0

Delete this key from the keyring? (y/N)
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.d0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  rsa3072/1D29E0B88B102FF2 2024-05-06 arkadiusz.ostrzyzek.d0

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
imienazwisko@ZKST:~$ gpg --delete-secret-keys arkadiusz.ostrzyzek.e0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
```

Open ▾  *Untitled Document 1 Save    

1 Arkadiusz Ostrzyżek

Terminalmaj 6 16:52

imienazwisko@ZKST: ~

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
imienazwisko@ZKST:~\$ gpg --delete-secret-keys arkadiusz.ostrzyzek.d0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec rsa3072/1D29E0B88B102FF2 2024-05-06 arkadiusz.ostrzyzek.d0

Delete this key from the keyring? (y/N)
imienazwisko@ZKST:~\$ gpg --delete-secret-keys arkadiusz.ostrzyzek.d0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec rsa3072/1D29E0B88B102FF2 2024-05-06 arkadiusz.ostrzyzek.d0

Delete this key from the keyring? (y/N)
imienazwisko@ZKST:~\$ gpg --delete-secret-keys arkadiusz.ostrzyzek.d0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec rsa3072/1D29E0B88B102FF2 2024-05-06 arkadiusz.ostrzyzek.d0

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
imienazwisko@ZKST:~\$ gpg --delete-secret-keys arkadiusz.ostrzyzek.e0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec rsa3072/A7AD3F1CB54949BB 2024-05-06 arkadiusz.ostrzyzek.e0

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
imienazwisko@ZKST:~\$

Open Untitled Document 1 Save

1 Arkadiusz Ostrzyżek

Text Editormaj 6 16:56

imienazwisko@ZKST: ~

.bash_history Desktop/ Music/ publickeys.txt Videos/
.bash_logout Documents/
.bashrc Downloads/ .profile .ssh/
.cache/ .gnupg/ Public/ .sudo_as_admin_successful
.config/ .local/ publickeys2 Templates/
imienazwisko@ZKST:~\$ gpg --delete-keys arkadiusz.ostrzyzek.a0 arkadiusz.ostrzyzek.a1 arkadiusz.ostrzyzek.a2 arkadiusz.ostrzyzek.b0 arkadiusz.ostrzyzek.b1 arkadiusz.ostrzyzek.c0 arkadiusz.ostrzyzek.d0 arkadiusz.ostrzyzek.e0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

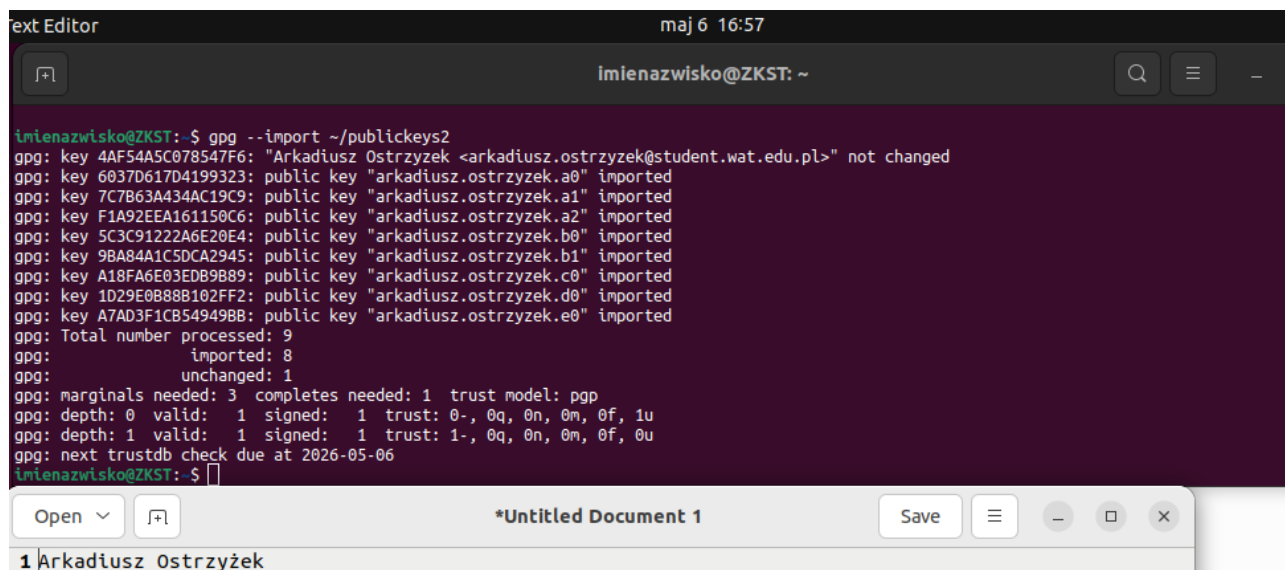
pub rsa3072/6037D617D4199323 2024-05-06 arkadiusz.ostrzyzek.a0
Delete this key from the keyring? (y/N) y
pub rsa3072/7C7B63A434AC19C9 2024-05-06 arkadiusz.ostrzyzek.a1
Delete this key from the keyring? (y/N) y

Open Untitled Document 1 Save

1 Arkadiusz Ostrzyżek

1.4

Importujemy z pliku do którego wcześniej eksportowaliśmy.



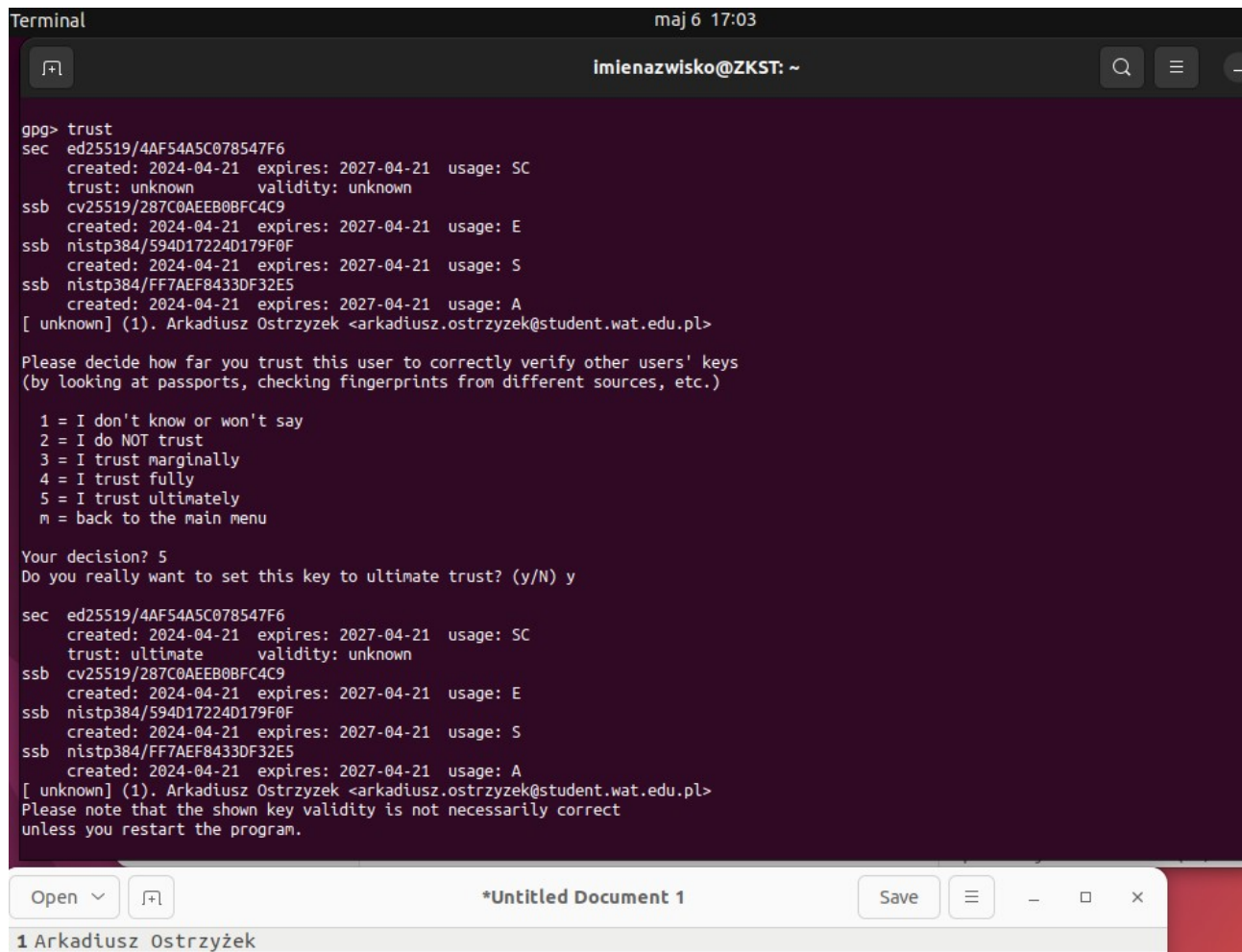
The screenshot shows a terminal window titled "maj 6 16:57" with the prompt "imienazwisko@ZKST: ~". The user has executed the command `gpg --import ~/publickeys2`. The output shows that 9 keys were processed, 8 were imported, and 1 was unchanged. The keys are for "Arkadiusz Ostrzyżek" with various email addresses. The terminal window is part of a desktop environment with a taskbar at the bottom showing "Open", "Save", and window controls. Below the terminal, a text editor window titled "*Untitled Document 1" is open, showing the text "1 Arkadiusz Ostrzyżek".

```
imienazwisko@ZKST:~$ gpg --import ~/publickeys2
gpg: key 4AF54A5C078547F6: "Arkadiusz Ostrzyżek <arkadiusz.ostrzyzek@student.wat.edu.pl>" not changed
gpg: key 6037D617D4199323: public key "arkadiusz.ostrzyzek.a0" imported
gpg: key 7C7B63A434AC19C9: public key "arkadiusz.ostrzyzek.a1" imported
gpg: key F1A92EEA161150C6: public key "arkadiusz.ostrzyzek.a2" imported
gpg: key 5C3C91222A6E20E4: public key "arkadiusz.ostrzyzek.b0" imported
gpg: key 9BA84A1C5DCA2945: public key "arkadiusz.ostrzyzek.b1" imported
gpg: key A18FA6E03EDB9B89: public key "arkadiusz.ostrzyzek.c0" imported
gpg: key 1D29E0B88B102FF2: public key "arkadiusz.ostrzyzek.d0" imported
gpg: key A7AD3F1CB549498B: public key "arkadiusz.ostrzyzek.e0" imported
gpg: Total number processed: 9
gpg:      imported: 8
gpg:      unchanged: 1
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: depth: 0 valid: 1 signed: 1 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1 valid: 1 signed: 1 trust: 1-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2026-05-06
imienazwisko@ZKST:~$
```

Open Save *Untitled Document 1 1 Arkadiusz Ostrzyżek

2.1

Po importowaniu musimy najpierw ustawić key trust naszego klucza z zajęć 5 na ultimate.



```
Terminal maj 6 17:03
imienazwisko@ZKST: ~

gpg> trust
sec  ed25519/4AF54A5C078547F6
    created: 2024-04-21  expires: 2027-04-21  usage: SC
    trust: unknown      validity: unknown
ssb  cv25519/287C0AEEB0BFC4C9
    created: 2024-04-21  expires: 2027-04-21  usage: E
ssb  nistp384/594D17224D179F0F
    created: 2024-04-21  expires: 2027-04-21  usage: S
ssb  nistp384/FF7AEF8433DF32E5
    created: 2024-04-21  expires: 2027-04-21  usage: A
[ unknown] (1). Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>

Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

 1 = I don't know or won't say
 2 = I do NOT trust
 3 = I trust marginally
 4 = I trust fully
 5 = I trust ultimately
 m = back to the main menu

Your decision? 5
Do you really want to set this key to ultimate trust? (y/N) y

sec  ed25519/4AF54A5C078547F6
    created: 2024-04-21  expires: 2027-04-21  usage: SC
    trust: ultimate      validity: unknown
ssb  cv25519/287C0AEEB0BFC4C9
    created: 2024-04-21  expires: 2027-04-21  usage: E
ssb  nistp384/594D17224D179F0F
    created: 2024-04-21  expires: 2027-04-21  usage: S
ssb  nistp384/FF7AEF8433DF32E5
    created: 2024-04-21  expires: 2027-04-21  usage: A
[ unknown] (1). Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>
Please note that the shown key validity is not necessarily correct
unless you restart the program.
```

Następnie możemy wypisać wszystkie klucze i ich zaufanie używając `–list-sigs`.

Terminalmaj 6 17:02

imienazwisko@ZKST: ~

imienazwisko@ZKST:~\$ gpg --list-sigs
/home/imienazwisko/.gnupg/pubring.kbx

pub ed25519 2024-04-21 [SC] [expires: 2027-04-21]
238D0655BAEF9828139692C34AF54A5C078547F6
uid [ultimate] Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>
sig 3 4AF54A5C078547F6 2024-04-21 Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>
sub cv25519 2024-04-21 [E] [expires: 2027-04-21]
sig 4AF54A5C078547F6 2024-04-21 Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>
sub nistp384 2024-04-21 [S] [expires: 2027-04-21]
sig 4AF54A5C078547F6 2024-04-21 Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>
sub nistp384 2024-04-21 [A] [expires: 2027-04-21]
sig 4AF54A5C078547F6 2024-04-21 Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>

pub rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
0F7D805F53F6B3A27AE757126037D617D4199323
uid [full] arkadiusz.ostrzyzek.a0
sig 3 6037D617D4199323 2024-05-06 arkadiusz.ostrzyzek.a0
sig 4AF54A5C078547F6 2024-05-06 Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>
sub rsa3072 2024-05-06 [E] [expires: 2026-05-06]
sig 6037D617D4199323 2024-05-06 arkadiusz.ostrzyzek.a0

pub rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
42C75184A8553426BC1F70B67C7B63A434AC19C9
uid [full] arkadiusz.ostrzyzek.a1
sig 3 7C7B63A434AC19C9 2024-05-06 arkadiusz.ostrzyzek.a1
sig 4AF54A5C078547F6 2024-05-06 Arkadiusz Ostrzyzek <arkadiusz.ostrzyzek@student.wat.edu.pl>
sub rsa3072 2024-05-06 [E] [expires: 2026-05-06]
sig 7C7B63A434AC19C9 2024-05-06 arkadiusz.ostrzyzek.a1

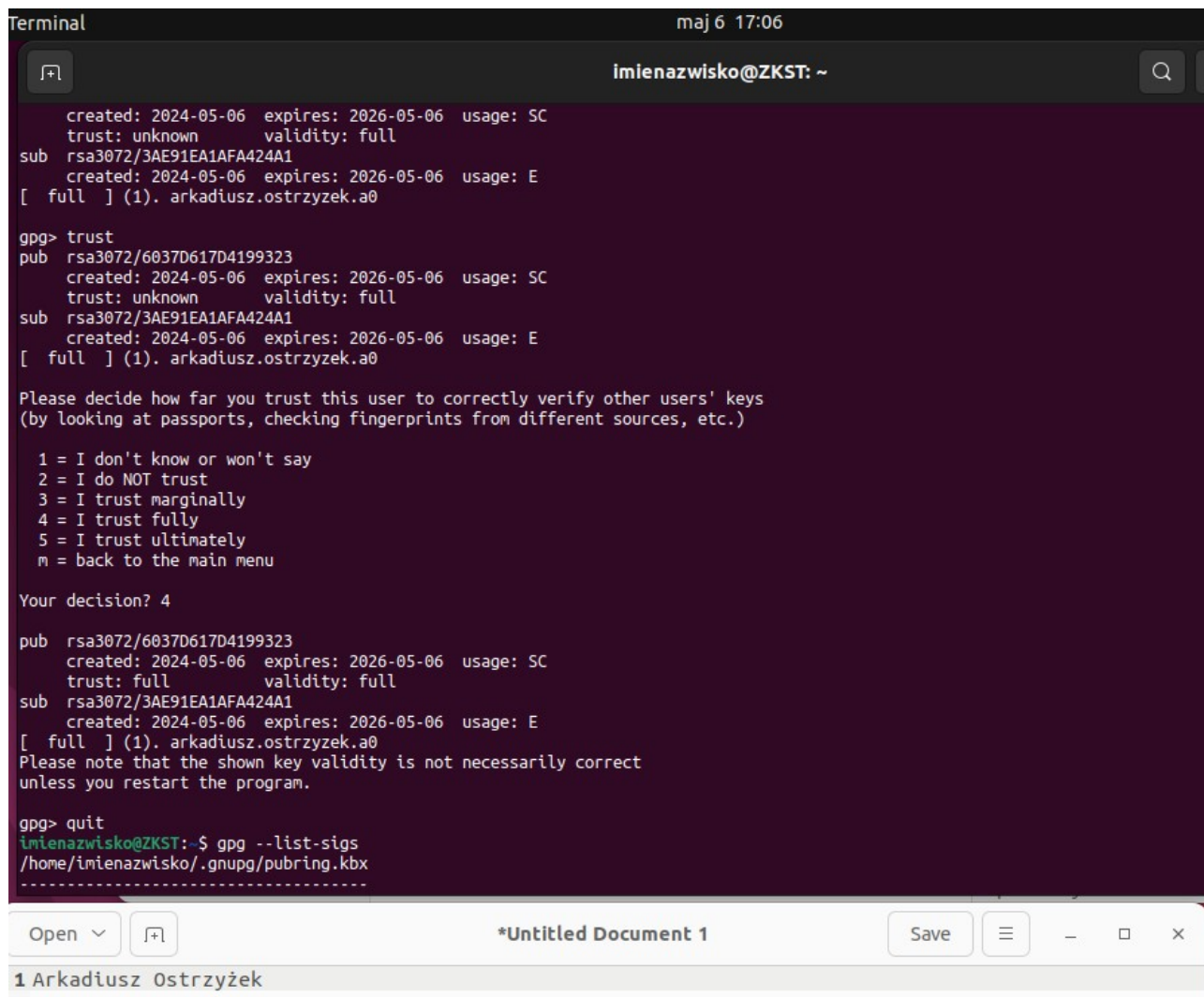
pub rsa3072 2024-05-06 [SC] [expires: 2026-05-06]
4880064668BF3F028201A17A5C3C91222A6E20E4
uid [undef] arkadiusz.ostrzyzek.b0
sig 3 5C3C91222A6E20E4 2024-05-06 arkadiusz.ostrzyzek.b0
sig 6037D617D4199323 2024-05-06 arkadiusz.ostrzyzek.a0
sig 7C7B63A434AC19C9 2024-05-06 arkadiusz.ostrzyzek.a1
sub rsa3072 2024-05-06 [E] [expires: 2026-05-06]
sig 5C3C91222A6E20E4 2024-05-06 arkadiusz.ostrzyzek.b0

Open *Untitled Document 1 Save

1 Arkadiusz Ostrzyzek

Klucze podpisane przez nas mają full validity, ponieważ zostały podpisane kluczem ultimate. Inne klucze podpisane przez nie są undefined, ponieważ zostały podpisane przez klucze osób, które nie mają trust marginal lub full.

2.2



```
Terminal
maj 6 17:06
imienazwisko@ZKST: ~

created: 2024-05-06 expires: 2026-05-06 usage: SC
trust: unknown validity: full
sub rsa3072/3AE91EA1AFA424A1
created: 2024-05-06 expires: 2026-05-06 usage: E
[ full ] (1). arkadiusz.ostrzyzek.a0

gpg> trust
pub rsa3072/6037D617D4199323
created: 2024-05-06 expires: 2026-05-06 usage: SC
trust: unknown validity: full
sub rsa3072/3AE91EA1AFA424A1
created: 2024-05-06 expires: 2026-05-06 usage: E
[ full ] (1). arkadiusz.ostrzyzek.a0

Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

1 = I don't know or won't say
2 = I do NOT trust
3 = I trust marginally
4 = I trust fully
5 = I trust ultimately
m = back to the main menu

Your decision? 4

pub rsa3072/6037D617D4199323
created: 2024-05-06 expires: 2026-05-06 usage: SC
trust: full validity: full
sub rsa3072/3AE91EA1AFA424A1
created: 2024-05-06 expires: 2026-05-06 usage: E
[ full ] (1). arkadiusz.ostrzyzek.a0
Please note that the shown key validity is not necessarily correct
unless you restart the program.

gpg> quit
imienazwisko@ZKST:~$ gpg --list-sigs
/home/imienazwisko/.gnupg/pubring.kbx
-----

Open [v] [f] *Untitled Document 1 Save [≡] - □ ×
1 Arkadiusz Ostrzyżek
```

Po zmianie arkadiusz.ostrzyzek.a0 na trust full, poziom b0 i b1 też będzie na full, ponieważ zostały podpisane przez zaufane klucze, jednak poziom reszty kluczy się nie zmieni.

2.3

Poziom zaufania w sieci się nie zmieni.

2.4

Po zmianie arkadiusz.ostrzyzek.b0 i b1 na trust full, poziom c0 też będzie na full, ponieważ zostały podpisane przez zaufane klucze, jednak poziom reszty kluczy się nie zmienia.

2.5

Po zmianie arkadiusz.ostrzyzek.c0 na trust full, poziom d0 też będzie na full, ponieważ zostały podpisane przez zaufane klucze, jednak poziom reszty kluczy się nie zmienia.

2.6

Poziom zaufania w sieci się nie zmienia.