



W sprawozdaniu zamieść zrzuty ekranu z istotnych etapów oraz odpowiedzi na pytania.

 Taki symbol oznacza, że trzeba w sprawozdaniu dodać zrzut ekranu (najczęściej 1) z wyniku działania polecenie.

 Taki symbol oznacza, że należy dodać opis (najczęściej 1 zdanie) z wyniku działania polecenia.

Wstęp

PGP jest oprogramowaniem, które w łatwy sposób pozwala na korzystanie ze współczesnych algorytmów kryptograficznych w celu zabezpieczenia korespondencji a także ochrony wszelkich innych danych w formie elektronicznej. Skrót PGP w języku angielskim rozwijamy jako "Pretty Good Privacy", co w tłumaczeniu na nasz ojczysty język oznacza „Całkiem niezłą prywatność”. Śmiało można powiedzieć, że stopień prywatności oferowany przez PGP jest o wiele wyższy, niż mogło by to wynikać z samej nazwy.

Philip Zimmermann stworzył PGP, by umożliwić szeroki dostęp do kryptografii. Pierwsza popularna wersja, PGP 2.3a z 1993 roku, wykorzystywała algorytm RSA do zarządzania kluczami i szyfr IDEA, z maksymalną długością klucza RSA do 1024 bitów. Wersje 2.x rozwijano mimo sporów patentowych, a Massachusetts Institute of Technology przejął ich dystrybucję. W 1995 roku powstało PGP Inc., a wersja PGP 5.0, w odpowiedzi na ograniczenia patentowe, wprowadziła nowe algorytmy (DSS/Diffie-Hellman, 3DES, CAST, SHA-1). Aby obejść przepisy eksportowe USA, kod PGP drukowano i przewożono do Europy. W 1997 roku firmę PGP Inc. kupiło Network Associates Inc., które rozwinęło PGP o funkcje VPN, certyfikaty X.509 i szyfrowanie dysków. Zimmermann odszedł z NAI w 2001 roku i obecnie angażuje się w rozwój OpenPGP.



Źródło: <https://jacobriggs.io/blog/posts/how-do-gpg-keys-work-6>

I. Przygotowanie środowiska pracy

1. Przygotuj maszynę wirtualną z systemem Kali Linux. (**rekomendacja:** [VMware Workstation Pro](#))

Możesz skorzystać z gotowej maszyny wirtualnej dostępnej na [stronie Kali Linux](#) lub samodzielnie zainstalować i skonfigurować system – wybór należy do Ciebie.

2. Upewnij się, że interfejs sieciowy dla Twojej maszyny wirtualnej ustawiony jest w trybie NAT.
3. Uruchom maszynę wirtualną.

Jeżeli skorzystasz z gotowej maszyny wirtualnej, domyślne dane logowania to: **kali/kali**

4. Otwórz terminal w Kali Linux.
5. Wykonaj aktualizację repozytoriów:

```
sudo apt update
```

6. Zainstaluj klienta pocztowego [Mozilla Thunderbird](#).

```
sudo apt install thunderbird -y
```

7. Uruchom klienta i połącz się ze swoim kontem pocztowym.

II. Praca z GnuPGP

Program GnuPGP jest domyślnie zainstalowany w systemie Kali Linux.

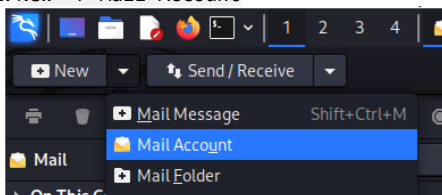
1. Niestety, Thunderbird od wersji 78 zablokował możliwość korzystania z kluczy PGP wygenerowanych w zewnętrznych źródłach dlatego zainstalujemy klienta poczty Evolution:

```
sudo apt install evolution -y
```

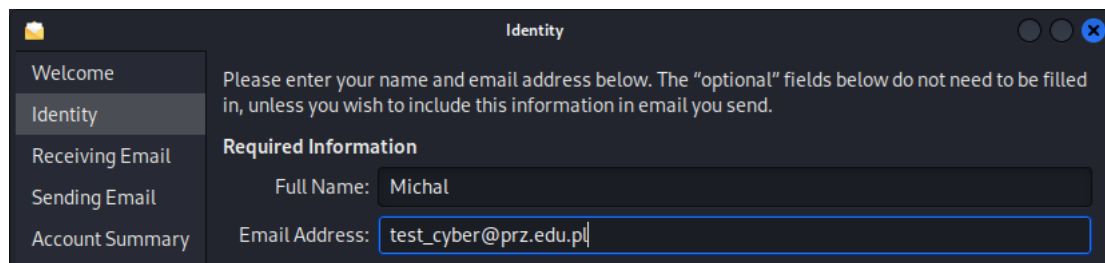
2. Uruchom klienta za pomocą poniższej komendy lub znajdź go w menu Aplikacje:

```
evolution
```

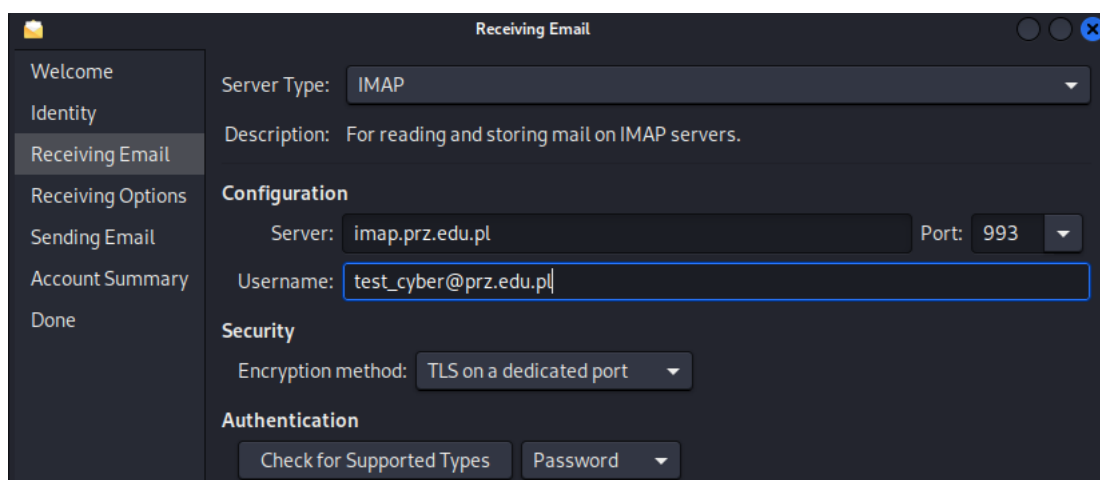
3. Dodaj swoje konto e-mail: **New -> Mail Account**



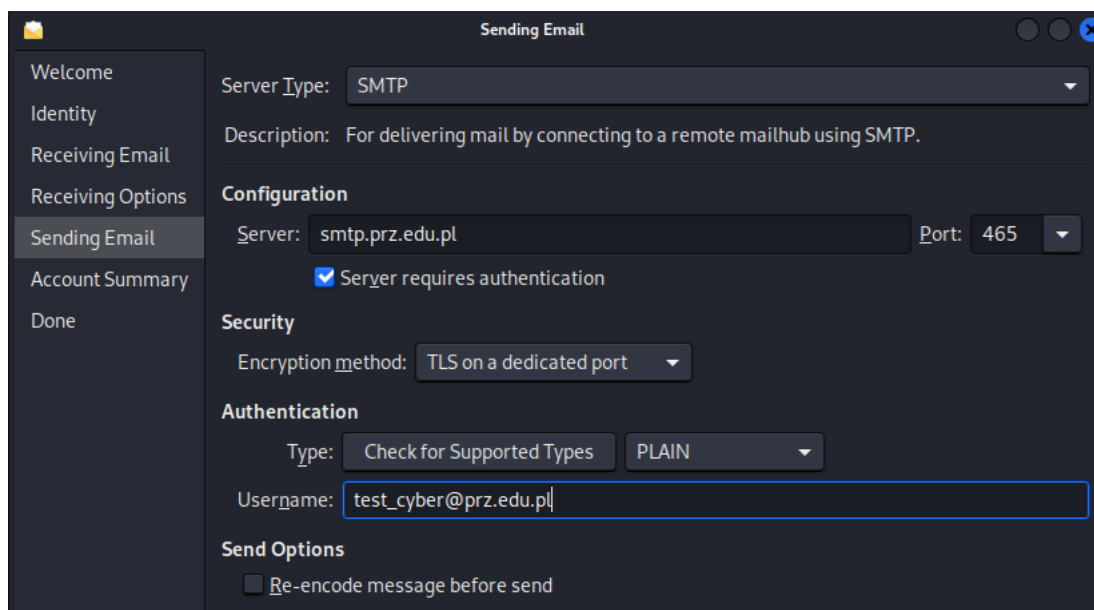
4. W polu `Welcome` naciśnij przycisk `Next`.
5. Wypełnij pola `Full Name` oraz `Email Address`, a następnie kliknij `Next`.



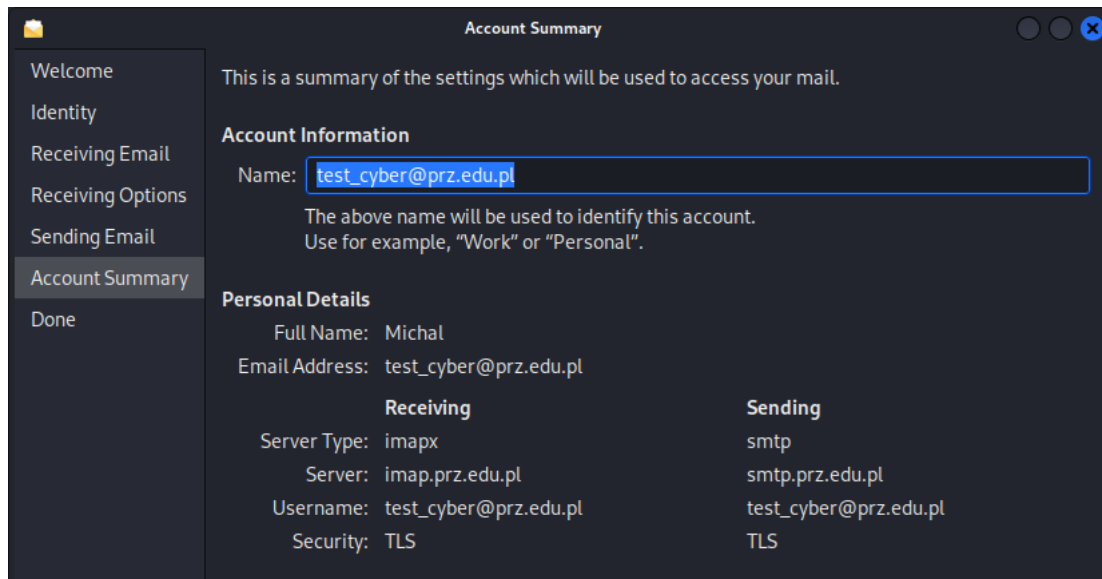
6. W oknie "Receiving Email" ustaw typ serwera na `IMAP`, a w polu `Server` wpisz `stud.prz.edu.pl`. W polu `Username` podaj swój adres email. Następnie kliknij `Next`.



7. W oknie "Receiving Options" kliknij `Next` bez wprowadzania zmian.
8. W kolejnym oknie, w polu "Server," wpisz `stud.prz.edu.pl` i zaznacz opcję `Server requires authentication`. W polu "Username" podaj swój adres email, a następnie kliknij `Next`.



9. Upewnij się, że wszystko wpisałeś poprawnie a następnie naciśnij przycisk Next.



10. Zatwierdź cały proces, klikając przycisk Apply.

11. Zostaniesz poproszony o potwierdzenie autoryzacji – podaj hasło do swojego emaila i kliknij ok.

12. Po połączeniu z kontem przejdź do terminala Kali Linux.

13. Wygeneruj klucz, używając następującego polecenia:

```
gpg --gen-key
```

- Jak nazwę podaj: u_twój_numer_indeksu (**np. u112233**).
- Wprowadź adres email, dla którego chcesz wygenerować klucz.
- Upewnij się, że dane są poprawne, i zatwierdź operację, wpisując literę "O".
- Wymyśl i wpisz hasło zabezpieczające Twój klucz.



14. Wyświetl listę posiadanych kluczy:

```
gpg --list-keys
```

```
(kali㉿kali)-[~]
└─$ gpg --list-keys
/home/kali/.gnupg/pubring.kbx

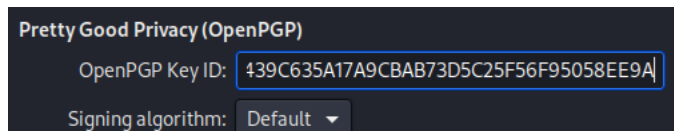
pub  rsa3072 2024-10-29 [SC] [expires: 2027-10-29]
     0A52439C635A17A9CBAB73D5C25F56F95058EE9A
uid  [ultimate] u112233 <test_cyber@prz.edu.pl>
sub  rsa3072 2024-10-29 [E] [expires: 2027-10-29]
```

15. Najważniejszą częścią jest Twój identyfikator klucza (key ID), który w przykładowym zrzucie ekranu to ciąg 40 znaków, zaczynający się od „0A52439C...”. Skopiuj swój key ID.

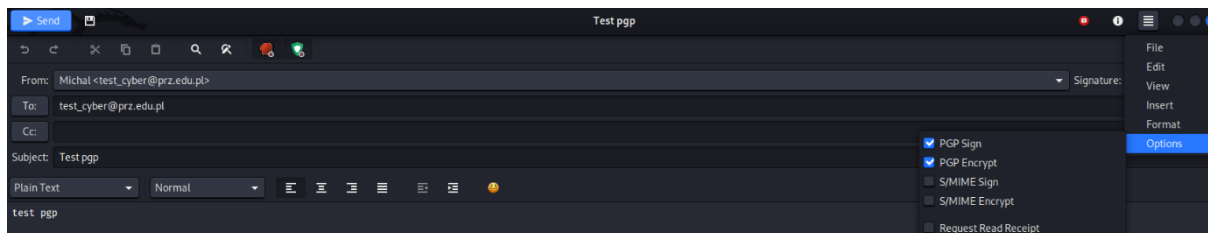
16. Wróć do klienta Evolution, kliknij prawym przyciskiem myszy na swoje konto email i wybierz opcję Properties.


17. W oknie "Account Editor" po lewej stronie wybierz zakładkę Security.

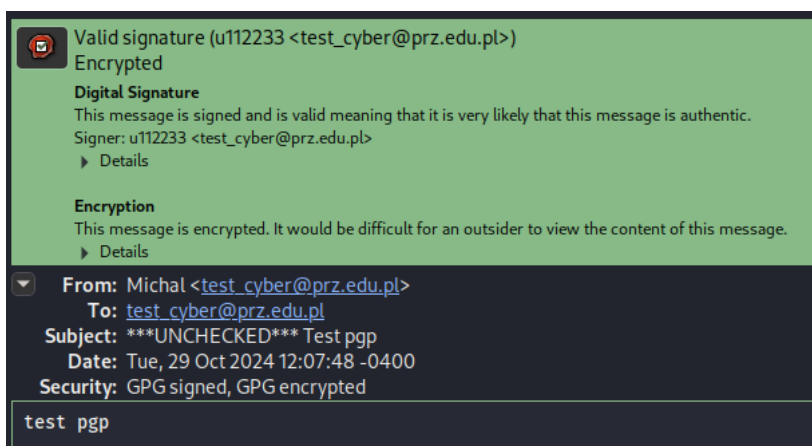
18. W polu OpenPGP Key ID wklej swój key ID i zatwierdź przyciskiem OK.




19. Przetestuj konfigurację, wysyłając podpisaną i zaszyfrowaną wiadomość do siebie. Uwaga: przy pierwszym wysłaniu możesz zostać poproszony o podanie o secret key swojego klucza (ppkt 13d) oraz hasła do poczty.



 20. Zamieść w sprawozdaniu dowód poprawnego wysłania wiadomości.



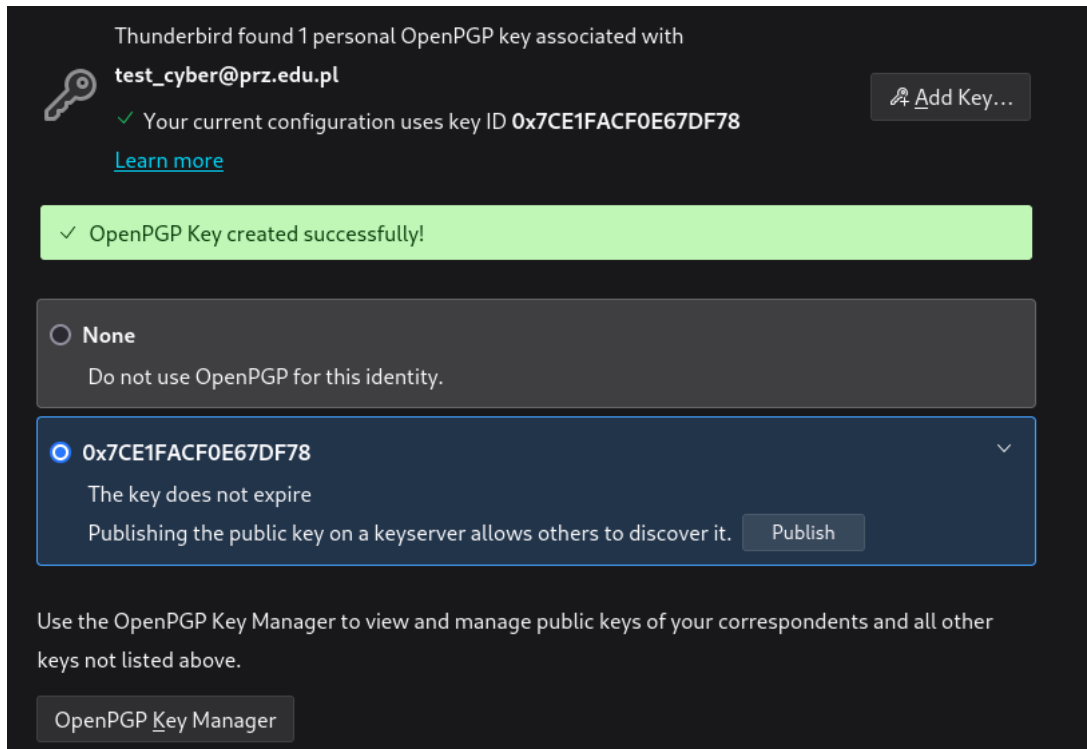
 21. Wymień się zaszyfrowanymi wiadomościami z kolegą/koleżanką z grupy. Pamiętaj, że aby nastąpiła szyfrowana komunikacja, obie strony muszą wymienić się kluczami publicznymi. Najlepszą metodą jest przesłanie sobie wcześniej jedynie podpisanych wiadomości.

III. OpenPGP w kliencie pocztowym Thunderbird

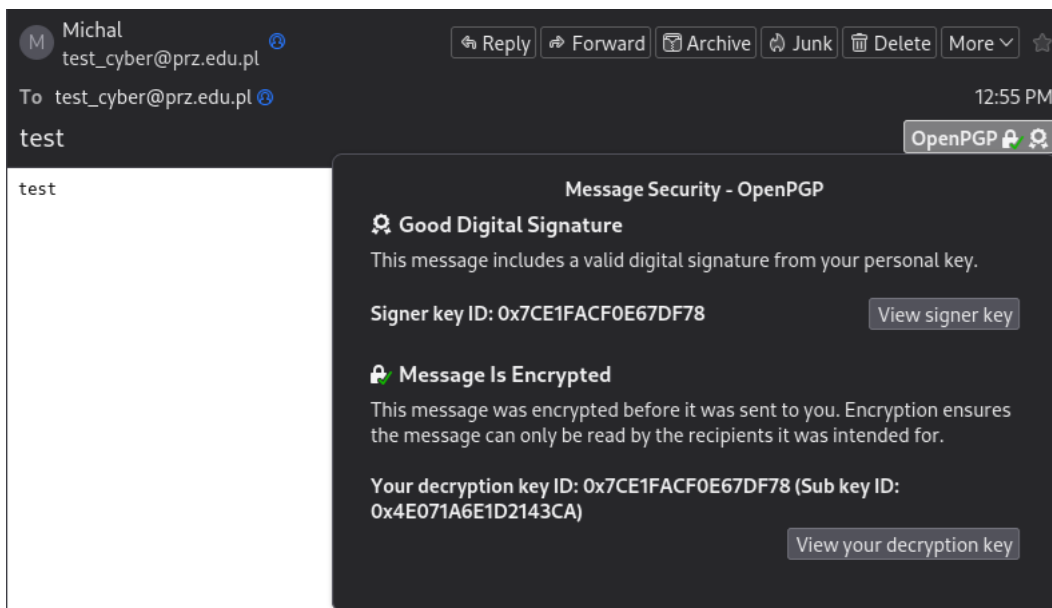
W programie Mozilla Thunderbird opcja OpenPGP jest zintegrowana bezpośrednio, bez potrzeby instalowania dodatkowych wtyczek.

1. Aby wygenerować parę kluczy, kliknij prawym przyciskiem myszy na swoje konto i wybierz Settings.
2. Przejdź do zakładki „End-To-End Encryption” i wybierz Add Key...
3. Wybierz Create a New OpenPGP Key.
4. Ustaw czas wygaśnięcia klucza, a następnie kliknij Generate Key.

5. Zatwierdź, klikając **Confirm**.
6. Po poprawnym dodaniu klucza powinieneś zobaczyć efekt podobny do poniższego przykładu.



7. Wybierz „OpenPGP Key Manager,” a następnie dwukrotnie kliknij na swój klucz.
8. Wykonaj zrzut ekranu otwartego okna i umieść go w sprawozdaniu.
9. Przetestuj, wysyłając wiadomość do samego siebie.



10. Aby wyeksportować klucz publiczny, kliknij prawym przyciskiem myszy na swoje konto i wybierz **Settings** -> **End-To-End Encryption** -> **OpenPGP Key Manager**. Następnie kliknij prawym przyciskiem na swój klucz i wybierz opcję **Export Public Key(s) to File**.

ZADANIE

Podobnie jak na poprzednich zajęciach wyślij zaszyfrowanego i podpisanego maila na adres test_cyber@prz.edu.pl