Politechnika Częstochowska
Wydział Inżynierii Mechanicznej i Informatyki

Laboratorium z przedmiotu
Bezpieczeństwo komunikacji elektronicznej

Sprawozdanie nr 10

Szyfrowanie i podpisywanie poczty elektronicznej

Piotr Zyszcak
nr. 113066
Damian Łukasik
nr. 112993
II stopień, 2 semestr , 1 rok

Częstochowa 28 grudnia 2015 r.

1. Cel ćwiczenia laboratoryjnego

Celem ćwiczenia laboratoryjnego jest zapoznanie się z mechanizmami szyfrowania i podpisywania poczty elektronicznej za pomocą jednego z popularniejszych algorytmów szyfrowania PGP. Z przeprowadzonego ćwiczenia zostały wyciągnięte wnioski. Do sprawozdania załączono zrzuty ekranu w postaci *printscreenów*.

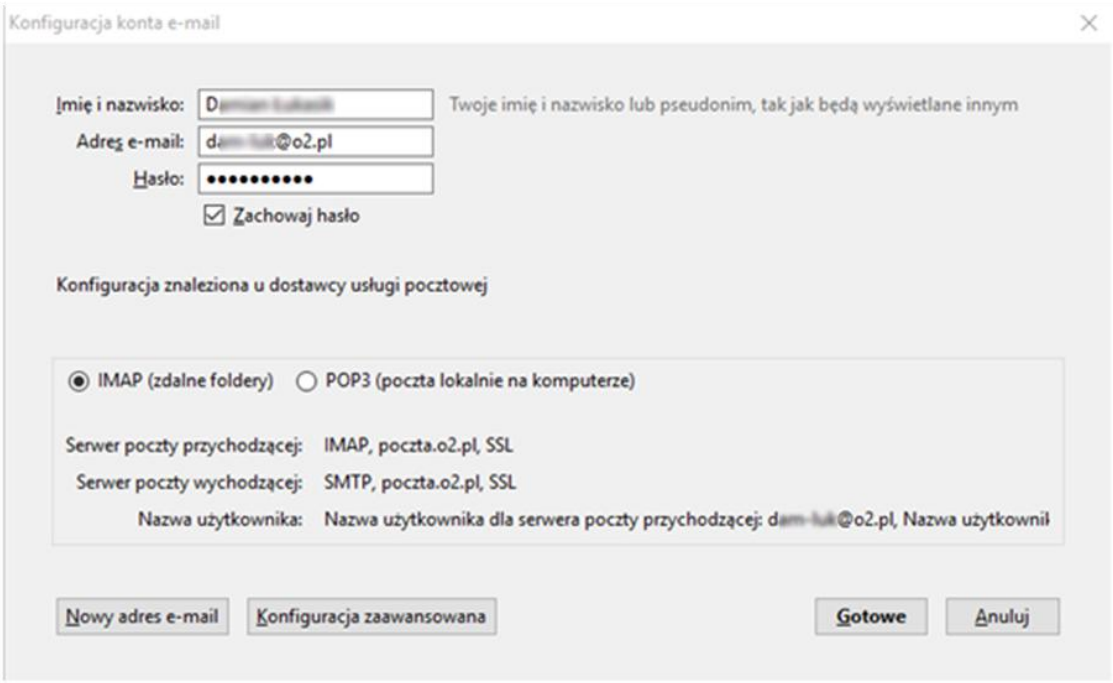
2. Opis ćwiczenia

PGP (ang. *Pretty Good Privacy*) jest stosowany głównie przy komunikacji za pośrednictwem poczty elektronicznej, umożliwia także podpisywanie i szyfrowanie plików na dysku. Na potrzeby laboratorium została wykorzystana darmowa implementacja algorytmów PGP, GnuPG[1]. W tym celu skorzystano z darmowego klienta poczty – *Thunderbird* oraz jeden z dodatków do niego pozwalający na łatwą konfigurację PGP – *Enigmail*

3. Przebieg ćwiczenia laboratoryjnego

W pierwszej kolejności zainstalowano *Thunderbird* oraz *GnuPG*.

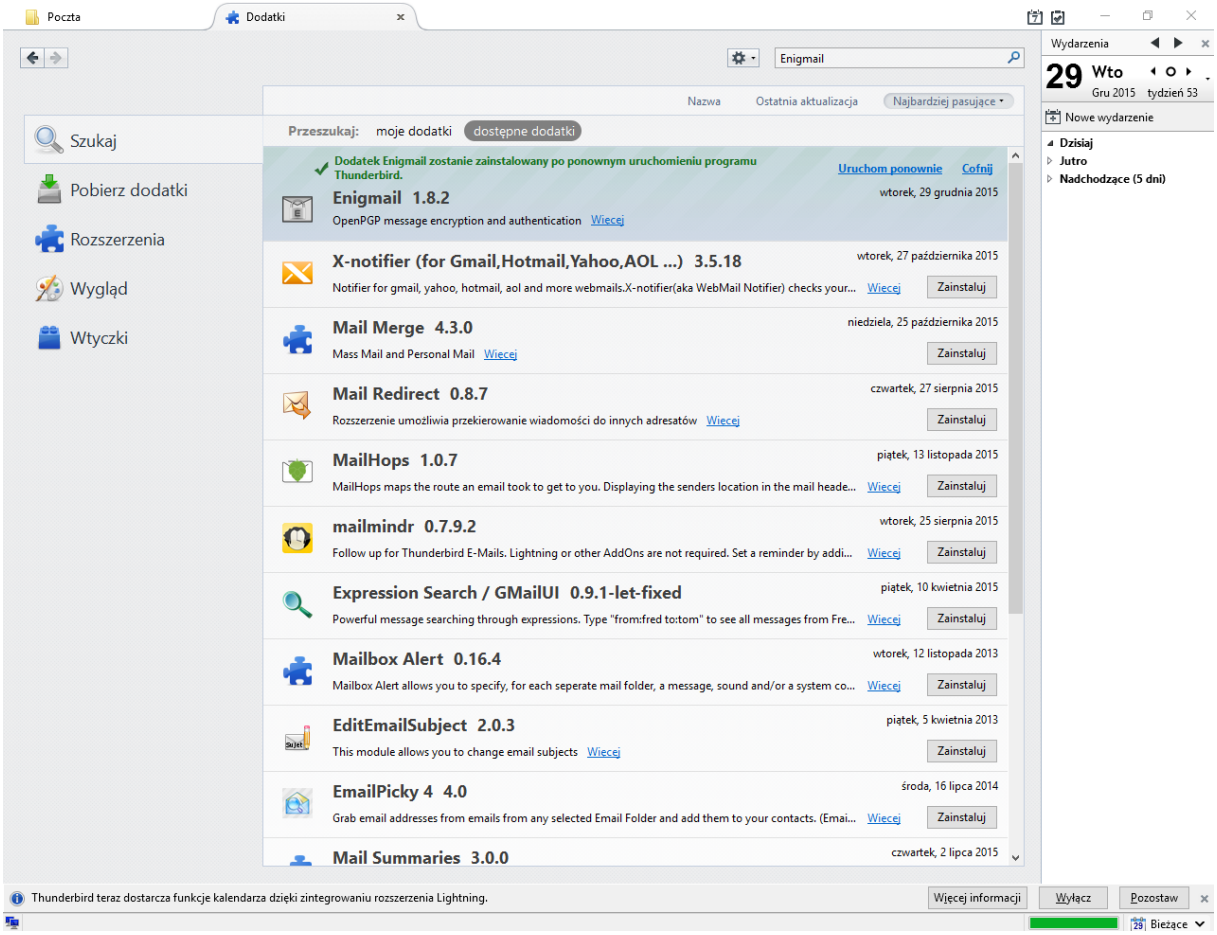
W drugiej kolejności skonfigurowano klienta poczty i dodatku *Enigmail*, który pozwoli w łatwy sposób zarządzać funkcjonalnościami GPG w Thunderbirdzie.



Rys1. Okno startowe Thunderbird.

Przy pierwszym uruchomieniu klienta poczty, otrzymujemy okno startowe w którym uzupełniamy dane naszego konta *e-mail*, bądź zakładamy nowe konto, z którego będziemy korzystać poprzez *Thunderbirda*.

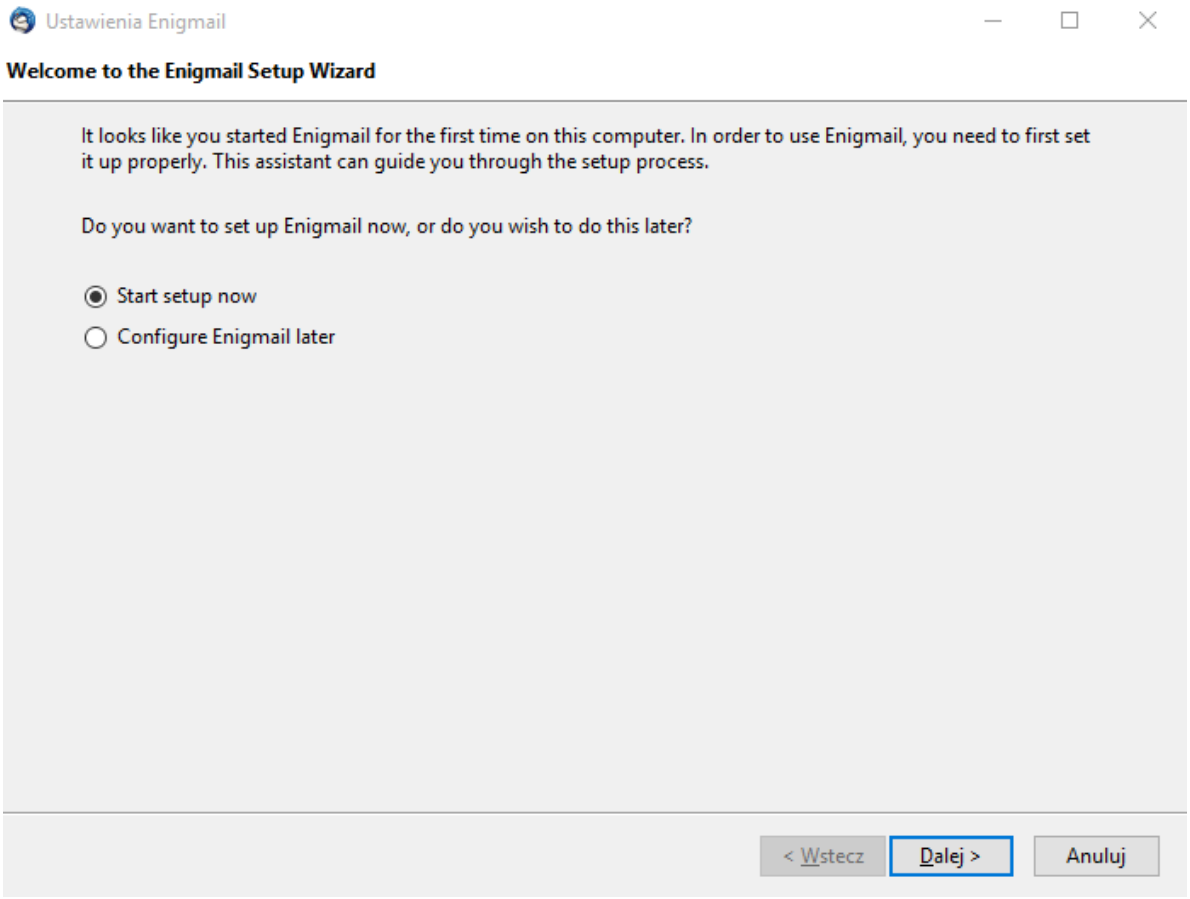
[1] http://www.gnupg.org/



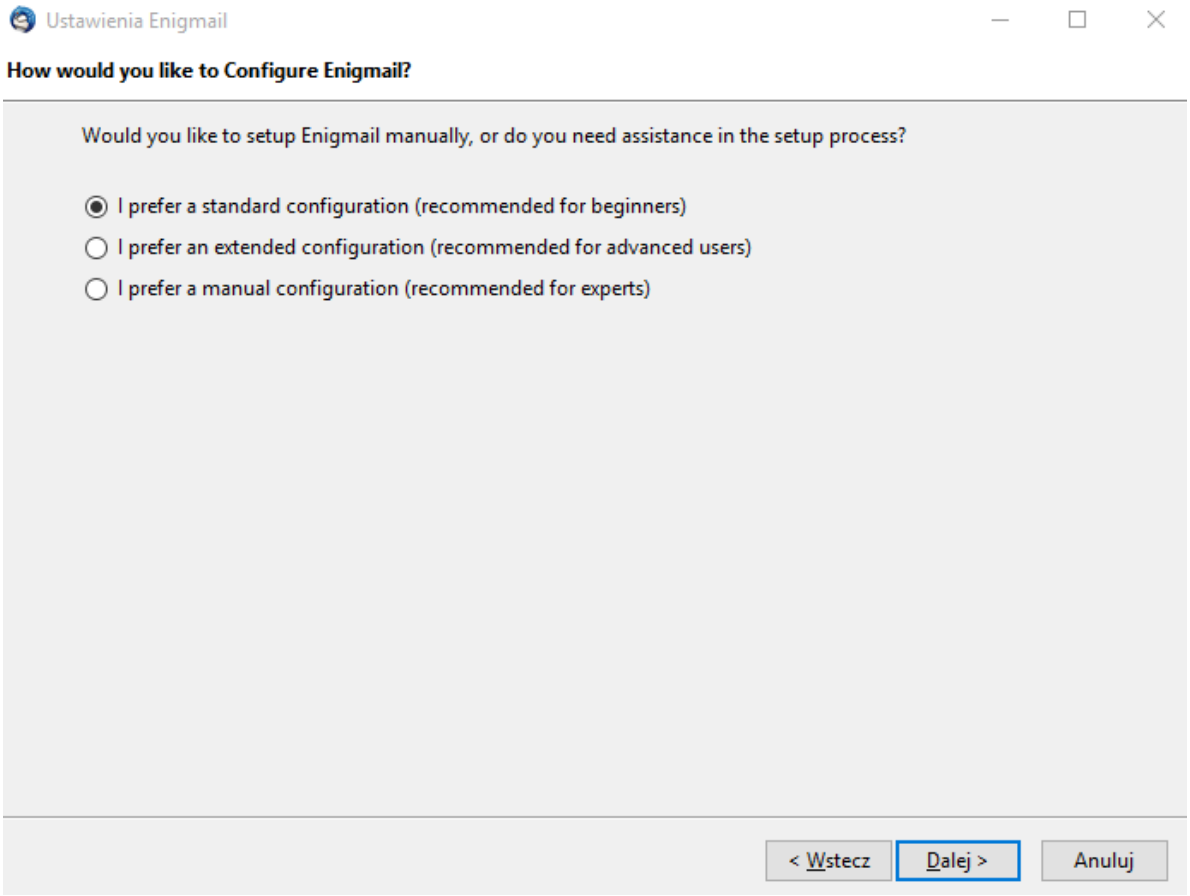
Rys2. Manager dodatków Thunderbird.

Po połączeniu klienta poczty z kontem, pobrano i zainstalowano dodatek *Enigmail* poprzez manager dodatków *Thunderbirda*.

W następnej kolejności skonfigurowano *OpenPGP* za pośrednictwem kreatora konfiguracji. Uruchamiany go po zainstalowaniu dodatku *Enigmail* poprzez uruchomienie z menu głównego *Thunderbirda* (*Enigmail → Asystent Konfiguracji*).

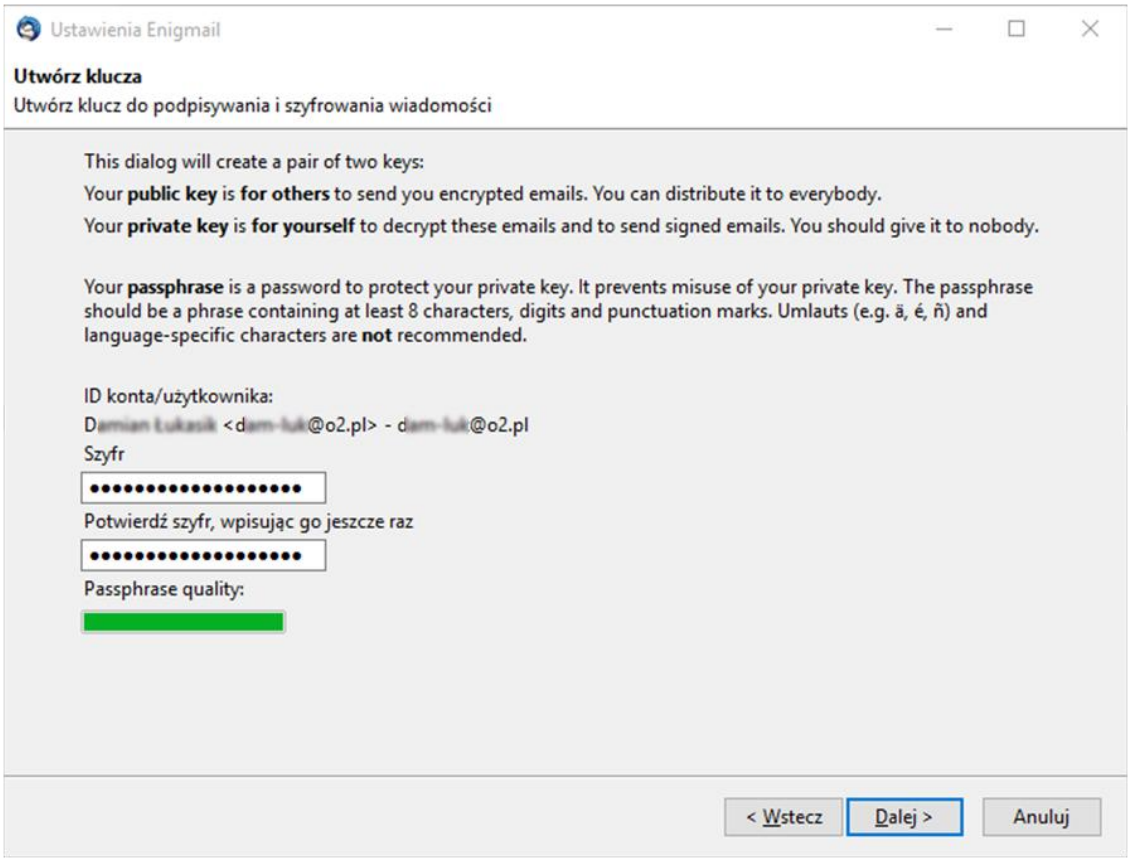


Rys3. Konfiguracja Enigmail.

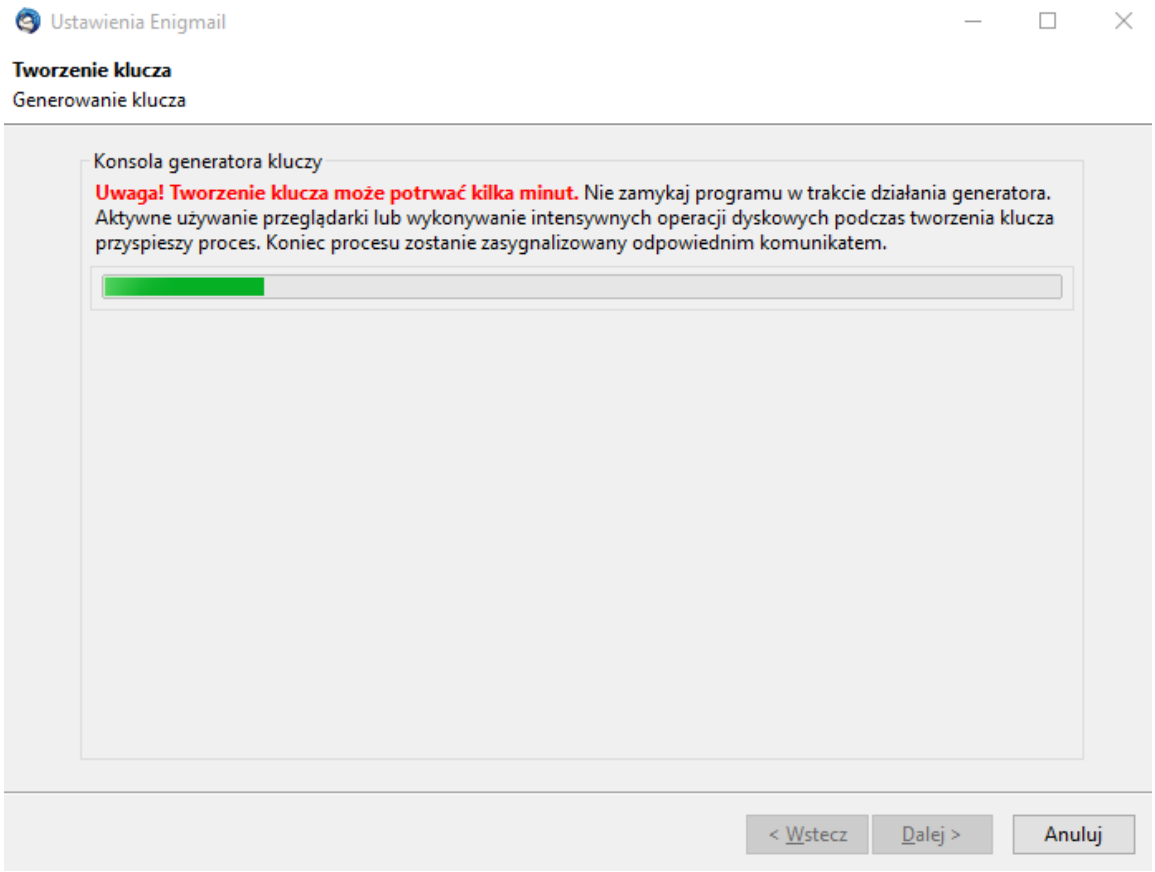


Rys4. Konfiguracja Enigmail.

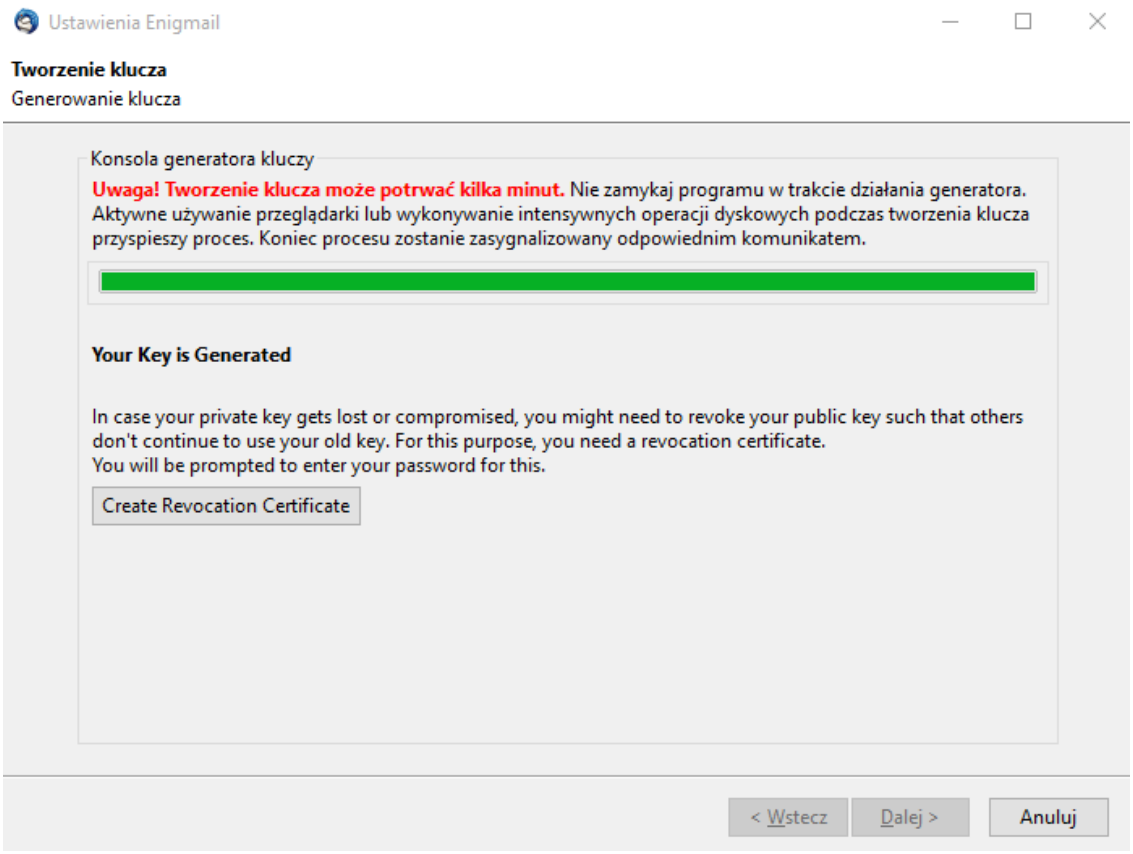
Następnie utworzono klucze do podpisywania wiadomości e-mail.



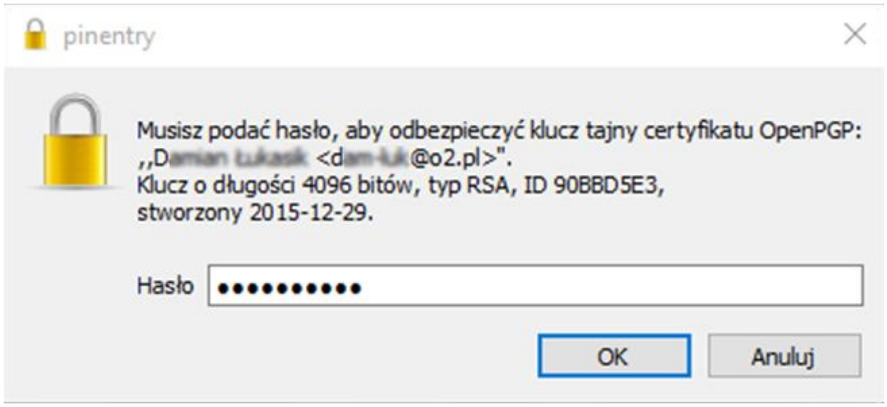
Rys5. Tworzenie kluczy szyfrujących.



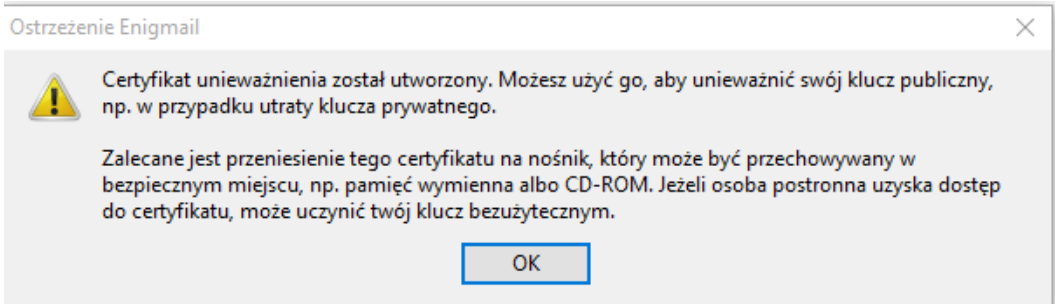
Rys6. Generowanie klucza.



Rys7. Tworzenie certyfikatu.

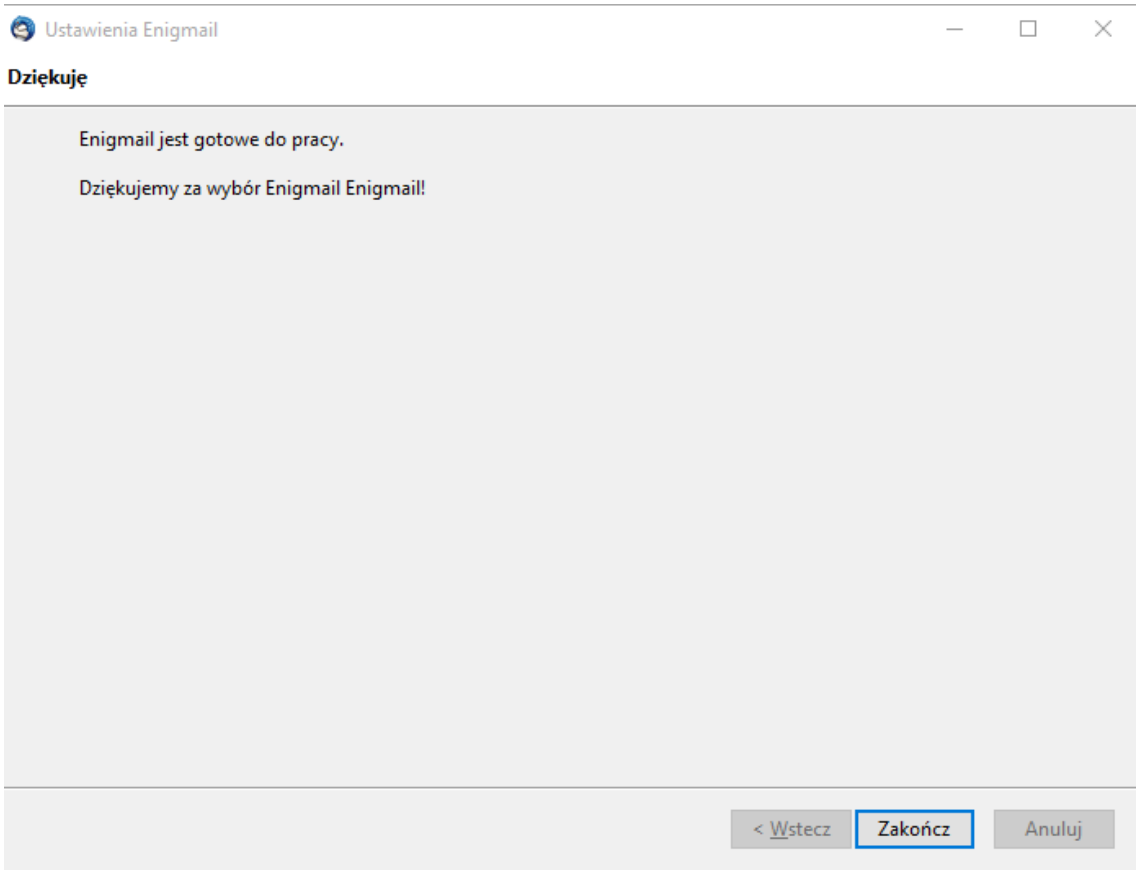


Rys8. Wprowadzanie hasła.

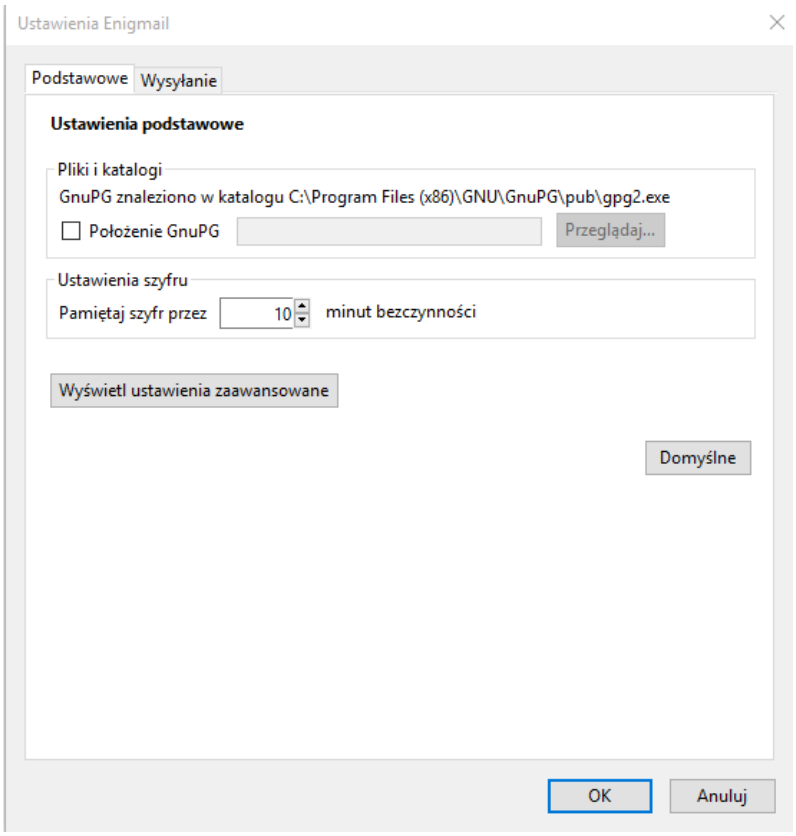


Rys9. Komunikat Enigmail.

Po wygenerowania pary kluczy prywatnego i publicznego, kreator oferuje również opcję wygenerowania klucza unieważniającego, którego możemy użyć w celu unieważnienia naszych kluczy w momencie np.: włamania na konto poczty.

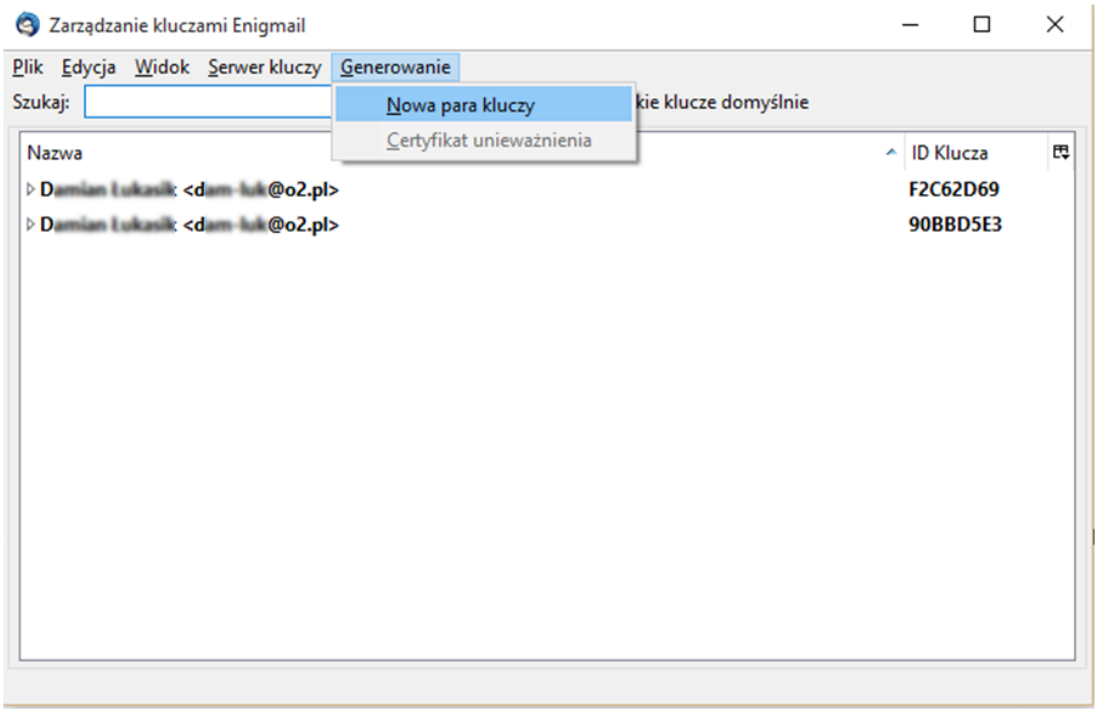


Rys10. Końcowe okno kreatora konfiguracji.

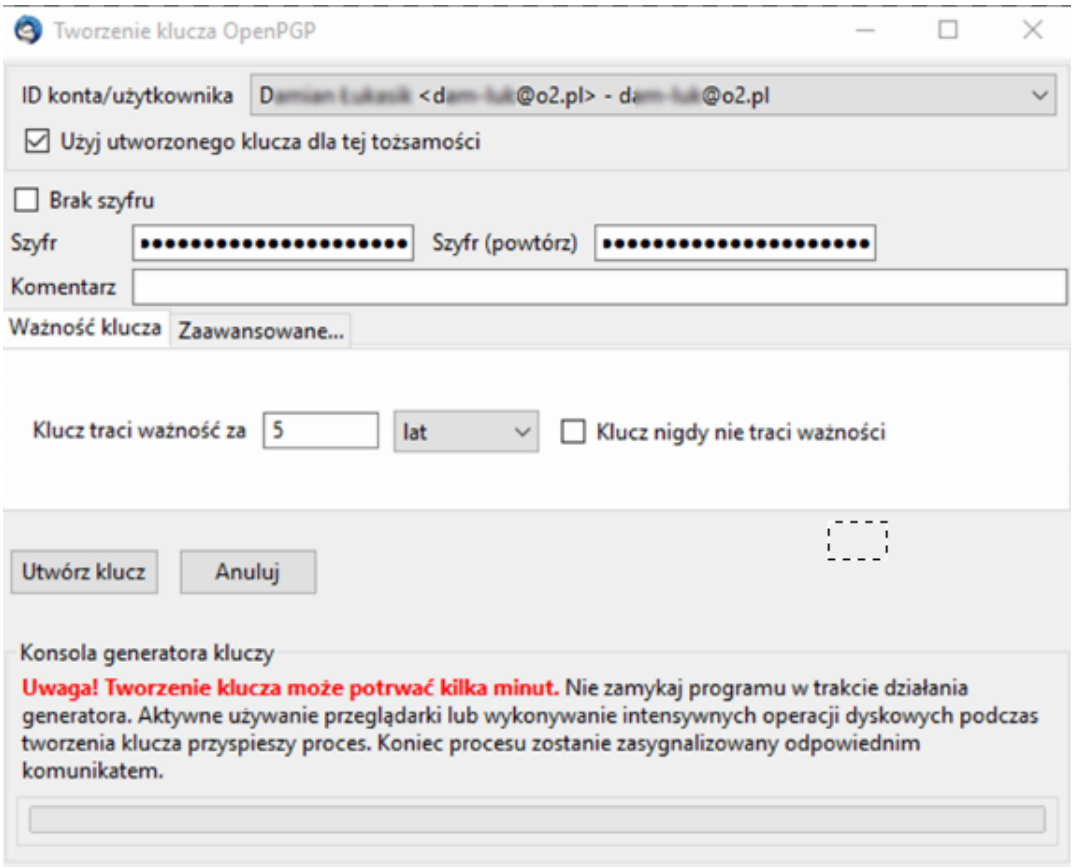


Rys11. Ręczna konfiguracja OpenPGP w Enigmail.

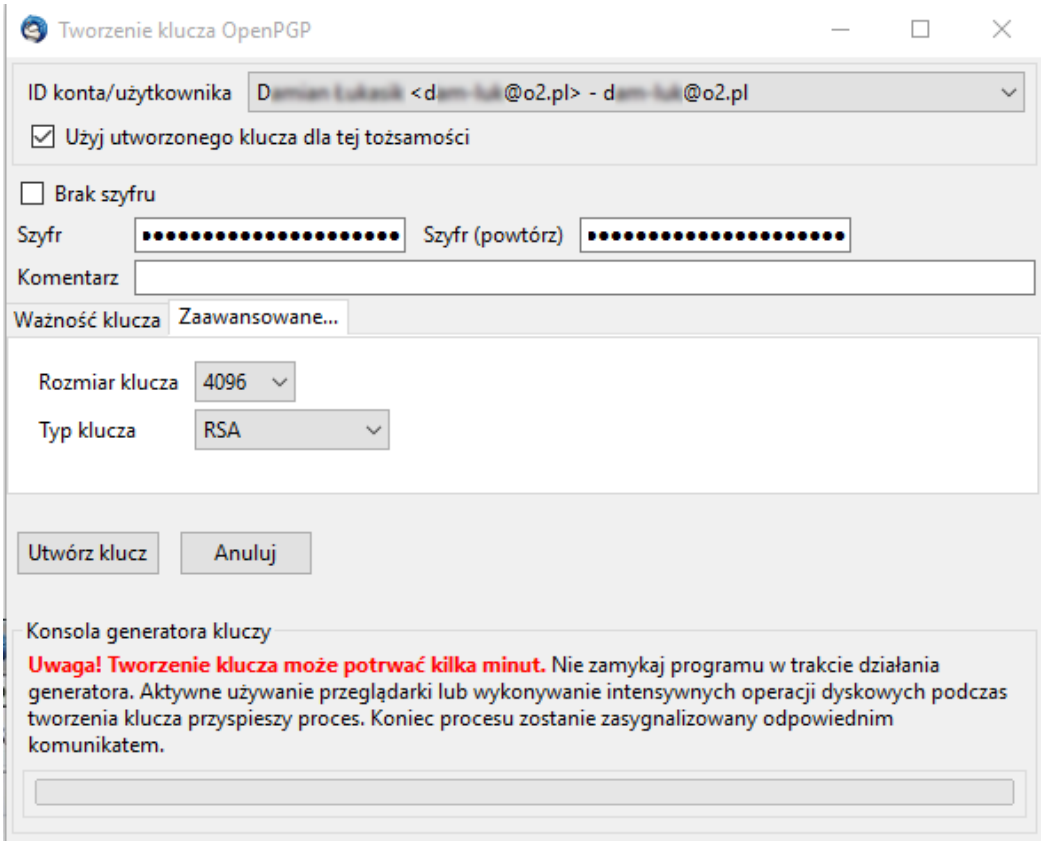
Konfigurację *OpenPGP* można przeprowadzić ręcznie (*OpenPGP → ustawienia*).



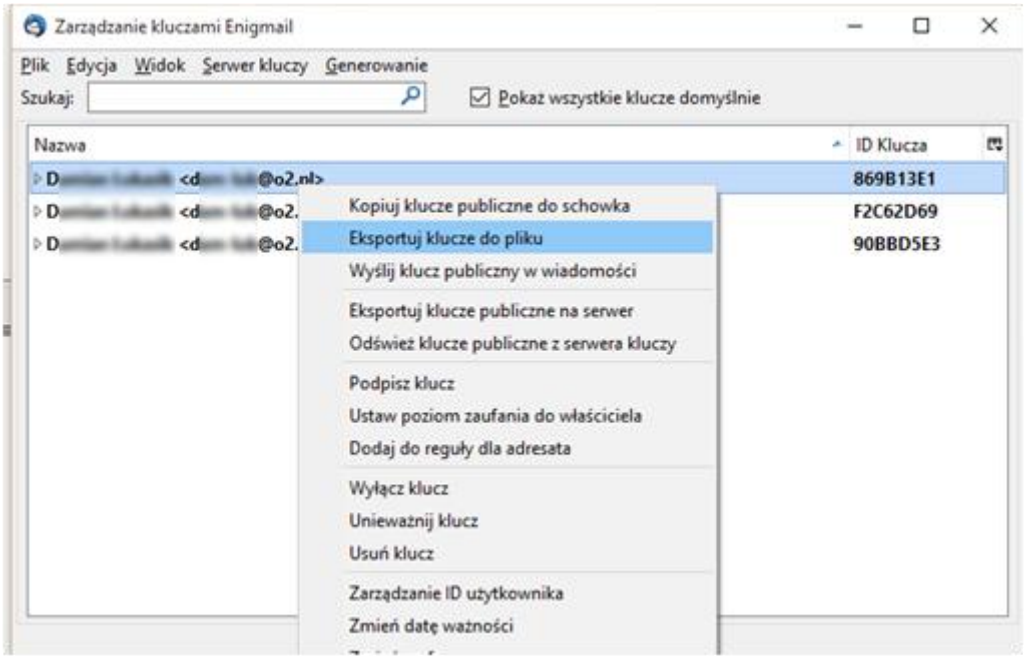
Rys12. Widok Zarządzania kluczami w Enigmail.



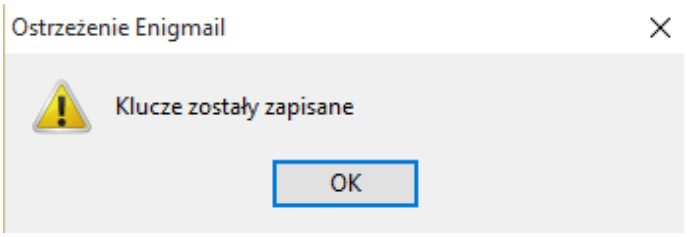
Rys13. Ręczne generowanie nowej pary kluczy.



Rys14. Ręczne generowanie nowej pary kluczy.

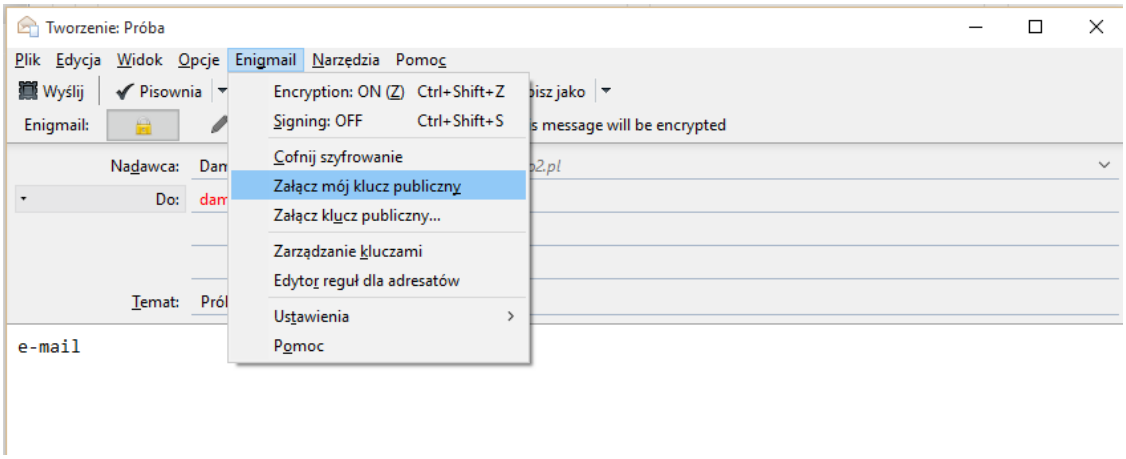


Rys15. Eksport klucza do pliku.

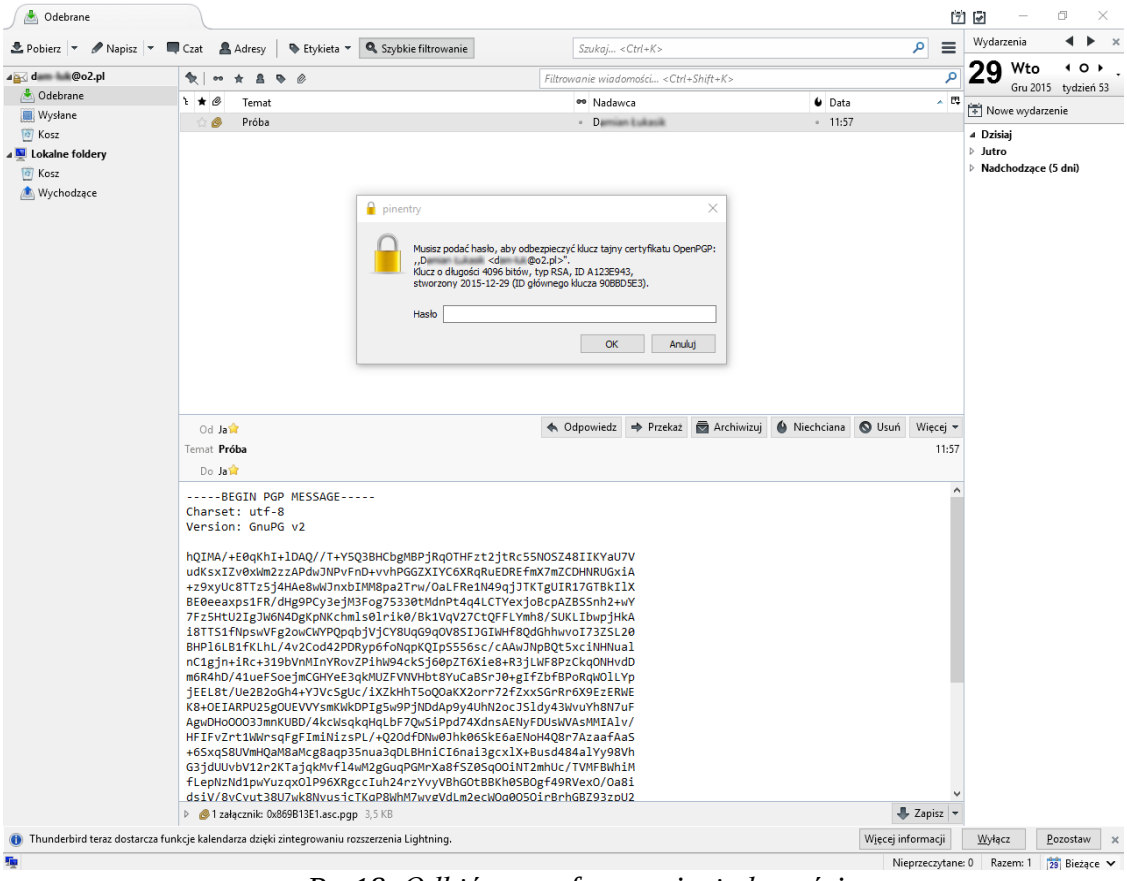


Rys16. Pomyślnie zakończony eksport klucza do pliku.

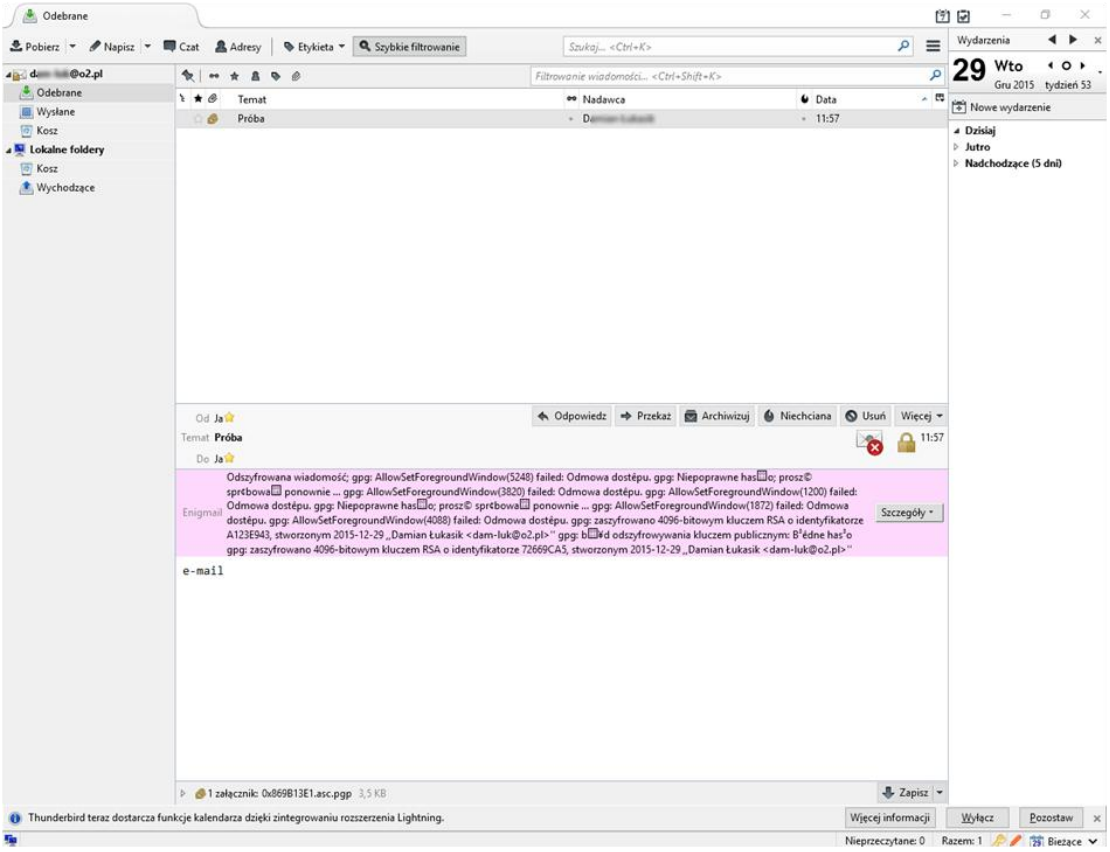
Po wygenerowaniu kluczy, przesłano klucz publiczny do osoby, z którą ma być przeprowadzona korespondencja zaszyfrowaną pocztą. W tym celu wystarczy załączyć klucz publiczny do przesyłanej wiadomości poprzez opcję *Załącz mój klucz publiczny* w menu *Enigmail*.



Rys17. Dołączanie klucza do szyfrowanej wiadomości.



Rys18. Odbiór zaszyfrowanej wiadomości.



Rys18. Odszyfrowana wiadomość.

4. Wnioski

Laboratorium zrealizowano zgodnie z instrukcją. Zapoznano się z bezpiecznym sposobem przesyłania poczty elektronicznej w oparciu o *OpenPGP*.

Wykorzystanie szyfrowania PGP w programie *Thunderbird* z dodatkiem *Enigmali* jest proste w obsłudze oraz w użytkowaniu, część opcji jest wykonywana automatycznie, a obsługa *OpenPGP* jest ograniczona do przeprowadzenia konfiguracji *Enigmail* przy pomocy kreatora konfiguracji. Dzięki zastosowaniu dodatku *Enigmail* przesyłane wiadomości były nie do odczytania bez posiadania odpowiedniego klucza.