ZAKŁAD SYSTEMÓW ROZPROSZONYCH
Politechnika Rzeszowska

BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH

Laboratorium 4:

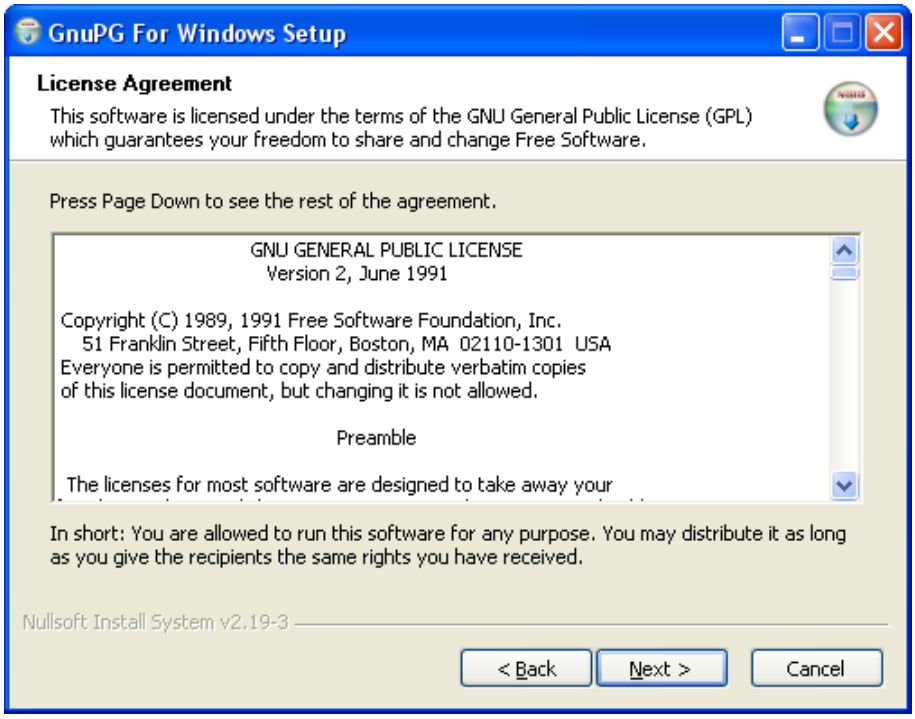
Szyfrowanie wiadomości e-mail przy pomocy dodatku GNUPG dla Mozilla Thunderbird

Gpg4win to pakiet instalacyjny dla środowiska Windows bazujący na GnuPG, który zawiera szereg narzędzi kryptograficznych wraz z nakładkami zapewniającymi im graficzny interfejs użytkownika. Całość pozwala szyfrować i podpisywać cyfrowe dane (pliki, tekst, wiadomości) standardami OpenPGP o S/MIME, zawiera system do zarządzania kluczami szyfrującymi i zapewnia dostęp dla wtyczek obsługujących publiczne katalogi kluczy.

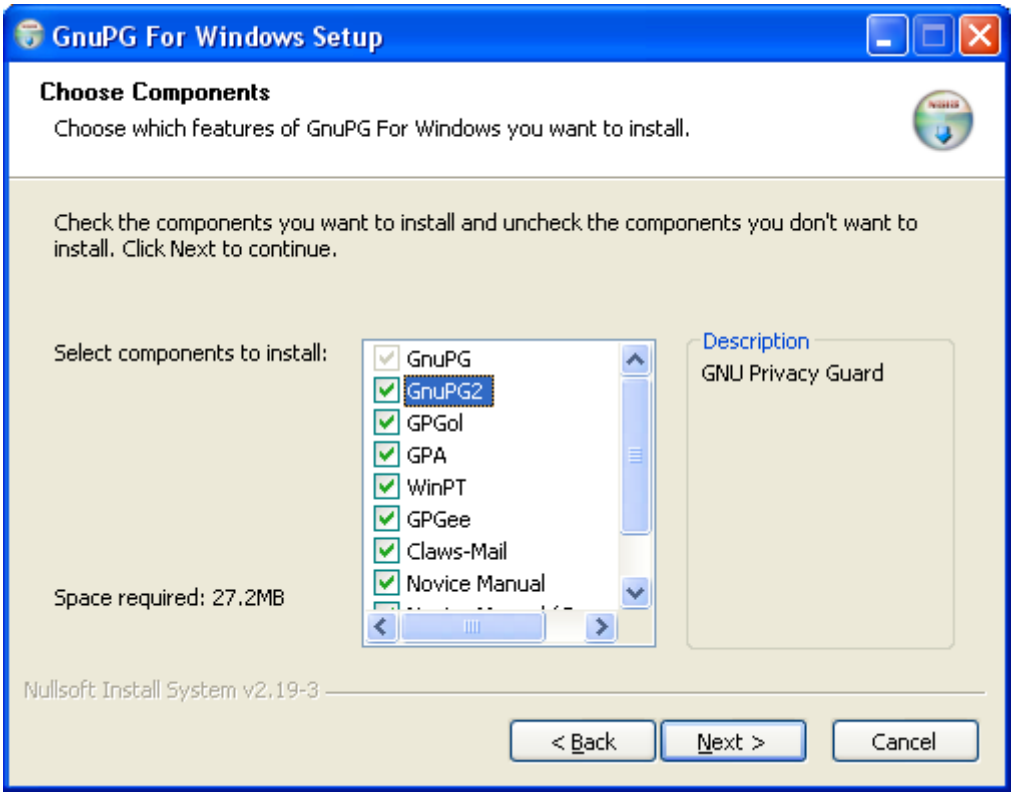
W skład wersji 1.1.3 wchodzą następujące komponenty:
- **GnuPG 1.4.7**
- **GnuPG2 2.0.7**
- **WinPT 1.2.0**
- **GPA 0.7.6**
- **GPGol 0.9.92**
- **GPGee 1.3.1**
- **Claws Mail 3.0.0-rc2**
- **Gpg4win for Novices 1.0.0**

1. Instalacja

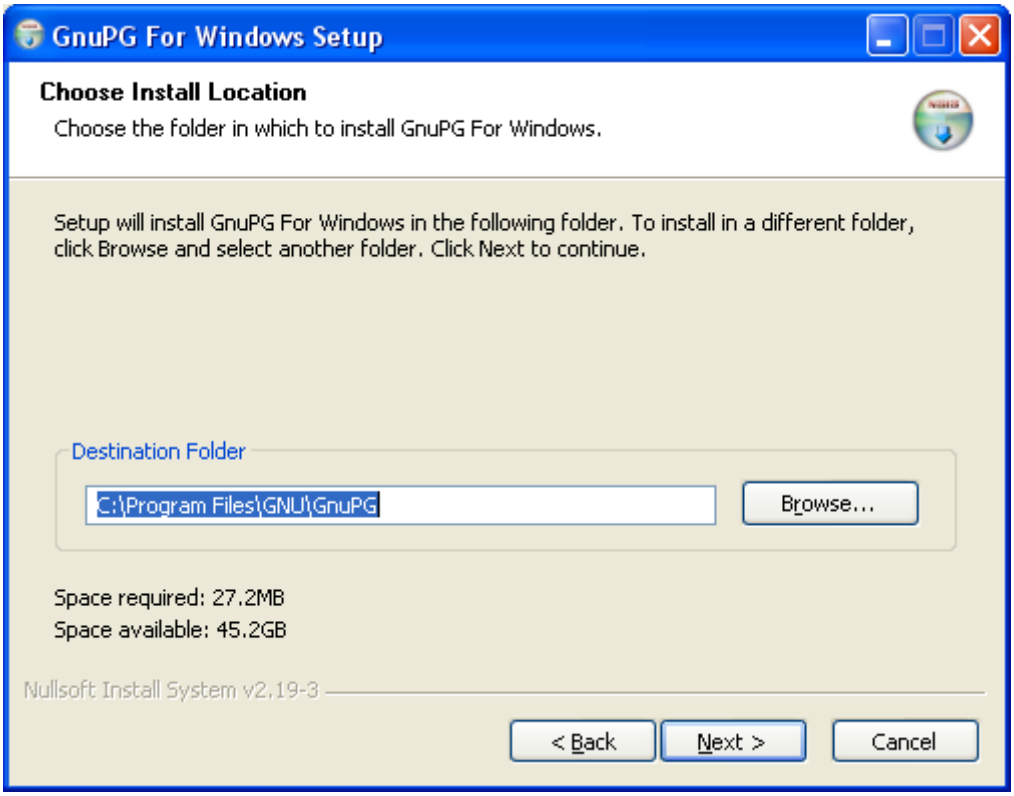
Po pobraniu pliku instalacyjnego ze strony *http://www.gpg4win.org/* rozpoczynamy instalację programu. Instalacja pakietu sprowadza się do akceptacji kolejnych kroków, które zostały przedstawione poniżej:



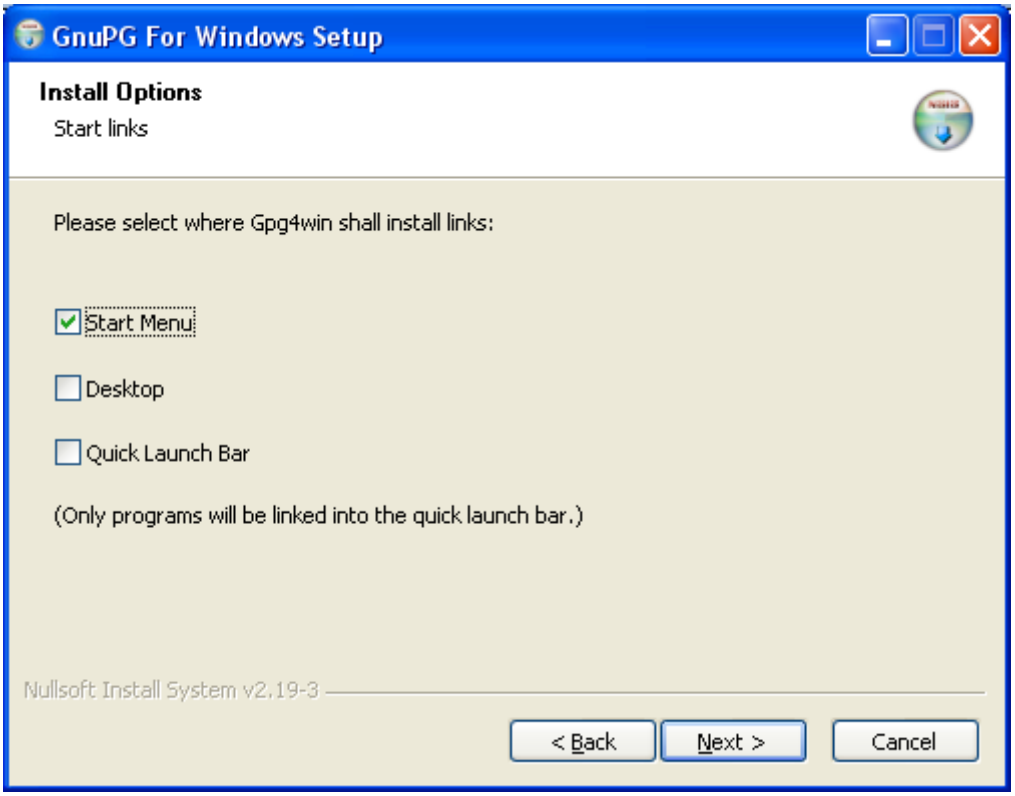
Akceptacja umowy licencyjnej.



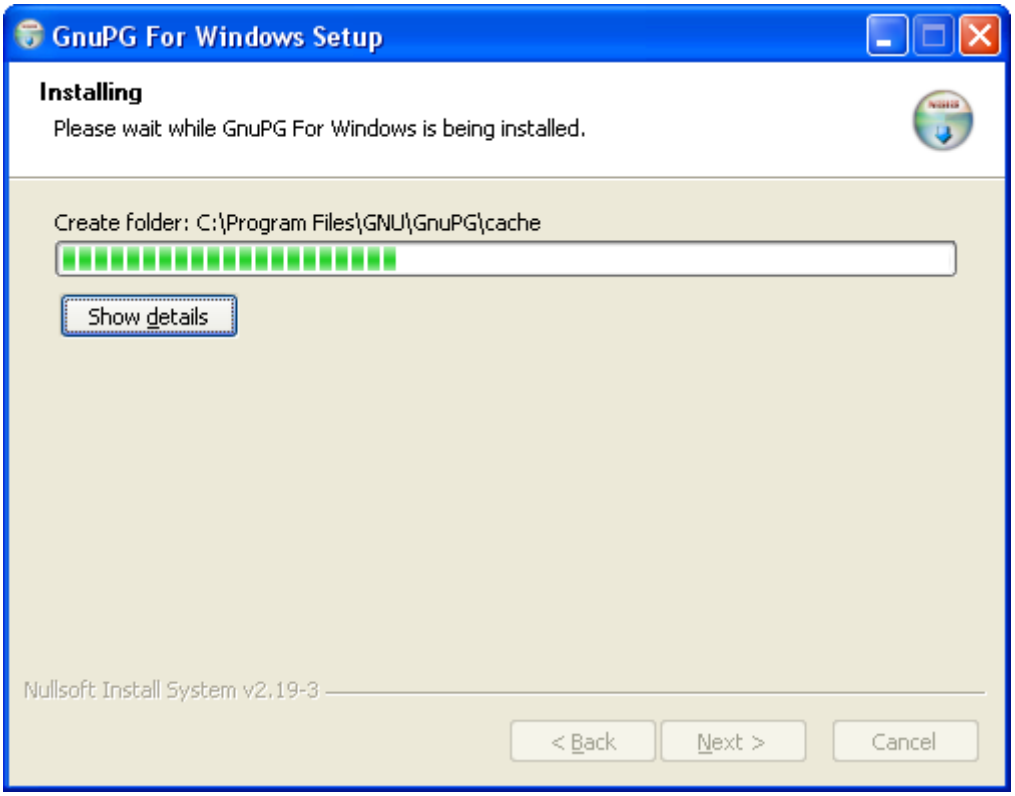
Wybór interesujacych nas kompotentów programu.



Wybór docelowego miejsca instalacji.



Wybór miejsca uruchomienia programu.


GnuPG For Windows Setup
Installing
Please wait while GnuPG For Windows is being installed.
Create folder: C:\Program Files\GNU\GnuPG\cache
Show details
Nullsoft Install System v2.19-3
< Back
Next >
Cancel

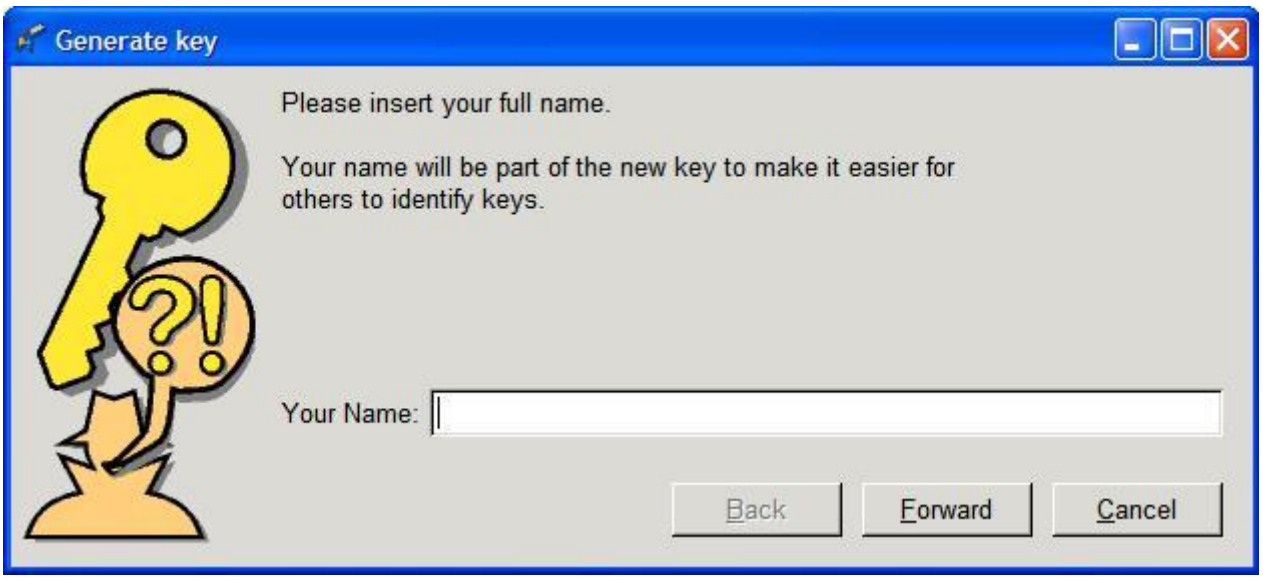
Instalacja.

Końcowy komunikat informujący poprawną instalacje.

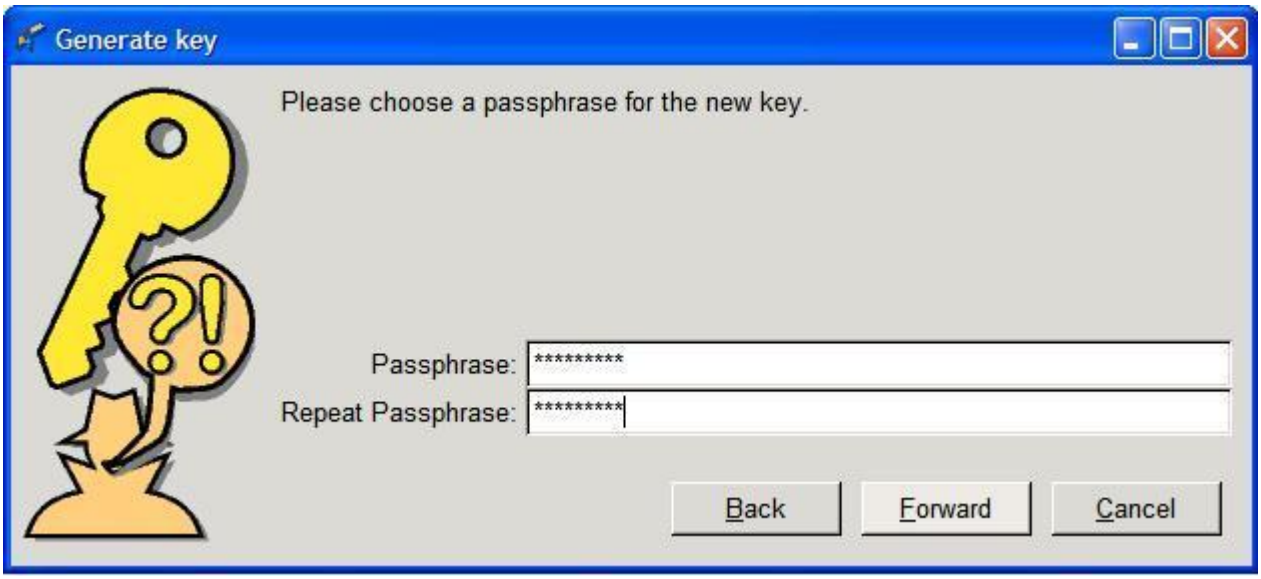
2. Generowanie klucza

Proces generowania klucza przebiega w kilku etapach, w których jest on przypisywany do użytkownika pod różnymi kryteriami, są to: imię, email, hasło dostępu, certyfikat bezpieczeństwa.

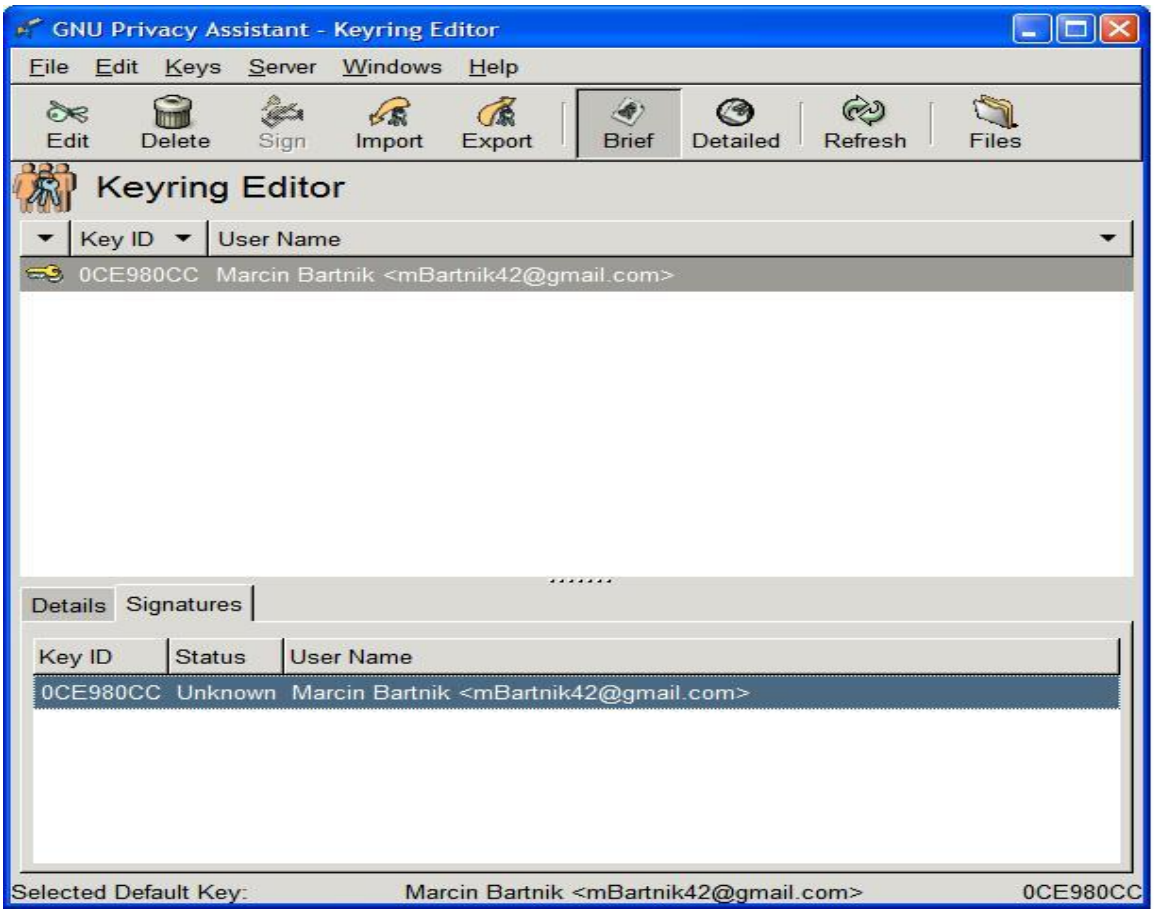
Pierwszy etap to podanie imienia i nazwiska, te dane zostaną zintegrowane z kluczem i staną się jednym z kryteriów jego autentykacji oraz wyszukiwania w bazie kluczy.



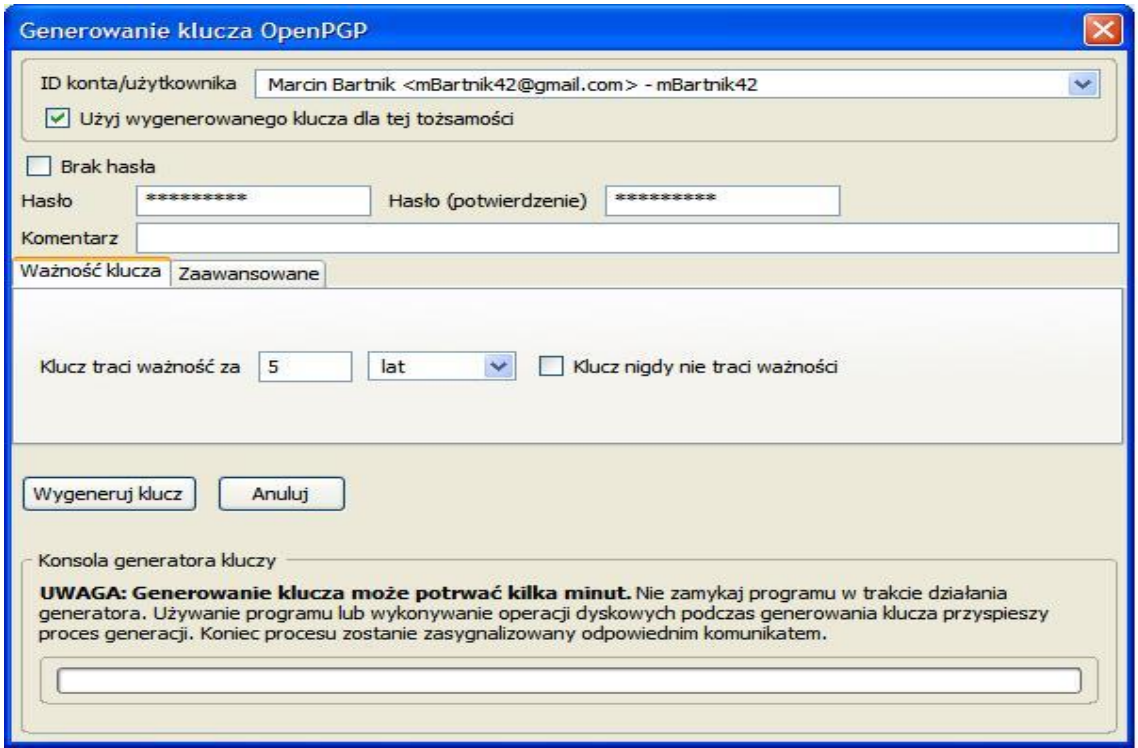
Podajemy hasło do nowo generowanego klucza.



Po wygenerowaniu klucza pojawia się on jako nowy wpis o unikalnym ID, które to może zostać użyte do wyszukania klucza publicznego w bazie danych kluczy (o ile został on wyeksportowany).



W oknie poniżej mamy możliwość wybrania kilku ważnych opcji dla procesu generowania klucza dla programu OpenPGP, są to: ustawienie hasła do klucza (podajemy je przy każdym jego wykorzystaniu), rodzaj szyfrowania i długość klucza (1024, 2048 lub 4096 bitów), a także okres ważności klucza, co umożliwia prowadzenia bezpiecznej polityki. W trakcie generowania klucza mamy możliwość ustanowienia certyfikatu dostępu do niego, który daje również opcję usunięcia go przed terminem jego wygaśnięcia, co również podwyższa poziom bezpieczeństwa.



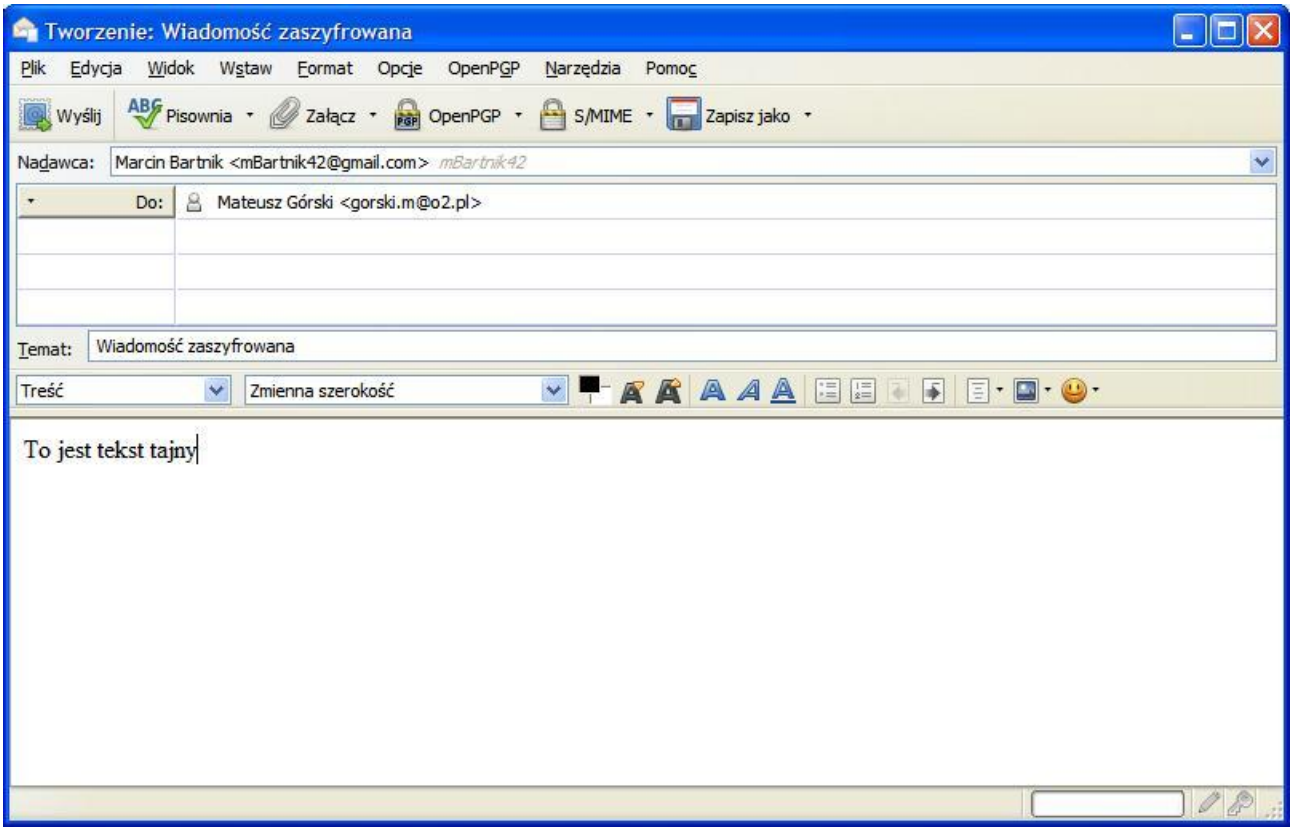
3. Instalowanie dodatku do klienta poczty Mozilla Thunderbird

Aby umożliwić szyfrowanie wiadomości konieczne jest korzystania z klienta pocztowego. My wybraliśmy sprawdzony produkt, jakim jest Mozilla Thunderbird. W tym przypadku konieczne jest zainstalowanie dodatku Enigmail, który powiązany jest z programem OpenPGP. Aby zainstalować dodatek należy ściągnąć go na dysk, a następnie w kliencie pocztowym wybieramy Narzędzia->Dodatki i wskazujemy ścieżkę do pliku z rozszerzeniem. Dodatek nie ma podpisu cyfrowego, lecz pomimo to instalujemy go, po tym procesie konieczne jest ponowne uruchomienie programu.

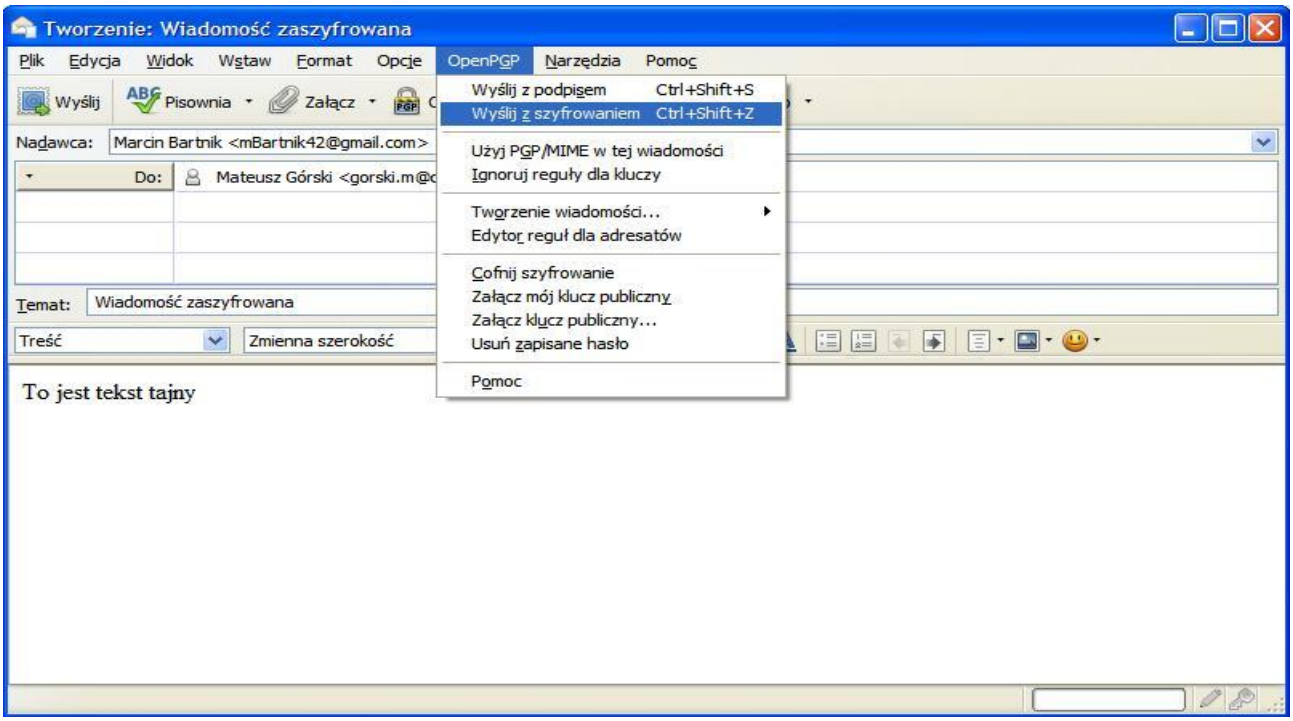
4. Wysyłanie kluczy publicznych i wiadomości

Wysyłanie zaszyfrowanych wiadomości po uprzednim skonfigurowaniu dodatku OpenPGP jest sprawą bardzo prostą i nie wymagającą włączania dodatkowych programów.

Najpierw tak jak przy pisaniu zwykłej niezaszyfrowanej wiadomości wybieramy adresata i wpisujemy treść wiadomości.



Następnie z menu wybieramy opcję „Wyślij z szyfrowaniem”, co sprawia że tekst zostanie zaszyfrowany kluczem publicznym odbiorcy. Jeśli po raz pierwszy wysyłamy wiadomości do adresata, to koniecznie musimy wybrać opcję „Załącz mój klucz publiczny...”, co zaprowadzi nas do menu wyboru klucza publicznego, dołączamy go, gdyż w innym przypadku odbiorca nie ma możliwości odszyfrowania wiadomości.



W tym momencie mamy tekst tajny zaszyfrowany za pomocą klucza publicznego odbiorcy. Mamy tu jeszcze komunikat o potwierdzenie wysłania wiadomości. Wybieramy opcję „Wyślij wiadomość”.