**Sprawozdanie z listy zadań nr 2A**

Zamiara Cyprian, Nr indeksu: 260518

Poniedziałek TN, 15:15

Zadanie: konfiguracja usług pocztowych w celu bezpiecznej komunikacji mailowej  
Narzędzia wykorzystane: System Microsoft Windows 10 Professional, Mozilla ThunderBird, serwis pocztowy gazeta.pl, serwis actalis.it  
Cel zadania: poznanie zagadnień z zakresu bezpiecznej komunikacji mailowej, nabycie umiejętności dotyczących podpisów cyfrowych oraz szyfrowanej korespondencji

**Zadanie 1. Konfiguracja konta pocztowego.**

Cel zadania: zdobycie umiejętności założenia konta pocztowego oraz identyfikacja informacji parametrów konfiguracyjnych dla danego klienta poczty.

Wykorzystane narzędzia: Mozilla Thunderbird, klient pocztowy gazeta.pl



rys 1

Zrzut ekranu (rys. 2) ilustruje parametry konfiguracyjne aplikacji klienta poczty dla serwisu gazeta.pl

Czynności wykonane:

* Będąc zalogowanym na poczcie, na lewym pasku nawigacyjnym należy kliknąć zębatkę 🡪 następnie wejść w panel „Informacje”

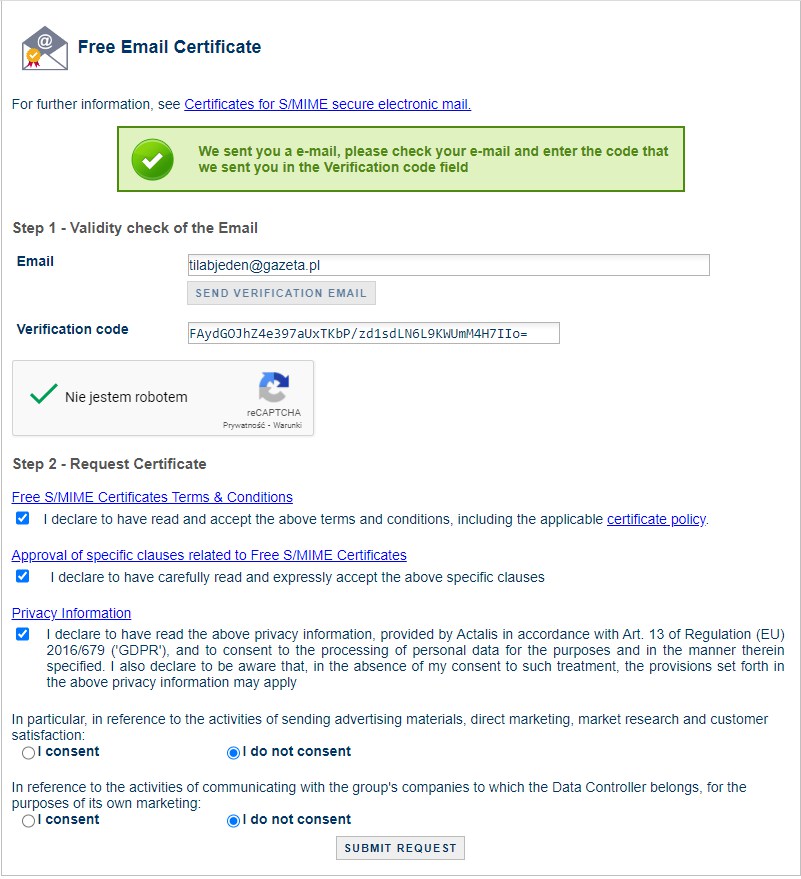
W parametrach poczty widnieją informacje o protokołach IMAP, POP3, SMTP oraz możliwość ich włączenia/wyłączenia.

* POP3 – protokół służący do odbioru poczty elektronicznej
* IMAP – następca protokołu POP3, dodaje więcej funkcjonalności – np. zarządzanie wieloma folderami pocztowymi
* SMTP – protokół służący do wysyłania wiadomości elektronicznej przez serwer pocztowy

**Zadanie 2. Klucze i certyfikaty.**

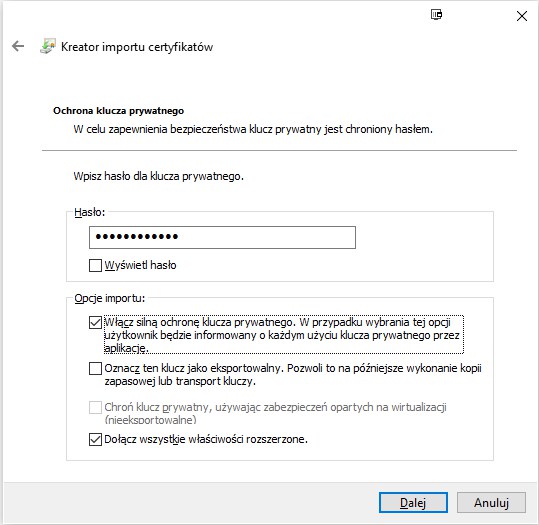
Cel zadania: pozyskanie umiejętności z zakresu pozyskiwania certyfikatów do zabezpieczania wiadomości mailowych

Wykorzystane narzędzia: System Microsoft Windows 10 Professional, Mozilla ThunderBird, serwis actalis.it



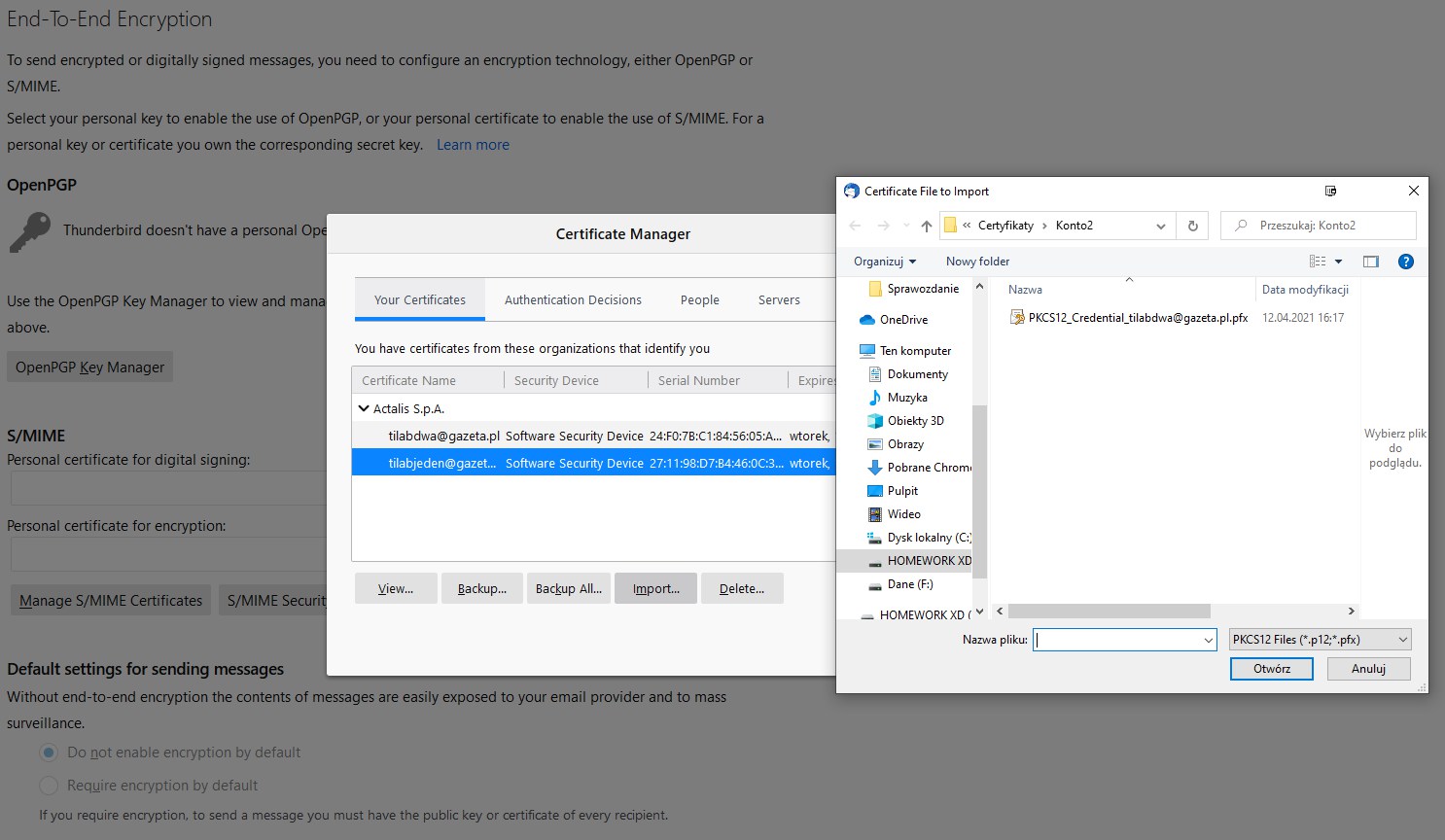
rys 2

Na zrzucie ekranu (rys. 2) znajduje się wypełnione podanie o certyfikat. Po udanym przesłaniu formularza na skrzynkę mailową przyjdzie wiadomość z hasłem do certyfikatu oraz archiwum, w którym znajdować będzie się certyfikat.



rys 3

Powyższy zrzut ekranu (rys. 3) prezentuję akcję importowania certyfikatu do magazynu Windows.  
Opcja włączenia silnej ochrony została zaznaczona w celu podwyższenia bezpieczeństwa oraz informowania użytkownika o każdej akcji związanej z wykorzystaniem klucza prywatnego.

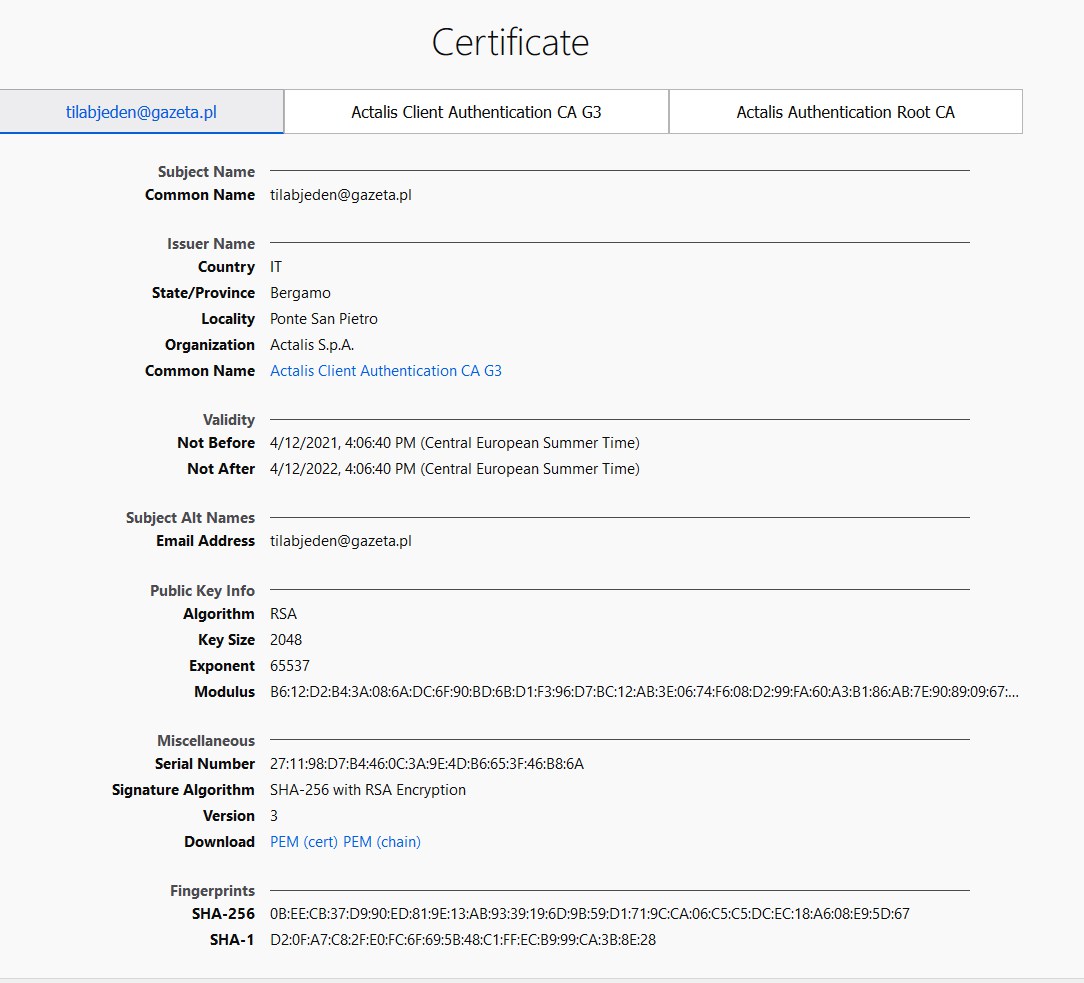


rys 4

Zrzut ekranu (rys.4) ilustruję akcję importu klucza do aplikacji Mozilla ThunderBird.

Czynności wykonane w celu zaimportowania danych:

Prawy przycisk myszy na konto mailowe w programie 🡪 Settings -> End-To-End Encryption 🡪 Manage S/MIME Certificates 🡪 Your Certificates 🡪 Import 🡪 Wybór pliku z certyfikatem



rys 5

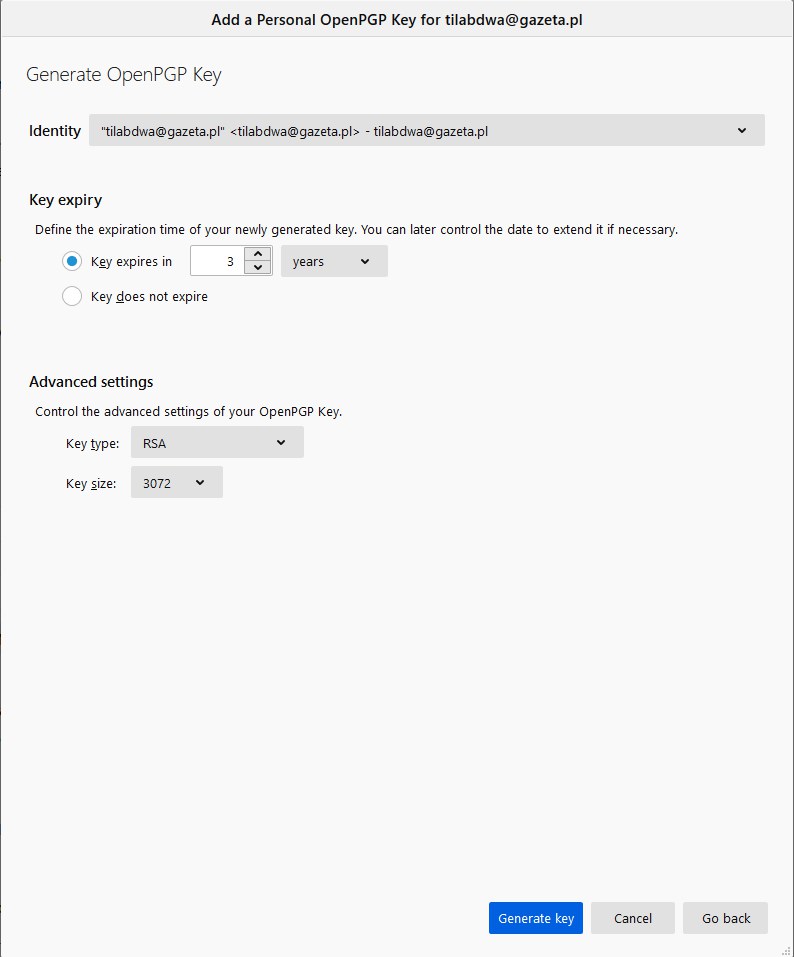
Powyższy zrzut ekranu (rys. 5) przedstawia właściwości certyfikatu w aplikacji Mozilla ThunderBird.  
Informacje, które możemy z nich wyczytać:

* Adres e-mail przypisany do certyfikatu (Email Address)
* Użyty algorytm szyfrujący (Algorithm)
* Odcisk palca certyfikatu – unikalny identyfikator danego certyfikatu (Finerprints)

**Zadanie 3. Szyfrowanie i podpisywanie wiadomości e-mail**

Cel zadania: pozyskanie umiejętności z zakresu wykorzystania certyfikatów (kluczy publicznych oraz prywatnych) do szyfrowania oraz podpisywania wiadomości mailowych

Wykorzystane narzędzia: Mozilla ThunderBird, serwis pocztowy gazeta.pl

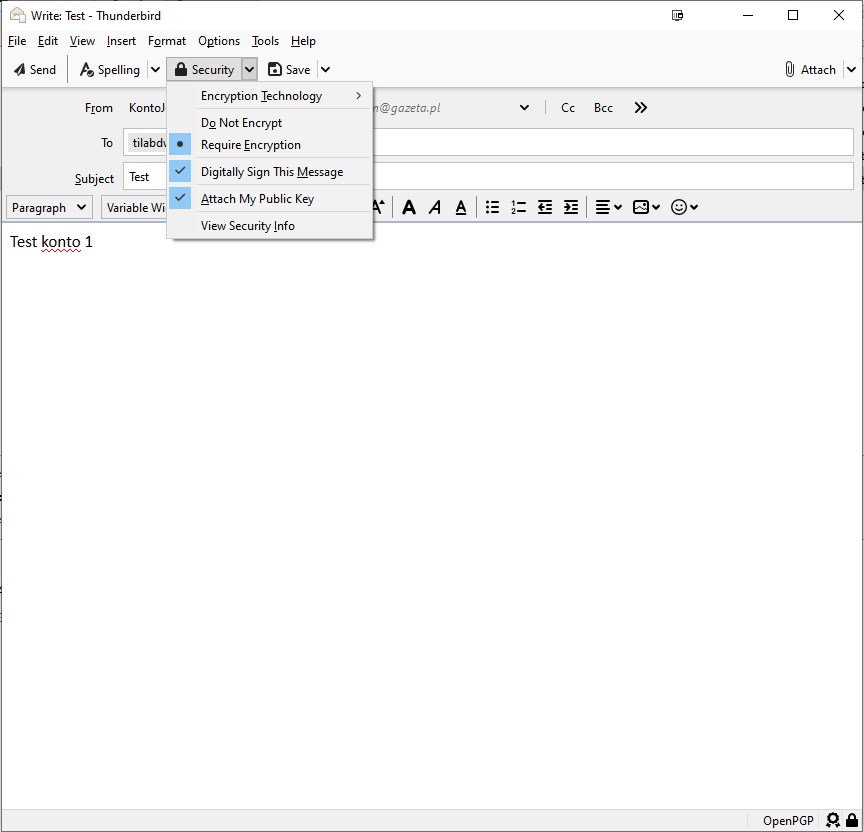


rys 6

Zrzut ekranu (rys. 6) prezentuje generowanie klucza publicznego dla konta mailowego.  
Wykonane czynności: W programie Mozilla ThunderBird prawy przycisk myszki na nazwie konta 🡪 opcja Settings 🡪 End-To-End Encryption 🡪 OpenPGP Add Key

Jesteśmy w stanie skonfigurować opcje dla klucza takie jak:

* Ważność klucza
* Rodzaj szyfrowania (algorytm)
* Rozmiar klucza



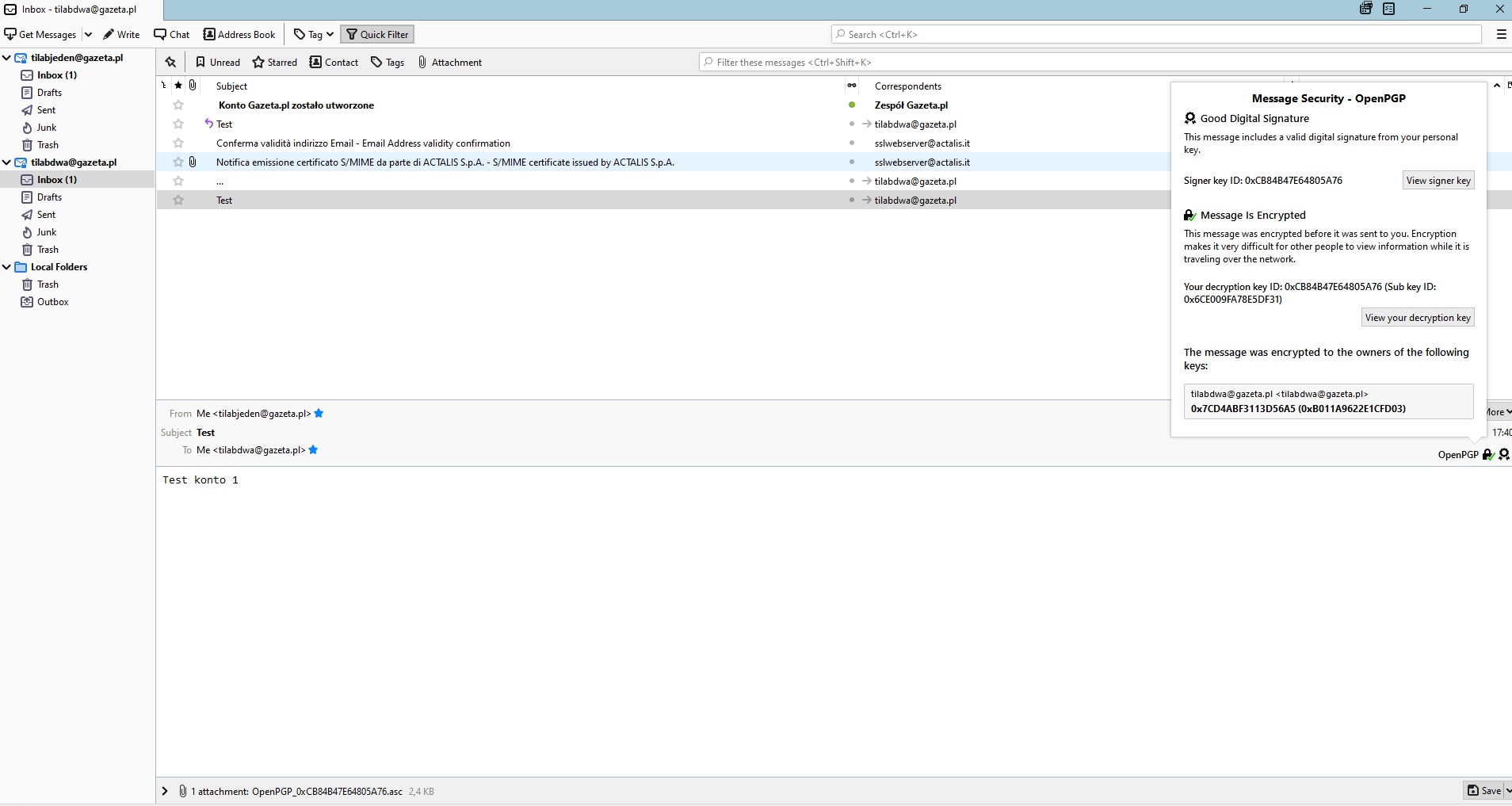
rys 7

Powyższa ilustracja (rys. 7) ilustruje akcję wysyłania zaszyfrowanej oraz podpisanej wiadomości email.  
Opcje zaznaczone reprezentują:

* Require Encryption – wiadomość szyfrowana
* Digitally Sign This Message – do wiadomości zostaje dołączony podpis cyfrowy
* Attach My Public Key – do wiadomości zostaje dołączony klucz publiczny osoby co wysyła wiadomość

Poprawność konfiguracji pokazują ikony w lewym dolnym rogu:

* Kłódka – plik jest szyfrowany
* Wstęga – został załączony podpis cyfrowy

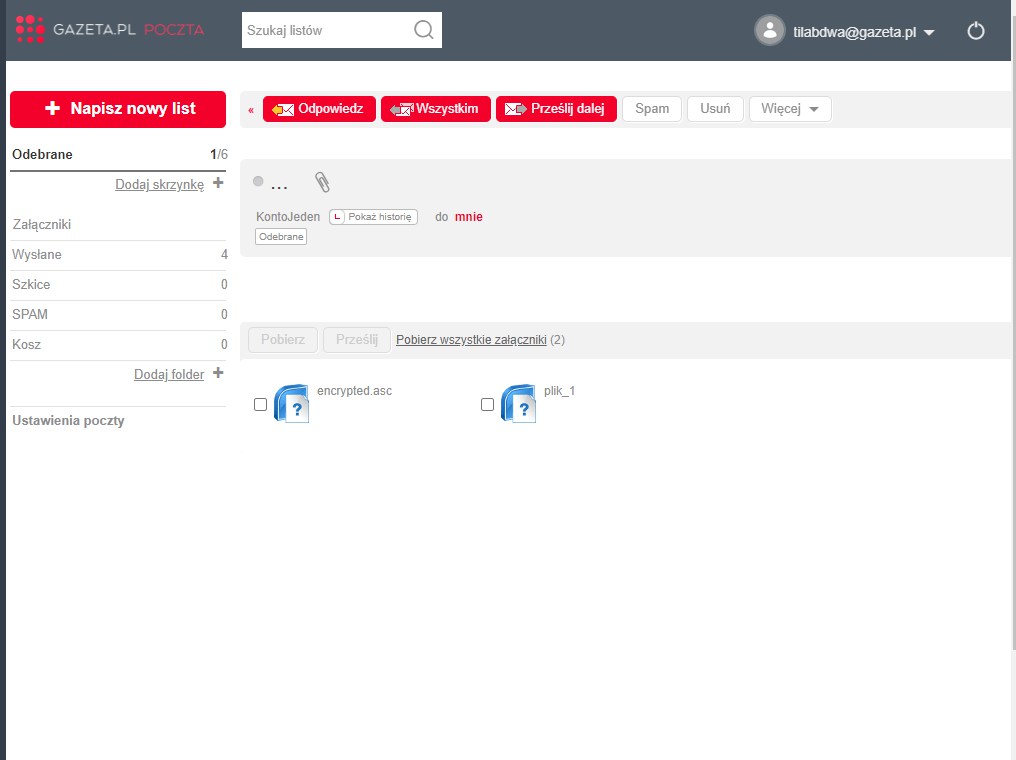


rys 8

Powyższy zrzut ekranu (rys. 8) ilustruje odebraną wiadomość przez odbiorcę.  
Wiadomość została automatycznie rozszyfrowana dzięki dostarczonemu kluczu publicznemu.

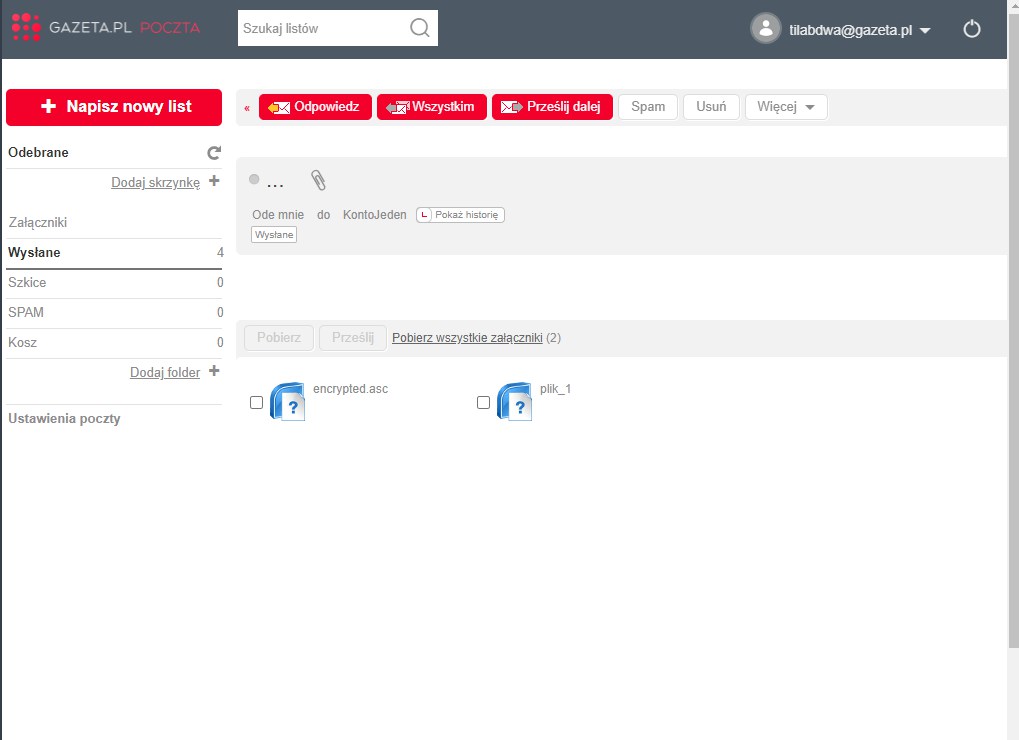
Klikając na ikony przy napisie „OpenPGP” jesteśmy w stanie znaleźć informacje takie jak:

* Good Digital Signature – oznacza, że wiadomość została podpisana
* Message is Encrypted – wiadomość została zaszyfrowana oraz rozszyfrowana z użyciem klucza publicznego
* Ostatnia sekcja – adres email odbiorcy oraz klucz publiczny odbiorcy oraz nadawcy



rys 9

Zrzut ekranu (rys. 9) przedstawia wiadomość zaszyfrowaną oraz podpisaną odebraną w aplikacji pocztowej serwisu gazeta.pl.  
Nie jesteśmy w stanie odczytać zaszyfrowanej wiadomości z poziomu aplikacji internetowej.



rys 10

Zrzut (rys.10) pokazuje zaszyfrowaną wiadomość nadaną w aplikacji internetowej.

W obu przypadkach (rys.9, rys.10) nie jesteśmy w stanie odczytać wiadomości szyfrowanej – ani wysyłanej ani odebranej. Aplikacja pocztowa gazeta.pl nie obsługuje tego typu operacji, do tych akcji wymagany jest w tym przypadku zewnętrzny program pocztowy.

**Podsumowanie**

**Wnioski:**

Umiejętności generowania certyfikatów oraz umiejętne korzystanie z nich jest bardzo ważne przy dokonywaniu korespondencji, które zawierają wrażliwe dane. Dane przesyłane przez protokół TCP/IP mogą zostać w prosty sposób wykradzione, szyfrowanie unikalnym kluczem prywatnym oraz odczytywanie z użyciem klucza publicznego zabezpiecza dane znajdujące się w wiadomości.

Dzięki temu tylko nadawca oraz odbiorca są w stanie wiadomości rozszyfrować, jest to bardzo ważny element zabezpieczania danych przy wysyłaniu danych pomiędzy różnymi serwerami w sieci internet.