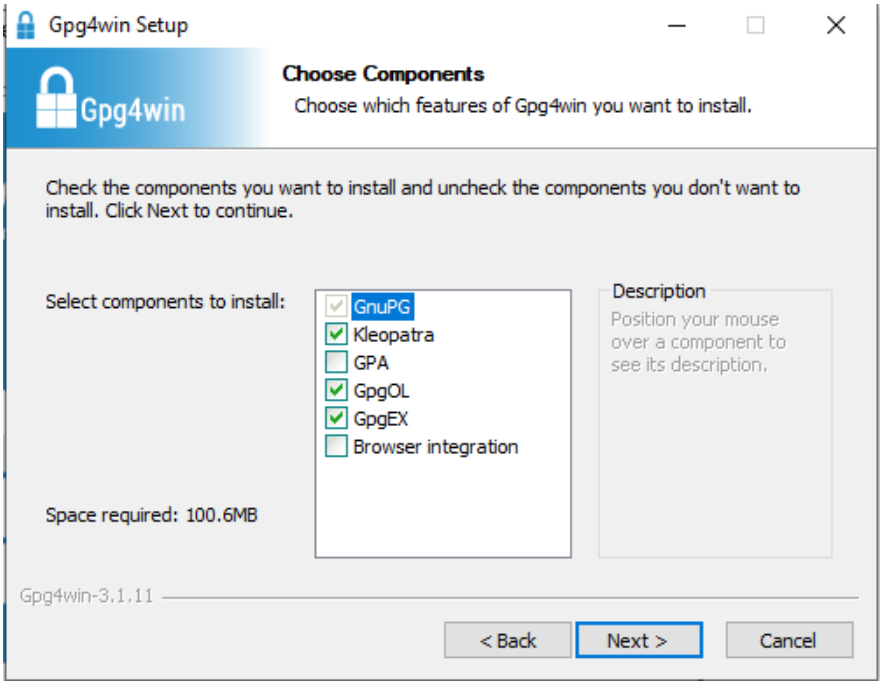
Instrukcja instalacji , szyfrowania i generowania kluczy GPG

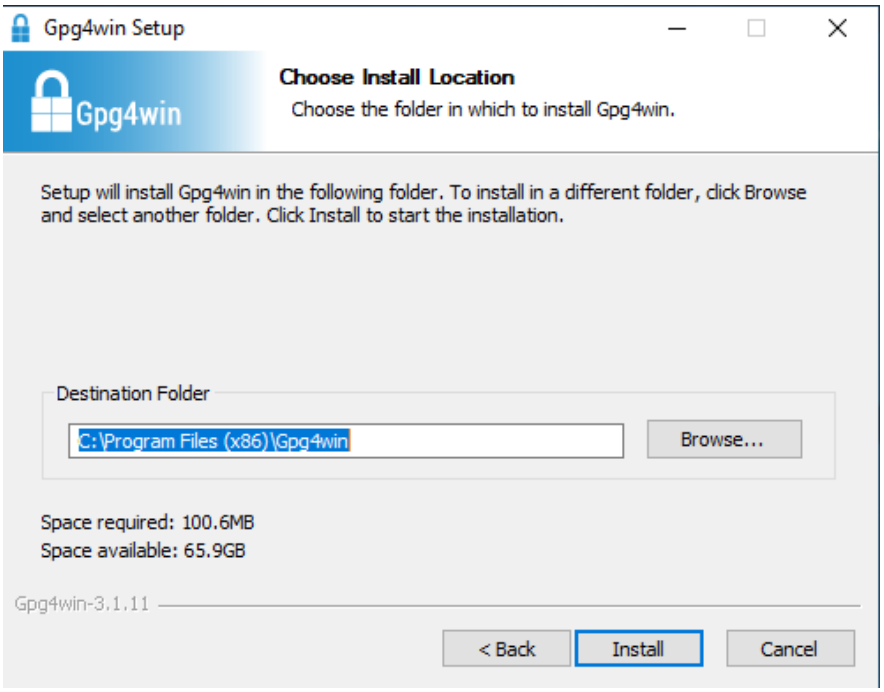
Ze strony https://www.gpg4win.org/ pobieramy program gpg4win.

Uruchamiamy i instalujemy oprogramowanie wybierając domyślne ustawienia.

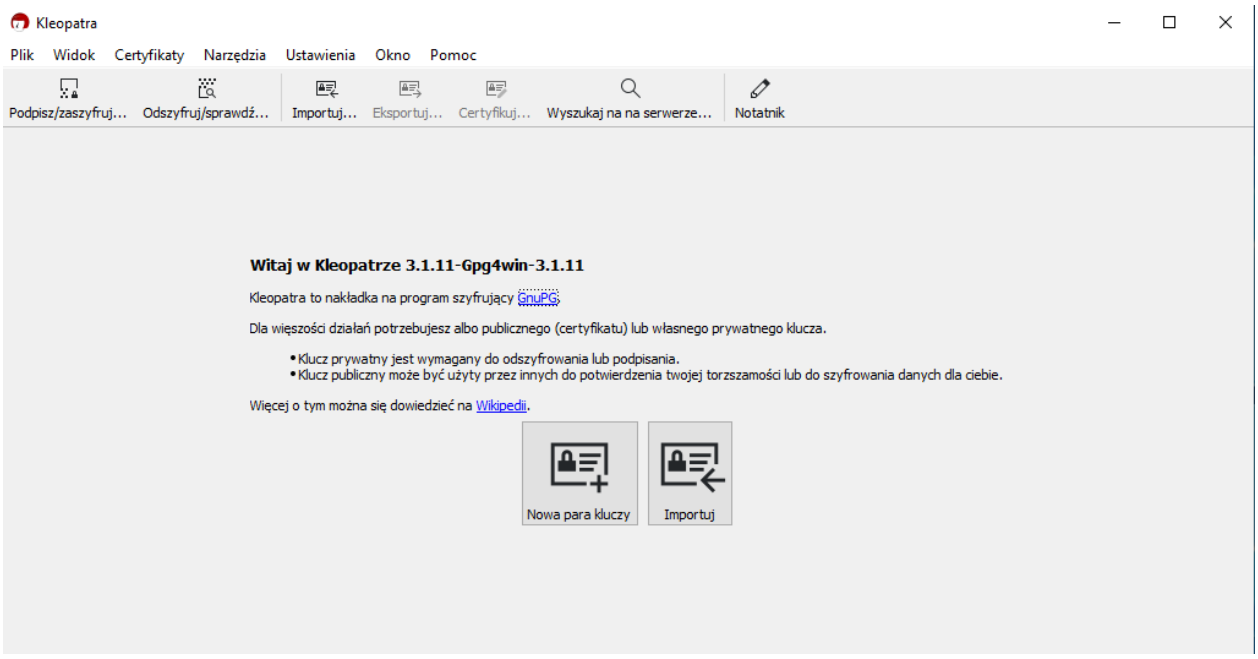
Next

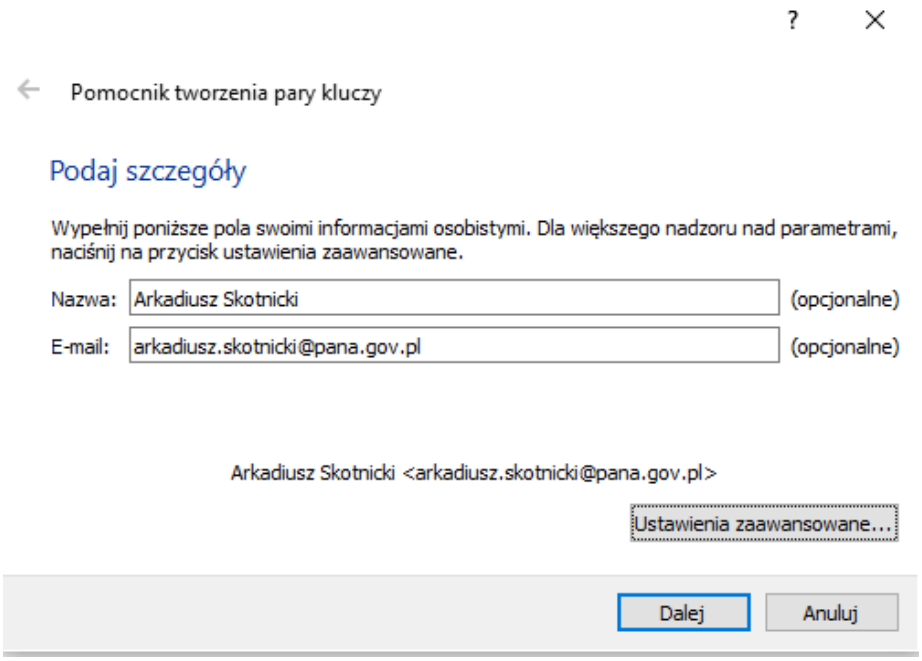


Wskazujemy ścieżkę do instalacji (może zostać domyślna)

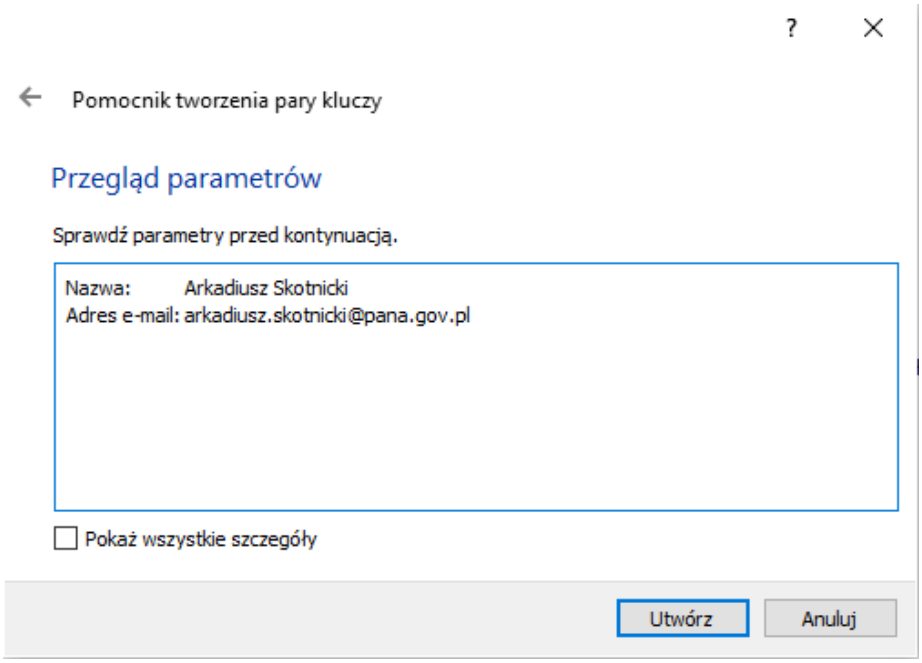


Po instalacji uruchamiamy program Kleopatra (Start-Programy – Kleopatra, jest to nakładka na system szyfrujący GPG) i generujemy klucze -> **NOWA PARA KLUCZY**



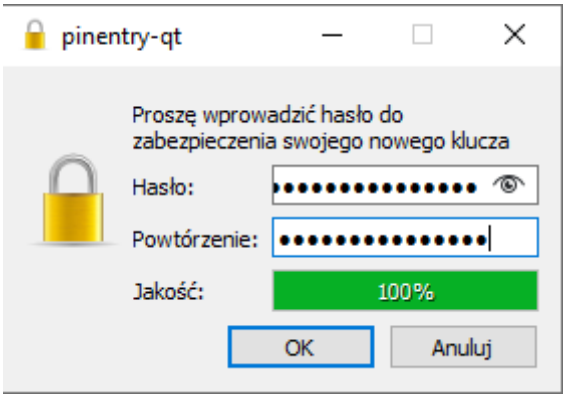


Podajemy Nazwę Firmy i mail.

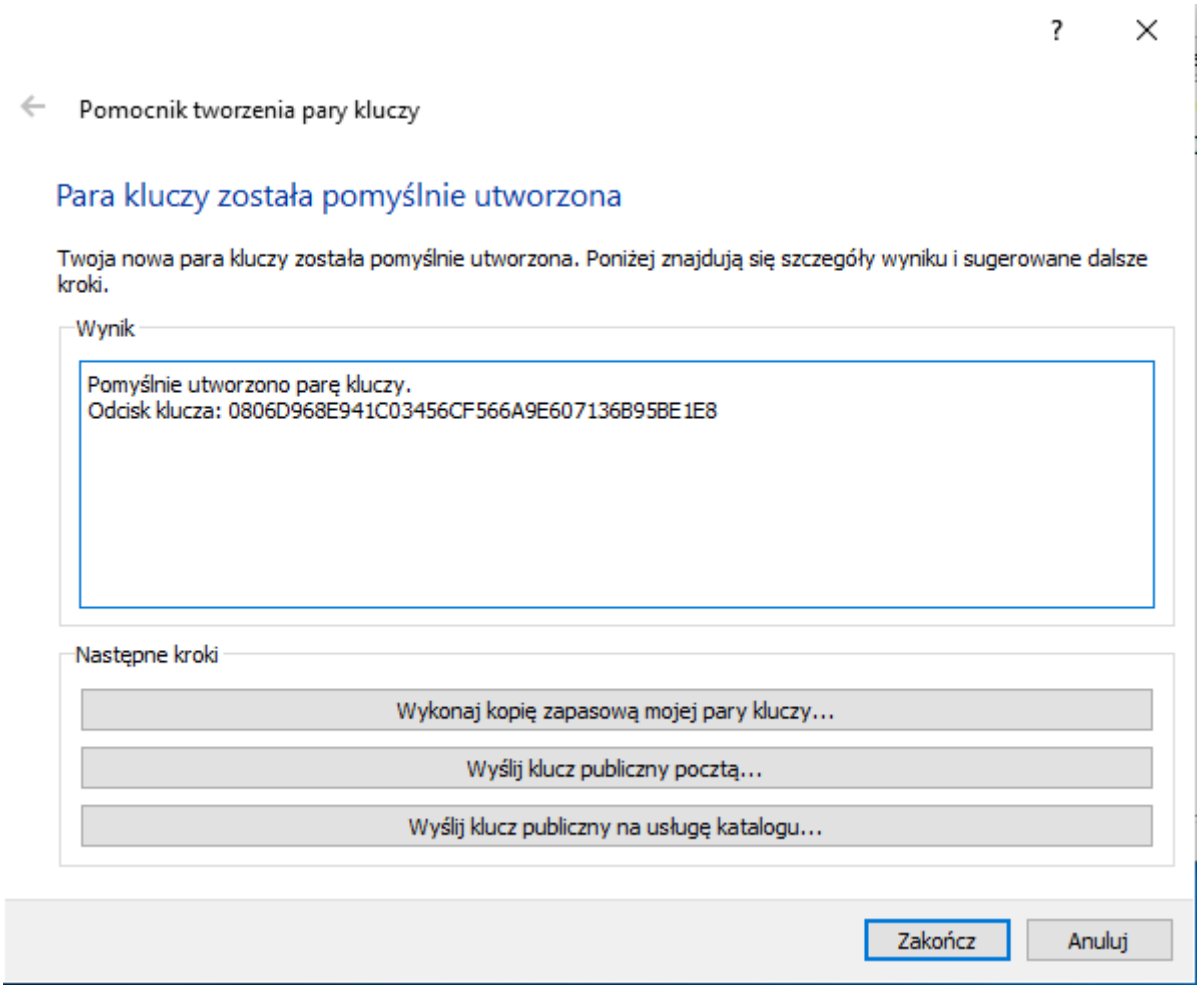


Potwierdzamy utworzenie kluczy.

Zostaniemy poproszeni o utworzenie hasła do kluczy. (którymi później będziemy zabezpieczać nasze pliki)

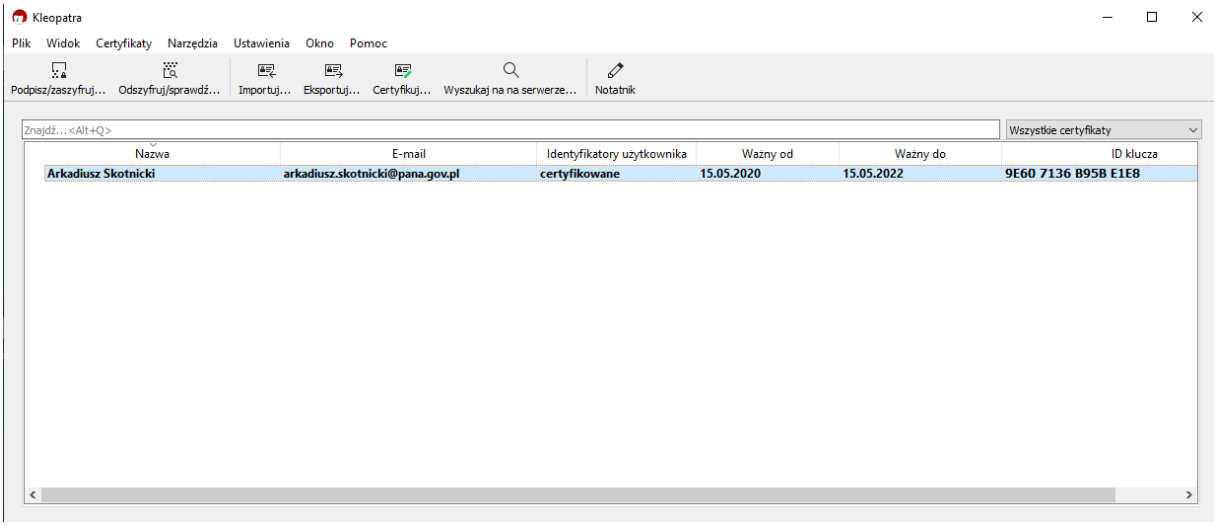


Podajemy dwukrotnie i ZAPAMIETUJEMY !!!

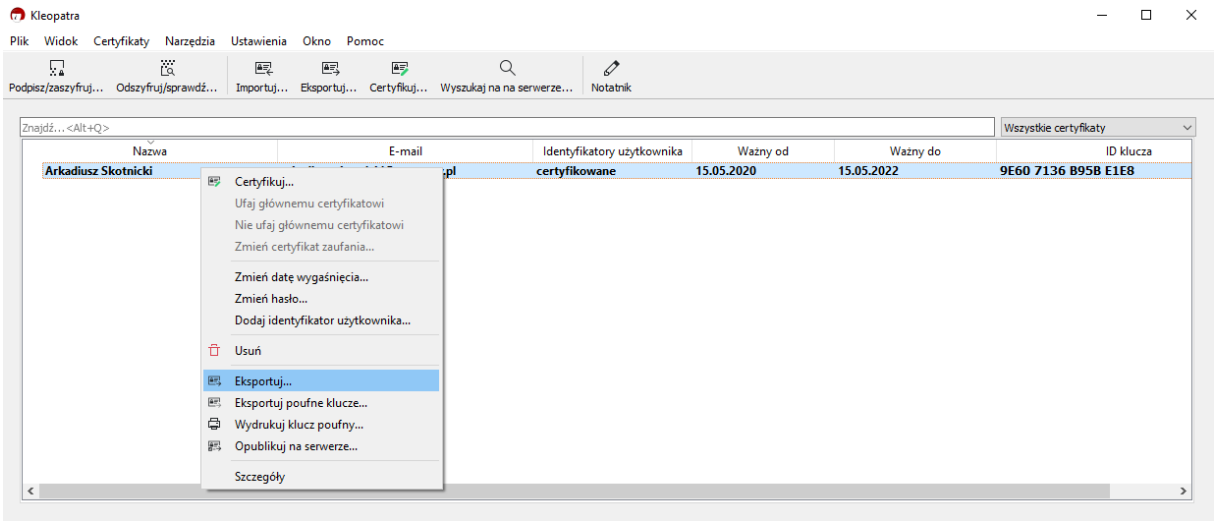


Para kluczy została pomyślnie utworzona. ZAKOŃCZ.

Kolejnym krokiem jest wyeksportowanie klucza publicznego i wysłanie go do osób do których będziemy wysyłać zaszyfrowane dokumenty.



Zaznaczamy klucz i prawym klawiszem myszy wybieramy export



Następnie zapisujemy klucz publiczny w dowolnym miejscu.

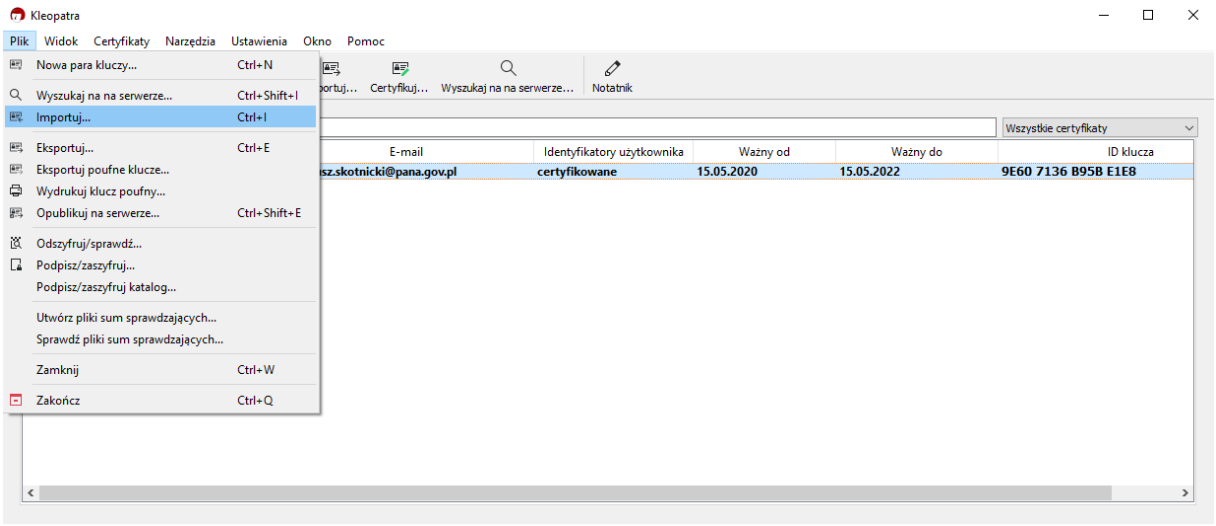
Kolejnym krokiem jest wysłanie tego wyeksportowanego klucza jako załącznik do osoby z którą będziemy się komunikować.

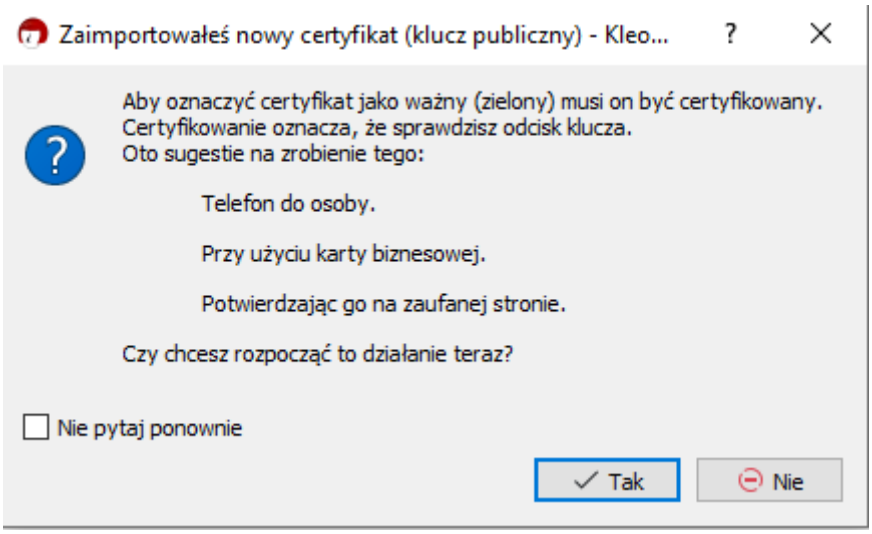
Od tej osoby powinniśmy tez dostać podobny plik (jej klucz publiczny) który powinniśmy zaimportować.

Import certyfikatów partnera

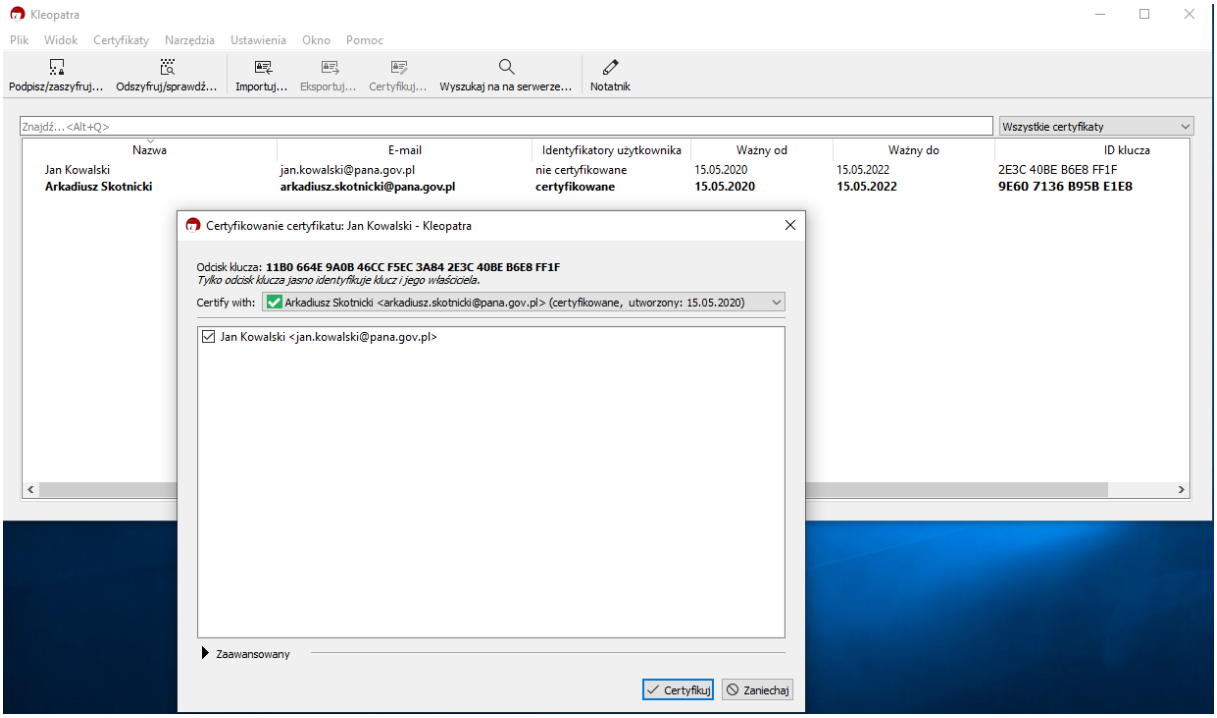
Aby móc zaszyfrowywać przesłane treści od innych osób , importujemy przesłany certyfikat partnera.

Uruchamiamy program Kleopatra , z menu Plik wybieramy opcje importuj, następnie wskazujemy przesłany plik.

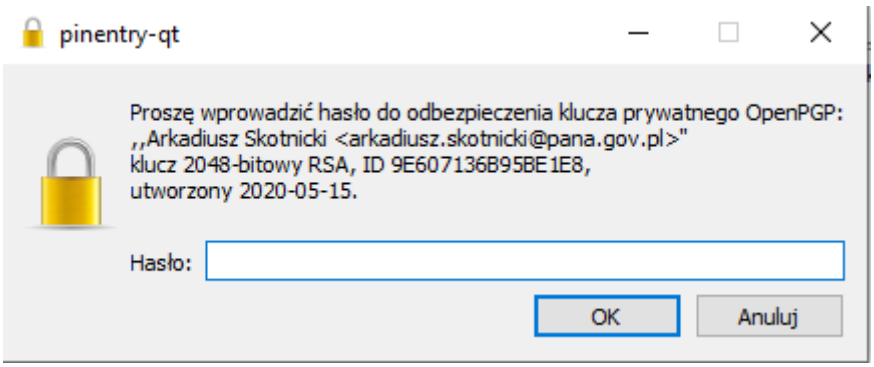




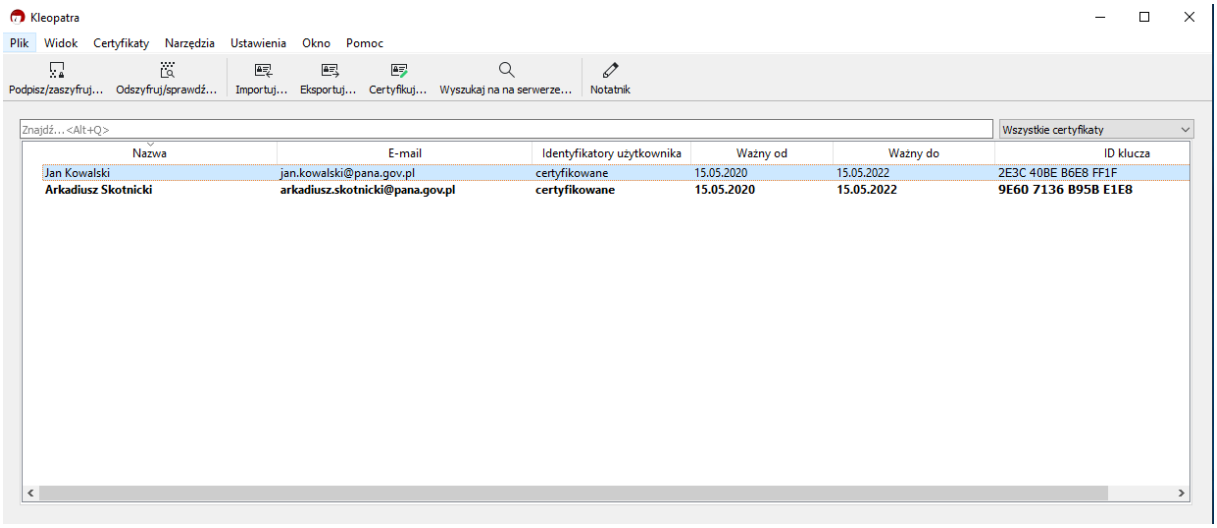
I potwierdzamy autentyczność.

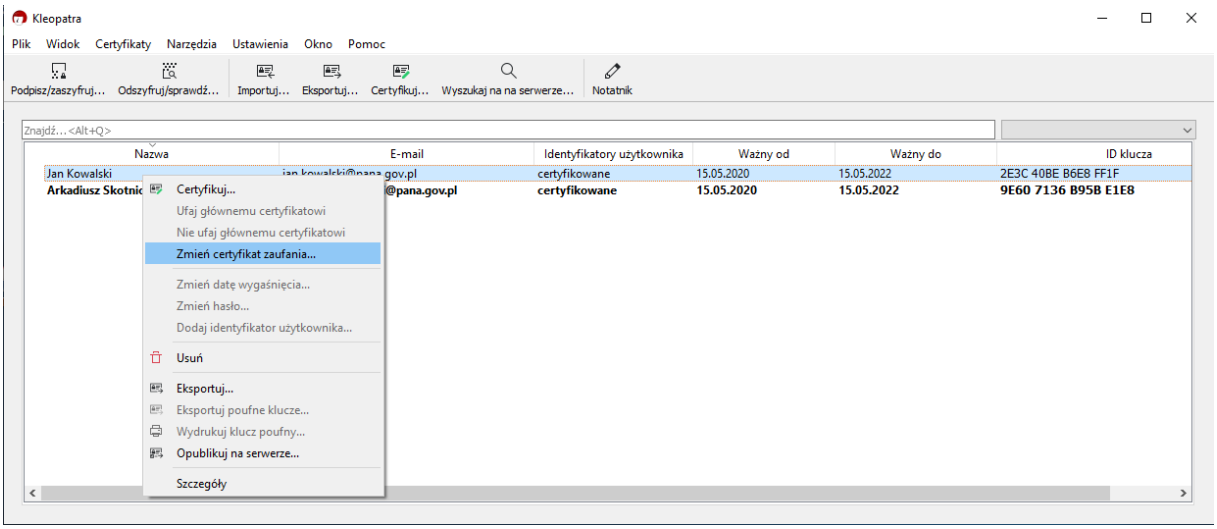


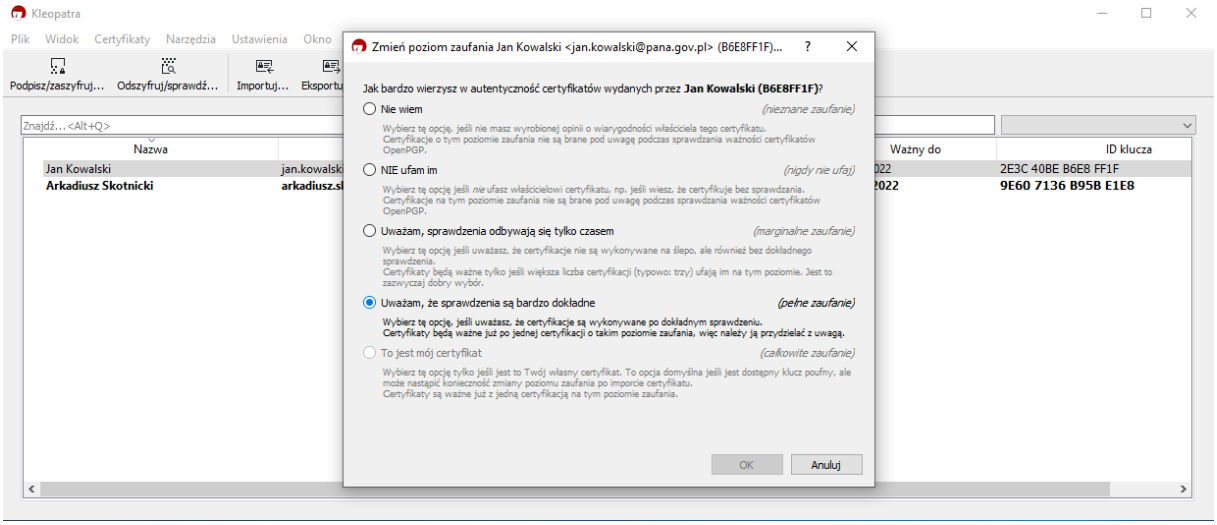
Klikamy prawym klawiszem myszy na certyfikat następnie – certyfikuj.



Wprowadzamy hasło utworzone podczas generowania pary kluczy.


Kleopatra
Plik Widok Certyfikaty Narzędzia Ustawienia Okno Pomoc
Podpisz/zaszyfruj… Odszyfruj/sprawdź… Importuj… Eksportuj… Certyfikuj… Wyszukaj na na serwerze… Notatnik
Znajdź… <Alt+Q>
Wszystkie certyfikaty
Nazwa E-mail Identyfikatory użytkownika Ważny od Ważny do ID klucza
Jan Kowalski jan.kowalski@pana.gov.pl certyfikowane 15.05.2020 15.05.2022 2E3C 40BE B6E8 FF1F
Arkadiusz Skotnicki arkadiusz.skotnicki@pana.gov.pl certyfikowane 15.05.2020 15.05.2022 9E60 7136 B95B E1E8

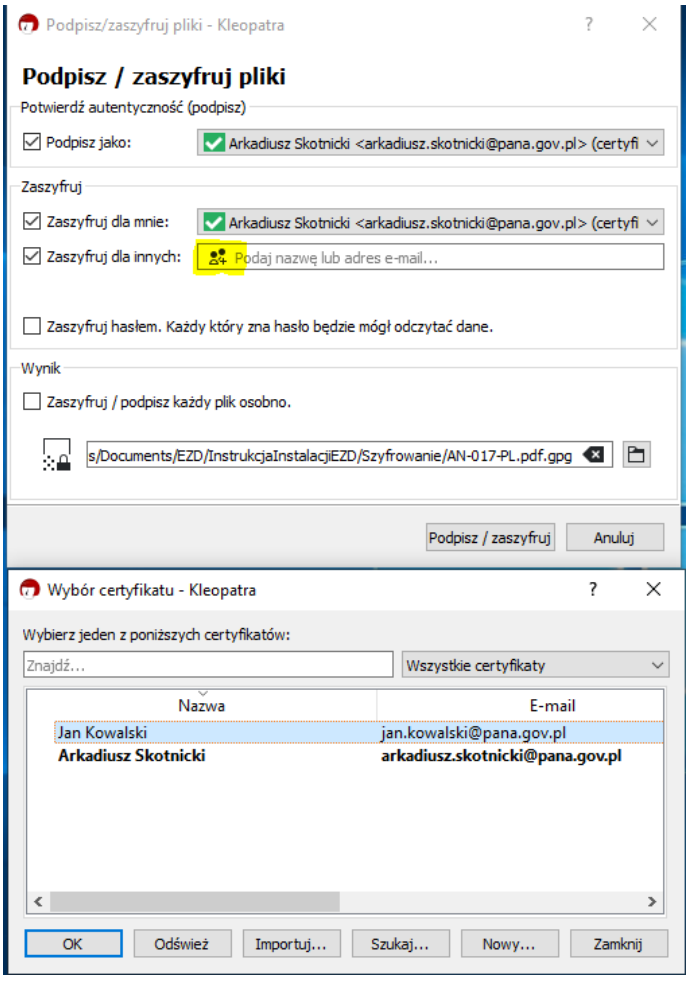

Kleopatra
Plik Widok Certyfikaty Narzędzia Ustawienia Okno Pomoc
Podpisz/zaszyfruj… Odszyfruj/sprawdź… Importuj… Eksportuj… Certyfikuj… Wyszukaj na na serwerze… Notatnik
Znajdź… <Alt+Q>
Nazwa E-mail Identyfikatory użytkownika Ważny od Ważny do ID klucza
Jan Kowalski certyfikowane 15.05.2020 15.05.2022 2E3C 40BE B6E8 FF1F
Arkadiusz Skotnic @pana.gov.pl certyfikowane 15.05.2020 15.05.2022 9E60 7136 B95B E1E8
Certyfikuj…
Ufaj głównemu certyfikatowi
Nie ufaj głównemu certyfikatowi
Zmień certyfikat zaufania…
Zmień datę wygaśnięcia…
Zmień hasło…
Dodaj identyfikator użytkownika…
Usuń
Eksportuj…
Eksportuj poufne klucze…
Wydrukuj klucz poufny…
Opublikuj na serwerze…
Szczegóły


Kleopatra
Zmień poziom zaufania Jan Kowalski <jan.kowalski@pana.gov.pl> (B6E8FF1F)…
Jak bardzo wierzysz w autentyczność certyfikatów wydanych przez Jan Kowalski (B6E8FF1F)?
Nie wiem (nieznane zaufanie)
Wybierz tę opcję, jeśli nie masz wyrobionej opinii o wiarygodności właściciela tego certyfikatu. Certyfikacje o tym poziomie zaufania nie są brane pod uwagę podczas sprawdzania ważności certyfikatów OpenPGP.
NIE ufam im (nigdy nie ufaj)
Wybierz tę opcję jeśli nie ufasz właścicielowi certyfikatu, np. jeśli wiesz, że certyfikuje bez sprawdzania. Certyfikacje na tym poziomie zaufania nie są brane pod uwagę podczas sprawdzania ważności certyfikatów OpenPGP.
Uważam, sprawdzenia odbywają się tylko czasem (marginalne zaufanie)
Wybierz tę opcję jeśli uważasz, że certyfikacje nie są wykonywane na ślepo, ale również bez dokładnego sprawdzenia. Certyfikaty będą ważne tylko jeśli większa liczba certyfikacji (typowo: trzy) ufają im na tym poziomie. Jest to zazwyczaj dobry wybór.
Uważam, że sprawdzenia są bardzo dokładne (pełne zaufanie)
Wybierz tę opcję, jeśli uważasz, że certyfikacje są wykonywane po dokładnym sprawdzeniu. Certyfikaty będą ważne już po jednej certyfikacji o takim poziomie zaufania, więc należy ją przydzielać z uwagą.
To jest mój certyfikat (całkowite zaufanie)
Wybierz tę opcję tylko jeśli jest to Twój własny certyfikat. To opcja domyślna jeśli jest dostępny klucz poufny, ale może nastąpić konieczność zmiany poziomu zaufania po imporcie certyfikatu. Certyfikaty są ważne już z jedną certyfikacją na tym poziomie zaufania.
OK
Anuluj

Szyfrowanie Pliku

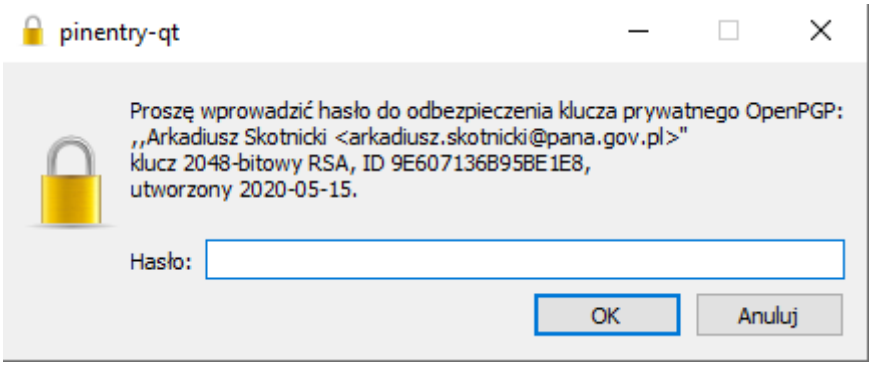
Zaznaczamy /prawym klawiszem myszy/ plik do zaszyfrowania.

Wybieramy opcje podpisz i zaszyfruj **, w polu zaszyfruj dla innych klikamy w ikonę plusa/osób** (lub wpisujemy w polu obok , adres mail - ręcznie) , **następnie wybieramy osobę/firmę której certyfikat wcześniej zaimportowaliśmy** .

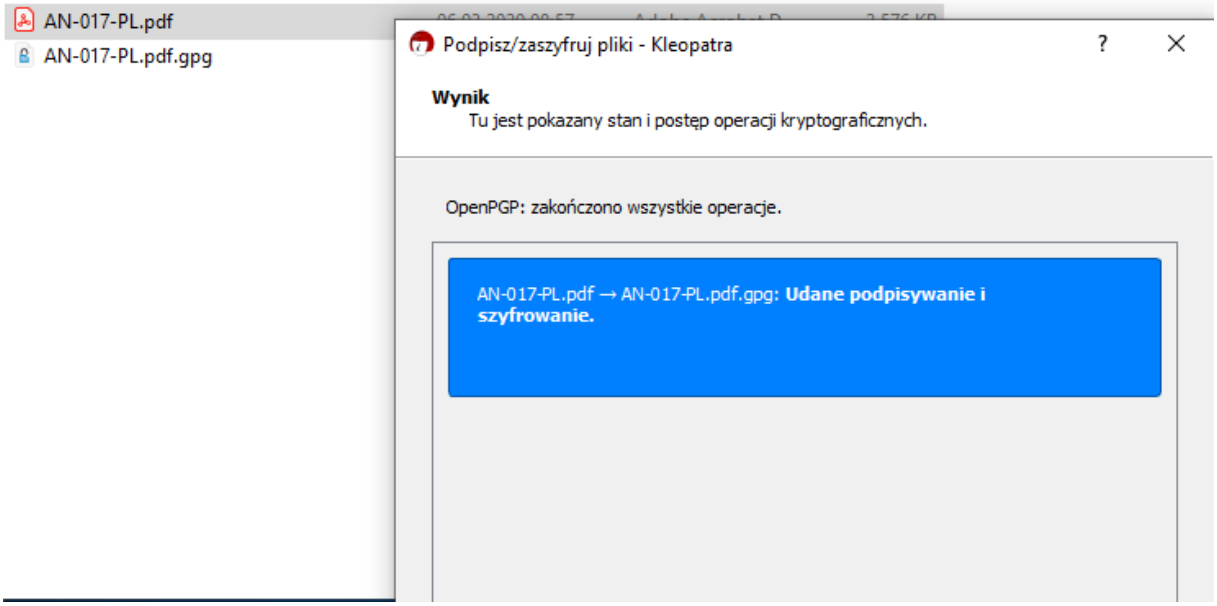


Zostawiamy domyślne opcje i naciskamy - podpisz i zaszyfruj.

Zostaniemy poproszeni ponownie o hasło.



Wprowadzamy je i plik zostaje zaszyfrowany.



Plik z rozszerzeniem .gpg wysyłamy jako załącznik.

Odszyfrowywanie pliku.

Aby odszyfrować otrzymany plik , dwukrotnie klikamy, podajemy hasło wskazujemy miejsce do odszyfrowania lub prawy klawisz myszy na zaszyfrowanym pliku i wybieramy

ew z menu plik - odszyfruj i sprawdź - wskazujemy plik następnie miejsce.

DZIAŁANIE KOMUNIKACJI Z UŻYCIEM GPG

1. Klucze PGP/GPG dzielą się na publiczne i prywatne.

2. Klucze publiczne odpowiadają za szyfrowanie i można je udostępniać osobom, które będą przesyłały do nas przesyłki szyfrowane.

3. Klucze prywatne odpowiadają za odszyfrowanie wiadomości i należy je chronić, nie udostępniać i pamiętać frazę która umożliwia odszyfrowanie

4. Szyfrując wiadomości, szyfrujemy je kluczem publicznym, osoby która jest odbiorcą wiadomości, oraz która będzie mogła odszyfrować wiadomość swoim kluczem prywatnym przy użyciu frazy.

5. Odszyfrowujemy wiadomości przeznaczone dla nas, tylko naszym kluczem prywatnym.

6. Zapomnianej frazy nie da się zmienić, ani ustalić. Zatem nie będzie możliwe odczytanie wiadomości w żaden sposób! Wymagana będzie ponowna generacja klucza.