

Opis sposobu generowania kluczy PGP do współpracy z DHL eCommerce (Poland) Sp. z o.o.

W jaki sposób wygenerować klucz PGP?

Aby wygenerować klucz PGP a następnie odszyfrować klucz certyfikatu SSL, wymagana jest odpowiednia aplikacja. Przykładowo jest to gpg4usb - aplikacja, która nie wymaga instalacji w systemie.

Można ją pobrać np. z tej lokalizacji: <https://gpg4usb.org/download.html> (jest to wolne oprogramowanie, publikowane na licencji GPL). Ten plik .zip zawiera wszystko, co jest potrzebne do uruchomienia aplikacji na systemie Windows, jak i Linux.

Po pobraniu i rozpakowaniu pliku należy uruchomić aplikację: w systemie Windows poprzez plik *start_windows.exe*, w systemie Linux poprzez *start_linux*. Przy pierwszym uruchomieniu, w pierwszym oknie należy wybrać odpowiedni język i kliknąć *Dalej*.



W kolejnym oknie należy wybrać odnośnik *utworzyć nową parę kluczy*.

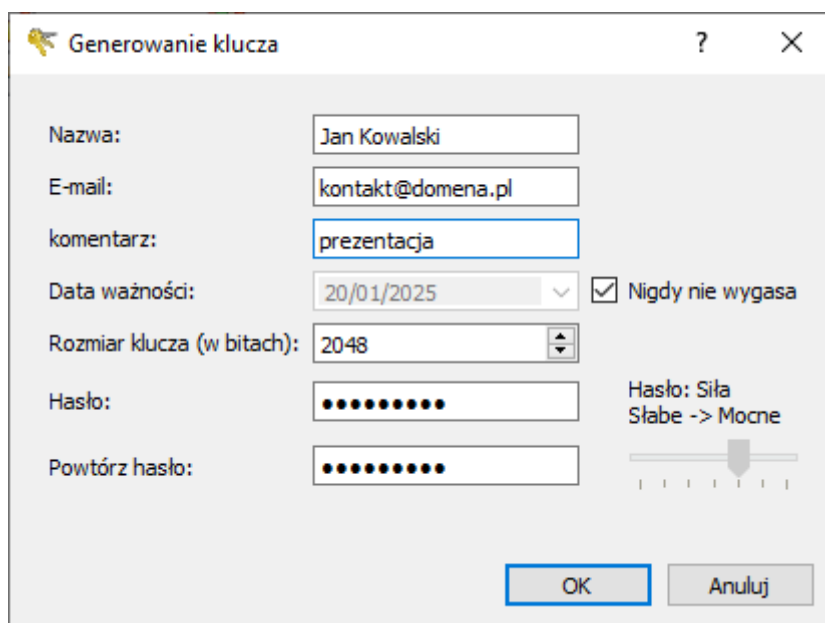


Następnie można skorzystać z dodatkowego samouczka lub wybrać *Utwórz nowy klucz*.

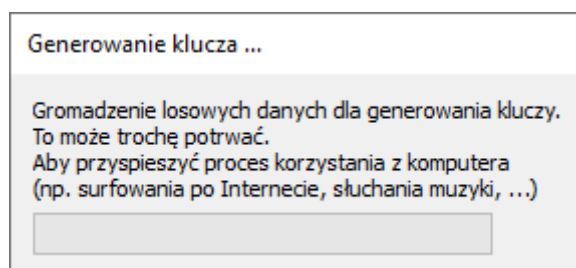


Dalej należy uzupełnić formularz dla nowego klucza zgodnie z opisami obok poszczególnych pól, a następnie potwierdzić OK.

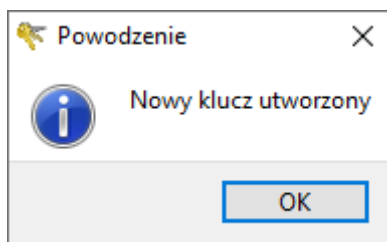
- **Nazwa:** nazwa użytkownika - sugerowane imię i nazwisko.
- **E-mail:** adres e-mail powiązany z kluczem. Ważne dla weryfikacji użytkownika klucza.
- **Komentarz:** dodatkowa notatka, w razie potrzeby.
- **Data ważności:** gdy klucz ma mieć określony termin użytkowania to należy ustawić tą datę. Jeżeli ważność klucza ma być bezterminowa to należy zaznaczyć opcję "Nigdy nie wygasa" (zalecane).
- **Rozmiar klucza (w bitach):** im większa liczba bitów, tym trudniej złamać zabezpieczenie klucza. Wartość 2048 jest wystarczająca.
- **Hasło/Powtórz hasło:** Dodatkowe zabezpieczenie kluczy.



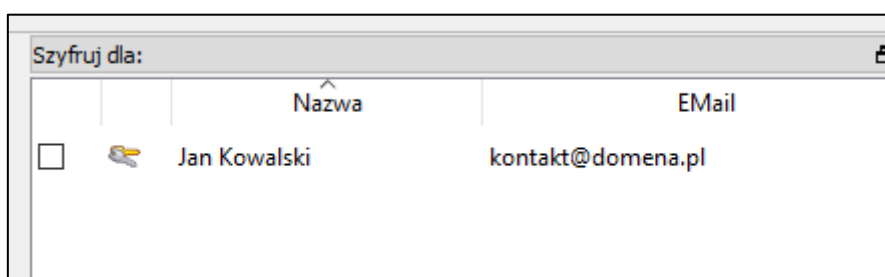
Pojawi się komunikat o tworzeniu klucza. Jeśli proces będzie trwał długo, można wykonać na komputerze inne czynności - losowe wartości potrzebne do utworzenia odpowiednio mocnego klucza aplikacja uzyskuje ze zdarzeń w systemie.



Po wygenerowaniu klucza, aplikacja wyświetli potwierdzenie. Należy zamknąć okno potwierdzenia i wybrać „zakończ” w głównym oknie programu.

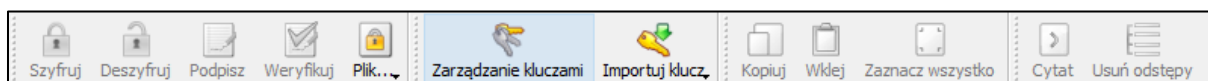


Utworzony klucz będzie widoczny na liście z prawej strony okna.

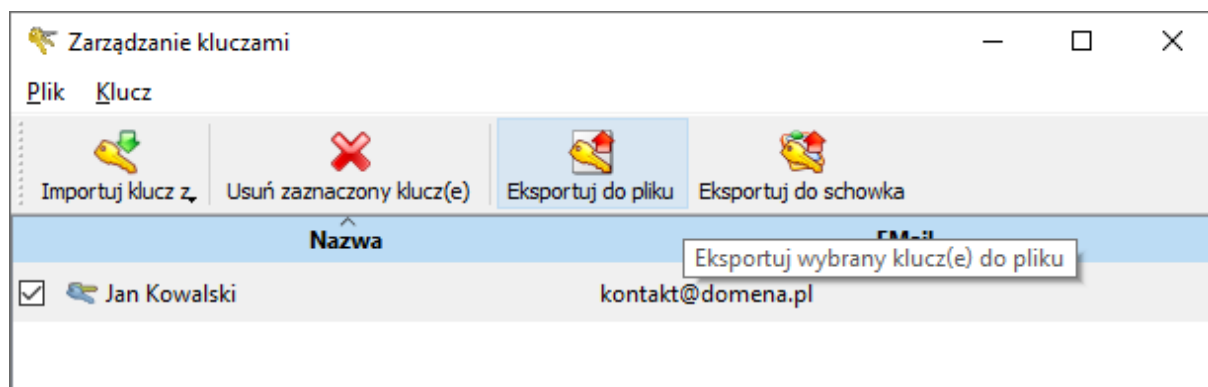


Jak wyeksportować klucz publiczny PGP, aby przekazać go innej osobie?

W górnym menu programu należy wybrać opcję „Zarządzanie kluczami”.



Należy zaznaczyć swój klucz na liście i wybrać opcję *Eksportuj do pliku*.



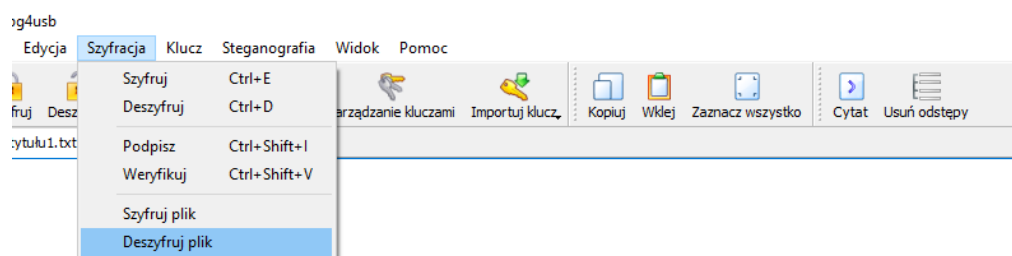
Plik należy zapisać w łatwo dostępnej lokalizacji. Ten plik jest Twoim kluczem publicznym.

Jak odczytać dane zaszyfrowane Twoim publicznym kluczem?

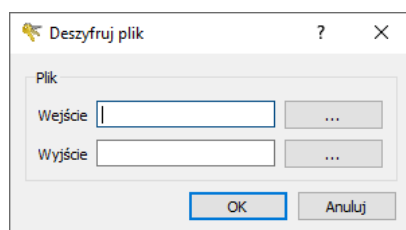
Po otrzymaniu zaszyfrowanej treści Twoim kluczem publicznym, należy uruchomić aplikację gpg4usb. Z prawej strony należy zaznaczyć na liście swój klucz - tego klucza program użyje do odszyfrowania treści.

Aby odszyfrować plik należy wybrać z menu opcję:

Szyfracja->Deszyfruj plik



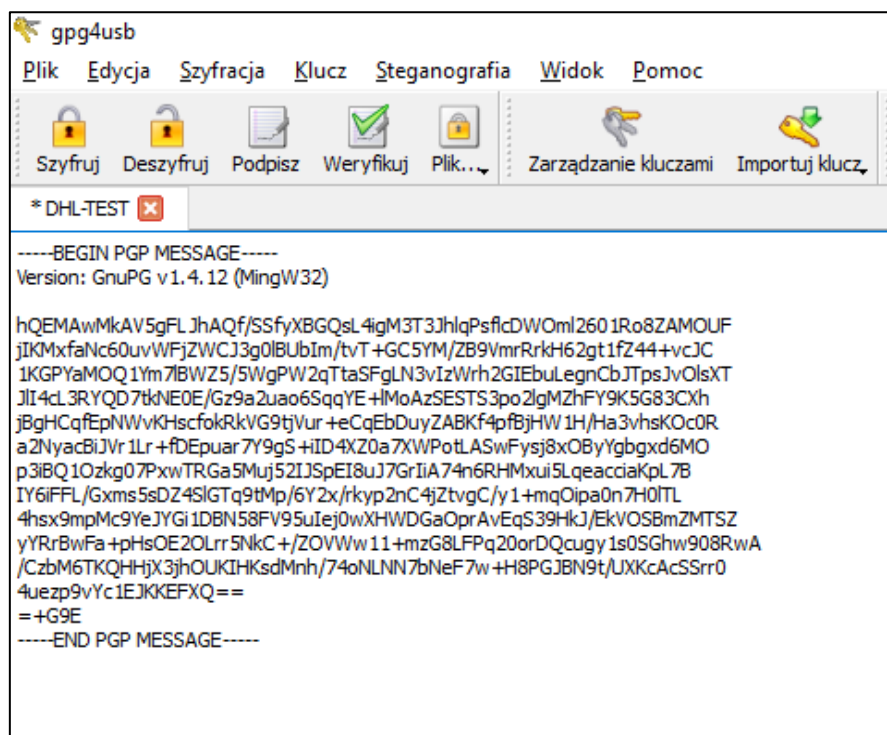
Następnie wybrać plik wejściowy (zaszyfrowany) i wskazać wyjście (nazwę rozszyfrowanego pliku). Należy przy tym pamiętać, że rozszerzenie pliku wyjściowego powinno być takie, jakie miał plik wysyłany do tej pory z DHL. Czyli, jeżeli przysyłany był plik spakowany (np. abc.zip) to w nazwie pliku wyjściowego należy na końcu dodać lub upewnić się czy już jest rozszerzenie .zip



Po kliknięciu „OK” aplikacja poprosi o hasło użyte podczas generowania kluczy.

Ten sposób deszyfrowania jest wskazany dla każdego pliku raportu.

Jeżeli jesteśmy w posiadaniu zaszyfrowanego tekstu, np. w treści emaila możemy taką wiadomość odszyfrować wklejając ją bezpośrednio do edytora w programie gpg4usb.



Treść zaszyfrowanego tekstu zawiera się między znacznikami:

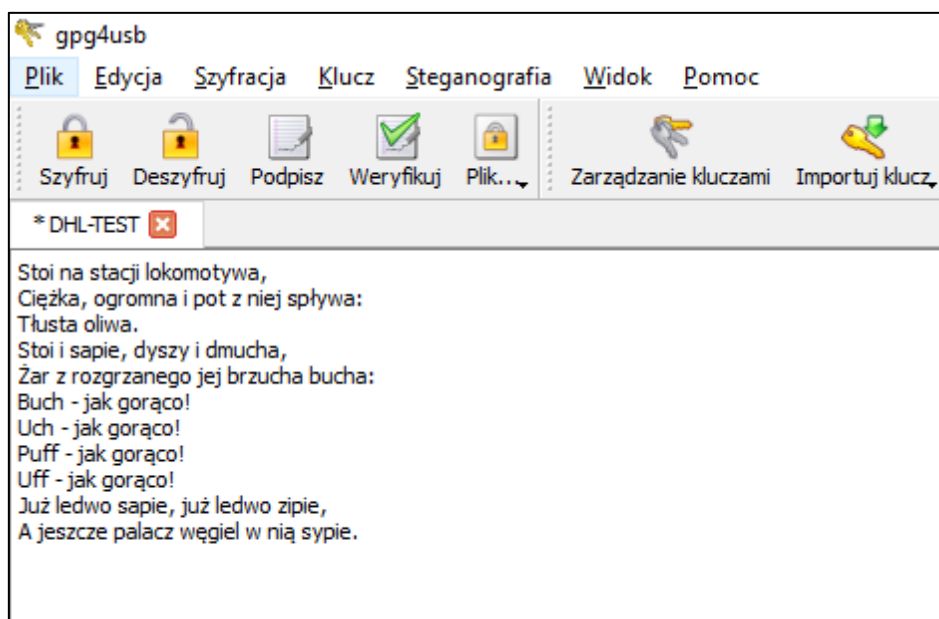
-----BEGIN PGP MESSAGE-----

...
...
...

-----END PGP MESSAGE-----

które też należy skopiować do edytora.

Następnie wybierając z menu opcję „Deszyfruj” oraz podając poprawne hasło użyte przy generowaniu klucza otrzymamy odszyfrowaną treść.



Uwaga!

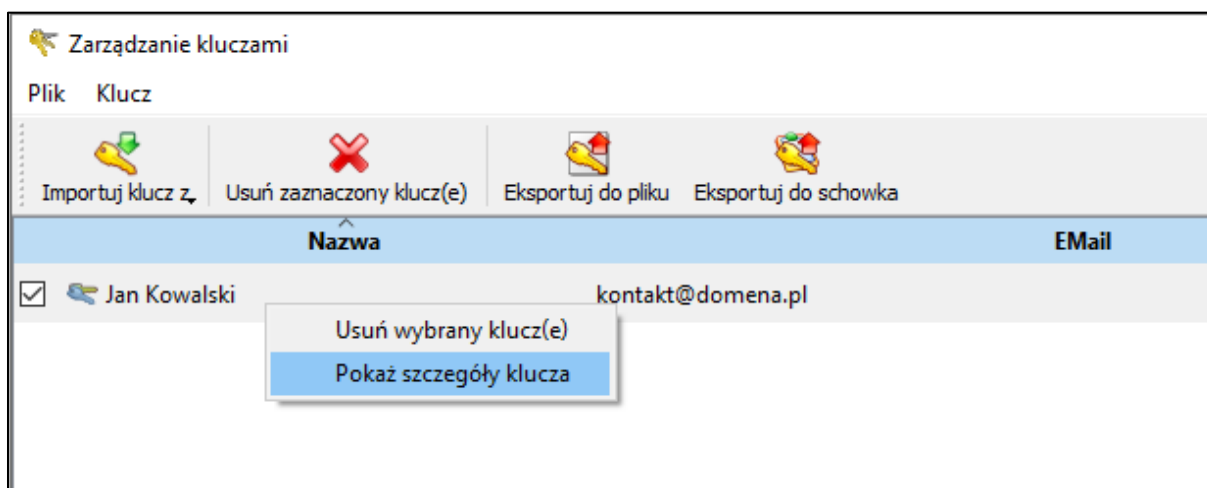
Edytor w programie gpg4usb służy do szyfrowania/deszyfrowania tekstu. Jeżeli skopiujemy treść plików *.txt, *.csv to deszyfrowanie też powinno się udać, ale nie ma gwarancji poprawnego kodowania znaków.

Do szyfrowania/deszyfrowania plików zalecane jest użycie opcji z menu Szyfracja->Deszyfruj plik oraz Szyfracja->Szyfruj plik.

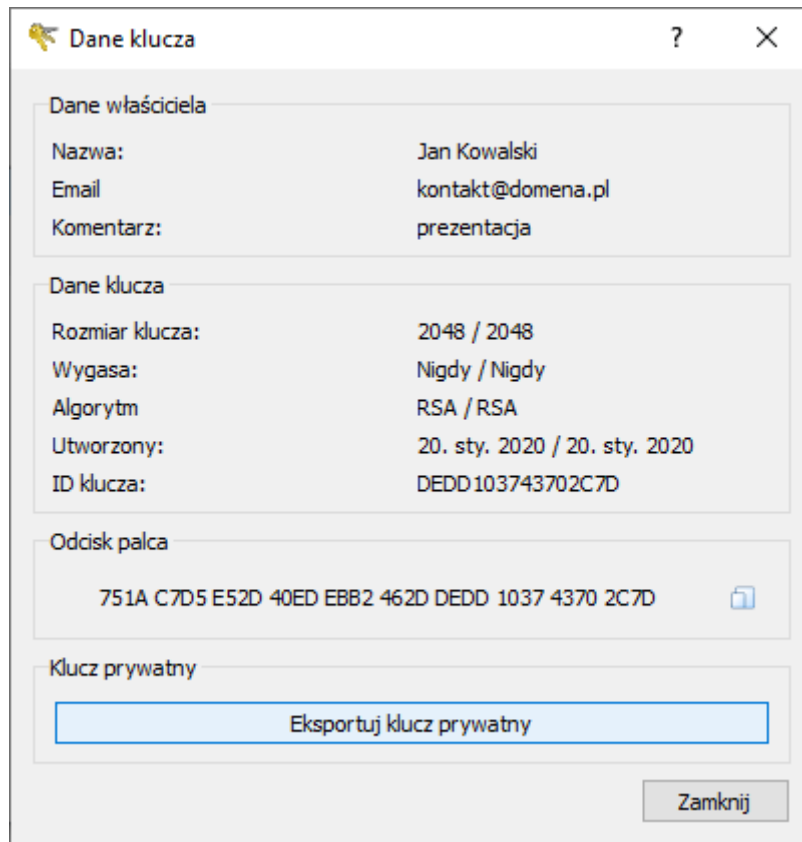
Jak wyeksportować klucze PGP, aby użyć ich na innym komputerze?

Aby móc deszyfrować pliki/wiadomości na różnych komputerach należy przenieść oryginalne klucze z komputera, na którym były one generowane na docelowy.

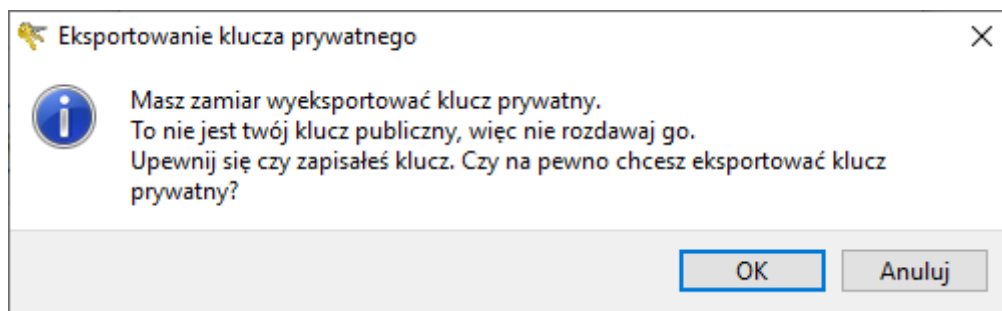
W tym celu należy w oknie do „Zarządzania kluczami” wybrać za pomocą (PPM) prawego przycisku myszy opcję z menu „Pokaż szczegóły klucza”.



Następnie kliknąć przycisk „Eksportuj klucz prywatny”.



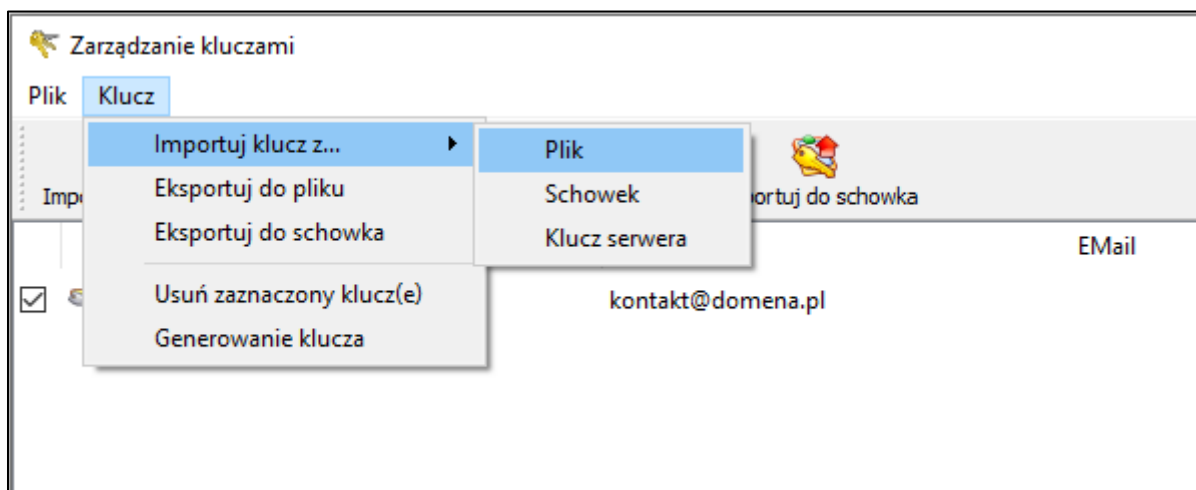
W kolejnym kroku potwierdzamy przyciskiem „OK” chęć eksportu.



W oknie dialogowym do zapisu pliku wskazujemy folder i jego nazwę.

Tak wyeksportowane klucze (prywatny i publiczny) możemy teraz przenieść i zaimportować na innym komputerze. Przenoszenie pliku na inny komputer nie będzie opisywane, należy tego dokonać w wygodny dla siebie sposób.

W celu zaimportowania pary kluczy na docelowym komputerze, w oknie do „zarządzania kluczami” wybieramy z menu *Klucz->Importuj klucz z...->Plik*, w oknie dialogowym wybieramy plik z kluczami i zatwierdzamy przyciskiem „OK”.



Od tej chwili możemy już deszyfrować te same pliki na dwóch różnych komputerach.