Guard

podręcznik użytkownika

Guard: podręcznik użytkownika

data wydania środa, 09. listopad 2016 Version 2.6.0

Spis treści

1 Informacje o tej dokumentacji

Poniższe informacje pozwolą sprawniej posługiwać się tą dokumentacją.

- Jaka jest grupa docelowa niniejszej dokumentacji?
- Jaka jest zawartość niniejszej dokumentacji?
- Dodatkowa pomoc

Jaka jest grupa docelowa niniejszej dokumentacji?

Niniejsza dokumentacja jest skierowana do użytkowników, którzy chcą szyfrować komunikację e-mail i pliki, chroniąc je przed nieuprawnionym dostępem.

Jaka jest zawartość niniejszej dokumentacji?

Niniejsza dokumentacja zawiera następujące informacje:

- W sekcji *Do czego służy aplikacja Guard?* znajduje się opis aplikacji Guard.
- . W sekcji *Korzystanie z aplikacji Guard* znajdują się informacje dotyczące usługi Guard

. Niniejsza dokumentacja przedstawia mechanizmy pracy z typową instalacją i konfiguracją oprogramowania do pracy grupowej. Wersja, której używasz, może różnić się od przedstawionej w tym dokumencie.

Dodatkowa pomoc

Pełna dokumentacja oprogramowania do pracy grupowej znajduje się w podręczniku użytkownika programu Oprogramowanie do pracy grupowej.

2 Do czego służy aplikacja Guard?

Guard jest składnikiem zabezpieczeń oprogramowania do pracy grupowej umożliwiającym szyfrowanie wiadomości e-mail i plików.

- Szyfruj korespondencję e-mail prowadzoną z innym użytkownikami lub partnerami zewnętrznymi.
- Zaszyfruj pojedynczy plik i podziel się zaszyfrowanymi danymi z innymi użytkownikami.
- Określaj poziom szyfrowania za pomocą opcji zabezpieczeń.
- Szyfrowane dane są chronione hasłem. Aby uchronić się przed skutkami utraty hasła, korzystaj z funkcji resetowania go.

3 Korzystanie z aplikacji Guard

Dowiedz się, jak pracować z aplikacją *Guard*.

- Stosowanie ustawień podstawowych
- Szyfrowanie korespondencji e-mail
- Szyfrowanie plików
- Stosowanie ustawień zabezpieczeń

3.1 Konfiguracja aplikacji *Guard*

Przed użyciem aplikacji *Guard* należy wprowadzić kilka ustawień podstawowych.

- Najpierw należy podać hasło zabezpieczające aplikacji Guard, które posłuży do szyfrowania danych oraz ich otwierania.
- Wpisz dodatkowy adres e-mail który przyda Ci się, gdy zapomnisz hasła do aplikacjiGuard. Dzięki niemu będziesz mieć możliwość zresetowania hasła zabezpieczającego aplikacji Guard i otrzymania nowego. Dlatego zalecamy wpisanie dodatkowego adresu e-mail. W przeciwnym razie nowe hasło zostanie wysłane na główny adres e-mail.

Podstawowe ustawienia można wprowadzić na dwa sposoby:

- Zdefiniuj podstawowe ustawienia podczas pierwszego użycia funkcji szyfrowania.
- Zdefiniuj podstawowe ustawienia na stronie ustawień oprogramowania do pracy grupowej przed pierwszym użyciem funkcji szyfrowania.

Jak zdefiniować podstawowe ustawienia podczas pierwszego użycia funkcji szyfrowania:

1. Włącz funkcję szyfrowania podczas tworzenia wiadomości e-mail, szyfrowania pliku lub przesyłania nowego pliku, klikając ikonę **Szyfrowanie** dostępną w drzewie folderów obok nazwy folderu.
2. Następnie pojawi się prośba o wpisanie hasła do aplikacji Guard oraz dodatkowego adresu e-mail. Wpisz potrzebne informacje.

Jak zdefiniować podstawowe ustawienia podczas pierwszego użycia funkcji szyfrowania:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij na pasku bocznym polecenie **Zabezpieczenia Guard** .

   Po pierwszym uruchomieniu ustawień bezpieczeństwa aplikacji Guard pojawi się okno *Utwórz klucze zabezpieczeń Guard* .
3. W polu **Hasło** wprowadź hasło, którego chcesz używać do szyfrowania danych.

   Potwierdź hasło, wprowadzając je ponownie w polu **Zweryfikuj**.
4. W polu **Wpisz nowy dodatkowy adres e-mail** wpisz adres, na który otrzymasz hasło tymczasowe pozwalające na zresetowanie hasła zabezpieczającego aplikacji Guard.
5. Kliknij przycisk **OK**.

3.2 Szyfrowanie konwersacji e-mail

Dostępne są następujące możliwości:

- Odczytywanie zaszyfrowanych konwersacji e-mail
- Wysyłanie zaszyfrowanych wiadomości e-mail
- Jak odbiorcy zewnętrzni mogą odczytać zaszyfrowaną wiadomość e-mail?

3.2.1 Odczytywanie zaszyfrowanych konwersacji e-mail

Aby móc odczytać zaszyfrowaną wiadomość e-mail, należy podać co najmniej hasło zabezpieczające aplikacjiGuard. Nadawca szyfrowanej wiadomości może ją dodatkowo zabezpieczyć jeszcze jednym hasłem.

Jak przeczytać zaszyfrowaną wiadomość e-mail:

1. Wybierz wiadomość e-mail z ikoną *Szyfrowanie* . W widoku szczegółów pojawi się powiadomienie *Zabezpieczona wiadomość e-mail. Wpisz hasło aplikacji Guard Security.*

   Uwaga: Jeśli przy ostatnim użyciu aplikacji Guard the ustawiono zapamiętywanie hasła bezpieczeństwa w aplikacji Guard wiadomość e-mail wyświetli się natychmiast.
2. Wpisz hasło zabezpieczające aplikacji Guard.

   Można ustawić czas pamiętania hasła przez aplikację Guard. Aby to zrobić, wybierz opcję Nie wylogowuj mnie z aplikacji **Guard** i wybierz odpowiednią wartość z listy.
3. Kliknij przycisk **OK**. Zawartość pojawi się w formacie zwykłego tekstu.

   Jeśli wiadomość e-mail ma załączniki, pojawią się funkcje obsługi załączników w formie zaszyfrowanej lub odszyfrowanej.

Uwaga: w przypadku korzystania z szyfrowanej korespondencji e-mail można tylko odpowiedzieć na tę wiadomość lub przesłać ją dalej.

3.2.2 Wysyłanie zaszyfrowanych wiadomości e-mail

Dostępne są następujące możliwości:

- Wysyłanie zaszyfrowanych wiadomości e-mail. Treść wiadomości e-mail będzie dostępna tylko dla nadawcy i odbiorcy wiadomości.

  Ostrzeżenie: w przypadku wysyłania wersji roboczej szyfrowanej wiadomości e-mail wysłana wersja robocza zostanie usunięta z folderu *Wersje robocze*.
- Wysyłanie wiadomości e-mail z podpisem. Podpis upewnia adresata, że wiadomość e-mail nie została zmodyfikowana po drodze.
- Wysyłanie zaszyfrowanych wiadomości e-mail z podpisem.

Jak wysłać zaszyfrowaną wiadomość e-mail:

1. Napisz wiadomość e-mail w aplikacji *E-mail* tak jak to zwykle robisz.

   Na stronie *Nowa wiadomość* kliknij widoczną w prawym górnym rogu ikonę **Szyfruj**

   Możesz też kliknąć pozycję **Zabezpieczenia** pod tematem. Wybierz opcję **Zaszyfruj**.

   Ikony wyświetlane obok odbiorców wskazują, czy możliwe jest zaszyfrowanie tej wiadomości u tego odbiorcy. Po ustawieniu kursora nad ikoną pojawi się odpowiedni opis.

2. Aby wyświetlić dodatkowe opcje, kliknij pozycję **Zabezpieczenia**. Możesz aktywować niżej wymienione opcje.

   Aby dodatkowo podpisać wiadomość e-mail, włącz opcję **Podpisz**.

   Jeśli klient poczty e-mail adresata nie obsługuje standardu PGP, a mimo to wiadomość powinna być czytelna, włącz opcję **PGP Inline**. Po włączeniu tego ustawienia nie będzie można wysyłać wiadomości e-mail w formacie HTML.

   Aby umożliwić odbiorcy e-mail wysłanie zaszyfrowanej odpowiedzi, odbiorca musi mieć Twój klucz publiczny. Możesz go wysłać jako załącznik. Aby to zrobić, kliknij polecenie **Dołącz mój klucz**.

3. Kliknij polecenie **Wyślij zaszyfrowane**.

   W przypadku wysyłania wiadomości do adresatów zewnętrznych pojawi się okno umożliwiające wysłanie im uwag dotyczących otwarcia zaszyfrowanej wiadomości e-mail [12].

   Odbiorca zaszyfrowanej wiadomości e-mail, z którym wcześniej nie prowadzono korespondencji, otrzyma załącznik z Twoim kluczem publicznym.

3.2.3 Jak odbiorcy zewnętrzni mogą odczytać zaszyfrowaną wiadomość e-mail?

Zaszyfrowane wiadomości e-mail można także wysyłać do odbiorców zewnętrznych, którzy nie są użytkownikami oprogramowania do pracy grupowej. Po dodaniu odbiorcy zewnętrznego aplikacja Guard sprawdzi, czy oferuje on klucz publiczny. Dalsze postępowanie zależy od wyniku tej kontroli.

- Jeśli odbiorca oferuje klucz publiczny:
  - Wiadomość zostanie zaszyfrowana za pomocą tego klucza. Odbiorca może ją odczytać za pomocą klucza prywatnego.
  - Aby umożliwić odbiorcy wysłanie zaszyfrowanej odpowiedzi, Twój klucz publiczny zostanie wysłany jako załącznik o nazwie public.asc. Odbiorca może go następnie zaimportować do używanego klienta poczty e-mail.
- Jeśli odbiorca nie oferuje klucza publicznego:
  - Użytkownik zewnętrzny, który ma już konto gościa, razem z wiadomością e-mail otrzyma odnośnik do strony logowania na to konto. Użycie go i zalogowanie się pozwoli na odczytanie zaszyfrowanej wiadomości e-mail i ewentualne przesłanie odpowiedzi.
  - Jeśli jeszcze nie ma konta gościa, zostanie ono utworzone. Odbiorca zewnętrzny otrzyma wiadomość e-mail z łączem do strony gościa oraz automatycznie utworzonym hasłem. Po zalogowaniu się na stronie gościa użytkownik utworzy własne hasło.

    W zależności od konfiguracji automatycznie utworzone hasło oraz łącze do strony gościa mogą zostać wysłane w osobnych wiadomościach e-mail.
  - Konta dla gości (do odczytu szyfrowanych wiadomości e-mail) są kasowane po pewnej liczbie dni wprowadzonej w konfiguracji oprogramowania do pracy grupowej. Aby zachować ich dostępność są one także przesyłane w zaszyfrowanej formie jako załączniki do wiadomości z odnośnikiem o nazwie encypted.asc. Taki załącznik można przesłać na stronę konta gościa, odszyfrować i odczytać.

3.3 Szyfrowanie plików

Dostępne są następujące możliwości:

- Szyfrowanie plików
- Tworzenie nowych zaszyfrowanych plików
- Otwieranie zaszyfrowanych plików
- Pobieranie zaszyfrowanych plików
- Odszyfrowywanie plików

3.3.1 Szyfrowanie plików

W przypadku szyfrowania plików zostaną zaszyfrowane tylko ich ostatnie wersje. Wszystkie inne wersje zostaną usunięte.

Jak zaszyfrować plik:

Ostrzeżenie: w przypadku szyfrowania pliku zostaną usunięte wszystkie jego wersje — oprócz bieżącej. Aby zachować starszą wersję, należy ją zapisać przed zaszyfrowaniem pliku.

1. Wybierz dowolną liczbę plików w aplikacji *Pliki*. Kliknij widoczną na pasku narzędzi ikonę **Działania** ☰▾. W menu kliknij pozycję **Zaszyfruj**.

   Można też użyć ikony **Działania** ☰ w *Przeglądarce*. Kliknij w menu pozycję **Zaszyfruj**.
2. Jeśli plik zawiera wiele wersji, pojawi się okno *Szyfrowanie plików*. Potwierdź, że chcesz zaszyfrować plik i usunąć wszystkie poprzednie wersje, klikając przycisk **OK**.

   Jeśli plik ma tylko jedną wersję, zostanie zaszyfrowany bez dalszych monitów.

3.3.2 Tworzenie nowych zaszyfrowanych plików

Nowy zaszyfrowany plik możesz utworzyć, przesyłając plik lokalny z szyfrowaniem.

Jak utworzyć nowy zaszyfrowany plik:

1. Wybierz folder w drzewie folderów w aplikacji *Pliki*.

   Uwaga: otwórz folder, w przypadku którego masz uprawnienia do tworzenia obiektów.
2. Kliknij dostępną na pasku narzędzi ikonę **Nowe**. Kliknij pozycję **Dodaj i zaszyfruj plik lokalny**.
3. W oknie *Prześlij plik* wybierz dowolną liczbę plików.

   Kliknij przycisk **Otwórz**. W obszarze wyświetlania będzie pokazywany bieżący status postępu.

   Aby anulować postęp, kliknij pozycję **Szczegóły pliku** z prawej strony u dołu obszaru wyświetlania. Kliknij pozycję **Anuluj** obok nazwy pliku w oknie *Postęp przesyłania*.

Wskazówka: nowy zaszyfrowany plik możesz także utworzyć, przeciągając go z pulpitu systemu operacyjnego do okna aplikacji *Pliki* i upuszczając w górnej części okna.

3.3.3 Otwieranie zaszyfrowanych plików

Zaszyfrowany plik możesz otworzyć i przeczytać. Plik będzie nadal zapisany na serwerze w zaszyfrowanej postaci.

Jak otworzyć zaszyfrowany plik:

1. W obszarze wyświetlania w aplikacji *Pliki* wybierz zaszyfrowany plik. Kliknij widoczną na pasku narzędzi ikonę **Widok** .
2. Pojawi się okno *Wpisz hasło zabezpieczające aplikacji Guard* . Wpisz hasło zabezpieczające aplikacji Guard.

   Można ustawić długość pamiętania hasła przez aplikację Guard. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość.

   Kliknij przycisk **OK**.

3.3.4 Pobieranie zaszyfrowanych plików

Zaszyfrowany plik możesz pobrać, aby go lokalnie przeczytać lub zmodyfikować. Plik będzie nadal zapisany na serwerze w zaszyfrowanej postaci.

Jak pobrać zaszyfrowany plik:

1. W obszarze wyświetlania w aplikacji *Pliki* wybierz zaszyfrowany plik. Kliknij widoczną na pasku narzędzi ikonę **Widok** .

   Uwaga: jeśli zamiast tego w wyskakującym okienku klikniesz polecenie **Pobierz**, pobrany plik pozostanie zaszyfrowany.
2. Pojawi się okno *Wpisz hasło zabezpieczające aplikacji Guard* . Wpisz hasło zabezpieczające aplikacji Guard.

   Można ustawić długość pamiętania hasła przez aplikację Guard. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość.

   Kliknij przycisk **OK**.
3. Kliknij ikonę **Działania** w przeglądarce. Kliknij polecenie **Pobierz odszyfrowane**.

3.3.5 Odszyfrowywanie plików

Aby usunąć szyfrowanie z pliku, należy go odszyfrować.

Jak odszyfrować plik:

1. W aplikacji *Pliki* wybierz zaszyfrowany plik w obszarze wyświetlania. Kliknij widoczną na pasku narzędzi ikonę **Działania** . W menu kliknij pozycję **Usuń szyfrowanie**.
2. Pojawi się okno *Wpisz hasło zabezpieczające aplikacji Guard* . Wpisz hasło zabezpieczające aplikacji Guard.

   Można ustawić długość ważności hasła w aplikacji Guard. Aby to zrobić, wybierz opcję **Pamiętaj hasło** i wybierz z listy odpowiednią wartość.

   Kliknij przycisk **OK**.

3.4 Wyloguj się z aplikacji Guard

Z aplikacji Guard możesz się wylogować bez zamykania oprogramowania do pracy grupowej. Aby potem otworzyć zaszyfrowane wiadomości e-mail, pliki lub foldery, musisz ponownie wpisać hasło zabezpieczające aplikacji Guard.
Uwaga: Ta funkcja jest dostępna wyłącznie po włączeniu funkcji **Pamiętaj hasło** przy otwieraniu zaszyfrowanej wiadomości e-mail lub zaszyfrowanego pliku.

Jak się wylogować z aplikacji Guard:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu.
2. Wybierz z menu polecenie **Wyloguj się z aplikacji Guard**

3.5 Ustawienia aplikacji Guard

Dostępne są następujące możliwości:

- Aby zmienić ustawienia hasła zabezpieczającego aplikacji Guard, użyj opcji Ustawienia zabezpieczeń aplikacji Guard.
- Aby zmienić domyślne ustawienia wysyłania zabezpieczonych wiadomości e-mail, użyj opcji Ustawienia szyfrowania PGP.
- Możesz także wykonać czynności administracyjne dla kluczy PGP.

3.5.1 ustawienia zabezpieczeń aplikacji Guard

Dostępne są następujące możliwości:

- zmiana hasła zabezpieczającego aplikacji Guard
- Jeśli zapomnisz hasła aplikacji Guard, możesz poprosić przesłanie tymczasowego hasła zabezpieczającego aplikacji Guard, resetując hasło zabezpieczające aplikacji Guard.
- Zmiana zapasowego adresu e-mail.

Jak zmienić hasło zabezpieczające aplikacji Guard

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Na pasku bocznym kliknij pozycję **Zabezpieczenia Guard**.
3. W polu **Wprowadź bieżące hasło zabezpieczające aplikacji Guard** widocznym poniżej pola *Hasło* wpisz hasło, które do tej pory było używane do szyfrowania danych.

   W polu **Wprowadź nowe hasło zabezpieczające aplikacji Guard** wpisz hasło, którego od teraz chcesz używać do szyfrowania danych.

   Potwierdź nowe hasło, wpisując je ponownie do pola **Potwierdź nowe hasło zabezpieczające aplikacji Guard**.
4. Kliknij polecenie **Zmień hasło zabezpieczające aplikacji Guard**.

Jak zresetować hasło zabezpieczające aplikacji Guard:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Na pasku bocznym kliknij pozycję **Zabezpieczenia Guard**.
3. Kliknij polecenie **Zresetuj hasło zabezpieczające aplikacji Guard**. Na wpisany dodatkowy adres e-mail zostanie wysłane nowe hasło.

   Jeśli nie został wprowadzony zapasowy adres e-mail, nowe hasło zostanie wysłane na podstawowy adres e-mail.
4. Nowe hasło od razu zostanie bieżącym hasłem zabezpieczającym aplikacji Guard . Należy je natychmiast zmienić.

Jak zmienić zapasowy adres e-mail na potrzeby resetowania hasła do szyfrowania:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Na pasku bocznym kliknij pozycję **Zabezpieczenia Guard**.
3. Wpisz hasło służące do szyfrowania danych do pola **Wprowadź bieżące hasło zabezpieczające aplikacji Guard** widocznego poniżej pola *Dodatkowy adres e-mail*

   W polu **Wpisz nowy dodatkowy adres e-mail** wpisz adres, na który otrzymasz hasło tymczasowe pozwalające na zresetowanie hasła zabezpieczającego aplikacji Guard.

   Kliknij polecenie **Zmień adres e-mail**.

3.5.2 Ustawienia szyfrowania PGP

Ustawienia szyfrowania PGP określają gotowe ustawienia wprowadzane podczas tworzenia wiadomości e-mail. Możesz je zmienić przed wysłaniem wiadomości.

Jak zmienić ustawienia szyfrowania PGP:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij na pasku bocznym pozycję **Zabezpieczenia Guard**. Kliknij **Ustawienia zaawansowane**.
3. Wybierz jedną z opcji pod nagłówkiem *Ustawienia szyfrowania PGP*.

Dostępne są następujące ustawienia.

Domyślnie podczas tworzenia wiadomości do wysłania w formie zaszyfrowanej

Umożliwia określenie, czy nowa wiadomość e-mail ma być domyślnie szyfrowana za pomocą PGP.

Domyślne dodawanie podpisu do wychodzących wiadomości e-mail

Umożliwia określenie, czy nowa wiadomość e-mail ma być domyślnie szyfrowana za pomocą PGP.

Włącz zaawansowane funkcje PGP

Określa, czy widoczne mają być niektóre funkcje PGP, takie jak zarządzanie kluczami.

Ustaw domyślnie w nowych wiadomościach PGP w tekście

Aby wyświetlić to ustawienie, zaznacz pole wyboru **Włącz zaawansowane funkcje PGP**.
Wskazuje, że szyfrowanie PGP ma być realizowane w tekście. Użyj tej opcji, jeśli wiadomość powinna być czytelna mimo tego, że klient e-mail odbiorcy nie obsługuje szyfrowania PGP. Po włączeniu tego ustawienia nie będzie możliwe wysyłanie wiadomości e-mail w formacie HTML.

3.5.3 Zarządzanie kluczami

Do wysyłania i otrzymywania zaszyfrowanych wiadomości funkcje zarządzania kluczami przeważnie nie są potrzebne. Można ich użyć do następujących zadań:

- Chcesz użyć klucza PGP z aplikacji Guard w innych klientach e-mail, np. uruchamianych lokalnie.
- Masz klucze PGP z innych aplikacji. Chcesz ich użyć w aplikacji Guard.
- Chcesz wprowadzić klucz publiczny partnera zewnętrznego do aplikacji Guard, aby móc odczytywać zaszyfrowane wiadomości od niego.
- Chcesz przekazać klucz publiczny adresatowi, aby umożliwić mu odczytywanie Twoich zaszyfrowanych wiadomości bez uzyskiwania dostępu do serwera kluczy.

Jak otworzyć stronę do zarządzania kluczami:

1. Kliknij ikonę **menu systemowego** widoczną z prawej strony paska menu. Kliknij pozycję menu **Ustawienia**.
2. Kliknij na pasku bocznym pozycję **Zabezpieczenia Guard**. Kliknij **Ustawienia zaawansowane**.
   Włącz opcję **Włącz zaawansowane funkcje PGP**

Strona zawiera niżej wymienione elementy.

- Opcje pozwalające na dopasowywanie domyślnych ustawień aplikacji Guard.
- Sekcja *Twoje klucze* zawierająca funkcje do zarządzania prywatnymi i publicznymi kluczami PGP.
  Istniejące klucze zostaną wyświetlone poniżej pozycji *Lista Twoich kluczy*. Znajdują się na niej dwie pozycje:
  - Klucz główny służący między innymi do szyfrowania wiadomości e-mail.
  - Klucz zależny służący do szyfrowania i odszyfrowywania wiadomości e-mail oraz plików.

  Różnica między kluczem głównym i zależnym polega na jednej z funkcji technologii PGP. Każdy klucz główny i zależny zawiera klucz prywatny i publiczny. Przy odpowiedniej konfiguracji program Guard użyje automatycznie odpowiedniego klucza.
- Sekcja *Klucze publiczne* zawierające klucze publiczne współużytkowane przez Ciebie lub innych użytkowników. Jeśli na liście znajduje się klucz publiczny użytkownika, możesz założyć, że może on odszyfrowywać wiadomości e-mail.
- Wygasłe klucze są oznaczane kolorem czerwonym.

Dostępne są następujące funkcje:

- Pobranie klucza publicznego
- Wysłanie klucza publicznego pocztą e-mail
- dodawanie nowych kluczy do istniejących przez przesłanie kluczy lokalnych lub utworzenie nowych kluczy w aplikacji Guard
- Zmiana klucza w klucz bieżący
- Pokazanie szczegółów klucza
- Usunięcie klucza
- Pobranie klucza prywatnego
- Dodanie kolejnego konta e-mail do klucza
- Przesłanie klucza publicznego partnera zewnętrznego

Jak pobrać klucz publiczny:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij polecenie **Pobierz klucz publiczny PGP** dostępne pod pozycją *Twoje klucze*.

Jak wysłać klucz publiczny pocztą e-mail:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij przycisk **Wyślij e-mailem swój klucz publiczny PGP** widoczny pod pozycją *Twoje klucze*.

Jak dodać nowe klucze:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Dodaj** + widoczną obok elementu *Lista Twoich kluczy* w sekcji *Twoje klucze*. Pojawi się okno *Dodawanie kluczy*.
3. Dostępne są następujące możliwości:
   - Aby dodać klucz prywatny, kliknij przycisk **Prześlij prywatny klucz**. Wybierz plik z kluczem prywatnym. Pojawi się okno *Prześlij prywatne klucze*.

     Aby przesłać nowy klucz, wpisz hasło zabezpieczające aplikacji Guard. Wpisz nowe hasło do nowego klucza.
   - Aby dodać klucz publiczny, kliknij przycisk **Prześlij tylko klucz publiczny**. Wybierz plik z kluczem publicznym.
   - Aby utworzyć nową parę kluczy, kliknij polecenie **Utwórz nowe klucze**. Pojawi się okno *Utwórz nowe klucze aplikacji Guard*.

     Wpisz hasło do nowego klucza i potwierdź je.

     Nowy klucz składa się z klucza głównego i odpowiedniego klucza zależnego.

   Nowy klucz zostanie umieszczony na górze listy kluczy i stanie się automatycznie kluczem bieżącym.

Jak ustawić klucz jako bieżący:

Możesz użyć tej funkcji, jeśli lista kluczy ma zawierać więcej niż jeden klucz główny i zależny. Od teraz szyfrowanie będzie realizowane za pomocą klucza bieżącego.

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij pole wyboru poniżej *Listy Twoich kluczy* z opisem **Bieżący**. Po ustawieniu klucza głównego jako bieżącego odpowiedni klucz zależny zostanie także ustawiony jako bieżący — i na odwrót.

Jak wyświetlić szczegóły klucza:

Istnieje możliwość wyświetlenia szczegółów klucza. To szczególnie przydatne dla użytkowników rozumiejących technologię PGP.

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Szczegóły** widoczną obok klucza w sekcji *Lista Twoich kluczy*. Otworzy się okno *Szczegóły klucza*. Aby wyświetlić podpisy danego klucza, kliknij pozycję **Podpisy**.

Jak usunąć klucz:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Usuń** widoczną obok elementu *Lista Twoich kluczy* w sekcji *Twoje klucze*. Pojawi się okno *Usuń klucz prywatny*.
3. Dostępne są następujące opcje:
   - Aby wycofać klucz prywatny, kliknij polecenie **Odwołaj**.

     Wpisz hasło do klucza prywatnego i ewentualnie wybierz powód odwołania klucza.

     Kliknij polecenie **Odwołaj**.
   - Aby usunąć klucz prywatny, kliknij polecenie **Usuń**.

     Wpisz hasło do klucza prywatnego.

     Kliknij polecenie **Usuń**.

   Po usunięciu klucza głównego zostanie także usunięty odpowiedni klucz zależny.

Jak pobrać klucz prywatny:

Uwaga: pobranie klucza prywatnego na komputer lokalny może stanowić zagrożenie bezpieczeństwa. Dopilnuj, aby nikt inny nie miał do niego dostępu.

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Pobierz** widoczną obok klucza na liście kluczy prywatnych w sekcji *Twoje klucze*.

Jak dodać kolejne konto e-mail do klucza:

Przy dodawaniu kolejnych identyfikatorów użytkownika do klucza możesz go wprowadzić do wielu kont e-mail.

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Edytuj** widoczną obok pozycji *Lista Twoich kluczy* w sekcji *Twoje klucze*. Otworzy się okno *Dodaj ID użytkownika*.
3. Wpisz nazwę identyfikatora użytkownika i adres e-mail, którego chcesz użyć w tym kluczu.
   Wpisz hasło do danego klucza.
   Kliknij przycisk **OK**.

Jak przesłać klucz publiczny partnera zewnętrznego:

1. W ustawieniach otwórz stronę do zarządzania kluczami.
2. Kliknij ikonę **Dodaj** widoczną obok pozycji *Lista kluczy publicznych PGP* w sekcji *Klucze publiczne*. Wybierz plik zawierający klucz publiczny.

Indeks