

Bezpieczna poczta w programie Thunderbird za pomocą wtyczki Enigmail

# BEZPIECZNY PTASZEK



Thunderbird oferuje szereg wbudowanych opcji zabezpieczających pocztę.

Dzięki rozszerzeniom można zapewnić dodatkowe warstwy bezpieczeństwa,

Enigmail jest wtyczką realizującą tę właśnie funkcję.

**PATRICK BRUNSCHWIG, OLAV SEYFARTH**

**K**lient poczty elektronicznej Thunderbird [1] to program o niewielkich zapotrzebowaniach na zasoby systemu, który zdobywa sobie coraz więcej zwolenników w społeczności Internetu. Większość dystrybucji Linuksa dostarcza Thunderbirda w standardowej instalacji. Na stronach projektu Mozilla można znaleźć gotowe pakiety binarne dla większości popularnych obecnie systemów. W stabilnej wersji Debiana nie ma co prawda pakietu Thunderbird, lecz można pobrać wersję testową z repozytorium opiekuna.

W swojej najnowszej wersji, 1.0.2, ptaszek jest już dość dobrze wyćwiczony w lataniu i posiada imponującą kolekcję bardzo wygodnych w użyciu funkcji bezpieczeństwa. W tym artykule postaramy się przekazać nieco wiedzy na temat bezpieczeństwa programu Thunderbird.

## Uwierzytelnianie

Thunderbird obsługuje protokoły pocztowe POP, IMAP oraz SMTP, jak również NNTP na potrzeby list dyskusyjnych oraz LDAP do

obsługi książek adresowych. Te usługi z reguły wymagają uwierzytelniania. W najprostszym przypadku klient próbuje przesyłać nazwę użytkownika i hasło w formie nieszyfrowanej, co naraża użytkownika na podsłuchanie (ang. eavesdropping). Aby temu zapobiec, Thunderbird oferuje szereg mechanizmów bezpiecznego uwierzytelniania użytkowników.

Mechanizm typu wyzwanie-odpowieź przesyła w sieci tzw. sekret (na przykład hasło), który służy do wygenerowania tymczasowego skrótu (ang. hash). Oczywiście serwer musi obsługiwać ten mechanizm, aby klient poczty mógł z niego skorzystać. Thunderbird może sprawdzić obsługę w serwerze określonych mechanizmów, lecz sukces nie jest gwarantowany. W serwerach SMTP Thunderbird potrafi wynegocjować wykorzystanie mechanizmów DIGEST-MD5 oraz CRAM-MD5, lecz aby skorzystać z mechanizmu CRAM-MD5 w komunikacji z serwerem POP lub IMAP, należy włączyć opcję *Enable secure authentication* w opcjach serwera w ramach parametrów konta pocztowego.

## Ruch sieciowy

Techniki typu wyzwanie-odpowieź nie chronią przed atakami pośrednika (ang. man-in-the-middle). Szyfrowanie ruchu sieciowego może zostać zastosowane jako dodatkowa warstwa bezpieczeństwa oraz funkcja ochrony prywatności pomiędzy klientem a serwerem. W tym celu stosuje się protokół Transport Layer Security (TLS). TLS (następca protokołu SSL) szyfruje komunikację pomiędzy klientem a serwerem. Thunderbird obsługuje TLS tylko dla serwerów SMTP.

Podczas konfiguracji nowego konta pocztowego w oknie *Konfiguracja konta pocztowego*, domyślne ustawienie połączenia nie będzie bezpieczne. Przed nawiązaniem połączenia z serwerem poczty należy uruchomić z menu głównego opcję *Edycja | Konfiguracja kont...* i w oknie konfiguracji konta ustawić opcje protokołu. W sekcji *Ustawienia serwera* wybrać *Używaj bezpiecznego połączenia (SSL)* (Rysunek 1). Thunderbird automatycznie wypełni właściwy numer portu. W polu *Używaj bezpiecznego uwierzytelnienia* najlepiej ustawić *CRAM-MD5*.

Dla *Serwera poczty wychodzącej (SMTP)* najlepiej wskazać Thunderbirdowi, aby wykorzystywał przy połączeniach nazwę użytkownika i hasło oraz bezpieczne połączenia. W tym przypadku zalecaną opcją jest *TLS*, która powoduje, że wykorzystywana jest funkcja *Start TLS* serwera SMTP. W razie wybrania opcji *SSL*, program automatycznie wypełni właściwy numer portu. W ustawieniu *Edycja | Konfiguracja kont | Tworzenie* można w sekcji *Adresowanie* dodatkowo skonfigurować wykorzystanie protokołu *SSL* w połączeniach z serwerem *LDAP*.

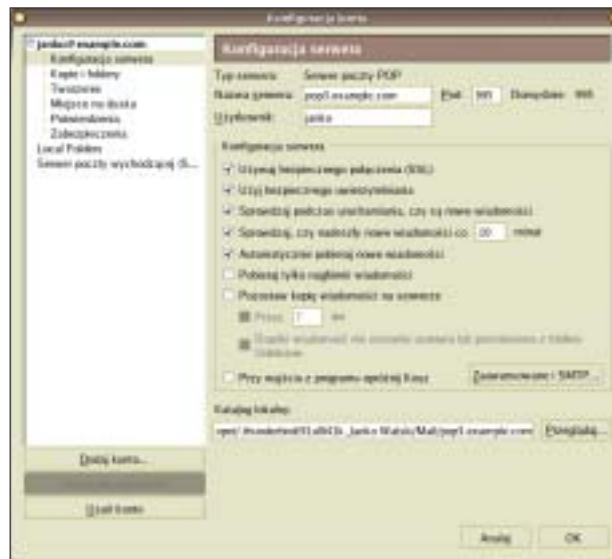
### Szyfrowanie haseł

Użytkownicy świadomi wagi bezpieczeństwa, posiadający wiele kont pocztowych u różnych dostawców, ustawiają różne hasła do każdego z tych kont. Zapamiętanie większej liczby haseł może być trudne, a z całą pewnością męczące jest każdorazowe wpisywanie haseł. Thunderbird ma możliwość zachowania wykorzystywanych haseł.

W domyślnych ustawieniach Thunderbird koduje hasła w formacie *Base64*. Oznacza to, że hasła nie są szyfrowane, lecz po prostu za-

pisane wraz z nazwą konta w pliku o przypadkowej nazwie i rozszerzeniu *.s*. To grozi poważnym naruszeniem bezpieczeństwa w przypadku uzyskania dostępu do systemu przez niepowołaną osobę. Thunderbird obsługuje jednak możliwość szyfrowania haseł z użyciem modułu kryptograficznego *Mozilla Network Security Services (NSS)*.

Istnieje wiele opinii na temat koncepcji zachowywania haseł na dysku, lecz rozwiązanie zaproponowane przez twórców Thunderbirda wydaje się rozsądnym kompromisem. Jeśli użytkownik zechce, aby Thunderbird przechowywał książkę adresową w zabezpieczonym hasłem katalogu *LDAP*, zapis hasła na dysku będzie niezbędny, ponieważ przy każdym nowym e-mailu będzie nawiązywane nowe połączenie z katalogiem



Rysunek 1: Konfiguracja bezpiecznego połączenia w sekcji *Ustawienia serwera konfiguracji konta*.

*LDAP*, co bez funkcji zachowania hasła na dysku wymagałoby każdorazowego ręcznego wprowadzania hasła.

Aby hasła zachowane na dysku były szyfrowane, należy włączyć opcję *Używaj głównego hasła do szyfrowania haseł*, którą można znaleźć w funkcji *Edycja | Preferencje | Zaawansowane | Zachowane hasła | Główne hasło*. Należy ustawić główne hasło, klikając przycisk *Zmień hasło...* (Rysunek 2). Hasło to będzie chronić wszystkie pozostałe hasła oraz certyfikaty *X.509*; należy więc zadbać, aby było bezpieczne, tj. powinno mieć odpowiednią długość, zawierać małe i wielkie litery, cyfry oraz znaki specjalne.

### Podpisane i opieczętwane

Po bezpiecznym uwierzytelnieniu z serwerem pocztowym, warto pomyśleć o zaszyfrowaniu poczty zapisanej na tym serwerze. Współczesne robaki internetowe (ang. worm) wykradają adresy pocztowe i rozprzestrzeniają się, wysyłając swój kod w wiadomościach elektronicznych. To jest dodatkowy powód, aby upewnić się, że poczta przychodząca pochodzi od tego nadawcy, za którego się podaje oraz że poczta pochodząca od uczciwych nadawców nie została zmodyfikowana po drodze.

Istnieją dwa standardy realizujące funkcje szyfrowania i podpisu elektronicznego w poczcie. Standardy te są wzajemnie niekompatybilne: *S/MIME* oraz *OpenPGP*. Thunderbird obsługuje obydwie z nich, przy czym drugi jest obsługiwany za pomocą dodatku

## Zarządzanie certyfikatami

W większości przypadków zaleca się stosowanie połączenia z ośrodkiem certyfikacji (*CA*) zabezpieczonego protokołem *SSL*. Zintegrowane pakiety, jakim jest klasyczna *Mozilla*, wykorzystują ten sam zasób certyfikatów na potrzeby programów klienta poczty i przeglądarki *WWW*. Thunderbird posiada własny zasób i nawet w przypadku, gdy użytkownik wykorzystuje program *Firefox*, certyfikat musi być pobrany z serwera przy użyciu przeglądarki, zapisany w formacie *PKCS-#12* i zaimportowany w programie *Thunderbird*.

Zarządzanie certyfikatami odbywa się w *Menedżerze certyfikatów (Edycja | Preferencje | Zaawansowane | Certyfikaty | Menedżer certyfikatów...)*. W oknie menedżera znajdują się osobne zakładki do zarządzania własnymi certyfikatami, certyfikatami innych osób, serwerów *WWW* (gdzie można znaleźć certyfikaty *SSL/TLS* serwerów poczty i grup dyskusyjnych) oraz certyfikaty ośrodków certyfikacji *CA* (znajdują się tu ośrodki standardowe, dostarczone z programem oraz ewentualnie dodane samodzielnie).

W wielu przypadkach jeden użytkownik poczty stosuje dwa certyfikaty: jeden z nich jest znany w organizacji i służy do

szyfrowania. Dzięki temu poczta może być odszyfrowana na bramie pocztowej i sprawdzona pod kątem zawierania szkodliwego kodu. Drugi certyfikat, indywidualny dla każdego użytkownika, jest wykorzystywany do cyfrowego podpisywania wiadomości. Po zaimportowaniu obydwu certyfikatów należy w ustawieniach konta pocztowego, w sekcji *Zabezpieczenia*, wybrać certyfikat do podpisywania cyfrowego poczty wychodzącej oraz drugi do szyfrowania i odszyfrowywania wiadomości.

Aby zaszyfrować wiadomość, użytkownik potrzebuje certyfikatu odbiorcy. Jeśli nie można uzyskać go z jakiegoś centralnego miejsca (w ramach *PKI*), należy poprosić adresata o jego przesłanie. W zupełności wystarczy, gdy odbiorca wyśle do nas podpisaną wiadomość elektroniczną, ponieważ certyfikaty są importowane przez Thunderbirda automatycznie z wiadomości podpisanych cyfrowo. Alternatywnie można wyszukać certyfikat adresata w serwerze kluczy ośrodka certyfikacji. Thunderbird nie ma jednak wbudowanych odpowiednich mechanizmów automatyzujących ten proces.

## Opcje Enigmilla

Włączenie opcji *Enigmail* | *Ustawienia* | *Wysyłanie* | *Dopuszczaj zawijanie wierszy typu 'flowed'* spowoduje, że Enigmail będzie zawiązywał zbyt długie wiersze wiadomości. Program pocztowy dodaje na początku cytowanych wierszy znak cytowania „>”. Niestety, ta funkcja jest w konflikcie z funkcją sygnatury, stosowaną przez Enigmail. Aby tego uniknąć, Enigmail zastępuje znaki „>” znakami „|”, zapobiegając modyfikacji tego wiersza przez Thunderbird. Mimo wszystko warto pozostawić tę opcję niezaznaczoną.

Aby odszyfrować wiadomość zakodowaną w formacie PGP/MIME, zapisaną na serwerze IMAP, nie można pobierać indywidualnych części MIME, lecz całe wiadomości. W przeciwnym wypadku Enigmail nie mógłby uzyskać pełnej wiadomości do odszyfrowania. Aby umożliwić obsługę odkodowywania poszczególnych części MIME, należy włączyć *Enigmail* | *Ustawienia* | *Zaawansowane* | *Ładuj części MIME na żądanie (foldery IMAP)*.

Aby odszyfrowywać wiadomości zakodowane w formacie Inline-PGP, należy wyłączyć opcję renderowania wiadomości w formacie HTML, włączając opcję *Widok* | *Wyświetl wiadomość jako* | *Zwykły tekst*.

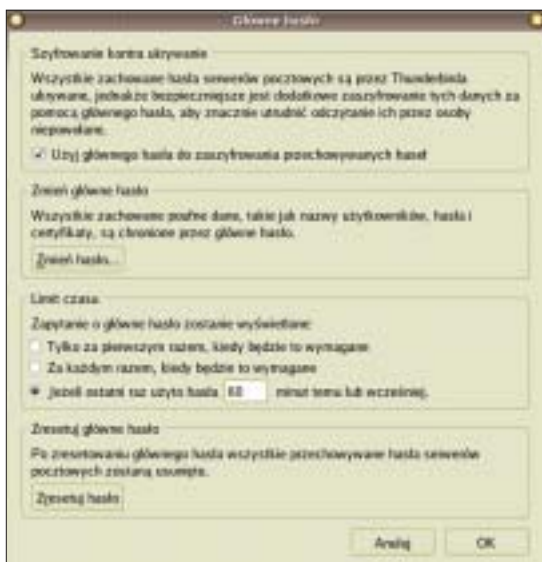
Enigmail obsługuje zarówno format Inline-PGP, jak i PGP/MIME. Jeśli wysyłane wiadomości zawierają załączniki, rozszerzenie zada dodatkowe pytanie, czy załączniki mają być kodowane osobno, czy ma zostać zastosowane PGP/MIME. Do odszyfrowania i otworzenia lub zapisu załącznika wiadomości wykorzystuje się funkcję menu kontekstowego. Enigmail ma możliwość zdefiniowania preferowanego formatu kodowania wiadomości na podstawie reguł zdefiniowanych w ramach konta nadawcy.

Użytkownicy standardowej wersji Thunderbirda muszą dodatkowo zainstalować Enigmail za pomocą menedżera rozszerzeń. Należy dostosować wersję Enigmilla do posiadanej wersji Thunderbirda, w przeciwnym wypadku można doprowadzić do problemów ze stabilnością. Dodatkowo należy zadbać o to, aby Thunderbird i Enigmail pracowały w tym samym języku.

Po instalacji należy sprawdzić, czy Enigmail pracuje poprawnie i czy potrafi odnaleźć GnuPG. W tym celu można posłużyć się funkcją *Enigmail* | *Informacje o Enigmail*. Przy pierwszym wywołaniu dowolnej funkcji Enigmail pojawi się okno dialogowe z pytaniem, czy użytkownik chce skonfigurować

ślugę standardu OpenPGP. Program ten został napisany jako przykład obsługi przez Mozillę systemowych mechanizmów komunikacji międzyprocesowej. W 2001 roku jeden z programistów projektu Mozilla, Ramalingam Saravana, opracował bibliotekę obsługującą potoki systemowe. Mozilla nie miała możliwości obsługi OpenPGP, z tego powodu Ramalingam napisał prosty dodatek, uzupełniający ją o tę funkcję. Ten dodatek przekazuje zaszyfrowaną treść do programu GnuPG i wyświetla odszyfrowany tekst w programie klienckim (Rysunek 3). To był początek użytecznego dodatku do programu pocztowego Mozilli, a potem do Thunderbirda.

Enigmail nie importuje kluczy publicznych w sposób automatyczny (ale można skonfigurować GnuPG, ustawiając opcję *keyserver-options auto-key-retrieve*), może jednak przeszukiwać serwery kluczy w poszukiwaniu kluczy pasujących do nadawcy wiadomości. W wielu dystrybucjach Linuksa Enigmail jest dostarczany standardowo z pakietem programu Thunderbird, w wielu dostępny jest podobny pakiet uzupełniający tę funkcjonalność, czego przykładem może być pakiet *mozilla-thunderbird-enig-mail* w dystrybucji Debian.

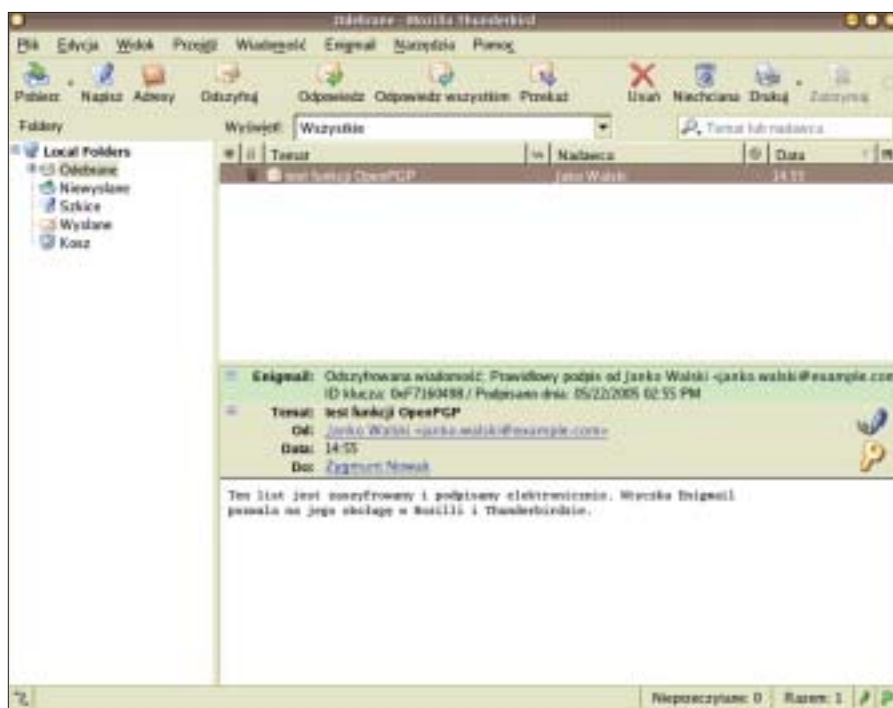


Rysunek 2: Okno dialogowe Główne hasło pozwala uaktywnić funkcję szyfrowania zachowanych haseł.

Enigmail [3]. Należy pamiętać, że ani S/MIME, ani OpenPGP nie stanowią pełnego kompletnego rozwiązania problemów bezpieczeństwa. Jak zostało wspomniane wcześniej w tym artykule, należy również zadbać o zabezpieczenie danych użytkownika oraz procesu logowania się na serwerze.

## Enigmatyczna poczta

Enigmail jest dodatkiem do Mozilli i Thunderbirda, uzupełniającym te programy o ob-



Rysunek 3: Enigmail szyfruje i odszyfrowuje wiadomości pocztowe w programie Thunderbird.



Rysunek 4: Okno ustawień reguły służy do zdefiniowania opcji OpenPGP dla poszczególnych adresatów.

rozszerzenie. Na tym etapie można odpowiedzieć, że nie, jako że do konfiguracji powrócimy za chwilę.

W oknie informacji o Enigmail (w przypadku, gdy zostanie zainstalowany polski pakiet tłumaczenia) pojawi się następująca informacja: *Szyfrowanie i weryfikacja programu gpg: /usr/bin/gpg*. Jeśli zamiast tego ukaże się komunikat o błędzie, oznacza to, że Enigmail nie odnalazł GnuPG, lub że zainstalowana wersja rozszerzenia nie jest zgodna z posiadaną wersją programu Thunderbird.

Jeśli użytkownik nie posiada własnego klucza OpenPGP, może wygenerować odpowiedni klucz, wykorzystując funkcję *Enigmail | Menedżer kluczy OpenPGP | Generowanie | Nowa para kluczy*. Aby wysłać wiadomość podpisaną, zaszyfrowaną w formacie OpenPGP, należy skonfigurować Enigmail dla konta, z którego będzie odbywać się wysyłka. W konfiguracji kont pojawia się dodatkowa sekcja *Ustawienia OpenPGP*. W tym miejscu można wybrać wykorzystywane klucze oraz skonfigurować domyślne ustawienia dotyczące szyfrowania i podpisu cyfrowego. Choć o wiele wygodniej jest, aby Enigmail dobierał klucze w oparciu o adres nadawcy, można również samodzielnie zde-

finiować odwzorowania adresów na odpowiednie klucze. Należy pamiętać, że przypisanie kilku kluczy do jednego adresu nadawcy jest praktyką obniżającą bezpieczeństwo.

OpenPGP obsługuje dwa standardy kodowania: Inline-PGP oraz PGP/MIME. Inline-PGP szyfruje jedynie treść wiadomości, załączniki muszą być osobno zaszyfrowane i załączone w wiadomości. Inline-HTML nie obsługuje też wiadomości w formacie HTML, a rozszerzone strony kodowe mogą sprawić problemy. PGP/MIME szyfruje wiadomość i załączniki oraz zachowuje bez zmian całe formatowanie, co rozwiązuje te problemy. Niestety, nie wszystkie programy pocztowe wspierające PGP potrafią obsługiwać standard PGP/MIME.

Enigmail obsługuje szereg opcji kontrolujących GnuPG oraz Thunderbirda. Opcje te znajdują się w funkcji *Enigmail | Ustawienia*. Domyślne ustawienia są wystarczające w większości przypadków, lecz można zmienić je w celu dalszego dostosowania funkcji OpenPGP w Thunderbirdzie. Aby uprościć to zadanie, rozszerzenie Enigmail dodatkowo ujawnia kilka opcji Thunderbirda, które są standardowo ukryte. Więcej informacji można znaleźć w ramce „Opcje Enigmala”.

## Reguły

Enigmail posiada edytor reguł, za pomocą którego można zdefiniować ustawienia szyfrowania, podpisywania cyfrowego oraz stosowania PGP/MIME i odpowiednich identyfikatorów kluczy dla adresatów i grup adresatów (Rysunek 4). Edytor pozwala zdefiniować preferencje w oparciu o poszczególne adresy pocztowe. Użytkownik ma możliwość zdefiniowania reguł dla poszczególnych adresatów, lecz również dla całych grup, na przykład adresów pracowników firmy.

Funkcja zintegrowanej pomocy zawiera szczegółowe informacje również na temat definiowania reguł adresatów. Thunderbird stosuje te reguły podczas wysyłania wiadomości, warto więc włączyć funkcję potwierdzenia przed wysyłką. Dzięki temu pojawi się komunikat pozwalający na weryfikację zastosowanych opcji wysyłki (na przykład wysyłkę niezasyfrowanej wiadomości).

Thunderbird posiada wszystkie funkcje, o których mógłby pomyśleć użytkownik świadomy bezpieczeństwa. Wydaje się jednak (w związku ze wspomnianymi problemami), że proste i uniwersalne rozwiązania w poczcie elektronicznej, związane z technologią kryptograficzną, to na razie niezbyt bliski cel. ■

## INFO

- [1] Strona projektu Thunderbird: <http://www.mozilla.org/products/thunderbird>
- [2] Pakiety dla Debiana z rozszerzeniem Enigmail [people.debian.org/~asac/testing/](http://people.debian.org/~asac/testing/)
- [3] Enigmail: <http://enigmail.mozdev.org>

## AUTORZY

**Patrick Brunschwig** jest menedżerem projektu w Whitestein Technologies. W wolnych chwilach Patrick zajmuje się rozwojem rozszerzenia Enigmail i innych rozszerzeń dla aplikacji projektu Mozilla.

**Olav Seyfarth** pracuje na stanowisku Security Manager i zajmuje się zabezpieczaniem danych w Telefónica Germany. Bezpieczeństwo jest jednym z podstawowych zainteresowań Olava od początku jego kariery w informatyce. Jego celem jest uczynienie kryptografii tak przyjazną użytkownikowi, jak to tylko możliwe, dzięki czemu bezpieczeństwo w poczcie elektronicznej stanie się tak proste, jak samo wysłanie e-maila.