



Instrukcja obsługi certyfikatów w programie pocztowym Pine

Spis treści	
Program PINE i protokół S/MIME.....	1
Wymagania systemowe.....	1
Kompilacja i instalacja PINE z nakładką do obsługi protokołu S/MIME.....	1
Źródła programu PINE.....	1
Rozpakowanie pakietu PINE i instalacja nakładki.....	2
Przygotowanie do kompilacji.....	2
Kompilacja pakietu PINE.....	2
Instalacja.....	3
Przygotowanie do pracy.....	3
Import certyfikatu z przeglądarki Netscape.....	3
Opcje konfiguracyjne programu PINE związane z protokołem S/MIME.....	4
Używanie protokołu S/MIME w programie PINE.....	5
Weryfikacja podpisu.....	5
Odczytywanie zaszyfrowanych wiadomości.....	6
Tworzenie wiadomości zaszyfrowanych lub podpisanych.....	7
Bezpieczeństwo użytkownika programu PINE.....	8
Ograniczenia nakładki protokołu S/MIME dla programu PINE.....	8

Program PINE i protokół S/MIME

PINE jest jednym z najbardziej rozpowszechnionych programów pocztowych pracujących w trybie tekstowym. Jednak standardowo nie posiada on obsługi protokołu S/MIME. Dopiero zainstalowanie nakładki, której autorem jest Jonathan Paisley daje możliwość korzystania z funkcjonalności PKI. W obecnym kształcie nakładka ta przystosowana jest dla systemów Solaris i Linux.

Wymagania systemowe

Wsparcie dla protokołu S/MIME w PINE zbudowane jest w oparciu o pakiet OpenSSL dostępny na stronie www.openssl.org. W większości dystrybucji Linuxa jest on zainstalowany w domyślnej konfiguracji. W przypadku braku programu OpenSSL, konieczna będzie instalacja tego oprogramowania przed przystąpieniem do instalacji PINE.

Kompilacja i instalacja PINE z nakładką do obsługi protokołu S/MIME

Źródła programu PINE

Oryginalne źródła programu PINE znajdują się na serwerze twórców programu dostępnym pod adresem <ftp://cac.washington.edu/pine/pine.tar.Z>. Dla wygody polskich użytkowników internetu Centrum Certyfikacji Signet przechowuje **lokalną kopię wersji 4.44**. Dalsza instrukcja instalacji przedstawia czynności niezbędne do kompilacji tej właśnie wersji. Nakładka pozwalająca na obsługę protokołu S/MIME jest zawarta w katalogu contrib/smime w źródłach programu, jednakże po jej

zainstalowaniu wymagane jest wprowadzenie paru poprawek, dlatego na serwerze CC Signet dostępna jest **zmieniona wersja**. Poprawki w stosunku do oryginału obejmują faktyczne zapewnienie "zapominania" przez program haseł do kluczy prywatnych, gdy wybrana jest odpowiednia opcja w konfiguracji oraz zmieniony został katalog, w którym poszukiwany będzie pakiet OpenSSL.

Rozpakowanie pakietu PINE i instalacja nakładki

W katalogu w którym zapisany został plik **pine4.44.tar.gz** należy wykonać komendę:

```
$tar xzf pine4.44.tar.gz
```

w wyniku której zostanie utworzony katalog **pine4.44/**, w którym zawarte będą kompletne źródła programu. Po wejściu do tego katalogu używając polecenia:

```
$cd pine4.44/
```

należy zainstalować nakładkę poprzez wykonanie

```
$patch -p1 < ../pine-smime-211101-fixed.diff
```

Przygotowanie do kompilacji

W plikach konfiguracyjnych do programu **make** na stałe zaszyty jest katalog w którym poszukiwane będą pliki pakietu OpenSSL. Czasem, zależnie od tego, gdzie ten pakiet został zainstalowany, domyślne wartości zawarte w nakładce są błędne. Należy więc przystąpić do skorygowania ich, poprzez edycję pliku **pine/makefile.lnx** (gdy kompilujemy dla systemu Linux) lub **pine/makefile.so5** (gdy kompilujemy dla systemu Solaris). Należy odszukać linijkę rozpoczynającą się od **SSLDIR=** i zamienić istniejący tam wpis **/usr/local/ssl** na nazwę katalogu gdzie faktycznie zainstalowany jest pakiet OpenSSL.

Kompilacja pakietu PINE

W celu skompilowania pakietu PINE, należy wykonać polecenie :

```
$/build system
```

gdzie zamiast słowa system należy wstawić:

dla systemu Linux:

lnx gdy używana jest funkcja crypt zawarta w bibliotece C

lnp gdy używane są moduły PAM

slx gdy do użycia funkcji crypt niezbędny jest parametr -lcrypt

sl4 gdy do użycia funkcji crypt niezbędny jest parametr -lshadow

sl5 gdy używane są hasła z pliku shadow i nie potrzeba innych bibliotek

lrh gdy używamy dystrybucji RedHat 7.2

dla systemu Solaris:

so5 gdy używamy Sun Solaris >= 2.5

gs5 gdy używamy Sun Solaris >= 2.5 z kompilatorem gcc

Jeśli podczas kompilacji nie wynikły jakieś problemy to powinniśmy w katalogu **bin** mieć gotowy do uruchomienia plik **pine**.

Instalacja

Instalacja sprowadza się do skopiowania pliku **bin/pine** do katalogu z binariami, do którego mamy (czy też użytkownicy systemu mają) dostęp. Najczęściej polega to na wykonaniu komendy :

```
$cp bin/pine /usr/local/bin/pine
```

Przygotowanie do pracy

Program PINE w wersji obsługującej protokół S/MIME korzysta z dodatkowego katalogu **.pine-smime** w katalogu domowym użytkownika. Struktura tego katalogu jest następująca :

- ~/**.pine-smime/ca/** w którym przechowywane są certyfikaty centrów autoryzacji
- ~/**.pine-smime/private/** w którym przechowywany jest klucz prywatny użytkownika
- ~/**.pine-smime/public/** w którym przechowywane są klucze publiczne

Drzewo takie należy stworzyć w katalogu domowym. Na serwerze Centrum Certyfikacji Signet dostępny jest pakiet **pine-smime.tar.gz** zawierający całą strukturę katalogów niezbędną do działania programu PINE, wraz z certyfikatami CA Signet. Plik ten, po pobraniu z serwera Centrum Certyfikacji Signet użytkownik powinien rozpakować w swoim katalogu domowym wykonując komendę:

```
$tar xzf pine-smime.tar.gz
```

Import certyfikatu z przeglądarki Netscape

Po wygenerowaniu osobistego certyfikatu za pomocą przeglądarki Netscape Messenger należy wyeksportować go do pliku tekstowego. Dokonuje się to poprzez wejście do okna **Security Info**, a następnie wskazanie pobranego certyfikatu i wciśnięcie przycisku **Export**. Program zapyta nas o hasło którym zabezpieczyliśmy certyfikat, oraz dwukrotnie o hasło którym chcemy zaszyfrować wyeksportowane dane. W ten sposób zostanie utworzony plik w formacie PKCS#12, zawierający nasz klucz prywatny i publiczny. Następnie należy przystąpić do konwersji tego pliku do formatu używanego przez PINE. Najpierw należy wydobyć klucz prywatny i zapisać go w katalogu **~/pine-smime/private/**. Nazwa pliku powinna być identyczna jak adres e-mail z dodatkową końcówką **.key**.

Przykładowo jeśli certyfikat został wystawiony dla adresu jan.kowalski@signet.pl plik klucza będzie miał nazwę jan.kowalski@signet.pl.key. Wydobyć klucza prywatnego dokonuje się wykonując polecenie:

```
$openssl pkcs12 -in plik_z_netscape -out plik_klucza -nocerts
```

przy czym **plik_z_netscape** to nazwa pliku utworzonego podczas eksportowania klucza z programu Netscape, a **plik_klucza** to wspomniana już nazwa pliku klucza poprzedzona nazwą katalogu **~/pine-smime/private/**.

Przykładowo, Jan Kowalski, posiadający adres e-mail jan.kowalski@signet.pl, i plik kowalski.p12 wykonałby polecenie:

```
$opensslpkcs12-inkowalski.p12-out~/pine-smime/private/jan.kowalski@signet.pl.key  
-nocerts
```

Program zapyta o hasło którego użyliśmy aby zabezpieczyć dane eksportowane z Netscape, oraz zapyta o hasło które ma być w końcowym efekcie używane wraz z danym kluczem prywatnym. Część publiczna certyfikatu powinna zostać zapisana w katalogu ~/pine-smime/public/, a jego nazwa powinna być identyczna jak adres e-mail z dodatkową końcówką .crt. W przypadku naszego Jana Kowalskiego plik ten nosiłby nazwę jan.kowalski@signet.pl.crt. Wydobycie publicznej części certyfikatu dokonuje się poleceniem:

```
$openssl pkcs12 -in plik_z_netscape -out plik_certyfikatu -nokeys -clcerts
```

przy czym **plik_z_netscape** to nazwa pliku utworzonego podczas eksportowania klucza z programu Netscape, a **plik_certyfikatu** to nazwa pliku certyfikatu poprzedzona nazwą katalogu ~/pine-smime/public/.

Przykładowo, Jan Kowalski, posiadający adres e-mail jan.kowalski@signet.pl, i plik kowalski.p12 wykonałby polecenie:

```
$opensslpkcs12-in kowalski.p12 -out ~/pine-smime/public/jan.kowalski@signet.pl.crt  
-nokeys -clcerts
```

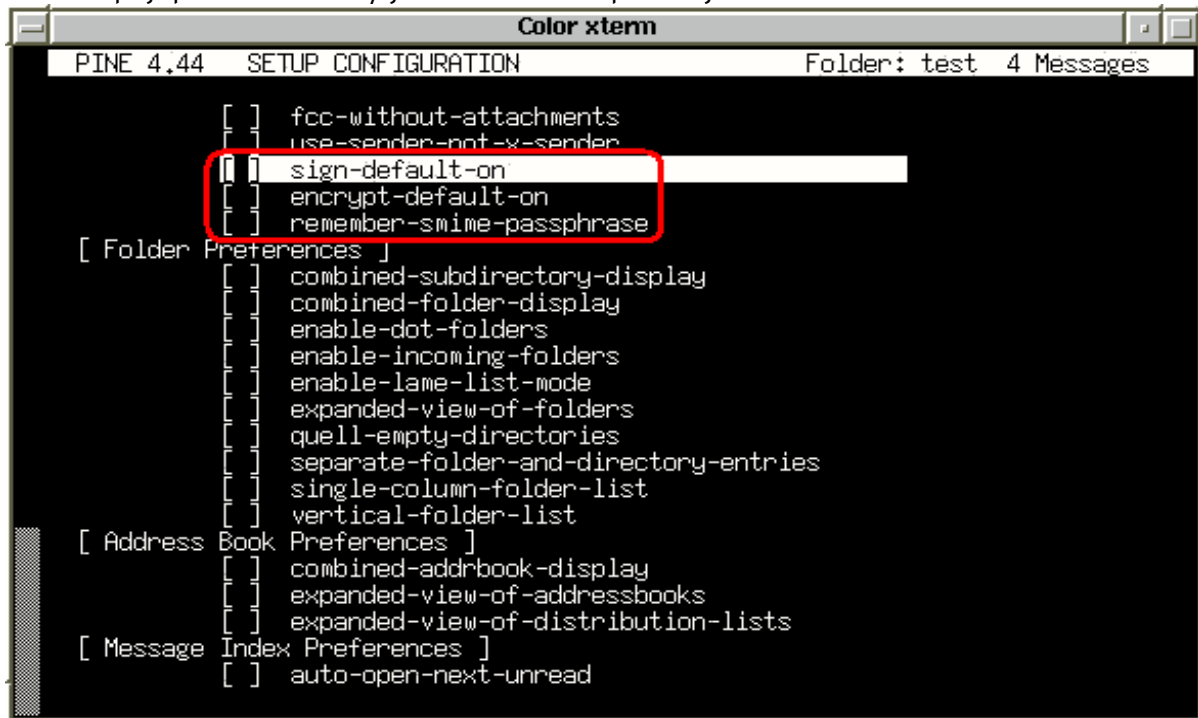
Po wykonaniu tych czynności możemy usunąć plik do którego wyeksportowaliśmy dane z Netscape i program PINE jest gotowy do pracy.

Opcje konfiguracyjne programu PINE związane z protokołem S/MIME

Po zainstalowaniu nakładki do konfiguracji programu dodane zostały trzy opcje. Dostępne one są z menu głównego po wybraniu SETUP (zazwyczaj klawisz s) a następnie CONFIGURATION (zazwyczaj klawisz c). Opcje te to:

- **sign-default-on** powodująca, że domyślnie wszystkie wysyłane listy są podpisywane cyfrowo,
- **encrypt-default-on** powodująca, że wszystkie wysyłane listy są automatycznie szyfrowane, o ile posiadamy certyfikat odbiorcy korespondencji,
- **remember-smime-passphrase** powodująca, że program tylko raz zapyta nas o hasło do klucza prywatnego, a rozszyfrowany klucz zapamięta, wykluczając konieczność wpisywania hasła za każdym razem gdy rozszyfrowujemy lub podpisujemy wiadomość.

Układ opcji przedstawiony jest na ekranie poniżej:



```
Color xterm
PINE 4.44  SETUP CONFIGURATION  Folder: test  4 Messages

[ ] fcc-without-attachments
[ ] use-sender-not-x-sender
[ ] sign-default-on
[ ] encrypt-default-on
[ ] remember-smime-passphrase

[ Folder Preferences ]
[ ] combined-subdirectory-display
[ ] combined-folder-display
[ ] enable-dot-folders
[ ] enable-incoming-folders
[ ] enable-lame-list-mode
[ ] expanded-view-of-folders
[ ] quell-empty-directories
[ ] separate-folder-and-directory-entries
[ ] single-column-folder-list
[ ] vertical-folder-list

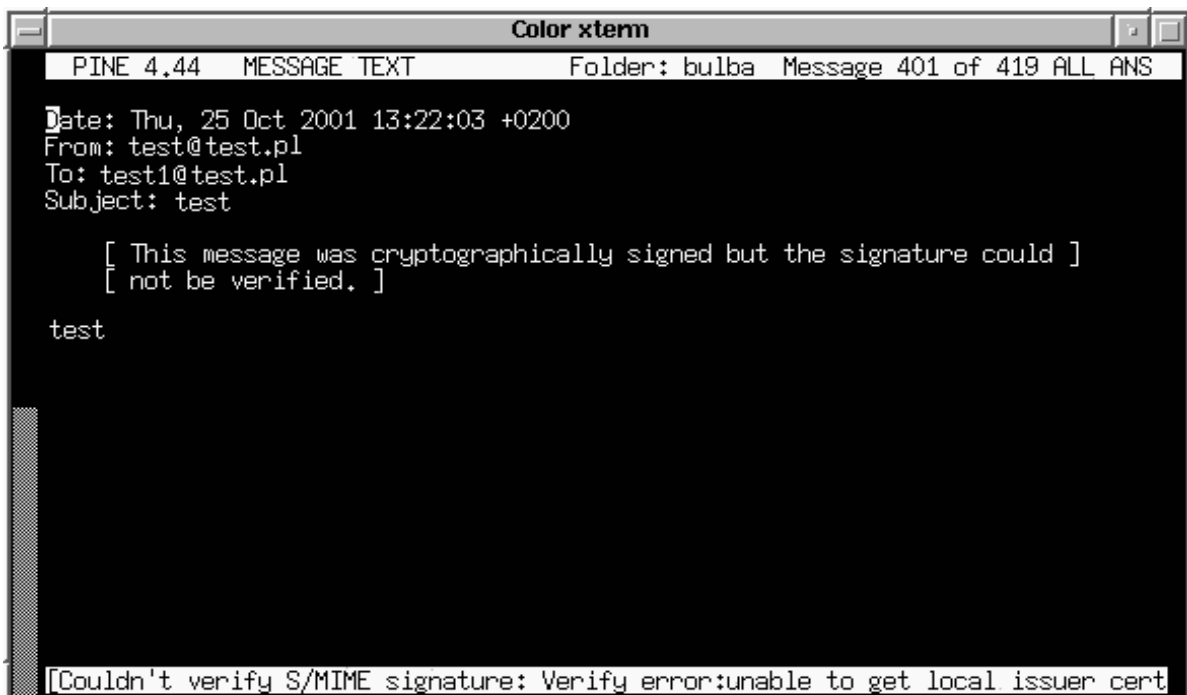
[ Address Book Preferences ]
[ ] combined-addrbook-display
[ ] expanded-view-of-addressbooks
[ ] expanded-view-of-distribution-lists

[ Message Index Preferences ]
[ ] auto-open-next-unread
```

Używanie protokołu S/MIME w programie PINE

Weryfikacja podpisu

Po otwarciu wiadomości e-mail podpisanej cyfrowo program PINE automatycznie dokonuje weryfikacji sygnatury. Rezultatem tego może być pojawienie się informacji o niemożności poprawnej weryfikacji podpisu objawiające się komunikatem błędu, wraz z opisem błędu na dolnej listwie informacyjnej:



```
Color xterm
PINE 4.44  MESSAGE TEXT  Folder: bulba  Message 401 of 419 ALL ANS

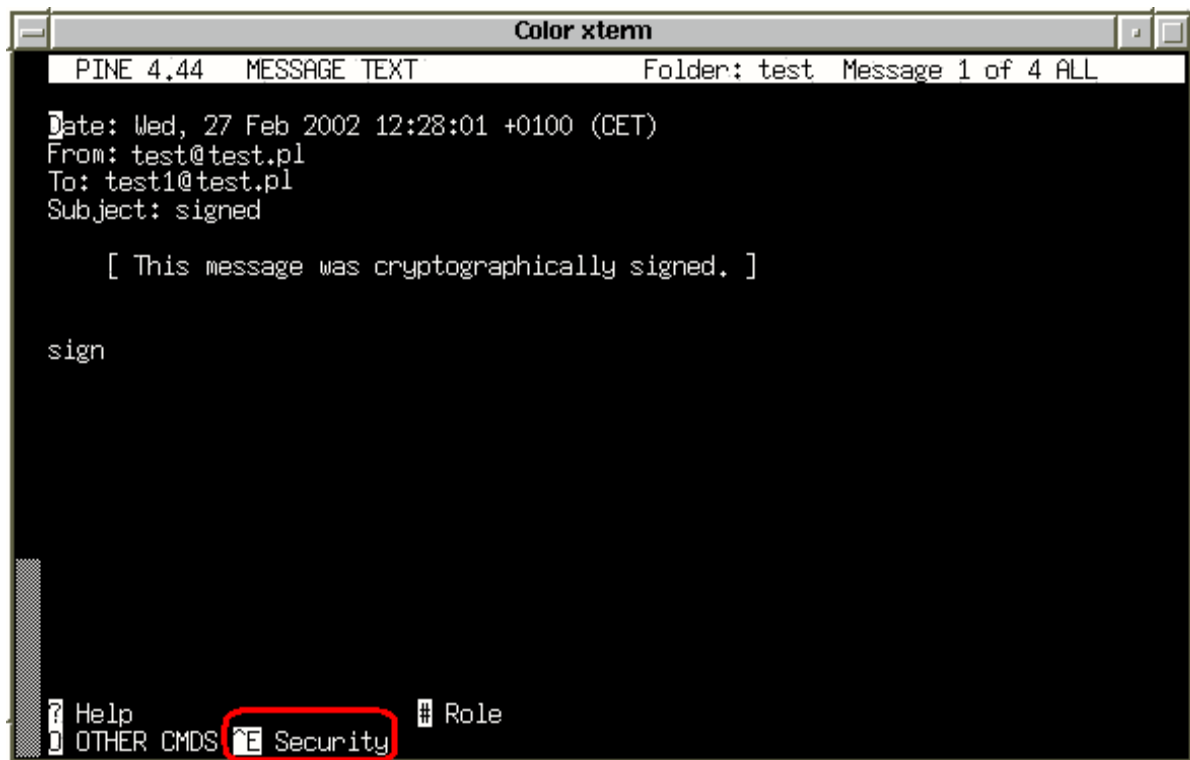
Date: Thu, 25 Oct 2001 13:22:03 +0200
From: test@test.pl
To: test1@test.pl
Subject: test

[ This message was cryptographically signed but the signature could ]
[ not be verified. ]

test

[Couldn't verify S/MIME signature: Verify error:unable to get local issuer cert
```

lub też potwierdzeniem jego autentyczności:



```
Color xterm
PINE 4.44 MESSAGE TEXT Folder: test Message 1 of 4 ALL
Date: Wed, 27 Feb 2002 12:28:01 +0100 (CET)
From: test@test.pl
To: test1@test.pl
Subject: signed

[ This message was cryptographically signed. ]

sign

? Help
OTHER CMDS Security # Role
```

W każdym z wypadków, w dolnym menu istnieje opcja **Security**, dzięki której możemy uzyskać informacje o certyfikacie użytym do podpisania wiadomości. Jeśli opcja **Security** nie jest widoczna, możemy klawiszem o przewijać dolne menu aż do jej pojawienia się. Poprawnie zweryfikowane certyfikaty są automatycznie zapisywane przez program PINE w katalogu `~/.pine-smime/public/` i są gotowe do użycia w dalszej korespondencji

Odczytywanie zaszyfrowanych wiadomości

Po otwarciu zaszyfrowanej wiadomości e-mail pojawia się nam informacja:

```

Color xterm
PINE 4.44 MESSAGE TEXT Folder: test Message 3 of 4 ALL
Date: Wed, 27 Feb 2002 12:28:27 +0100 (CET)
From: test@test.pl
To: test1@test.pl
Subject: encrypt

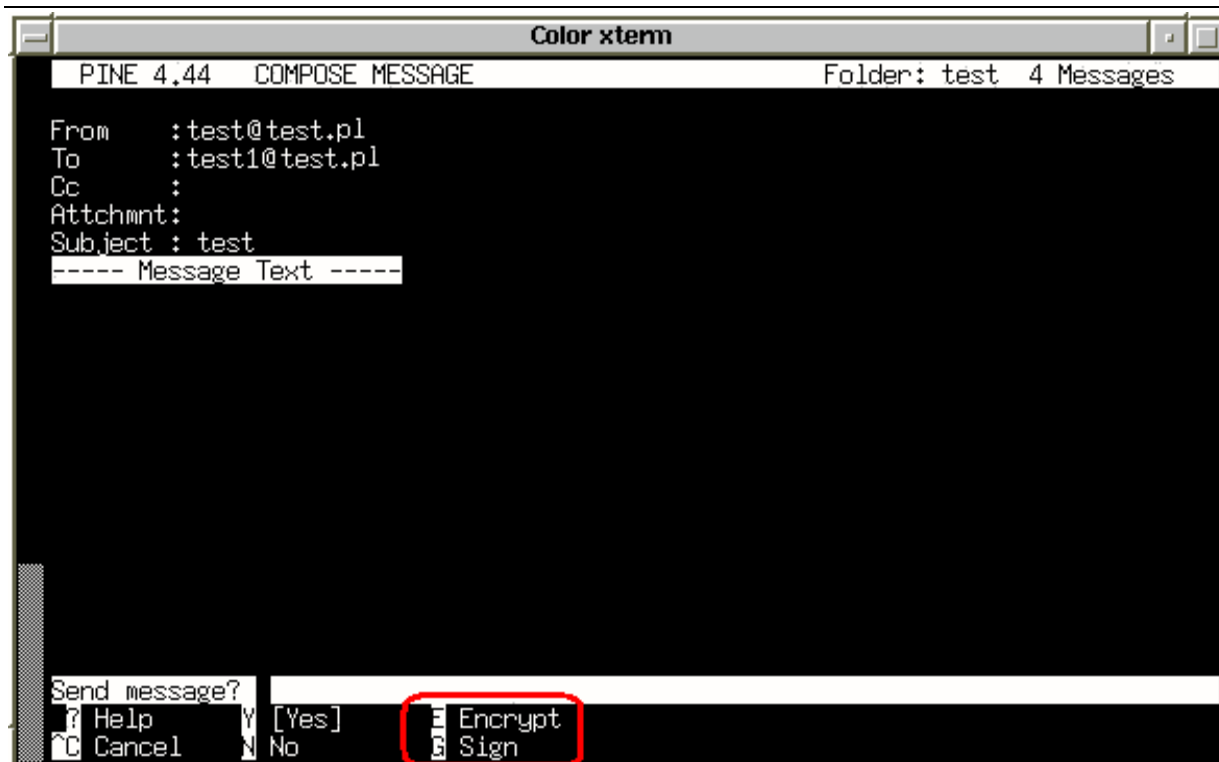
[ Part 1, "S/MIME Encrypted Message" Application/X-PKCS7-MIME ]
[ 564bytes. ]
[ This part is a PKCS7 S/MIME enclosure. You may be able to view it ]
[ by entering the correct passphrase with the "^D" command. Press ]
[ "^E" for more information. ]

? Help      ^D Decrypt  # Role
OTHER CMDS ^E Security
  
```

Aby rozszyfrować wiadomość, należy zgodnie ze wskazówkami na ekranie, wcisnąć kombinację klawiszy CTRL i D, a następnie podać hasło użyte do zabezpieczenia klucza prywatnego. Rozszyfrowana wiadomość zostanie wyświetlona na ekranie. W przypadku podania złego hasła, lub też otrzymania wiadomości do rozszyfrowania, do której nie posiadamy klucza, zostanie wyświetlony komunikat o błędzie. Podobnie jak przy wiadomości podpisanej cyfrowo, uzyskujemy dostęp do opcji Security w menu dolnym, dającej możliwość obejrzenia informacji o certyfikacie użytym do zaszyfrowania wiadomości e-mail.

Tworzenie wiadomości zaszyfrowanych lub podpisanych

Tworzenie podpisanych lub zaszyfrowanych wiadomości przebiega podobnie jak przy zwykłych wiadomościach. Przed każdorazowym wysłaniem wiadomości e-mail, PINE poprosi o potwierdzenie.



W menu dolnym pojawiają się opcje Encrypt i Sign. Wciskając odpowiednio klawisze e i s możemy włączyć i wyłączyć szyfrowanie i podpisywanie wiadomości. Program poinformuje nas o błędzie lub o pomyślnym przetworzeniu wiadomości e-mail. W przypadku wiadomości podpisanej niezbędne będzie podanie hasła zabezpieczającego nasz klucz prywatny.

Bezpieczeństwo użytkowania programu PINE

Bezpieczeństwo naszego użytkowania certyfikatów zależy od bezpieczeństwa klucza prywatnego. Na systemach UNIX-owych, należy zadbać o odpowiednie uprawnienia katalogów i plików. Najlepiej, gdyby prawa dostępu do katalogu `~/pine-smime` miał tylko właściciel. Można to zapewnić wydając polecenie:

```
$chmod 700 ~/.pine-smime
```

Poza plikami należy też chronić hasło. W związku z tym, zalecane jest nie włączanie opcji **remember-smime-passphrase** w konfiguracji PINE, gdyż ktoś kto uzyska dostęp do konsoli z której odczytujemy pocztę, lub też przechwyci sesję wykorzystywaną do połączenia się z serwerem na którym uruchomiony jest PINE może dowolnie dysponować naszym kluczem prywatnym, tj. podszywać się pod nas podpisując wiadomości na treść których nie mamy wpływu.

Ograniczenia nakładki protokołu S/MIME dla programu PINE

Niestety wsparcie dla protokołu S/MIME w obecnym kształcie jest dość ubogie. Nie ma całego systemu zarządzania certyfikatami, nie jest możliwa weryfikacja on-line certyfikatów, brak jest też wielu drobnych cech pomocnych przy wysyłaniu i odbieraniu zabezpieczonej poczty. Jednakże prace nad tym trwają i o ich efektach Centrum Certyfikacji Signet będzie na bieżąco informował.