Używanie wtyczki pluginu Enigmail w progamie Mozilla Thunderbird





Spis treści

1. Generowanie kluczy	2
2. Podpisywanie i szyfrowanie e-maili	5
3. Sprawdzanie podpisu, odszyfrowanie e-maila	7
······································	

1. Generowanie kluczy

Do zaprezentowania możliwości GPG wybraliśmy program Mozilla Thunderbird oraz wtyczkę Enigmail. W Thunderbirdzie należy skonfigurować konto pocztowe. Wtyczkę Enigmail można zainstalować wybierając z menu Narzędzia pozycję Rozszerzenia.

Po instalacji wtyczki w pasku menu pojawi się opcja OpenPGP. Najprostszym sposobem na wygenerowanie kluczy jest wybranie pozycji OpenPGP->Key Management. Przy pierwszym wybraniu tej pozycji powinno pokazać się okno konfiguratora, która pomoże nam w całym procesie.

🦃 OpenPGP Setup Wizard	_ 🗆 🗙
OpenPGP Setup Wizard - zapraszamy	
 This wizard helps you to start using OpenPGP right away. Over the next few screens we'll ask you some questions to get everything setup. To keep everything simple, we make some assumptions about configuration. These assumptions try to provide a high level of security for the average user without creating confusion. Of course, you can change all of these settings after you finish the wizard. You can find out more about the OpenPGP features in the Help menu or on the Enigmail website. If you have any trouble using this wizard, please let us know by emailing us. This wizard is only invoked when you first install Enigmail. It will not be shown again and cannot be called from the menu. Thank you for choosing Enigmail OpenPGP! Would you like to use the wizard now? Yes, I would like the wizard to get me started. No, thanks. I prefer to configure things manually 	
< Wstecz Dalej > Ar	iuluj

Rys. 1 Okno powitalne kreatora generacji kluczy

Na pytanie czy chcemy użyć wizarda odpowiadamy Yes i klikamy Naprzód. Następnie jesteśmy pytani o podpisywanie maili. Można wybrać automatyczne podpisywanie każdego maila lub własnoręczne stworzenie reguł. Kolejne pytanie dotyczy szyfrowania maili. Jeśli posiadamy lub jesteśmy w stanie zdobyć klucz osób, do których wysyłamy pocztę można wybrać opcję Yes w przeciwnym razie wybieramy No. Podczas wysyłania maila będzie możliwość wybrania czy chcemy szyfrować przesyłkę, ewentualnie można stworzyć reguły i wybrać adresy e-mail dla których poczta ma być domyślnie szyfrowana.

W kolejnym kroku można spersonalizować ustawienia klienta poczty. Do wyboru mamy:

Opcja	Znaczenie
Disable loading IMAP parts on demand	Dotyczy tylko protokołu IMAP. Domyślnie z serwera IMAP pobierane są tylko nagłówki wiadomości. W tym miejscu można zdefiniować czy na żądanie pobierać także pozostałe części maila.
Disable flowed text	Definiuje czy zablokować przepływanie tekstu. Klient poczty może łamać linie wg wewnętrznych ustawień. Tym parametrem ustawiamy czy chcemy, aby mail wyglądał dokładnie tak, jak wysłał go nadawca.
View message body as plain text	Definiuje czy pokazywać wiadomość jako czysty tekst.
Use 8-bit encoding for messaage sending	Definiuje czy używać 8-bitowego kodowania podczas wysyłania maili.
Do not compose HTML message	Definiuje czy wyłączyć możliwość tworzenia maili w HTMLu.

Po wybraniu opcji jesteśmy pytani o hasło do klucza. Należy wprowadzić mocne hasło, ale łatwe do zapamiętania. Jeśli zapomnimy hasła nie będzie możliwości jego odtworzenia.

Preferences X		
The following preferences are modified by this Wizard:		
Disable loading IMAP parts on demand		
Disable flowed text (RFC 2646)		
View message body as plain text		
☑ Use 8-bit encoding for message sending		
Do not compose HTML messages		
OK Anuluj		

Rys. 2 Preferencje wysyłania listów.

W kolejnym kroku pokazuje się krótkie podsumowanie. Domyślnie konfigurator generuje klucz 2048-bitowy ważny przez 5 lat. Po kliknięciu Naprzód widzimy okno generowania klucza.

_				
10 million (10		icn c	-	
	111121112		erin	WIZARI
	Spen.	-	ccup.	THEAT

Create Key Create A Key To Sign And Encrypt Email
You need to have a 'key pair' to sign and encrypt email, or to read emails that are encrypted. A key pair has two keys, one public and one private.
You need to give your public key to everyone in your contact list who will want to verify your signature, or to encrypt email to you. Meanwhile, you need to keep your private key secret. You must not give it away, or leave it unprotected. It can read all the email people encrypt and send to you. It can also encrypt email in your name. Because it's secret, it's protected by a passphrase.
Account / User ID:
Managements <mmanagements@ppmanagements@ppmanagements@ppmanagements@ppmanagements@ppmanagements@ppmanagements@p< td=""></mmanagements@ppmanagements@ppmanagements@ppmanagements@ppmanagements@ppmanagements@ppmanagements@p<>
Passphrase

Please confirm your passphrase by typing it again

< Wstecz Dalej > Anuluj

_ 🗆 🗙

Rys 3. Kreator kluczy – wprowadzenia hasła klucza prywatnego

Aby klucz był wygenerowany w sposób losowy potrzebna jest duża ilość entropii. Konfigurator podpowiada by w trakcie generowania intensywnie wykorzystywać dysk twardy lub aktywnie przeglądać strony internetowe. Aby dostarczyć odpowiednią entropię można włączyć kopiowania dużego pliku, z różnymi odstępami czasowymi naciskać klawisze i losowo przesuwać kursor myszy. Po zamknięciu konfiguratora widzimy okno, gdzie można zarządzać dostępnymi kluczami.

2. Podpisywanie i szyfrowanie e-maili.

Program Thunderbird umożliwia bardzo wygodnie szyfrować, deszyfrować, podpisywać i weryfikować podpis wiadomości e-mail oraz zarządzać bazą kluczy.

Najważniejszą funkcją oferowaną przez wtyczkę Enigmail podpisywanie i szyfrowanie maili. Wystarczy zaledwie kilka kliknięć myszką, żeby bezpiecznie wymieniać nawet najbardziej poufne dane przez Internet. Zaszyfrowana w programie wiadomości może być odkodowana dopiero przez odbiorce. Nawet jeśli wiadomość zostanie podsłuchana podczas transportu przez sieć jej zawartość, dla osoby nieposiadającej klucza prywatnego, będzie bezużyteczna. Równie łatwo można cyfrowo podpisywać maile, aby odbiorcy naszych wiadomości mieli pewność, że pochodzą one od autentycznego nadawcy.

Należy podkreślić, że szyfrowana jest treść maila i ewentualnie załączniki. Nagłówki wiadomości pozostają niezaszyfrowane (część z nich musi być dostępna dla serwerów poczty, część zmienia się podczas transportu), w związku z tym temat maila, który jest jednym z nagłówków, pozostanie niezaszyfrowany.

Domyślnie w mailach wykorzystywane jest tzw. PGP/inline. Informacje o kluczu użytym do zaszyfrowania przechowywane są w treści wiadomości. Stwarza to problemy z szyfrowaniem i podpisywaniem załączników oraz znaków spoza standardowej tablicy ASCII. W związku z tym powstało udoskonalenie w postaci PGP/MIME (PGP Multipurpose Internet Mail Extensions, opisane w RFC 2015 i RFC 3156). W mailach korzystających z PGP/MIME informacje o PGP zawarte są w nagłówkach, a nie w ciele wiadomości. Większość klientów e-mail obsługuje PGP/MIME, więc jeśli mamy pewność, że korespondujemy z osobą, która używa takiego klienta zalecane jest włączenie PGP/MIME. Popularnym programem pocztowym, która nie wspiera PGP/MIME jest Outlook.

Należy pamiętać, że zaszyfrowanie załącznika może przynieść zaskakujące efekty. Przykładowo jeśli w zaszyfrowanym załączniku znajduje się malware, przejdzie on niepostrzeżenie przez skaner antywirusowy znajdujący się na w systemie lub na bramach pocztowych.

Kolejnym problemem jest odczytywanie e-maili w webowych klientach poczty. Aby odszyfrować wiadomość należałoby umieścić klucz prywatny na serwerze WWW, tak aby skrypty klienta mogły odszyfrować e-maila. Zgodnie z zasadą głoszącą, że klucz prywatny powinien być dostępny tylko dla jego właściciela, trzymanie klucza na publicznie dostępnym serwerze jest niedopuszczalne. Oczywiści uniemożliwia to odszyfrowanie wiadomości z poziomu czytnika webowego.

Aby zaszyfrować lub podpisać wiadomość oczywiście należy ją najpierw stworzyć. Po wpisaniu adresu odbiorcy, tematu i treści klikamy przycisk OpenPGP.

Do wyboru są trzy opcje:

- Sign message podpisanie wiadomości
- Encrypt message zaszyfrowanie wiadomości
- Use PGP/MIME użycie PGP/MIME

😢 Tworzenie: My votes		
<u>Plik E</u> dycja <u>Wi</u> dok W <u>s</u> taw Eormat Opcje Ope <u>n</u> PGP <u>N</u> ar	zędzia Pomo <u>c</u>	
Wyślij Adresy Pisownia Załącz OpenPGP 5/1	🗿 🔹 🔔 🔹 MIME Zapisz jako	
Nadawca:		
Do: 🔝 rms@gnu.org		
Temat: My votes	OpenPGP Encryption & Sig 🗙	
Treść 🔹 Zmienna szerokość 💌 📕	I Encrypt Message	1: 전 편 문· 제· @·
	🔲 Use PGP/MIME	
I'm voting on "yes" in free software case. Cheers	OK Anuluj	
nii i i i i i i i i i i i i i i i i i i		

Rys 4. Okno podpisywania e-maila w programie Mozilla Thunderbird

Wybieramy żądane opcje i klikamy OK. Teraz pozostało już wybrać pozycję wyślij.

This message contains attachments. How would you like encrypt/sign	them?
O Just encrypt/sign the message text, but not the attachments	
Encrypt each attachment separately and send the message using	g inline PGP
C Encrypt/sign the message as a whole and send it using PGP/MIME	E
NOTE: PGP/MIME is only supported by a limited number of mail clien/ Mozilla/Thunderbird, Sylpheed, Pegasus and Mulberry are known to Linux/UNIX and Mac OS X most popular mail clients support it. If you option.	ts! On Windows only support this standard; on u are unsure, select the second
Use the selected method for all future attachments	
	OK Anuluj

Rys. 5 Wybór między PGP/inline i PGP/MIME

Jeśli do e-maila zostały dodane załączniki pokaże się powyższe okno. Do wyboru jest:

- Zaszyfrowanie/podpisanie samej wiadomości, bez załączników
- Zaszyfrowanie każdego załącznika osobno używając PGP/inline
- Zaszyfrowanie/podpisanie całego e-maila używając PGP/MIME

Wybieramy stosowną opcję, klikamy *OK*, a następnie *wyślij*. Jeśli została wybrana opcja podpisania wiadomości Thunderbird automatycznie użyje klucza prywatnego nadawcy. Jeśli została wybrana opcja szyfrowania użyty zostanie klucz publiczny odbiorcy. Oczywiście klucze powinny być dostępne w bazie programu.

3. Sprawdzanie podpisu, odszyfrowanie e-maila.

Sprawdzenie podpisu użytego w dostarczonej wiadomości jest równie łatwe jak jego złożenie.

Istnieje możliwość zdefiniowania czy wiadomości maja być automatycznie deszyfrowane i autentykowane. Opcję tą można zmienić w menu OpenPGP/Automatically Decrypt/Verify Messages.



Rys. 6 Menu OpenPGP, wybór automatycznego deszyfrowania/weryfikowania wiadomości

Jeśli otrzymany e-mail jest podpisany poprawnie w oknie wiadomości pokaże się informacja *Good* signature from <nazwa nadawcy>.

OpenPGP: Good signature Key ID: 0xDFC8	from Estimation 3996 / Signed or	n: 2006-10-28 20:	≕@ ⊯	>
🗄 Temat: Test			Od:	
Content-Type: text/pla	in: charset=	ISO-8859-2		
	,			
Podpisana wiadomość.				
12				
_				

Rys 7. Poprawnie podpisany e-mail.

W przeciwnym wypadku ujrzymy ciąg signature verification failed.

OpenPGP: Error - signature verification failed; click Pen icon for details
 Temat: Wyniki głosowania
 Od: ______i

Rys 8. Niepoprawnie podpisany e-mail.

Taka sytuacja może zajść jeśli adres nadawcy nie pasuje do podpisu lub jeśli treść wiadomości

uległa zmianie od czasu podpisania.

Oczywiście, aby sprawdzić czy podpis jest poprawny należy posiadać klucz publiczny nadawcy. Jeśli klucz publiczny jest niedostępny dla Thunderbirda zobaczymy informację *Unverified signature*. Program zaoferuje nam możliwość ściągnięcia klucza z serwera kluczy.



Rys 9. Nieznana sygnatura e-maila.

Podobnie sytuacja wygląda przy deszyfrowaniu e-maili. Jeśli zaznaczono opcję Automatically Decrypt/Verify Messages maile będą automatycznie odszyfrowane przed wyświetleniem (oczywiście jeśli dostępny jest klucz prywatny odbiorcy).

OpenPGP: Decrypted message	
Temat: Wyniki sprzedaży	Od:

Rys 10. Poprawnie odszyfrowana wiadomość.

Jeśli widzimy informację Decrypted message, wiadomość została poprawnie odszyfrowana.

Jeśli zdarzy się, że w bazie kluczy nie ma klucza prywatnego odpowiadającego kluczowi publicznemu, którym została zaszyfrowana wiadomość ujrzymy napis *secrey key needed to decrypt message*.

OpenPGP: Error - secret key needed to decrypt message; click Key icon for details Rys 11. Brak klucza prywatnego do odszyfrowania wiadomości.