Ghid de utilizare a PGP pentru semnarea și criptarea mesajelor de e-mail

Serviciul de Telecomunicații Speciale

Introducere

Acest ghid descrie configurarea rapidă a aplicațiilor necesare pentru a folosi semnarea și/sau criptarea de tip *"Pretty Good Privacy (PGP)"*. Pentru a atinge acest scop se folosesc trei aplicații:

1. GNU Privacy Guard (GnuPG)

   GNU Privacy Guard este utilitarul de bază care permite operațiunile de semnare, criptare și management de chei PGP. Este disponibil în mod gratuit pentru diferite sisteme de operare, precum Windows, OS X, UNIX, OS/2, OpenVMS etc., la adresa http://www.gnupg.org/.

2. Thunderbird

   Următorul pas după instalarea GnuPG este descărcarea și instalarea clientului de e-mail Thunderbird 2.0, de la adresa http://www.mozillamessaging.com/thunderbird/.

3. Enigmail

   Enigmail este un add-on pentru Thunderbird care permite interfațarea Thunderbird cu GnuPG. Acesta poate fi descărcat gratuit de la adresa http://enigmail.mozdev.org/.

Descărcarea și instalarea Enigmail

După descărcarea Enigmail (fișierul *"Enigmail.xpi"*), se deschide Thunderbird, apoi din bara de meniu a ferestrei principale se selectează *"Tools -> Add-ons"*. Se va deschide o noua fereastră în care se văd toate add-on-urile din Thunderbird. În colțul din stânga al ferestrei, se apasă butonul *"Install"* și apoi se alege calea către fișierul *"Enigmail.xpi"*.

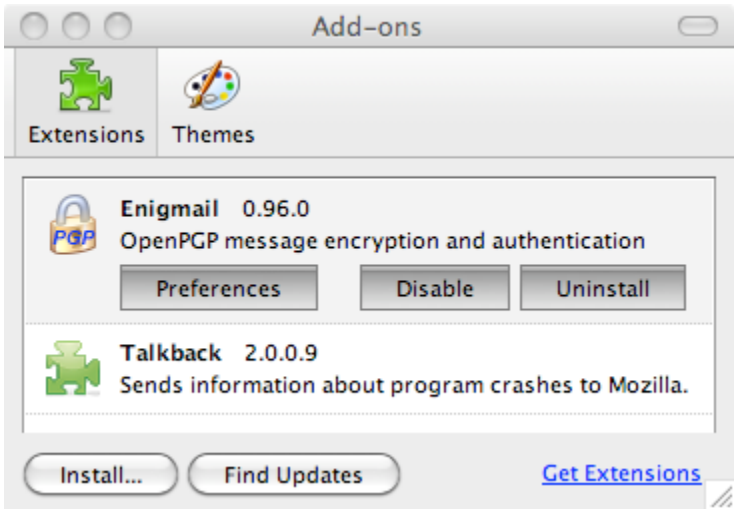

Figura 1. Managerul de add-on-uri Thunderbird cu Enigmail instalat

După instalare, clientul de e-mail Thunderbird trebuie repornit.

Dezinstalarea Enigmail

Dacă se dorește dezinstalarea Enigmail, se pornește Thunderbird și se selectează din meniu *"Tools -> Add-ons"*. Se va deschide o noua fereastră în care se văd toate add-on-urile din Thunderbird. Se selectează "Enigmail" și apoi se apasă butonul *"Uninstall"*.

Enigmail va fi dezinstalat după închiderea clientului de e-mail Thunderbird.

Crearea primei perechi de chei

Criptografia cu chei publice

Enigmail foloseşte criptografia cu chei publice pentru a asigura caracterul privat al comunicaţiilor între utilizatori. În criptografia cu chei publice se folosesc două tipuri diferite de chei, cu ajutorul cărora se asigura confidenţialitatea datelor și autentificarea utilizatorilor.

Prin confidenţialitatea unui mesaj se înţelege că numai persoanele cărora le-a fost destinat mesajul îl vor putea citi. Prin autentificarea utilizatorilor se înţelege că persoanele care primesc un mesaj pot verifica dacă acesta provine într-adevăr de la persoana specificată ca expeditor.

Astfel, pentru a putea folosi Enigmail, utilizatorii vor crea o pereche de chei formată dintr-o cheie publică şi o cheie privată. Cheia publică poate fi distribuită oricui, în timp ce cheia privată nu trebuie să fie cunoscută de altcineva decât de proprietar.

Utilizarea aplicației de generare a cheilor

Pentru a genera o noua pereche de chei se vor realiza următorii paşi:

1. Lansarea Thunderbird. Se pornește clientul de e-mail Thunderbird.
2. Crearea unui cont de e-mail. Trebuie să existe cel puţin un cont de e-mail configurat în Thunderbird pentru a putea continua. În caz contrar, utilizatorul trebuie mai întâi să configureze un astfel de cont.
3. Pornirea *"Enigmail Key Manager"*. Se apasă pe *"OpenPGP"* din bara de meniu a ferestrei principale Thunderbird şi se selectează *"Key Management"*.
4. Pornirea aplicației de generare de chei. După deschiderea *"Enigmail Key Manager"*, se apasă butonul *"Generate"* din meniu şi se selectează "New key pair", ceea ce va deschide o nouă fereastră.

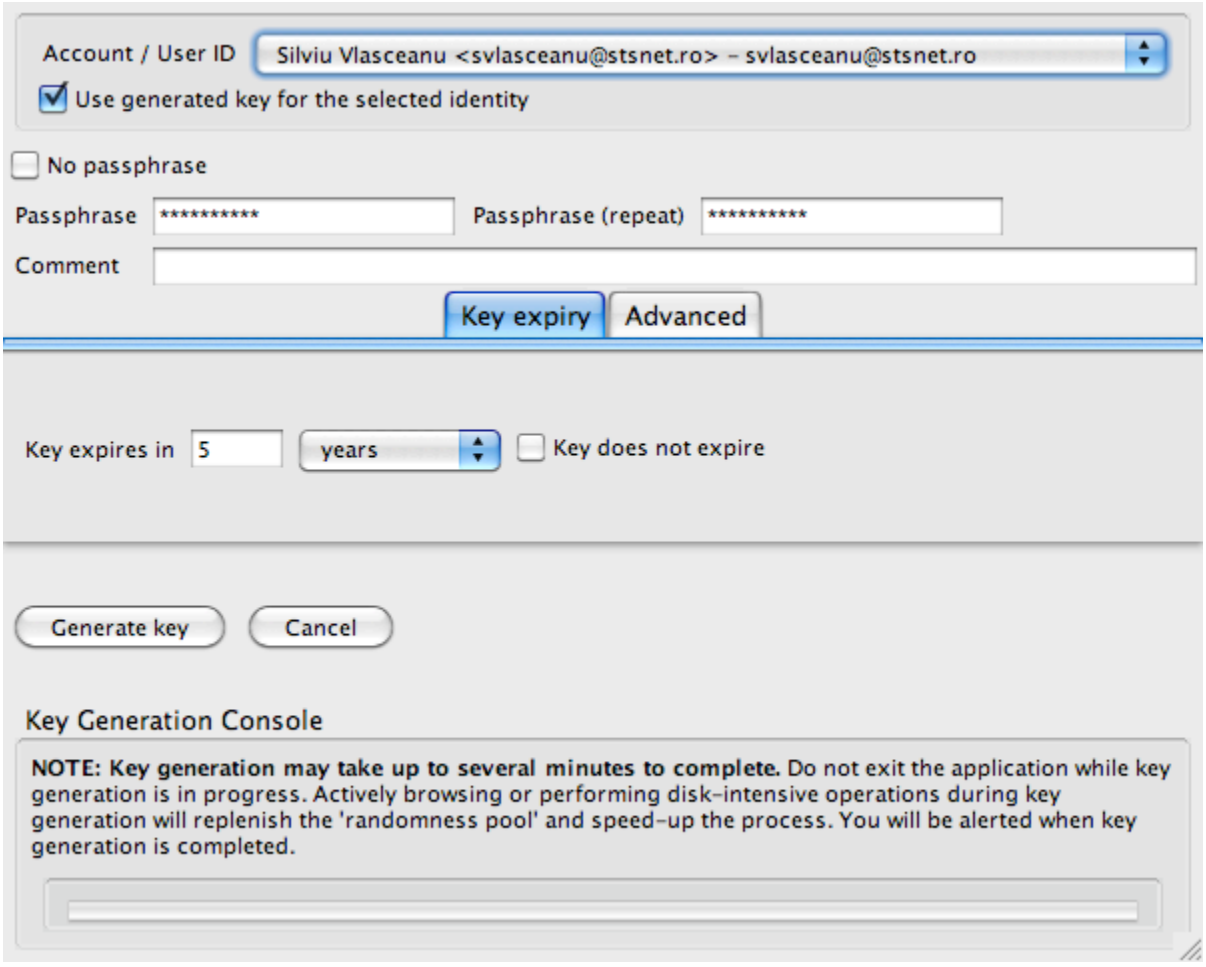

Figura 2. Fereastra Enigmail pentru generarea de chei

5. Selectarea contului de e-mail. În partea de sus a ferestrei nou deschise se află o casetă de tip listă în care sunt afişate toate conturile de e-mail configurate în Thunderbird. Aplicaţia GnuPG va asocia

noua cheie cu una din aceste adrese de e-mail. Se selectează în caseta de tip listă contul pe care se vor primi mesaje criptate.

6. Introducerea parolei. Cheile private sunt foarte importante şi de aceea aplicaţia GnuPG nu le va putea folosi decât dacă utilizatorul cunoaşte parola secretă. În acest pas se va specifica parola aleasă de utilizator pentru protecţia cheii private. Aceasta se introduce de două ori – în caseta *"Passphrase"* și în caseta *"Passphrase (repeat)"*. Prin introducerea parolei de două ori se evită introducerea greșită a acesteia. Parola nu va fi vizibilă în timpul introducerii.
   Atenţie! În cazul în care ulterior utilizatorul nu îşi mai aminteşte parola introdusă, accesul la cheia privată nu va mai fi posibil.
7. Generarea cheii. Se apasă pe butonul *"Generate key"*.
8. Generarea unui certificat de revocare. Pentru cazurile în care, din diferite motive, nu mai este posibil accesul la cheia secretă sau securitatea acesteia este compromisă, este nevoie ca utilizatorul să anunţe persoanele cu care corespondează că valabilitatea cheii secrete a încetat. Acest lucru se realizează prin trimiterea unui certificat de revocare. Certificatul de revocare este generat pe baza cheii private și astfel persoanele care îl primesc pot fi sigure de autenticitatea acestuia. După generare certificatul de revocare trebuie păstrat într-un loc sigur.
   După terminarea procesului de generare a cheilor, Enigmail oferă utilizatorului posibilitatea generării unui certificat de revocare. Se va selecta *„Yes"* şi apoi se va introduce parola de protecţie a cheii secrete. Apoi, aplicaţia va genera automat un certificat de revocare.

Publicarea cheii

Cea mai simplă metodă de distribuire a cheii este publicarea acesteia în reţeaua publică de servere de chei – o bază de date pentru chei la nivel global (după ce o cheie a fost publicată în această reţea, ştergerea ei de acolo nu mai este posibilă). Pentru a publica o cheie, se selectează cheia în aplicaţia Enigmail Key Manager, apoi se selectează din meniu "*Keyserver -> Upload Public Keys*".

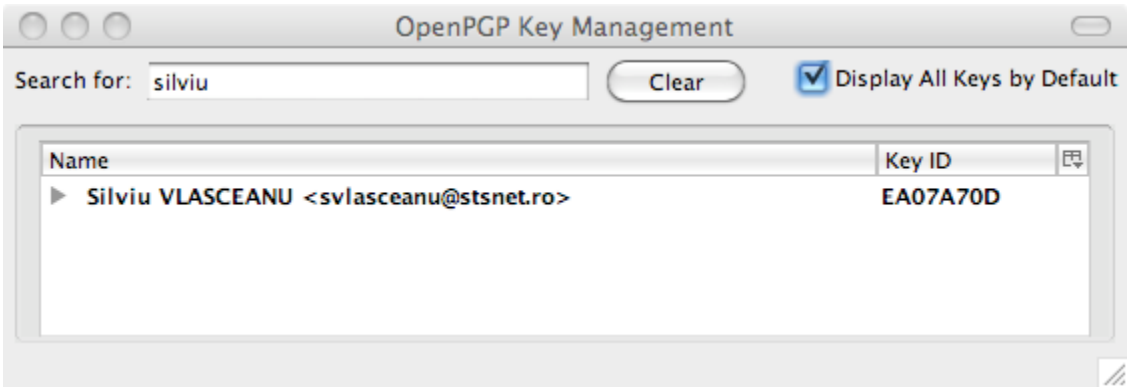

Figura 3. Fereastra Enigmail pentru management de chei cu meniul "Keyserver"

Aplicaţia va cere locaţia în care se doreşte încărcarea cheii. Se va introduce în caseta corespunzătoare "**sks.stsisp.ro**" si se va apăsa *"OK"*. Cheia va fi imediat publicată şi oricine doreşte să iniţieze o comunicaţie

securizată va putea găsi această cheie foarte uşor cunoscând numele şi/sau adresa de e-mail a utilizatorului.

Semnarea şi criptarea e-mail-urilor

Semnarea digitală a unui e-mail

După crearea unei chei, se poate experimenta trimiterea de e-mail-uri criptate şi/sau semnate către robotul OpenPGP. Acesta, denumit Adele, are adresa de e-mail adele-en@gnupp.de. Adele răspunde oricărui tip de mesaj OpenPGP.

Pentru trimiterea unui e-mail semnat se procedează astfel:

1. Se apasă butonul *"Write"* din interfața Thunderbird. Din meniul OpenPGP din partea de sus a ferestrei se selectează opțiunea *"Attach My Public Key"*, dacă este prima dată când se trimite un e-mail către acest destinatar.
2. Se scrie e-mail-ul în format text simplu, nu HTML. Dacă de obicei folosiți mesaje HTML (cu formatare, culori, imagini etc.), atunci se menține apăsată tasta *"Shift"* în momentul apăsării butonului *"Write"*, pentru a scrie mesajul în mod text simplu.
3. Se apasă butonul *"OpenPGP"* din Thunderbird și se bifează numai opțiunea *"Sign Message"*.

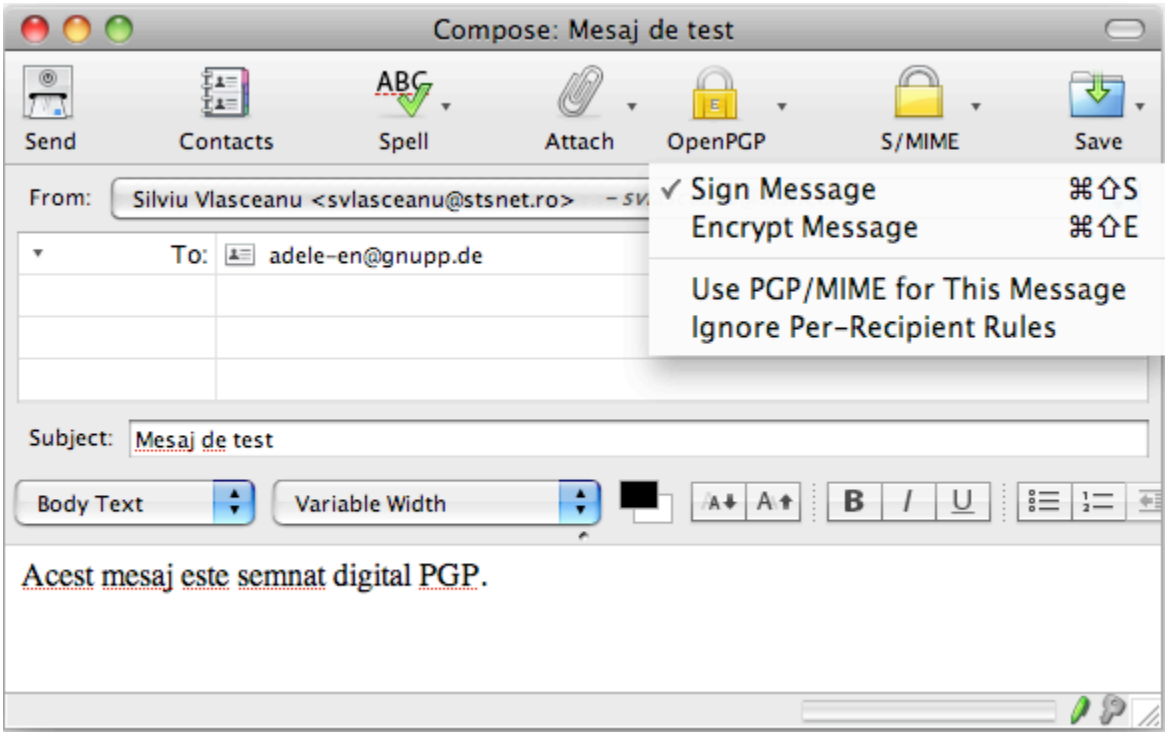

Figura 4. Semnarea PGP a unui e-mail cu Enigmail

4. La final, se apasă butonul *"Send"*. După introducerea parolei pentru cheie, Enigmail va semna mesajul și îl va trimite destinatarului.

Criptarea unui e-mail

Pentru criptarea unui e-mail se folosește cheia publică a destinatarului. Pentru a o afla, aceasta se caută după ID-ul ei. ID-ul cheii trebuie comunicat a priori de către destinatar, sub forma unui șir de 8 caractere (litere și/sau cifre). Etapele căutării sunt următoarele:

1. După primirea ID-ului cheii publice a destinatarului, în fereastra principală Thunderbird, se selectează din meniu *"OpenPGP -> Key Management"*. La deschiderea ferestrei *"Key Manager"*, se selectează din meniu *"Keyserver -> Search for Keys"*. Se introduce ID-ul cheii dorite în caseta de căutare, adăugând în fața acestuia prefixul "`0x`", dacă nu există deja.

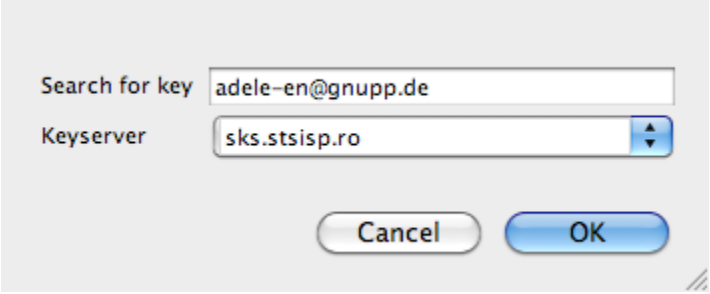

Figura 5. Fereastra de căutare a unei chei

2. Se apasă butonul *"OK"*. Enigmail va căuta cheia dorită pe serverul de chei. Dacă aceasta este găsită, va fi copiată local, în mod automat.

După obținerea unei copii a cheii publice a destinatarului, Enigmail este pregătit de trimiterea unui e-mail criptat. Se apasă butonul *"Write"* din interfața Thunderbird și se scrie un mesaj, în mod obișnuit. Înainte de a fi trimis, se apasă butonul *"OpenPGP"* și se selectează opțiunea *"Encrypt Message"*. Se trimite apoi e-mail-ul, apăsând butonul *"Send"*.

În acest moment, există două posibilități. Dacă adresa de e-mail a destinatarului este găsită într-una din cheile locale, trimiterea este terminată; mesajul va fi criptat și trimis destinatarului. Dacă apare o problemă la asocierea adresei destinatarului cu cheia locală corespunzătoare, Enigmail va solicita selectarea manuală a unei chei pentru criptare. În acest caz, se selectează cheia potrivită din meniul afișat, urmând ca mesajul să fie criptat și trimis destinatarului.