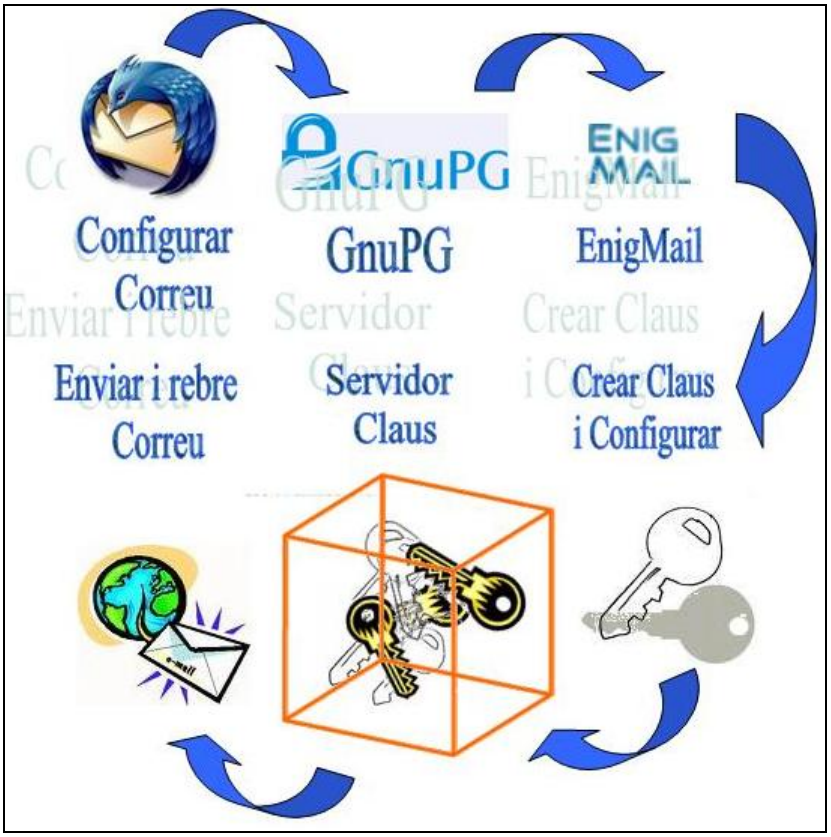
Correu segur

Hem de poder configurar el nostre programa de correu electrònic per aconseguir el **correu segur**. Vegem com ho faríem en un programa de correu habitual (i lliure) com és el programari *Thunderbird*. En la figura 1 es poden veure tots els passos de manera esquemàtica, i tot seguit els expliquem en detall perquè es pugui dur a terme en un equip real.

Figura1. Configuració d'un correu electrònic segur



Una vegada configurat el compte de correu, instal·larem l'eina de criptografia. Aquesta serà la que faci el **xifratge dels missatges** i incorpori la **signatura digital**, que després haurà de ser verificada pel receptor del missatge. En el cas del programari *Thunderbrid*, els complements són *Enigmail* i *GnuPG*.

> La instal·lació del programari *Thunderbird*, gratuït es pot descarregar de http://www.mozilla.org/

1. Crear i configurar el compte de correu en Thunderbird.

Primer de tot heu de comprovar que teniu les dades bàsiques del compte, concretament necessitareu:

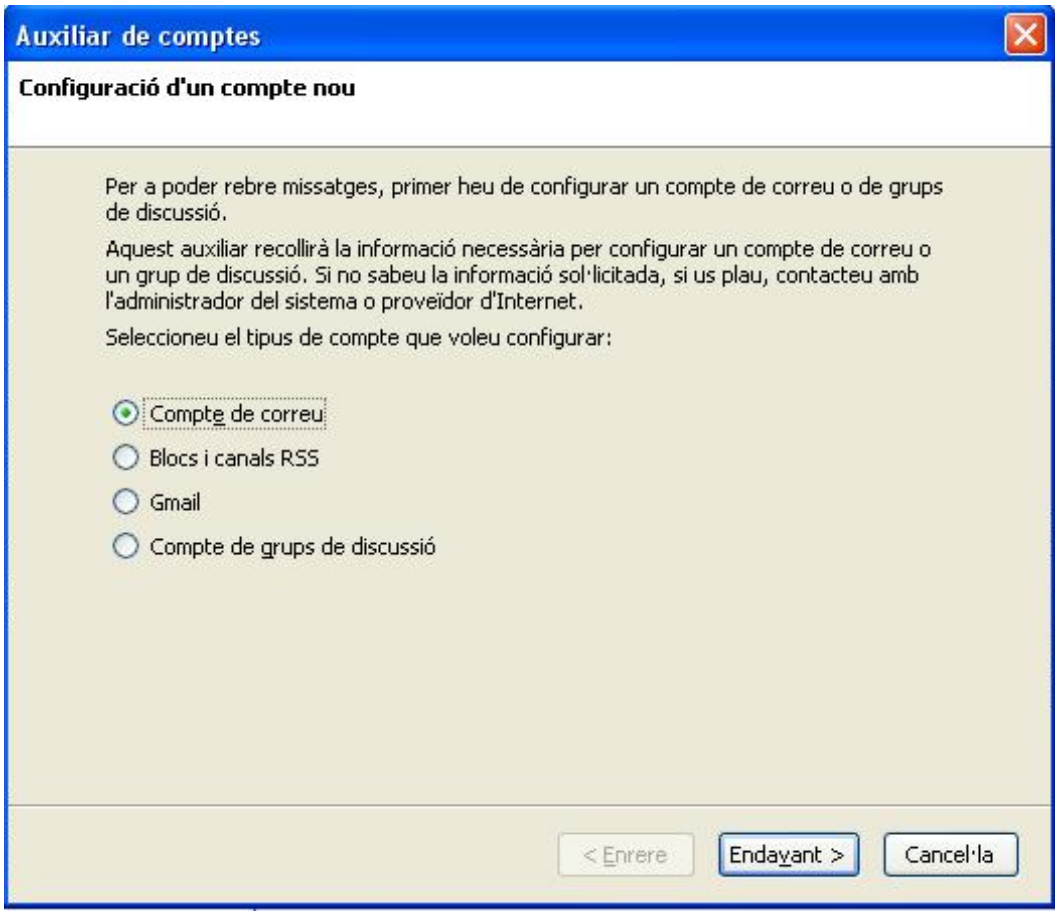
- Adreça de correu.
- Servidor d'entrada.

- Servidor de sortida.
- Nom del compte.
- Contrasenya.

A continuació obrireu el programari Thunderbird. Us apareixerà l'*Auxiliar de Comptes* (si és la primera vegada que executeu el programa, us apareixerà un assistent inicial que informa de la possibilitat d'importar dades d'altres programaris). Anireu al menú **Eines** \ **Configuració dels comptes ...** i fareu clic al botó **Afegir compte ...**

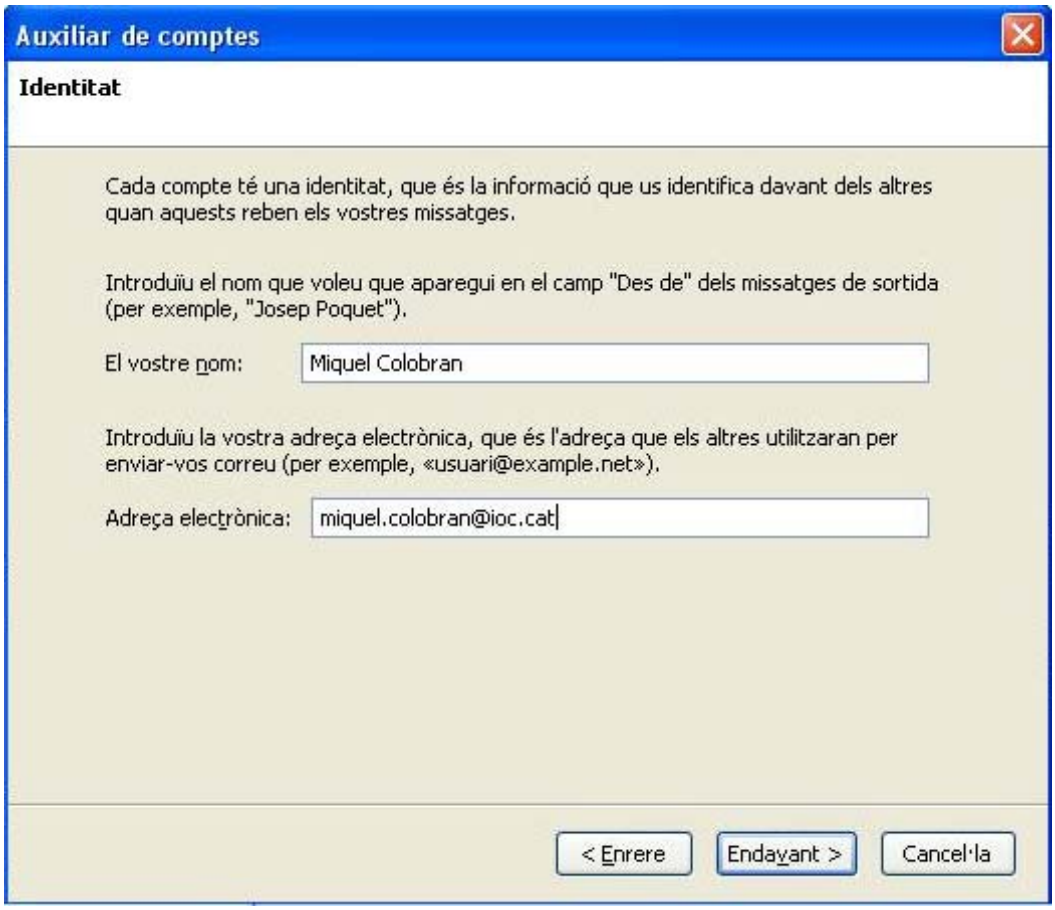
- Triareu l'opció **Compte de correu** (figura 2) i **Endavant**.

Figura 2. Finestra de configuració d'un compte nou



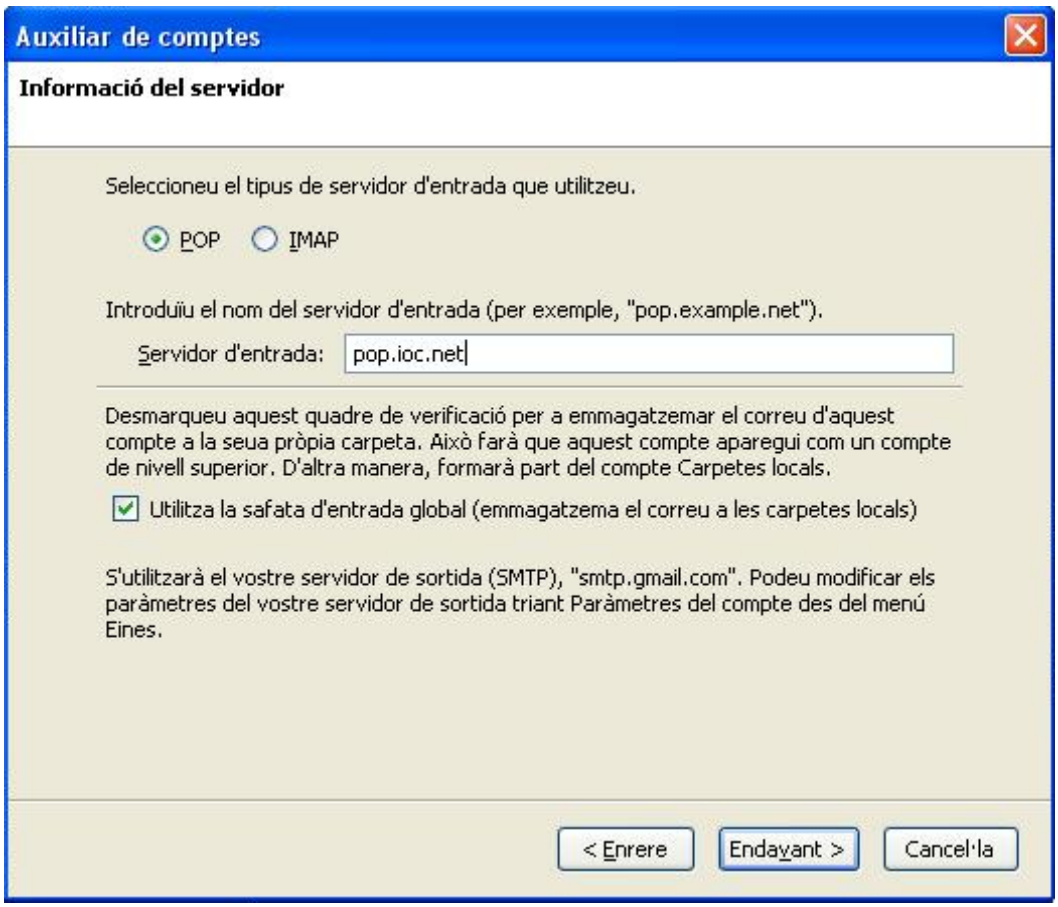
- A continuació omplireu les següents dades, referides al nom i a l'adreça electrònica de l'usuari (figura 3). Fareu clic a **Endavant**.

Figura 3. Finestra de configuració de la identitat



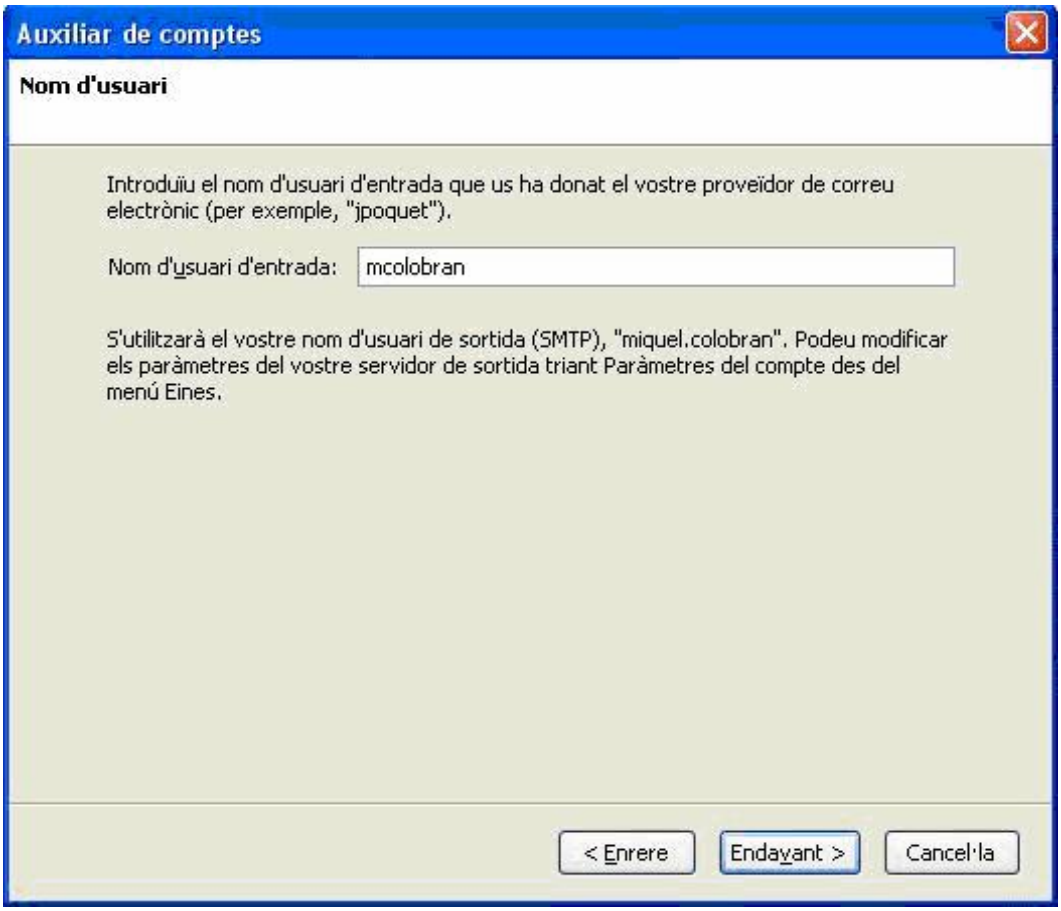
- Triareu l'opció de tipus de servidor POP o IMAP (figura 4) i ompliu els valors dels camps, nom de servidor entrant i servidor de correu sortint.

Figura 4. Finestra d'informació del servidor



- Escriureu el nom del compte de correu (figura 5).

Figura 5. Introducció del nom d'usuari



- Finalment donareu un nom per identificar el compte que acabeu de configurar (figura 6). Aquest nom pot ser la pròpia adreça de correu o qualsevol altra descripció que us serveixi per a reconèixer el compte.

Figura 6. Introducció del nom del compte

Ja heu acabat de configurar el compte. El programa us demanarà la contrasenya del correu i una vegada introduïda correctament, el programari *Thunderbird* descarregarà els vostres missatges des del servidor de correu.

2. Instal·lar *GnuPG.*

GnuPG és gratuït i es pot descarregar de http://www.gnupg.org/

En primer lloc cal descarregar el programari *GnuPG* i instal·lar-lo (figura 7).

Figura 7. Instal·lació del programari *GnuPG*

3. Instal·lar *Enigmail.*

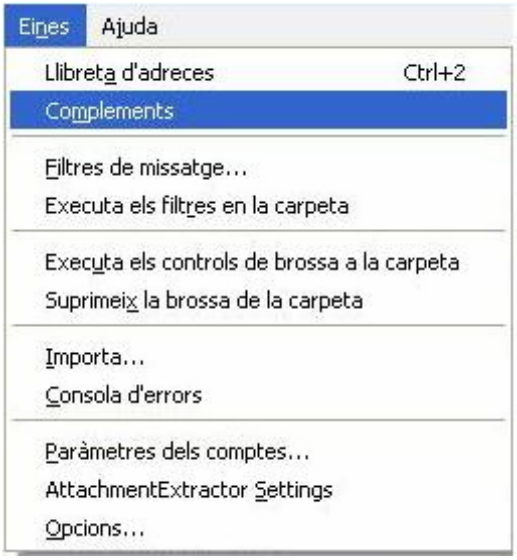
Enigmail és una extensió addicional per *Mozilla* i *Mozilla Thunderbird*. No és en si mateix cap programari criptogràfic, sinó que empra *GnuPG* (instal·lat en el pas previ) per a realitzar les operacions criptogràfiques.

Enigmail es pot descarregar de: https://addons.mozilla.org/ca/thunderbird/addon/71

Premeu amb el botó dret del ratolí a l'enllaç d'*Enigmail* i trieu l'opció **Guardar l'enllaç com...** per a descarregar el complement a l'ordenador.

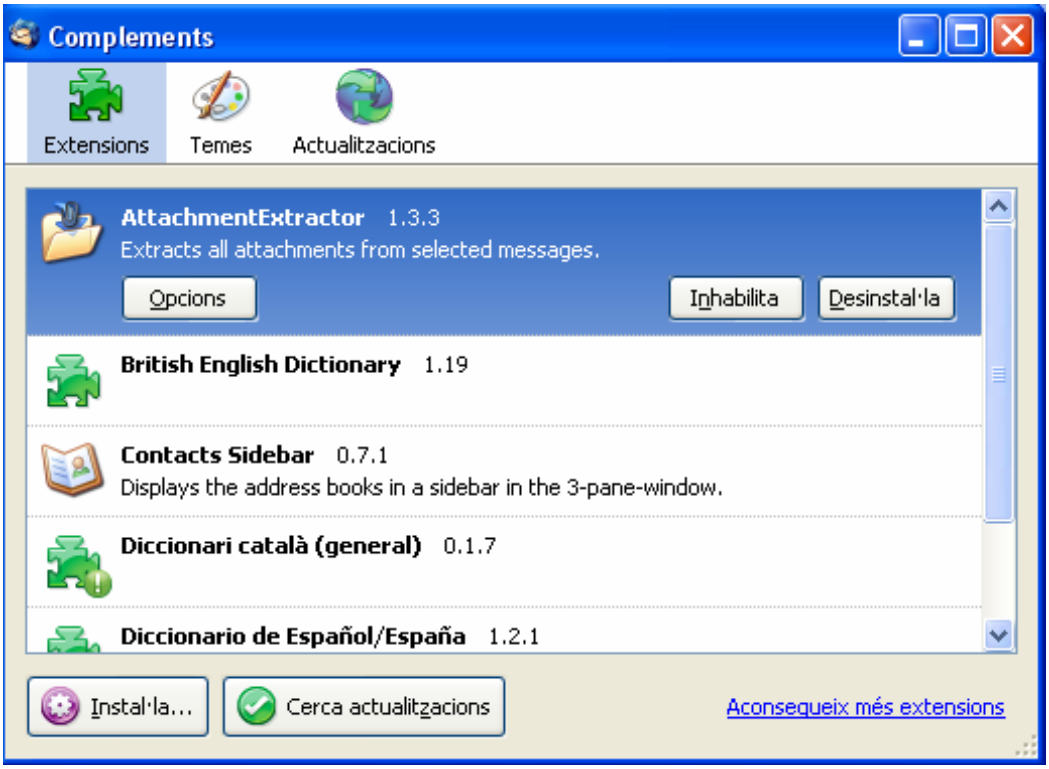
- A continuació obriu *Thunderbird* i seleccioneu: **Eines** \ **Complements**, tal i como es pot veure a la figura 7.

Figura 7. Activació de la finestra de complements



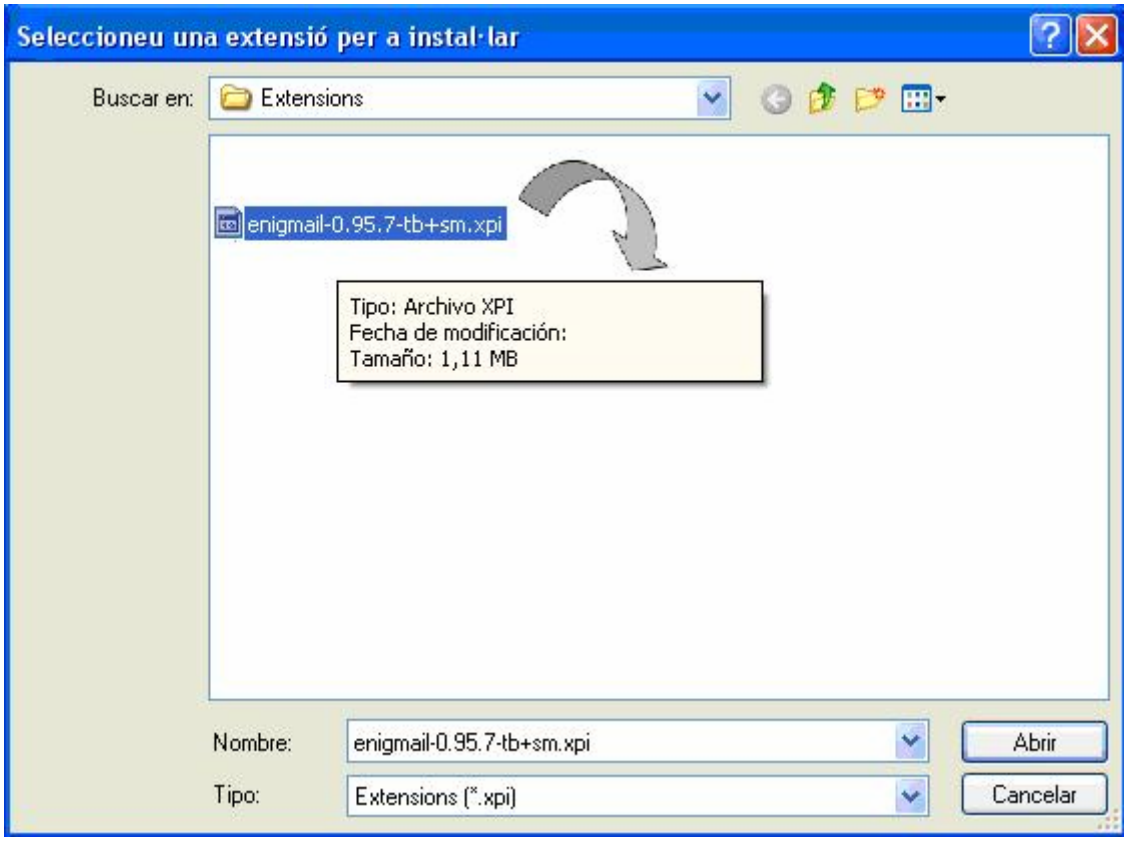
- Seguidament s'activarà la pantalla de **Complements**, tal i com es mostra en la figura 8.

Figura 8. Finestra de Complements del *Thunderbird*



- Premeu **Instal·lar** per activar la pantalla i seleccioneu l'extensió a instal·lar (figura 9).

Figura 9. Selecció de l'extensió a instal·lar



Trieu el fitxer **enigmail-0.95.7-tb+sm.xpi** i premeu **Obrir** per activar la pantalla d'instal·lació de programari. Premeu **Insta-lar Ara**. L'extensió s'instal·larà. Després us preguntarà si voleu reiniciar *Thunderbird* per a que els canvis siguin efectius.

Si la instal·lació ha estat correcte, veureu una opció de menú **OpenPGP** que apareix en el programari *Thunderbird* després d'haver-lo reiniciat.

4. Generar parell de claus. En el programa veureu una nova opció al menú superior a l'esquerra d'**Eines**, titulat **OpenPGP**. Seleccioneu **OpenPGP** \ **Administració de claus**. S'obrirà una finestra. Trieu al menú l'opció **Generar** \ **Nou parell de claus**.

> A la pestanya **Avançades**, s'especifica la mida i el tipus de clau. Assegureu-vos que seleccioneu un tipus de clau DSA i l'algorisme de El Gamal. Quant més gran sigui la clau, més segura serà, però també requerirà més recursos el xifrat i desxifrat lícit de missatges.

En el quadre de diàleg que apareix especificareu diversos paràmetres de les claus:

- La **identificació a usar** per al parell de claus.

- La **contrasenya o frase clau** del parell de claus. La contrasenya protegeix la clau privada contra un ús fraudulent. Si algú aconsegueix robar aquesta clau privada, necessitarà conèixer la contrasenya associada per poder utilitzar-la.

- El **temps d'expiració de la clau**. Es a dir, el temps durant el qual la clau que generem serà vàlida.

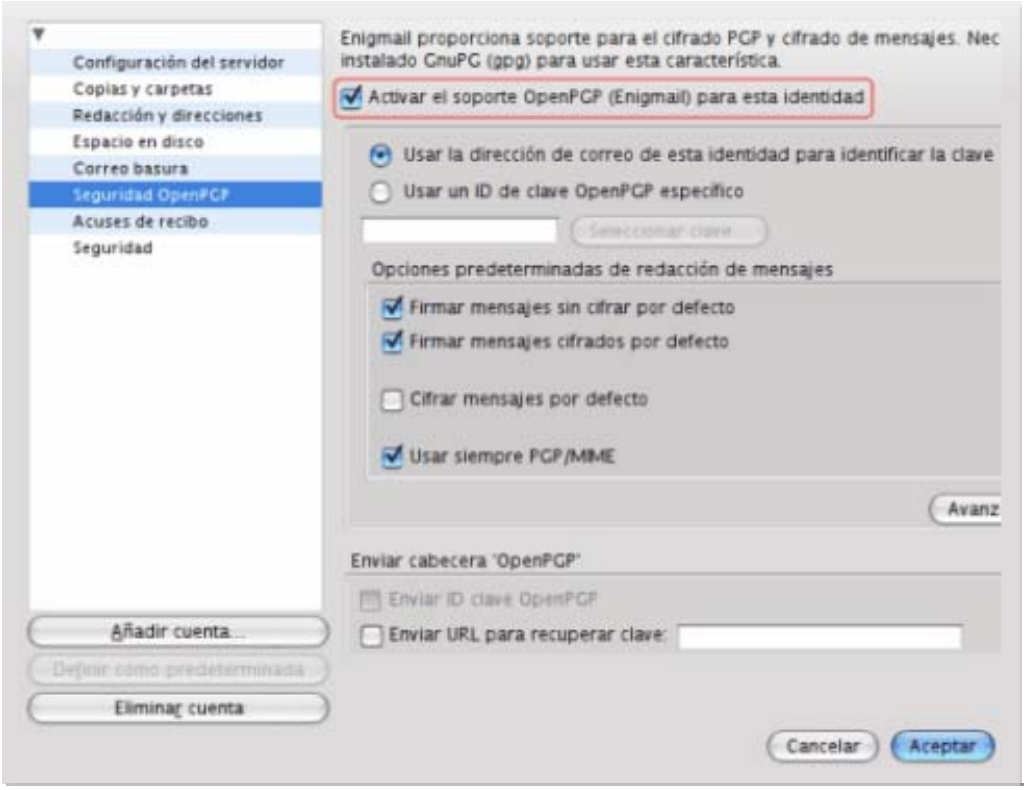
Premeu el botó **Generar clau**. El procés pot arribar a tardar alguns minuts. Quan hagi acabat, us preguntarà si voleu crear un **certificat de revocació**. Us pot fer falta si perdeu o us roben la clau privada. Guardareu el certificat en alguna carpeta **que no sigui d'accés públic** (un bon lloc per guardar-la és un llapis USB o un CD-ROM).

Tan bon punt hàgiu guardat el certificat de revocació en un lloc segur, veureu la nova clau en la llista de claus conegudes en negreta. En el camp **Tipus** us apareixerà com a **pub/sec**, que significa pública/secreta, és a dir, que disposeu tant la clau pública com la clau privada.

5. Configuració de les claus.

Ja heu creat les claus. Ara ja esteu a punt per utilitzar-les per signar els correus que envieu. Per a això, obrireu el quadre de diàleg de configuració dels comptes i a la secció **Seguretat OpenPGP** triareu **Activar el suport OpenGPG (Enigmail) per a aquesta identitat**.

Figura 10. Activació de la signatura.



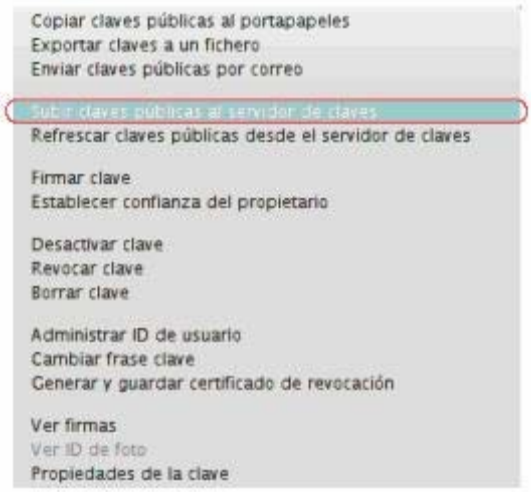
Si només disposeu de la clau que acabeu de generar, s'ha d'usar l'opció **Usar l'adreça de correu d'aquesta identitat per identificar la clau OpenPGP**. Però si en teniu més d'una, usareu l'opció **Usar un ID de clau OpenPGP específic** per triar la que vulgueu emprar.

Immediatament podeu veure les opcions d'activació de la signatura (figura 10) i/o xifrat dels missatges per defecte. Si no les activeu, sempre ho podreu fer mentre redacteu un correu a través del menú **OpenPGP** o els botons **OpenPGP** i **S/MIME** de la finestra de redacció, que se us mostraran per defecte després d'instal·lar *Enigmail*.

6. Pujar la clau pública a un servidor de claus.

Les claus públiques (**mai les privades**) es poden distribuir per correu electrònic, amb un llapis USB, per correu electrònic, etc. Però la manera més habitual és usar els anomenats **servidors de claus** (figura 11), que no són res més que "magatzems" a Internet de claus públiques, d'accés lliure. Publicar la vostra clau en un d'aquests servidors és molt senzill, només us cal fer clic a la finestra d'administració de claus d'*Enigmail* i seleccionar l'opció de pujar claus públiques al servidor de claus. A la llista de servidors que apareix, en triareu un, per exemple, pgp.mit.edu.

Figura 11. Publicació de la clau a un servidor de claus



L'usuari a qui vulgueu enviar un correu xifrat haurà de realitzar el mateix procés (o l'equivalent amb el seu gestor de claus) per pujar la seva clau pública a un servidor de la seva elecció (us haurà de dir quin servidor és). A la finestra de l'administrador de claus d'**OpenPGP**, seleccionareu al menú **Servidor de claus \ Buscar claus**. En el quadre de diàleg que apareix, introduireu l'adreça del servidor de claus que us proporcioni l'altre usuari i el nom o identitat amb què ha registrat la seva clau. Us apareixerà una finestra amb les claus trobades al servidor que coincideixen amb el vostre criteri de cerca. Seleccionareu la que vulgueu importar. Podreu veure la

clau pública del contacte a la vostra llista de claus disponibles. Aquesta vegada amb el tipus "pública" present a la columna **Tipus**.

Recordeu

Si només teniu la vostra clau privada i pública no podreu xifrar missatges, només signar-los, ja que necessiteu la clau pública del destinatari a qui voleu enviar el missatge xifrat per poder fer-ho. Si l'usuari a qui voleu enviar missatges xifrats ja té clau pública, li heu de demanar.

7. Signar i/o xifrar missatges.

Una vegada heu fet tot l'anterior, signar i xifrar missatges des de la finestra de redacció és molt senzill.

Si voleu **signar un missatge**, seleccionareu al menú superior **OpenPGP** \ **Signar missatge**, o premereu el botó **OpenPGP** de la barra d'eines. En enviar el missatge us demanarà la contrasenya de la vostra clau privada, i es generarà un codi a partir del contingut del vostre missatge que s'adjuntarà a aquest i permetrà al destinatari verificar que el cos del missatge no ha estat alterat en el seu trajecte.

Si el que voleu és **xifrar el missatge**, seleccionareu al menú superior **OpenPGP** \ **Xifrar missatge** (figura 12), o premereu el botó **OpenPGP** de la barra d'eines. Les claus dels destinataris especificats en els camps **Per**. es buscaran a l'anell de claus en funció de la seva adreça electrònica. Si a l'enviar el missatge no trobeu alguna clau o no és de confiança, s'obrirà una finestra demanant-vos de seleccionar les claus públiques que s'usaran per xifrar. En aquest punt podeu descarregar-vos les claus que us faltin des dels servidors de claus.

Recordeu que per enviar un missatge xifrat a algú necessitareu la seva clau pública.

Figura 12. Enviar un missatge usant claus