Agència Catalana de Certificació

MANUAL D'ÚS DEL CLAUER idCAT
- LINUX -

006_20060220

Versió: v2.2
Data: 14/12/2011

Índex

044 20060904

Guia d'instal·lació del programari del clauer idCAT

L'Agència Catalana de Certificació fa un nou pas en la seva tasca de difusió de la identitat digital, i lliura el certificat idCAT dins d'un clauer amb connexió USB a qualsevol ciutadà que sol·liciti el certificat digital idCAT.

Recordeu que el certificat idCAT està reconegut per fer tràmits amb les administracions públiques, a nivell estatal (ministeris), autonòmic (generalitat i amb altres comunitats autònomes) i a nivell local (ajuntaments i consells comarcals).

Podeu trobar els tràmits que es poden realitzar amb el certificat digital idCAT i vídeos dels mateixos al web www.idcat.cat.

Els principals avantatges que aporta aquest dispositiu són els següents:

- **Portabilitat:** es pot utilitzar en qualsevol ordinador amb connexió USB.
- **Seguretat:** l'accés al certificat idCAT està protegit amb paraula de pas, com en el cas de les targetes de crèdit; és a dir, no es pot realitzar una signatura electrònica sense l'autorització de l'usuari, reduint així el perill davant la pèrdua del clauer.
- **Ús com a memòria USB:** el clauer idCAT també funciona com a memòria USB , per tal de transportar els fitxers que l'usuari vulgui.

044 20060904

La instal·lació d'aquest programari[1] permet convertir una memòria USB en un dispositiu segur per tal d'emmagatzemar certificats protegits amb una paraula de pas.

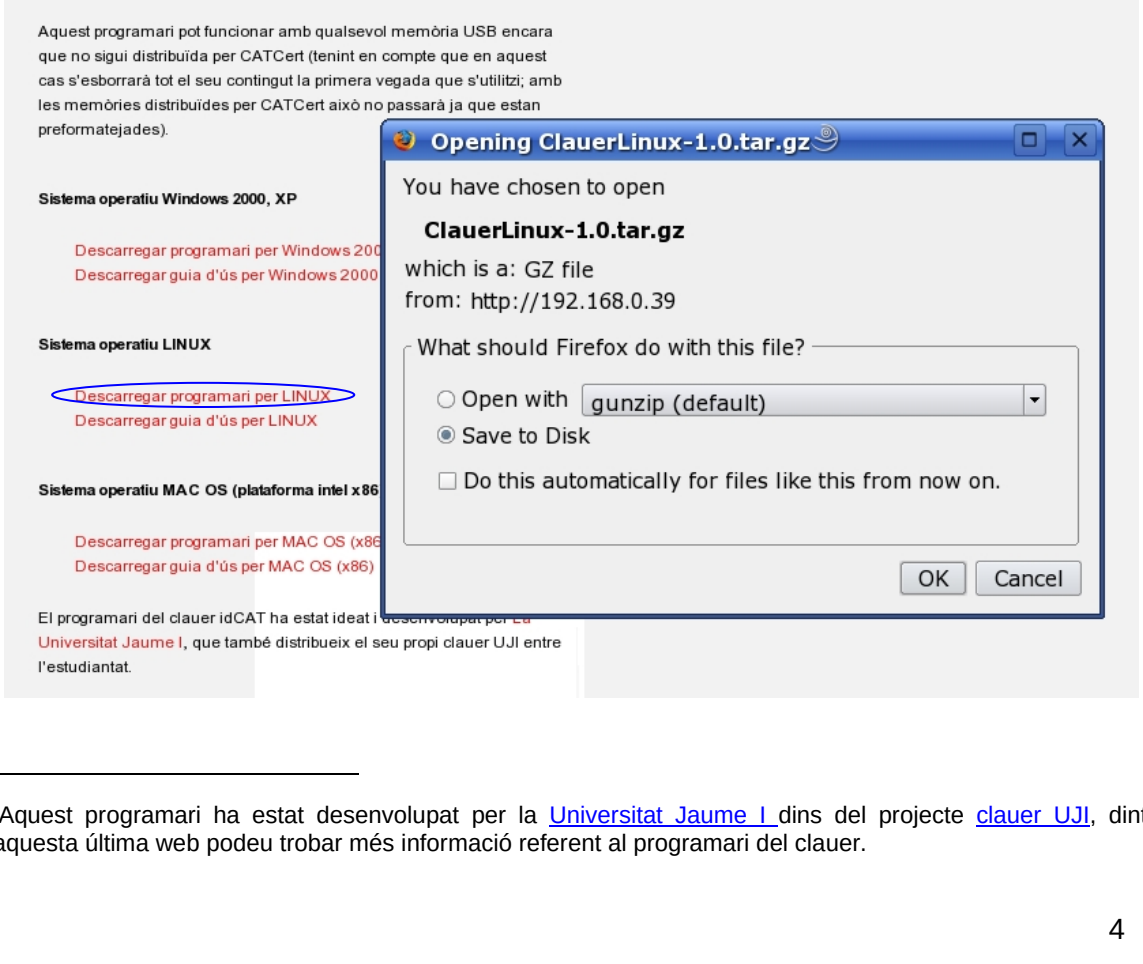
A continuació es detallen els passos que cal seguir per instal·lar correctament el clauer idCAT.

PAS 1 - Instal·lació del programari del clauer idCAT a Linux-Firefox

Només caldrà fer aquest procés una vegada en cadascun dels ordinadors des dels quals vulgueu fer servir el clauer idCAT:

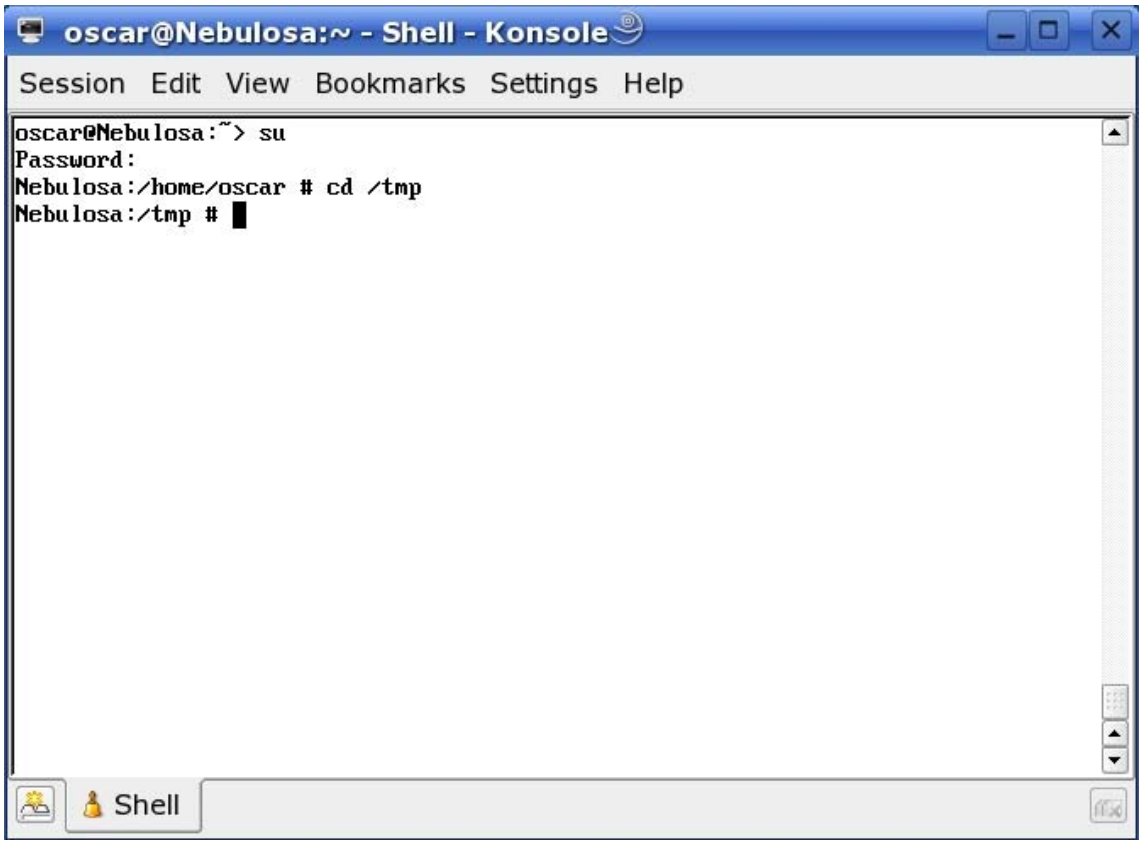
1. Introduïu el clauer idCAT en un port USB de l'ordinador.

2. Aneu al directori: */Programari clauer/linux* i copieu el fitxer *ClauerLinux-1.0.tar.gz* a la carpeta */tmp* del vostre sistema Linux. Alternativament podeu descarregar la última versió del fitxer des del web www.idcat.cat/clauer.



[1] Aquest programari ha estat desenvolupat per la Universitat Jaume I dins del projecte clauer UJI, dintre d'aquesta última web podeu trobar més informació referent al programari del clauer.

3. Obriu una consola de comandes de sistema.
4. Accediu com a usuari administrador *(root)* executant la comanda *su* i aneu al directori */tmp* on abans heu copiar el fitxer *ClauerLinux-1.0.tar.gz*



5. Executeu les següents comandes per tal de compilar la llibreria que farà de driver entre el navegador *Firefox* i el clauer idCAT[2].

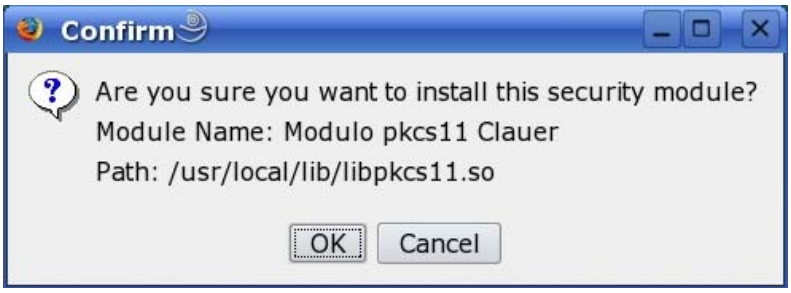
```
#tar zxvf ClauerLinux-x.y.tar.gz
#cd ClauerLinux*
#./configure
```

[2] NOTA: Per compilació per processador x86_64, s'ha d'invocar el configure amb l'opció *--enable-64* per tal que utilitzi les biblioteques sota */usr/lib64*

Si a l'executar la comanda ./configure us dona un error, verifiqueu que la vostra distribució de Linux tingui instal·lat el compilador estàndard *g++* i també tingui la llibreria criptogràfica *openssl-devel 0.9.7* (també es suporta la 0.9.8) en cas que el vostre Linux suporti sistema de paquets RPM o la llibreria criptogràfica libssl-dev en cas que el vostre Linux suporti el sistema de paquets DEB.

```
#make
#make install
#/etc/init.d/clos start
#exit
>firefox-install-pkcs11.sh
```

6. Us apareixerà aquesta finestra i haureu de clicar el botó OK.



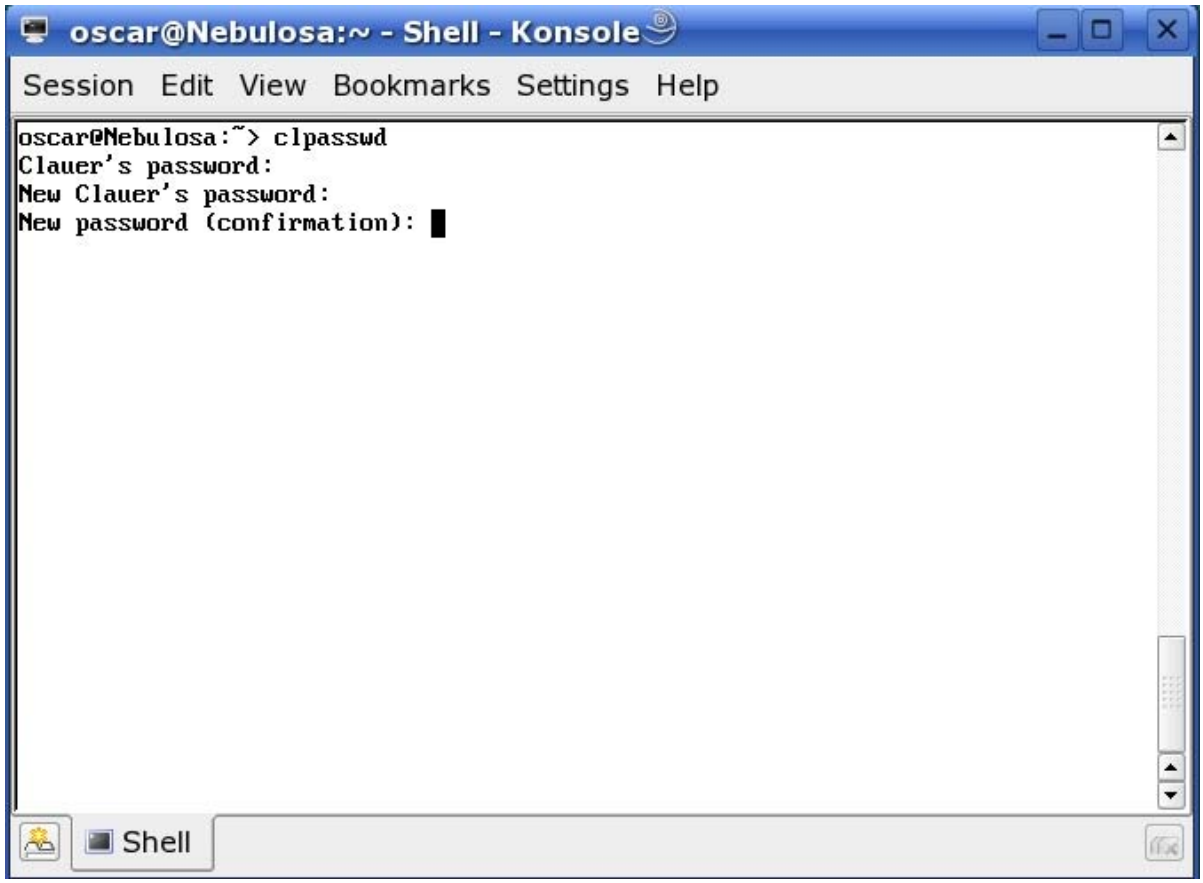
En cas que no us aparegui la finestra anterior si us plau seguiu les instruccions d'instal·lació manual a Firefox que trobareu al web de CATCert a l'apartat de suport, a continuació teniu l'enllaç directe:

http://www.catcert.cat/descarrega/manuals_guies/Guia_rapida_Configuracio_idCAT_amb_FireFox+Linux.pdf

PAS 2 - Canvi del PIN del clauer idCAT (recomanat)

El canvi de PIN és recomanat per tal de començar a fer servir el clauer idCAT. Per fer-ho heu de:

1. Obrir una consola de comandes i executar la comanda *clpasswd* . Se us demanarà que introduïu la password actual (la que trobareu imprès al full que us han donat a l'entitat de registre[3]), i que introduïu després el nou password dos vegades:



ATENCIÓ! NO OBLIDEU aquesta password ja que se us demanarà cada vegada que vulgueu signar o autenticar-vos electrònicament.

[3] En cas que ja tinguéssiu certificat digital idCAT i que us hagin donat un clauer verge aquest password es "clauer" sense cometes.

PAS 3 - Prova del clauer

Si heu realitzat el PAS 1 ja disposeu d'un clauer idCAT 100% operatiu i preparat per a fer-se servir. Si voleu comprovar el seu bon funcionament podeu provar per exemple descarregar el vostre informe de vida laboral des del web de la seguretat social.

Per a fer-ho si us plau seguiu les instruccions del següent vídeo:
http://www.youtube.com/watch?v=ZNA-16WUoT0

Recordeu que podeu trobar més vídeos d'usos al canal youtube de l'idCAT:
http://www.youtube.com/idCATvideo

i al web:
www.idcat.cat

Tinc una pregunta o comentari

Les últimes versions del programari i d'aquesta guia les tindreu disponibles a www.idcat.cat/clauer.

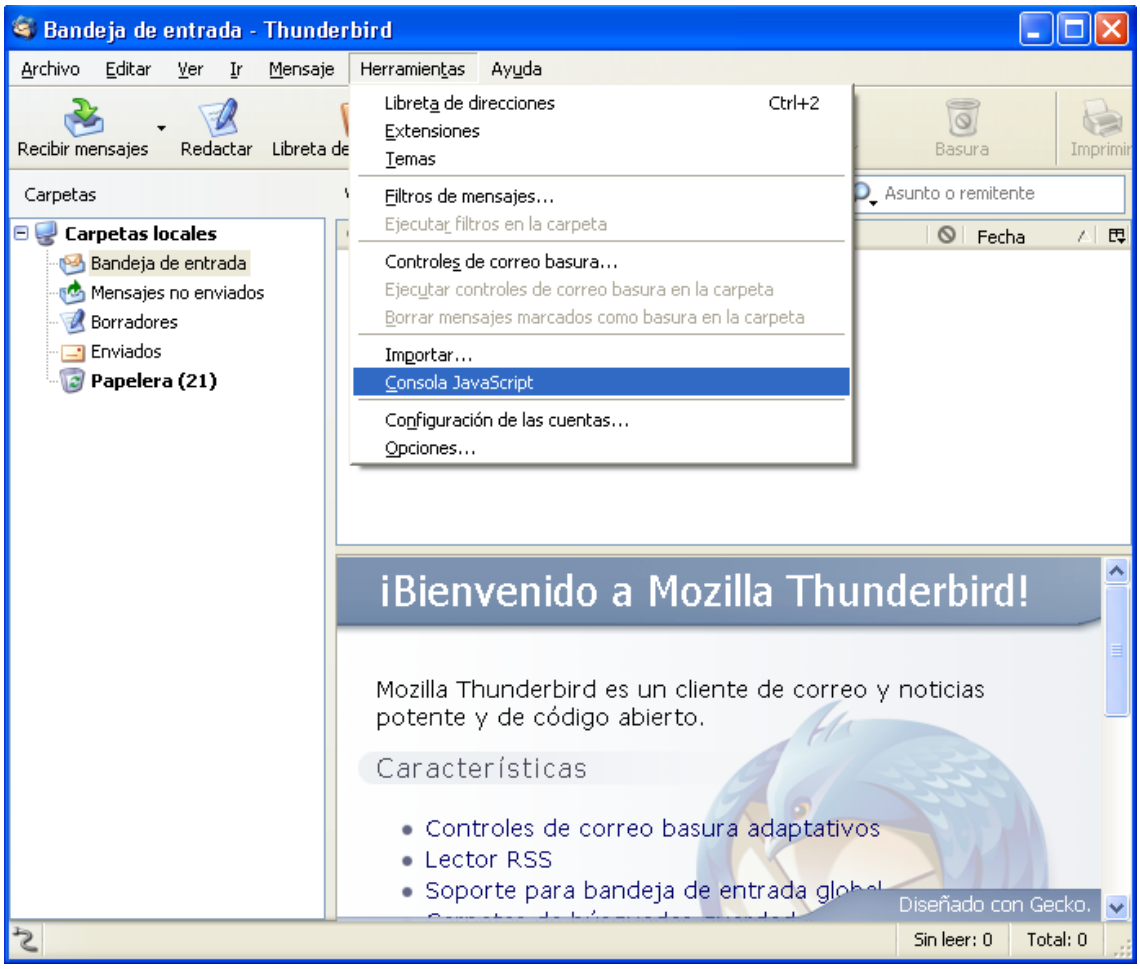
Si teniu algun dubte o comentari, consulteu els diversos recursos disponibles al web www.idcat.cat .

044 20060904

Annex A: Instal·lació especifica pel client de correu Thunderbird

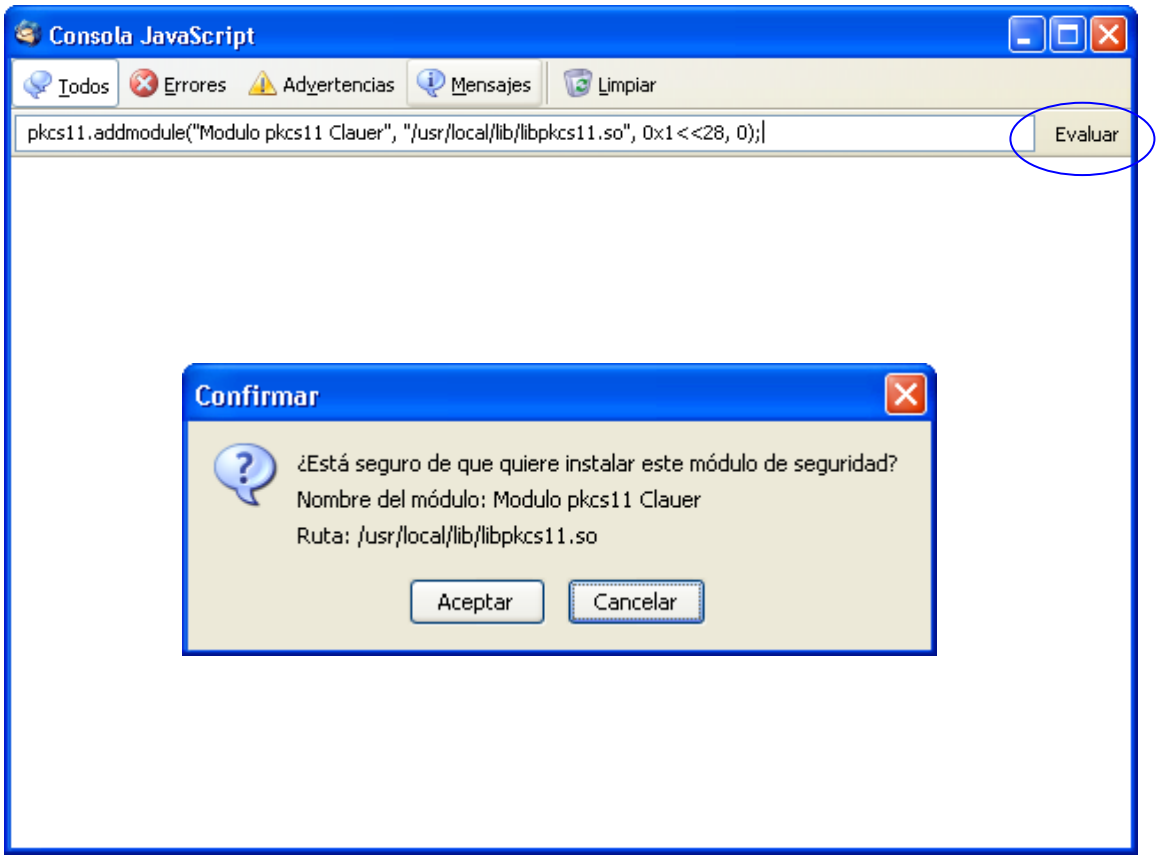
Un cop realitzada la instal·lació estàndard per *Firefox* al punt 1, caldrà fer el següent per acabar de configurar la comunicació entre *Thunderbird* i el clauer idCAT*:*

1. Obrir el client de correu *Thunderbird* i anar al menu *"Herramientas-> Consola Javascript"*



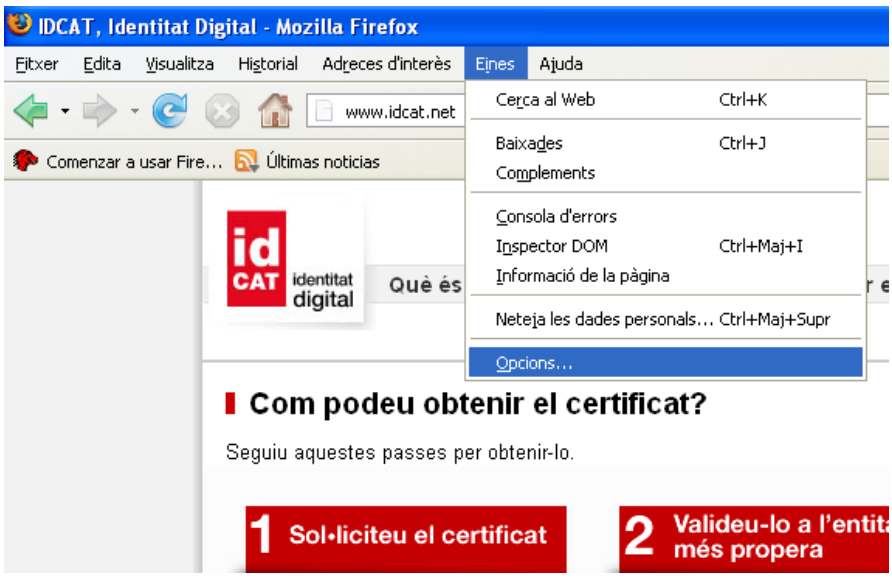
2. Copiar la següent línia:
   pkcs11.addmodule("Modulo pkcs11 Clauer", "/usr/local/lib/libpkcs11.so", 0x1<<28, 0);

   al camp de text i prémer el botó *"Evaluar":*

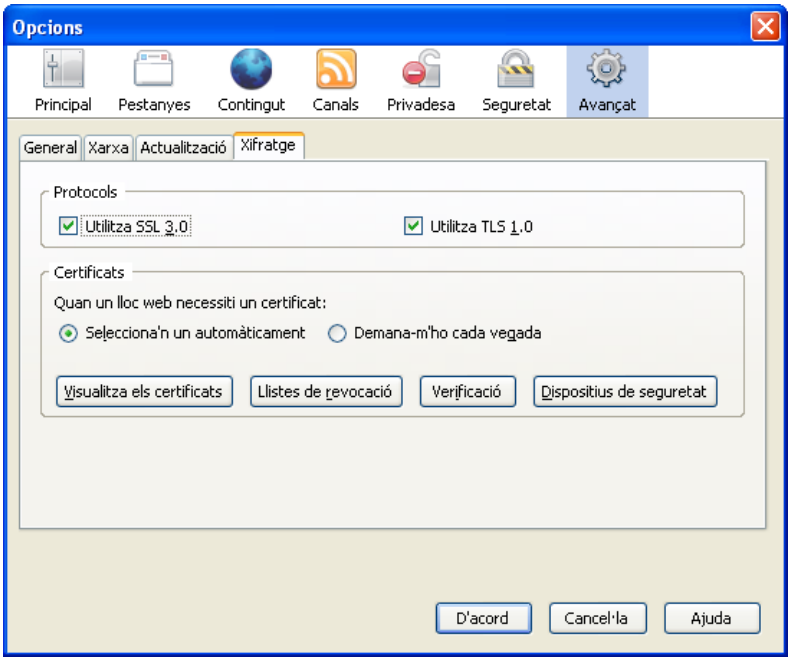


Annex B: Com exportar un certificat digital, instal·lat a Firefox, a un fitxer en format P12

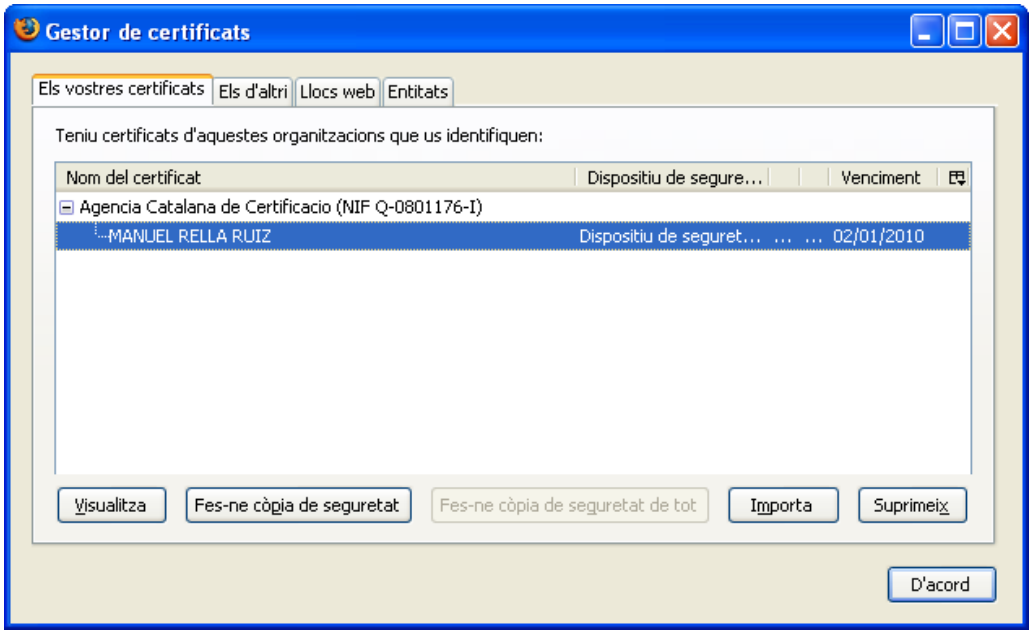
1. Obriu el navegador Firefox i cliqueu l'opció de menú *Eines* → *Opcions:*



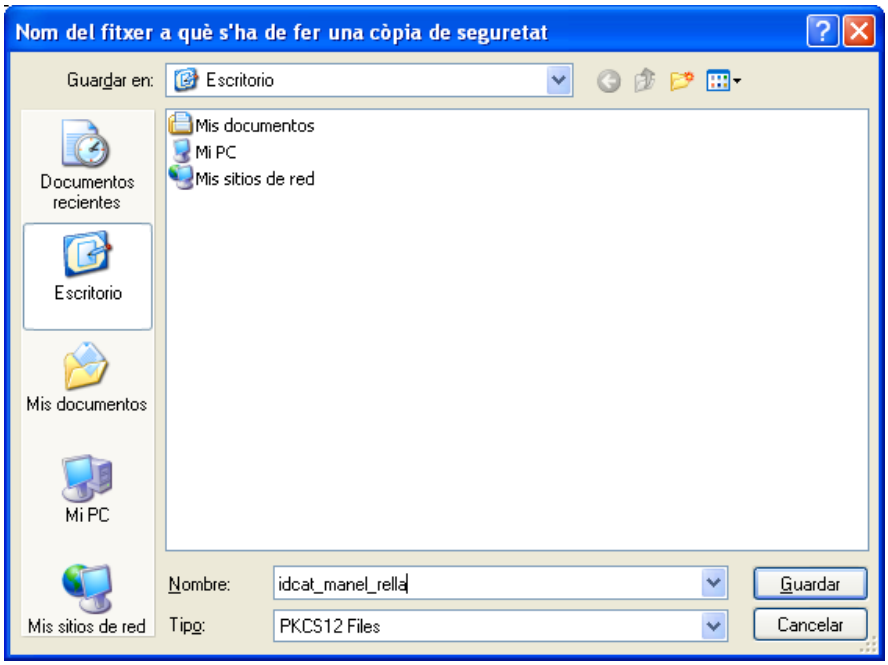
2. Cliqueu sobre la icona *d'Avançat* i sobre la pestanya de *Xifratge.* Després cliqueu el botó *Visualitza els certificats.*



3. Cliqueu sobre el certificat que vulgueu exportar i després premeu el botó *Fes-ne còpia de seguretat.*



4. Caldrà indicar el nom del fitxer i la ubicació al disc dur on es vol guardar el fitxer P12.



5. Si estava protegit per password, ara l'heu introduir:

6. Indiqueu la paraula de pas per tal de protegir el fitxer exportat i premeu el botó *D'acord*:

7. El fitxer ja està exportat:

Annex C: Com importar certificats dins el clauer des d'un fitxer P12 o PFX. Com llistar-los i esborrar-los

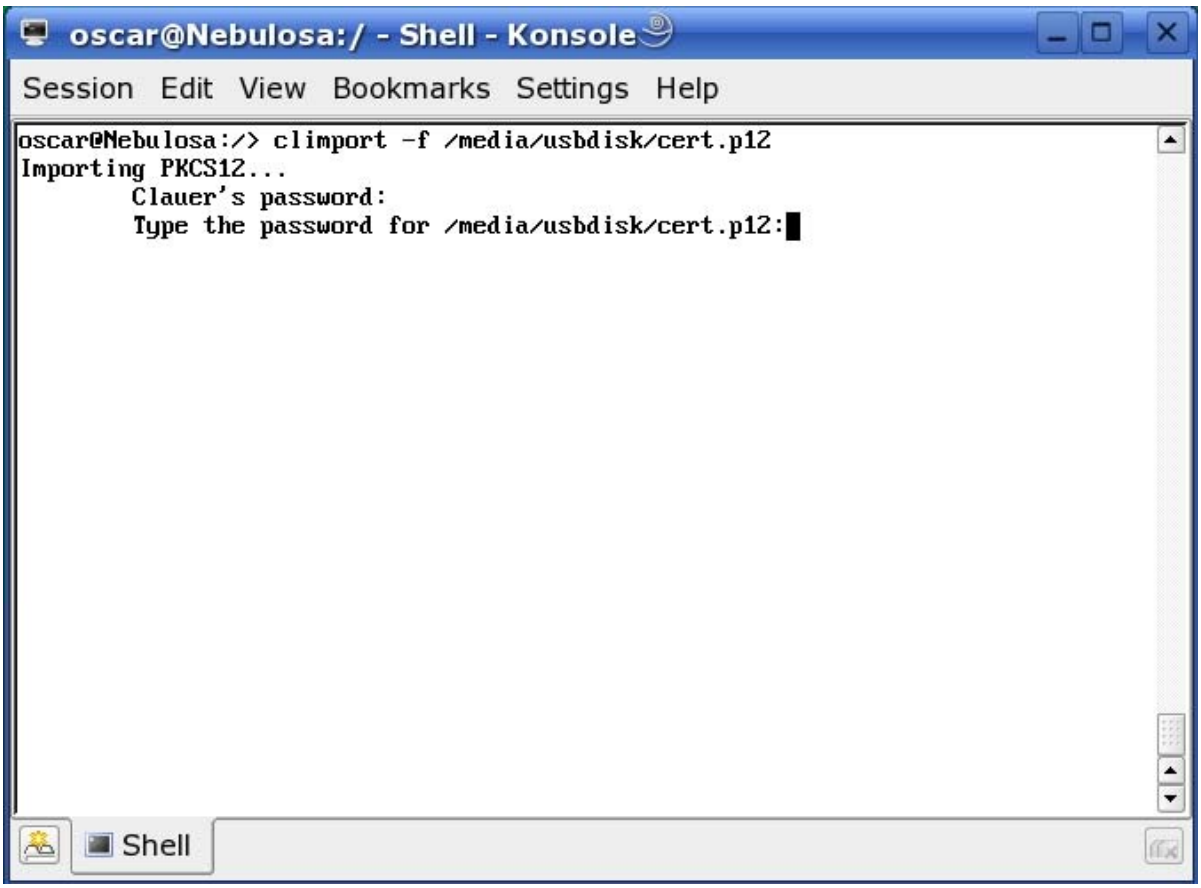
Importar certificats dins del clauer

1. Per tal d'importar un certificat dins del clauer a partir d'un fitxer .P12 o .PFX cal fer la crida:

   >climport –f cert.p12

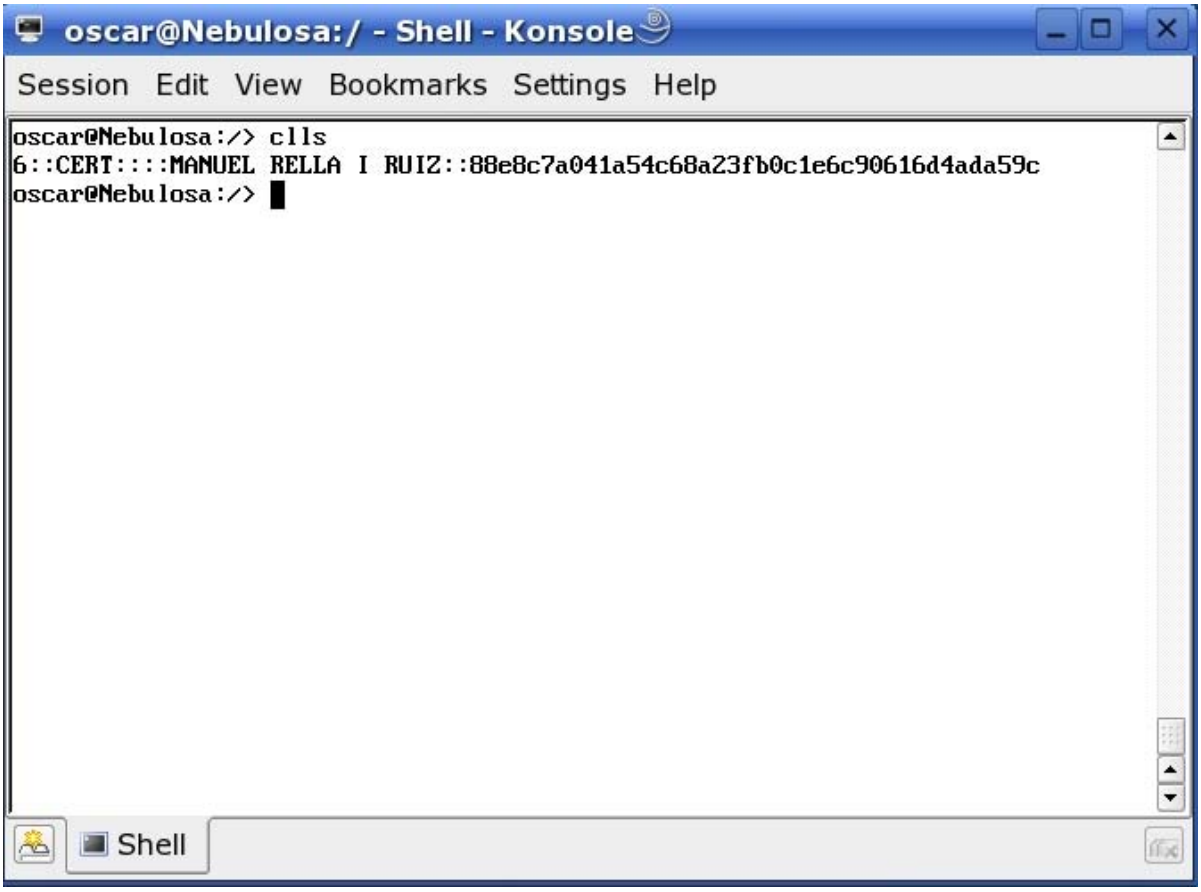
   On cert.p12 es la ruta al fitxer .P12 que conté el certificat i la clau privada.

   Un cop fet això us demanarà primer el password del clauer i després el password del fitxer .P12



Llistar els certificats dins del clauer

1. Per obtenir un llistat dels certificats instal·lats al clauer caldrà executar la comanda: *clls*



Esborrar certificats dins del clauer

1. Primer caldrà fer un llistat dels certificats amb la comanda: *clls*
2. Amb el número que apareix a la primera columna del llistat feu la invocació a la comanda: *cldel –c <número_del_llistat>*