Agència Catalana de Certificació

MANUAL D'ÚS DEL CLAUER IDCAT

Per MAC OS basats en processadors Intel amb Firefox

006_20060220

Versió: v1.0
Data: 25/09/2007

Índex

Guia d'instal·lació del programari del clauer idCAT

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

Es pot fer servir tant amb els clauers idCAT distribuïts per CATCert com amb qualsevol altra memòria USB.

L'última versió del programari sempre estarà disponible a www.idcat.net/clauer.

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

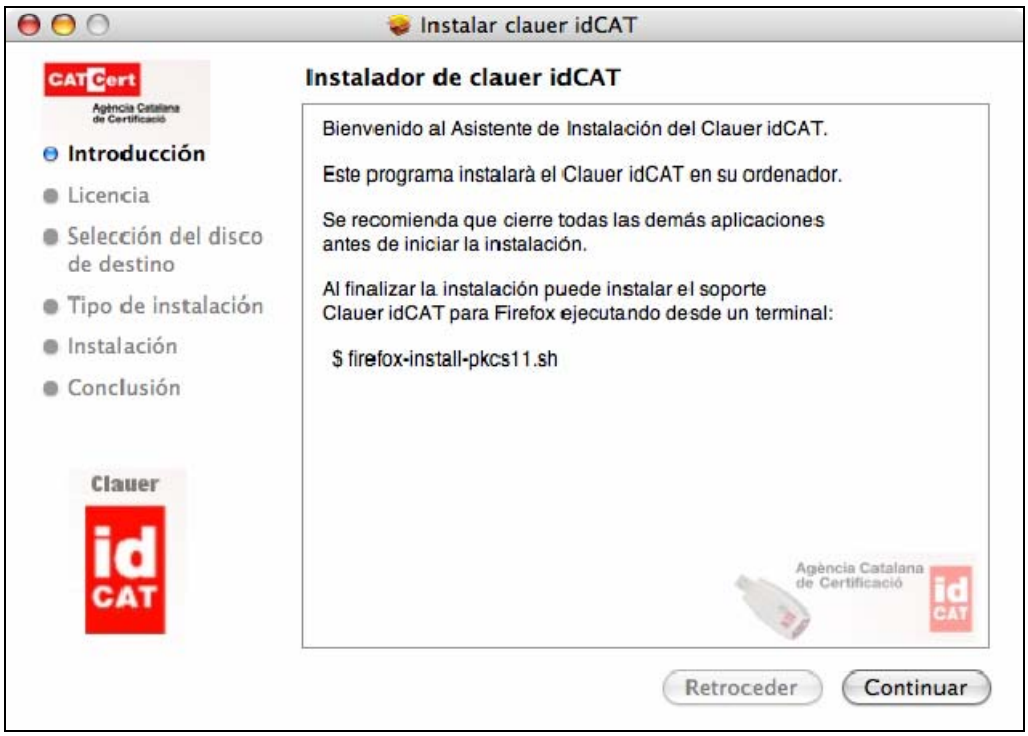
[1] Aquest programari ha estat desenvolupat per la Universitat Jaume I dins del projecte clauer UJI, dintre d'aquesta última web podeu trobar més informació referent al programari del clauer.

PAS 1 - Instal·lació del programari del clauer idCAT

Aquest procés només cal fer-lo una vegada per a cada ordinador on vulgueu fer servir el clauer idCAT:

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

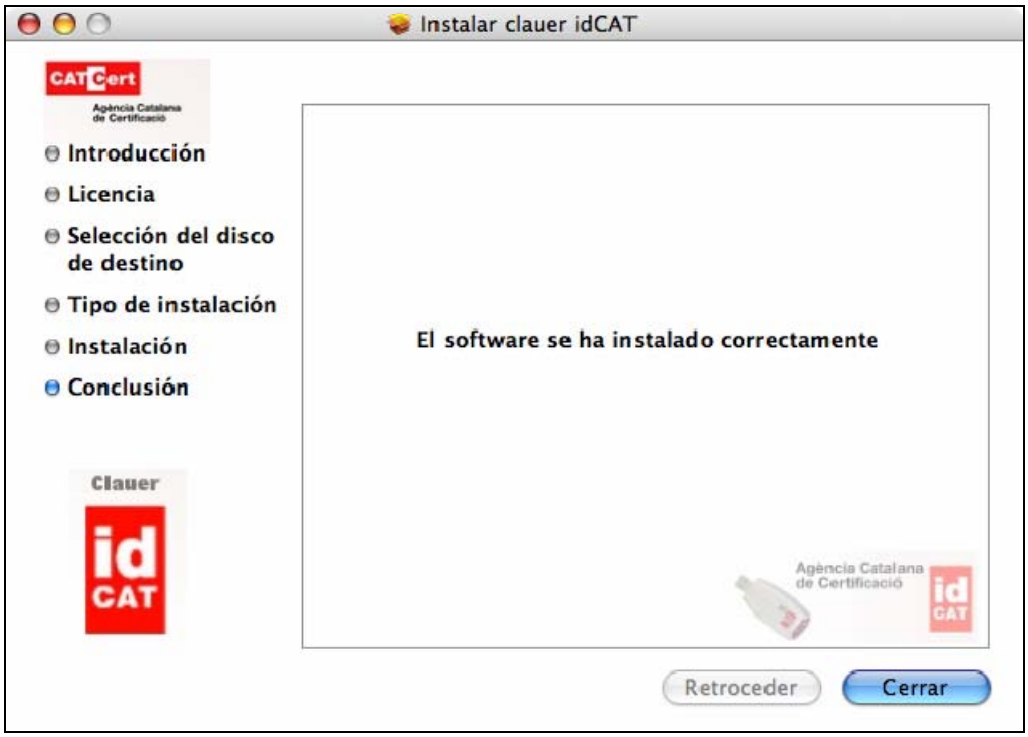
2. Aneu al directori: */Programari clauer/mac os* dins de la memòria USB i executeu el fitxer *.dmg.* També podeu descarregar la última versió d'aquest programari a la web de l'idCAT, www.idcat.net/clauer:



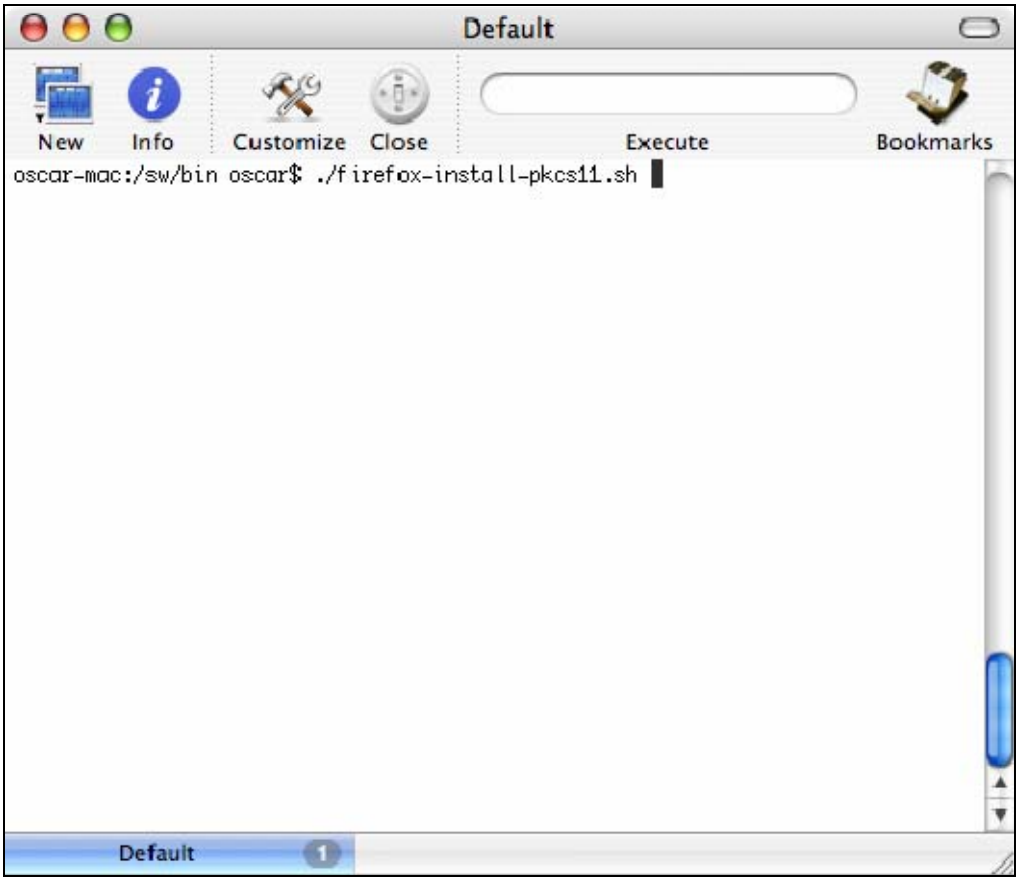
3. Seguiu les instruccions de la pantalla:

4. Accepteu la llicencia:

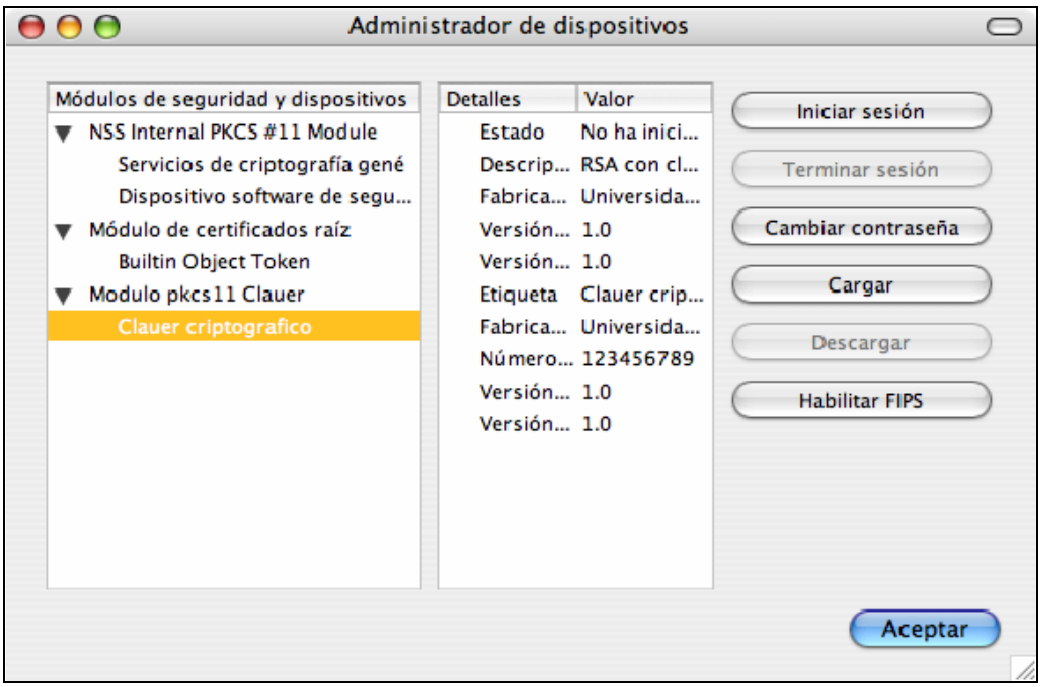
5. Cliqueu al botó Instal·lar:

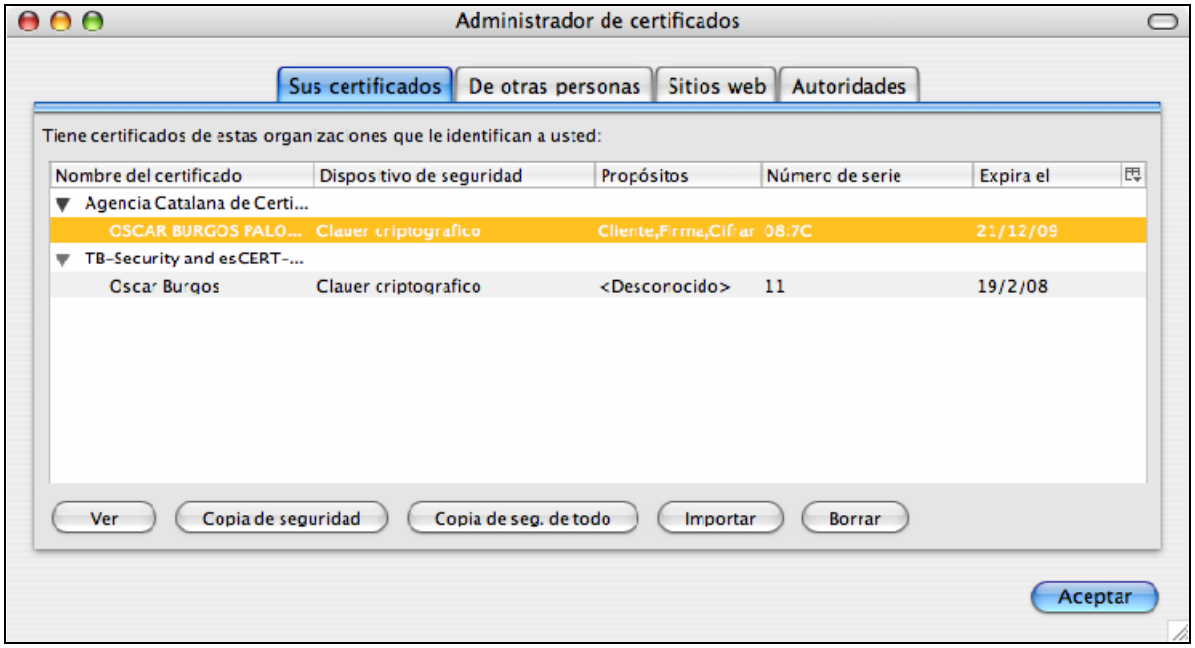


6. Per tal d'instal·lar el mòdul criptogràfic al navegador firefox. Obriu una consola, aneu al directori /sw/bin i executeu l'script de la imatge següent:



7. Anant a l'administrador de dispositius criptogràfics de Firefox veureu que teniu un nou mòdul instal·lat i a l'administrador de certificats us apareixerà el vostre certificat.



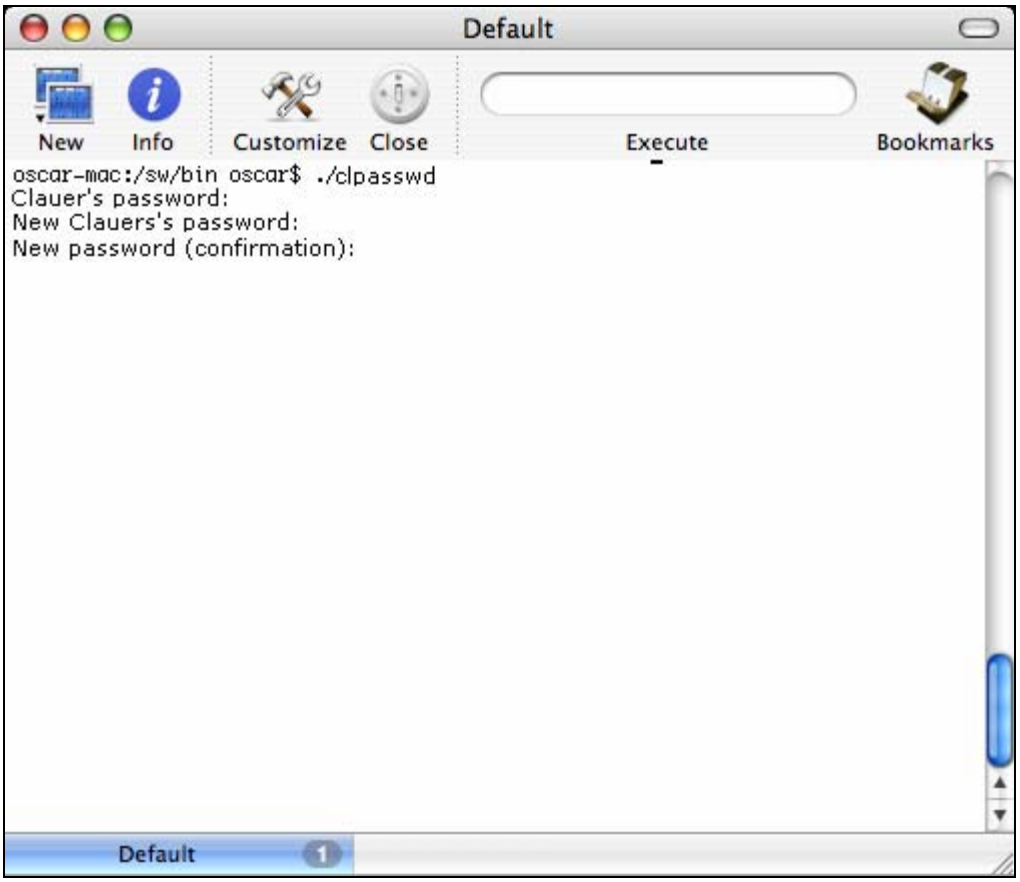


044 20060904

PAS 2 - Canvi del PIN clauer idCAT

El canvi de PIN és **obligatori** 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 (que **trobareu impresa al full que us han donat a l'entitat de registre**[2]), 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. Recordeu que aquesta password ha de complir les següents característiques:

- Ha de tenir un mínim de 8 caràcters
- 3 dels quals han de ser lletres i 3 números

[2] 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

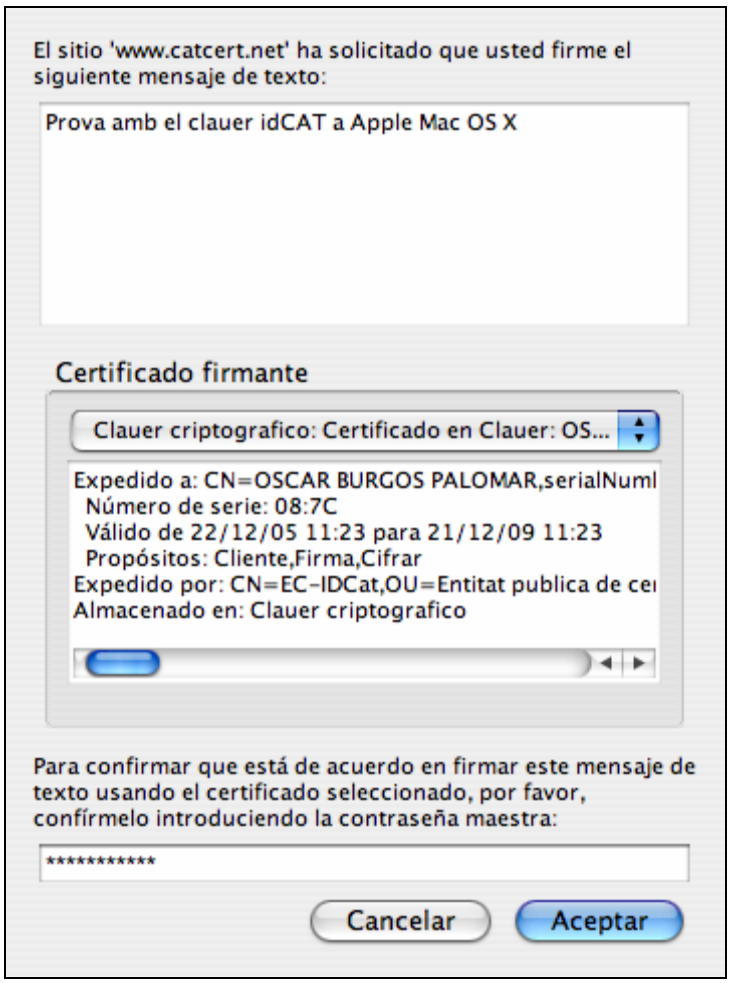
1. Si heu seguit els passos anteriors ja disposeu d'un clauer idCAT 100% operatiu i llest per fer-se servir.

2. Si voleu comprovar el seu bon funcionament, extraieu el clauer idCAT del port USB i torneu a introduir-lo. Accediu a la següent web amb un navegador internet explorer:

   http://www.catcert.net/web/cat/6_3_prova.jsp

   Introduïu un text qualsevol i cliqueu el botó *Generar signatura.*

3. Seleccioneu el vostre certificat idCAT:



4. Finalment apareixerà la signatura electrònica del text a la finestra de sota

Recordeu que podeu trobar tots els usos del certificat idCAT al web www.catcert.net/usos

Altres possibilitats

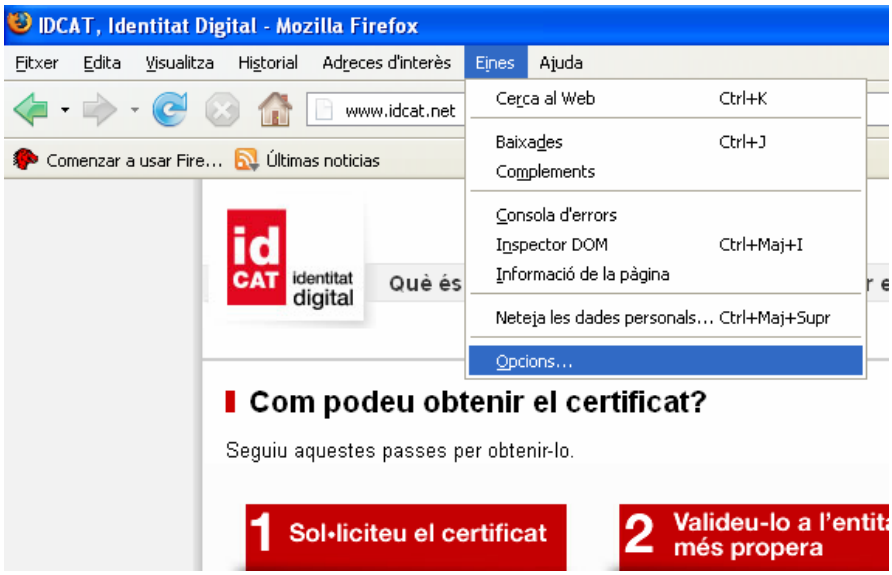
- Es poden importar més certificats a dins del clauer siguin o no emesos per l'Agència Catalana de Certificació (veure annexos)

Tinc una pregunta o comentari

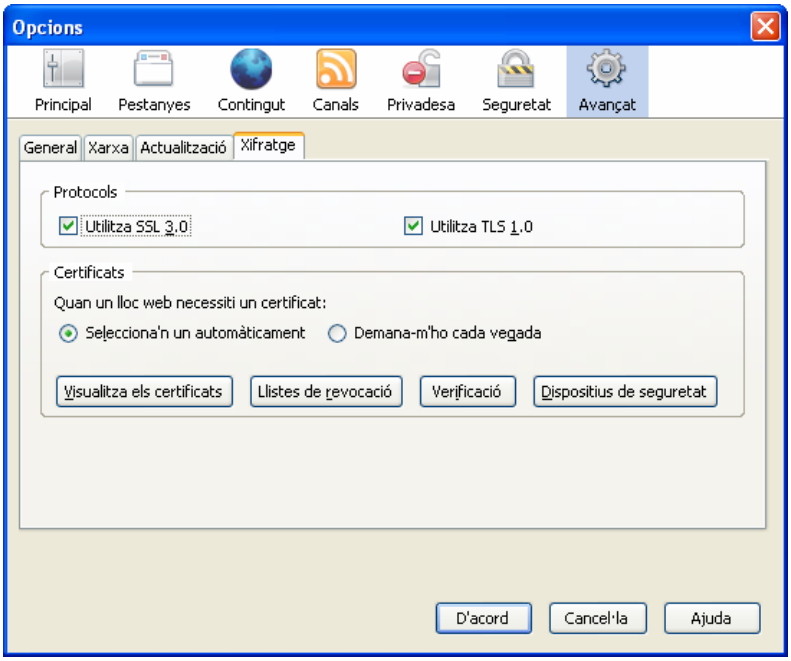
Qualsevol dubte o comentari podrà ser resolt via telefònica trucant al servei d'atenció del ciutadà de l'Agència Catalana de Certificació: **902 901 080** o enviant un correu a **info@catcert.net**

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

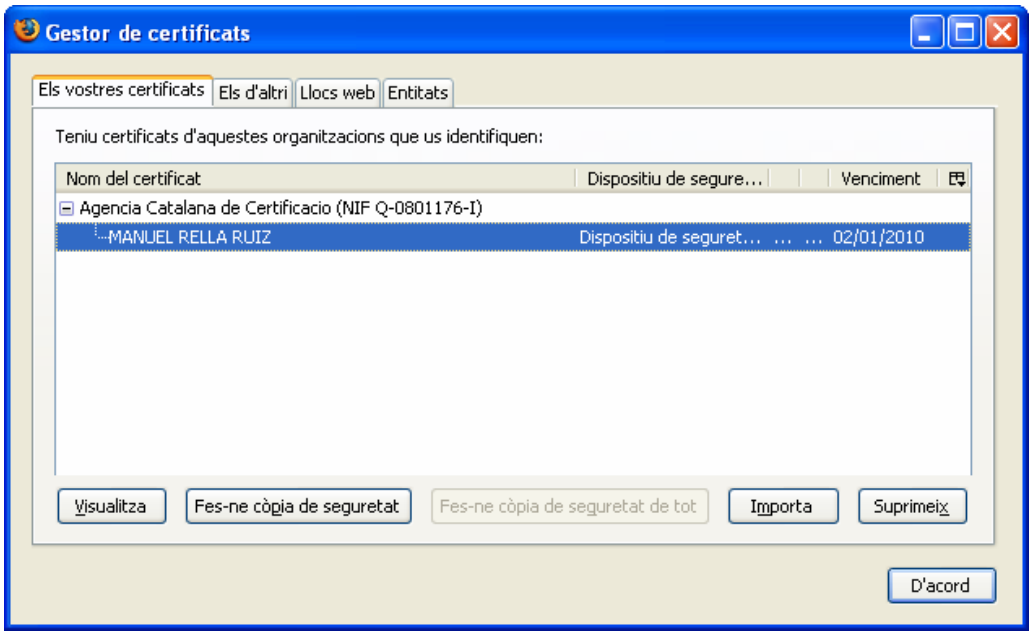
1. Obriu el navegador Firefox i cliqueu l'opció de menú *Eines* → *Opcions:*



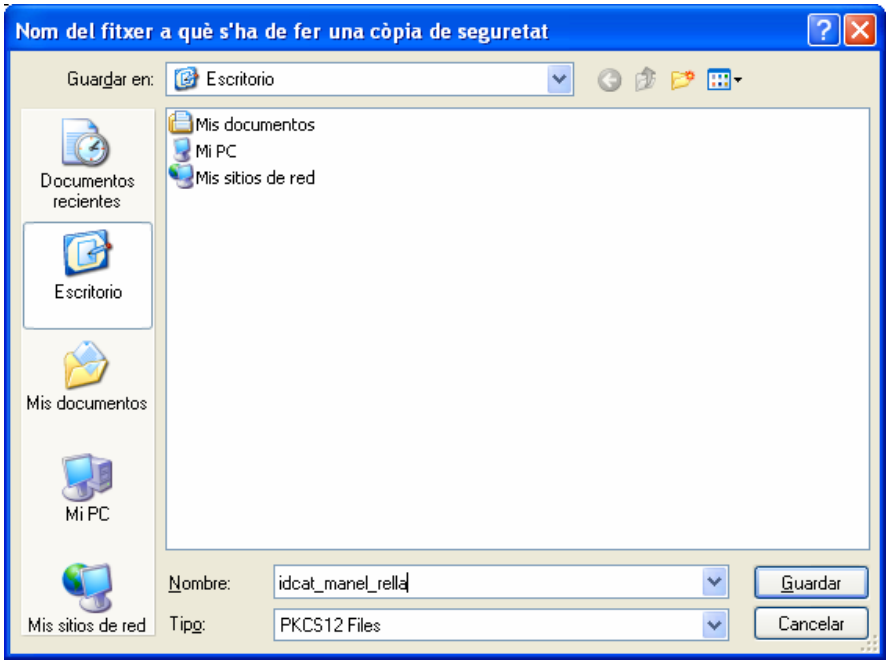
2. Cliqueu sobre la icona *d'Avançat* i sobre la pestanya de *Xifratge.* Després cliqueu el botó *Visualitza els certificats.*



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

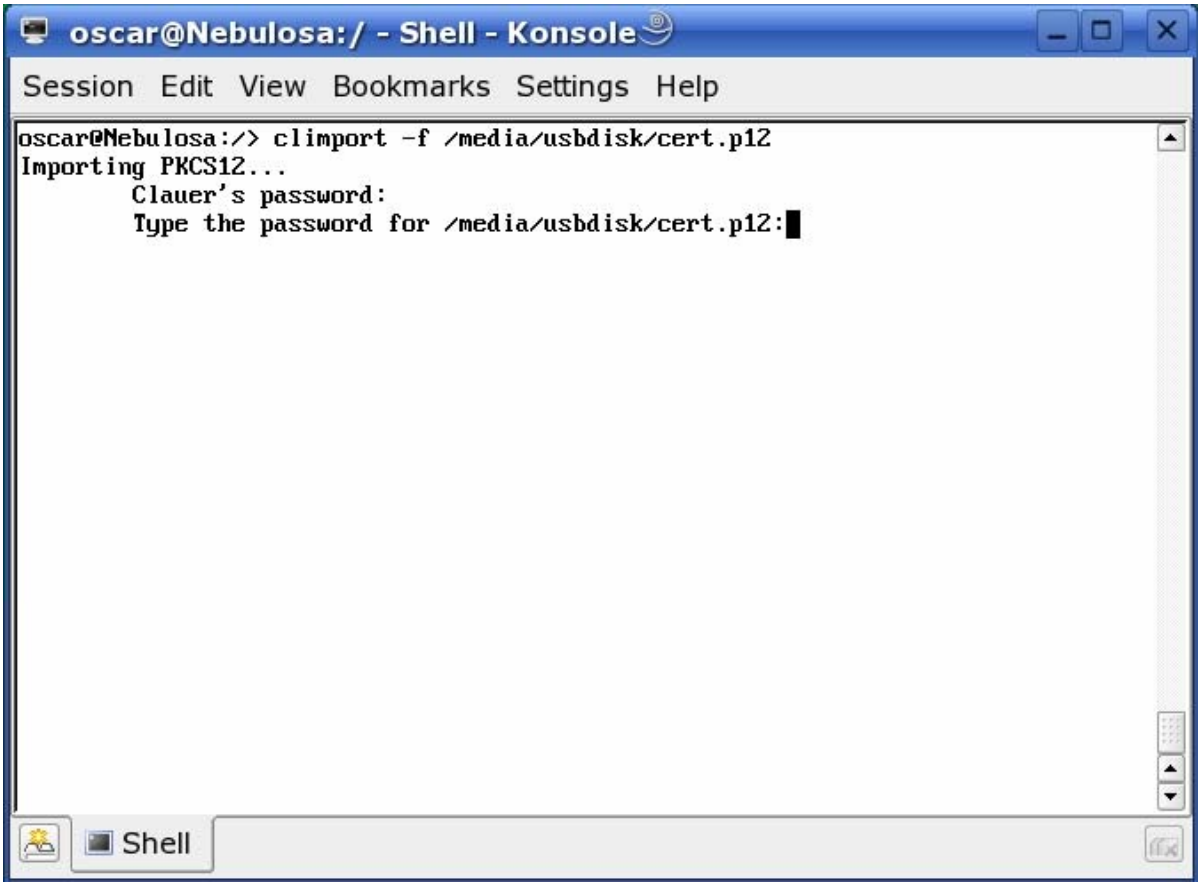
Importar certificats dins del clauer

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

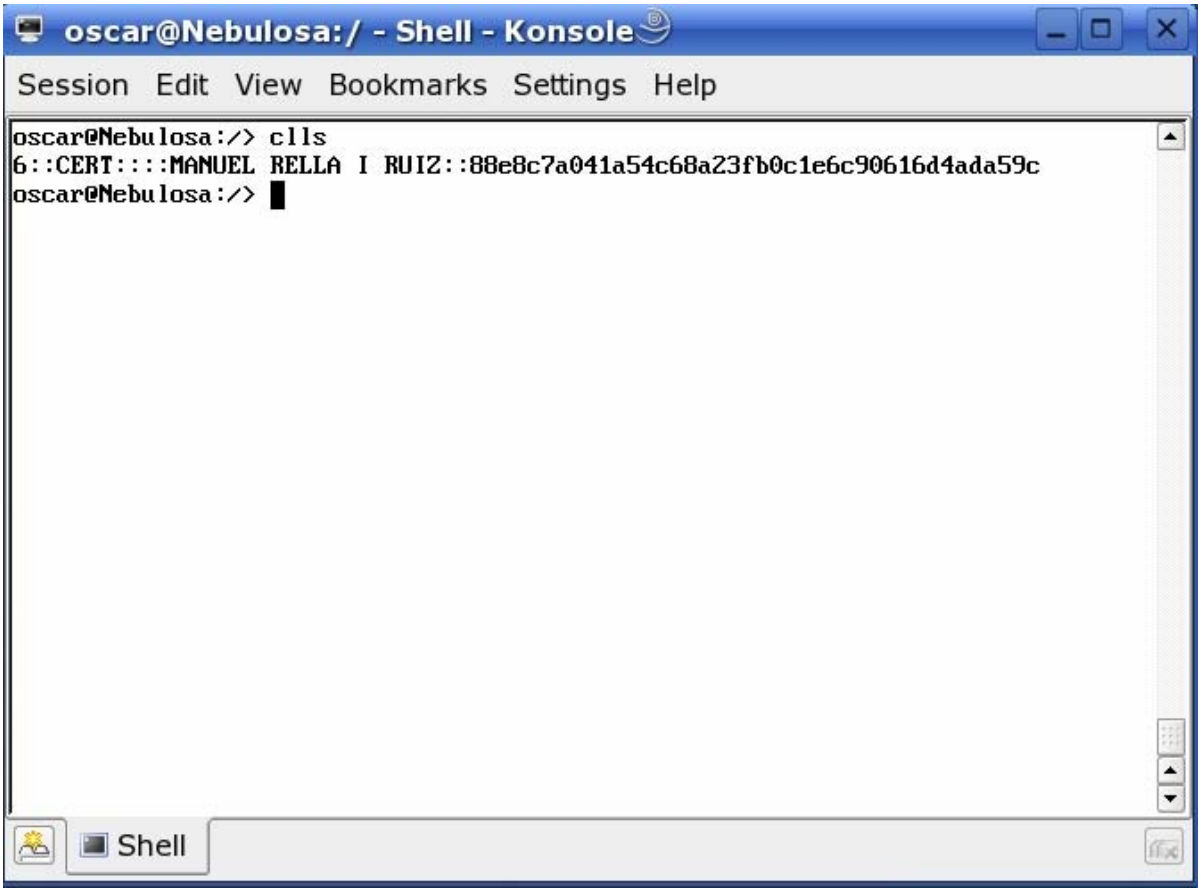
   On cert.p12 es la ruta al fitxer .P12 que conté el certificat i la clau privada.

   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>*