

MANUAL D'ÚS DEL CLAUER IDCAT

Per MAC OS basats en processadors Intel amb
Firefox



Versió: v1.0
Data: 25/09/2007

Índex

MANUAL D'ÚS DEL CLAUER IDCAT.....	1
Per MAC OS basats en processadors Intel amb Firefox.....	1
Índex.....	2
Guia d'instal·lació del programari del clauer idCAT.....	3
PAS 1 - Instal·lació del programari del clauer idCAT.....	4
PAS 2 - Canvi del PIN clauer idCAT.....	10
PAS 3 - Prova del clauer.....	11
Tinc una pregunta o comentari.....	14
Annex A: Com exportar un certificat digital, instal·lat a Firefox, a un fitxer en format P12...	15
Annex B: Com importar certificats dins el clauer des d'un fitxer P12 o PFX. Com llistar-los i esborrar-los	19

Guia d'instal·lació del programari del clauer idCAT

La instal·lació d'aquest programari¹ 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.



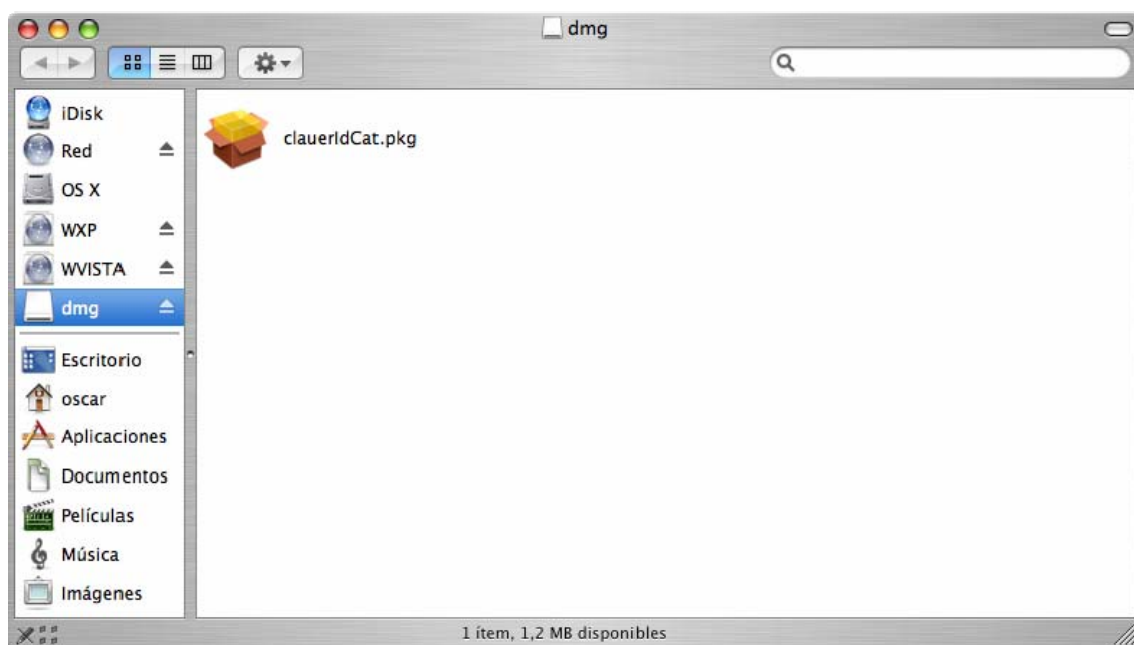
A continuació es detallen els passos que cal seguir per instal·lar correctament el clauer idCAT:

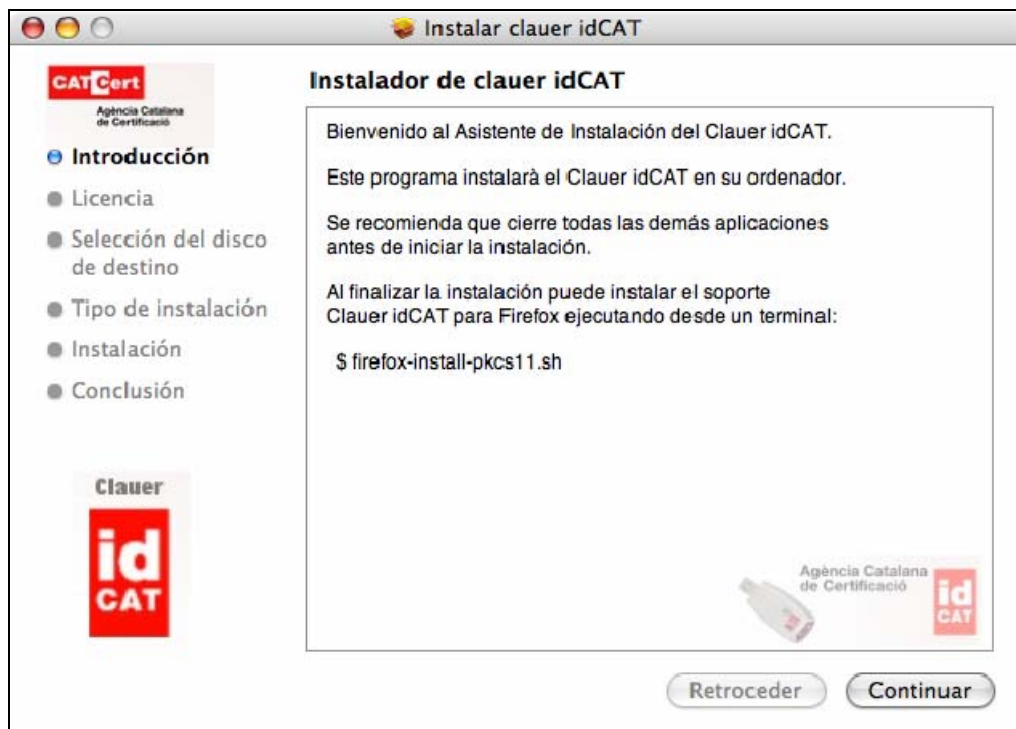
¹ Aquest programari ha estat desenvolupat per la [Universitat Jaume I](#) dins del projecte [clauer UJI](#), dintre d'aquesta última web podeu trobar més informació referent al programari del clauer.

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:





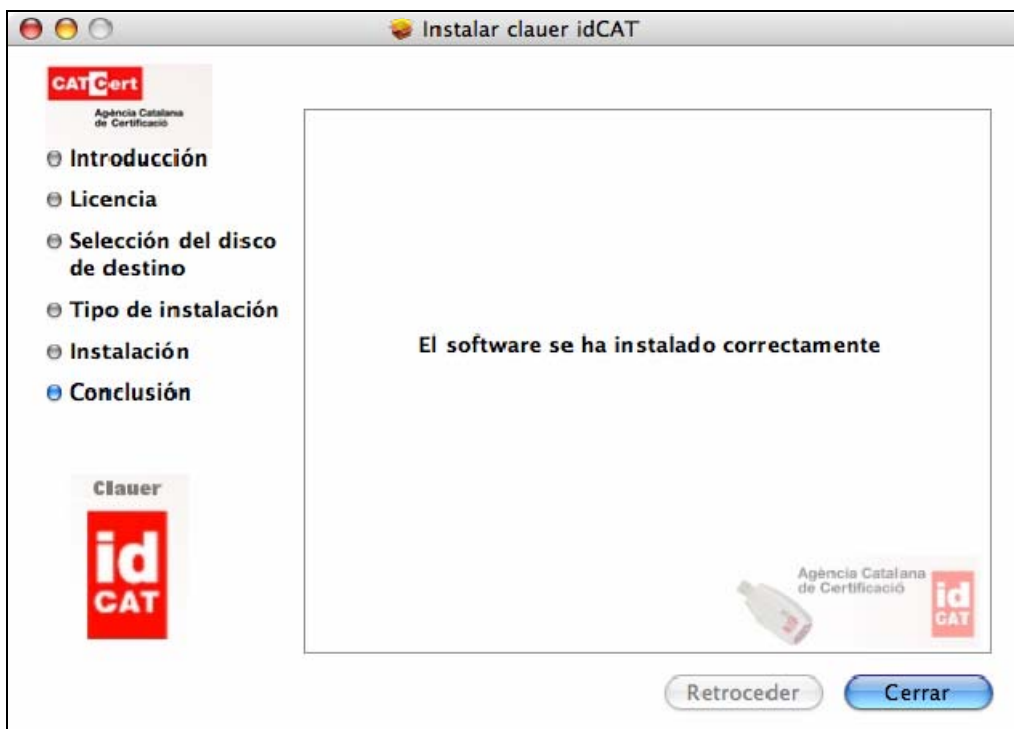
3. Seguiu les instruccions de la pantalla:



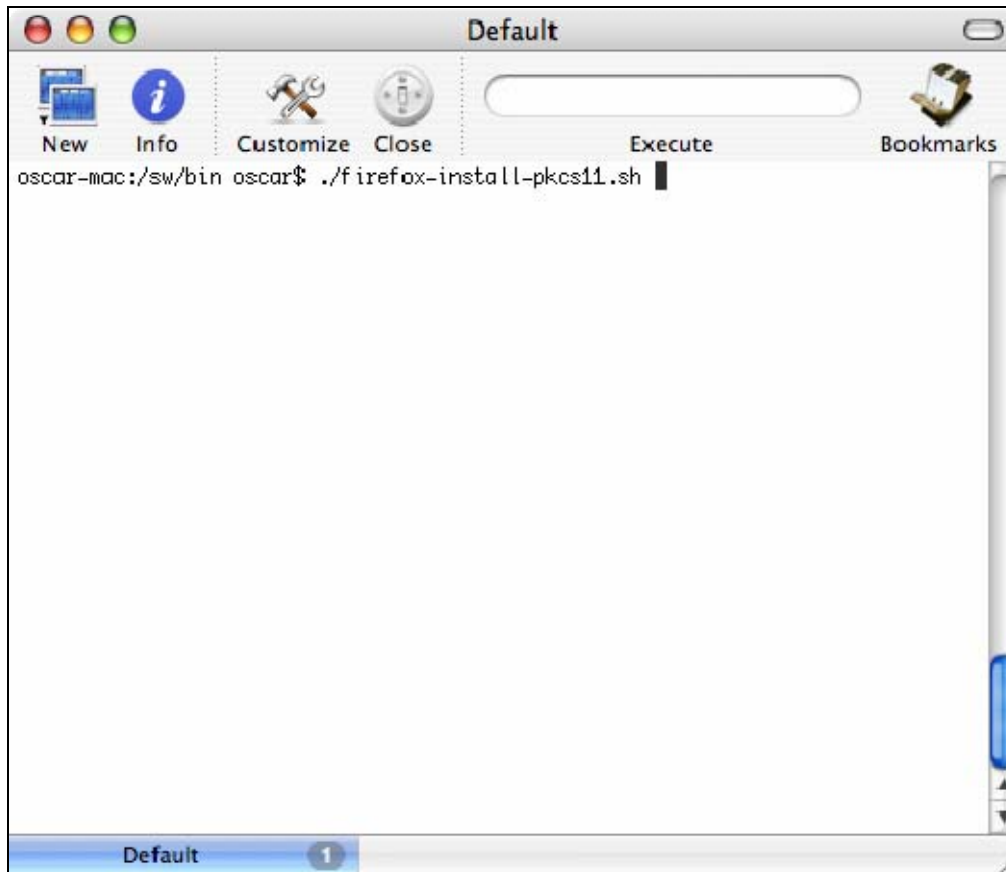
4. Acepteu la llicència:



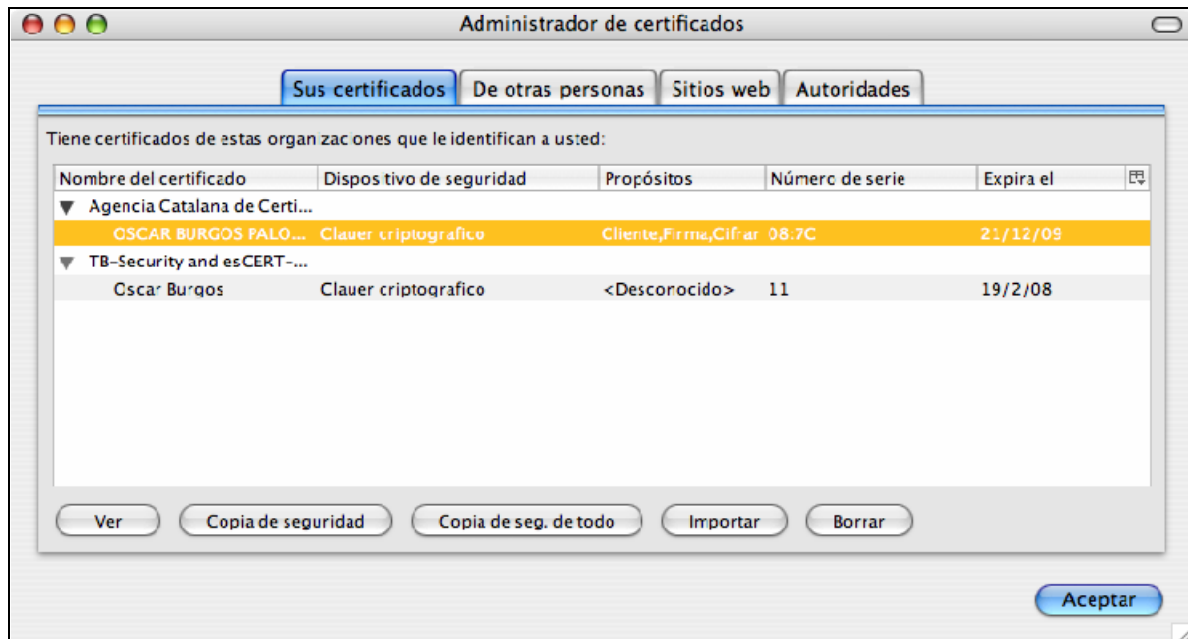
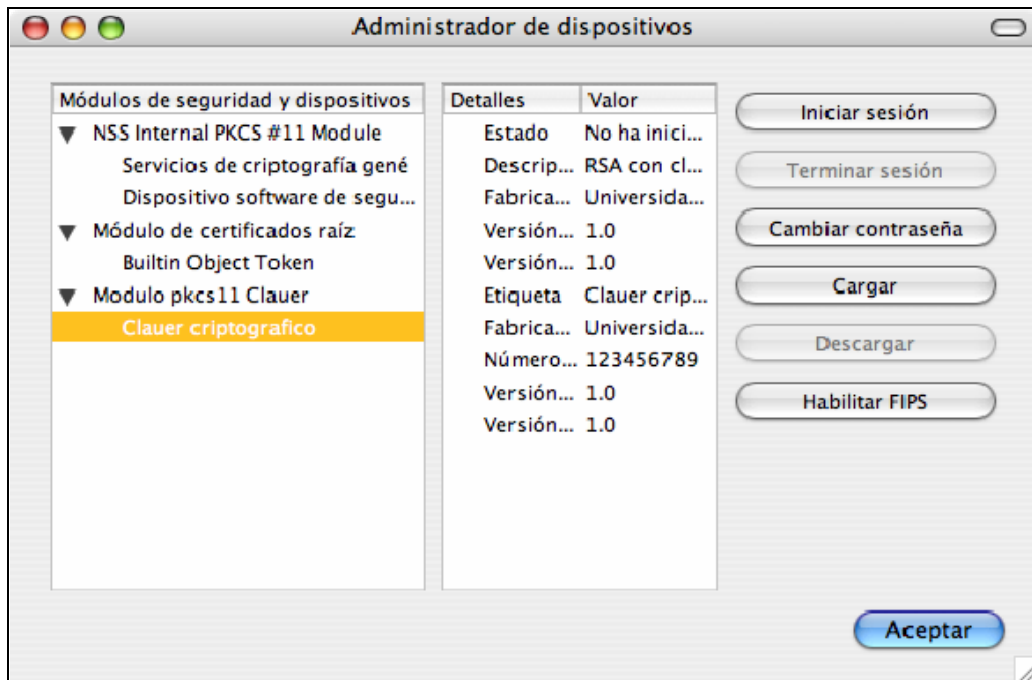
5. Cliqueu al botó Instal·lar:



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:



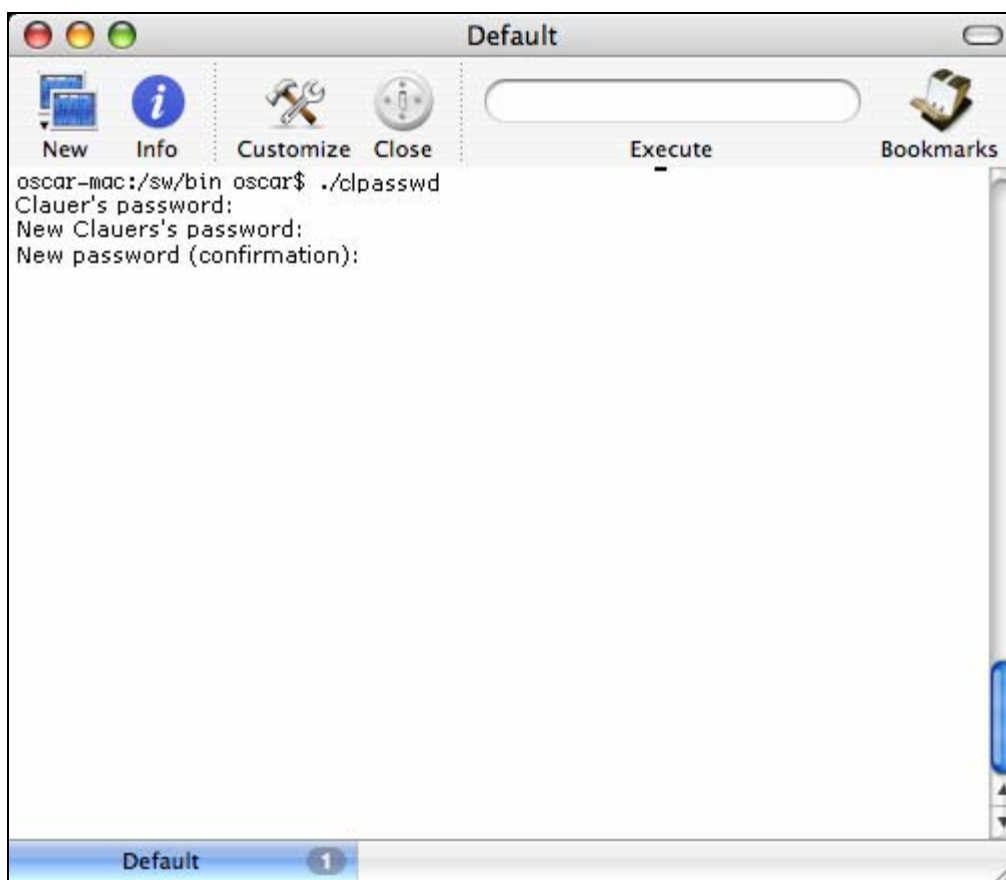
7. Anant a l'administrador de dispositius criptogràfics de Firefox veureu que teniu un nou mòdul instal·lat i a l'administrador de certificats us apareixerà el vostre certificat.



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*.



The screenshot shows the CATCert website interface. At the top, there is a red navigation bar with the CATCert logo and the text 'Agència Catalana de Certificació'. To the right of the logo, the words 'CERTIFICATS', 'QUÈ OFERIM', and 'ADMINISTRACIÓ' are visible. Below the navigation bar, there is a breadcrumb trail: 'Inici / Documentació i utilitats / Prova de signatura de text'. The main heading is 'Prova de signatura de text'. Below this, a paragraph explains: 'Des d'aquest apartat es pot realitzar una prova amb el certificat digital, signant un petit text.' Underneath, the heading 'Prova de signatura de text' is repeated. There is a label 'Text a signar:' followed by a text input field containing the word 'Prova'. Below the input field are two red buttons: 'Generar signatura' and 'Esborrar'. At the bottom, there is a label 'Signatura:' followed by an empty text input field.

3. Seleccioneu el vostre certificat idCAT:

El sitio 'www.catcert.net' ha solicitado que usted firme el siguiente mensaje de texto:

Prova amb el clauer idCAT a Apple Mac OS X

Certificado firmante

Clauer criptografico: Certificado en Clauer: OS...

Expedido a: CN=OSCAR BURGOS PALOMAR,serialNum1
Número de serie: 08:7C
Válido de 22/12/05 11:23 para 21/12/09 11:23
Propósitos: Cliente,Firma,Cifrar
Expedido por: CN=EC-IDCat,OU=Entitat publica de cei
Almacenado en: Clauer criptografico

Para confirmar que está de acuerdo en firmar este mensaje de texto usando el certificado seleccionado, por favor, confírmelo introduciendo la contraseña maestra:

Cancelar Aceptar

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

CATCert Agència Catalana de Certificació CERTIFICATS QUÈ OFERIM ADMINISTRACIÓ

[Inici](#) / [Suport](#) / Prova de signatura de text

Prova de signatura de text

Des d'aquest apartat es pot realitzar una prova amb el certificat digital, signant un petit text.

Prova de signatura de text

Text a signar:

Prova amb el clauer idCAT a Apple Mac OS X

Generar signatura **Esborrar**

Signatura:

MIISUAYJKoZIHvcNAQcCoIISQTCCEj0CAQExCzAJBgUrDgMCGgUAMAsDQEHAaCCD9gwgggggMIHCKADAgECAGII fDANBgkqhkiG9w0BAQUFADCBgNVBAYTAkVTMTswOQYDVQQKEzJBZ2V2Y21hIENhdGFsYW5hIGRlIENYWNpbyAoTk1GIFEtMDgwMTE3Ni1JKTE0MDIGA1UEBxMrUGFzc2F0Z2UQ29uY2VwY21vIDExIDA4MDA4IEJhcmN1bG9uYTEuMCwGA1UECzMlU2V

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

Altres possibilitats

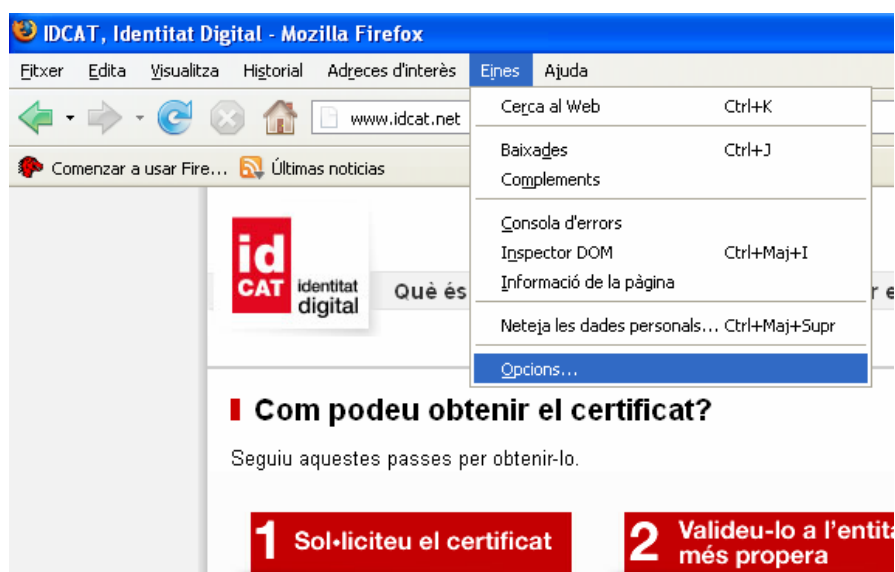
- Es poden importar més certificats a dins del clauer siguin o no emesos per l'Agència Catalana de Certificació (veure annexos)

Tinc una pregunta o comentari

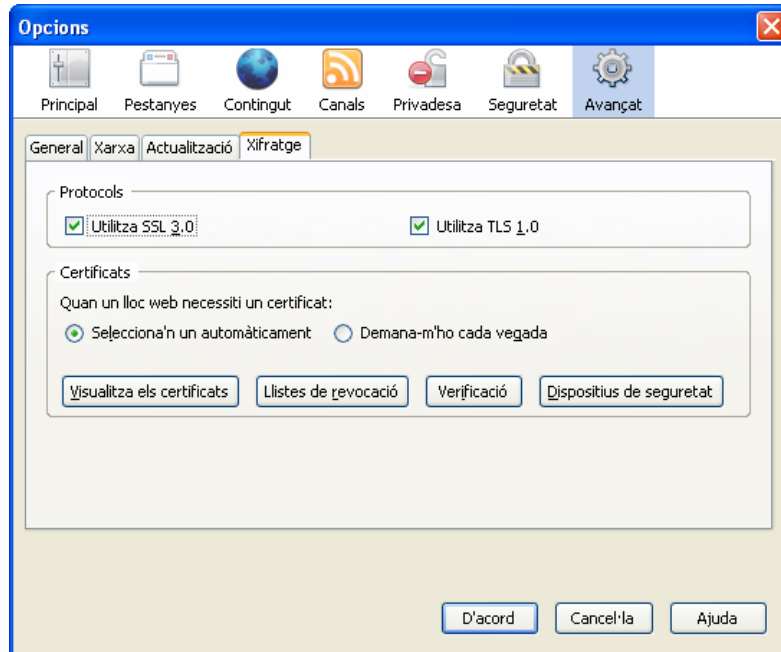
Qualsevol dubte o comentari podrà ser resolt via telefònica trucant al servei d'atenció del ciutadà de l'Agència Catalana de Certificació: **902 901 080** o enviant un correu a **info@catcert.net**

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

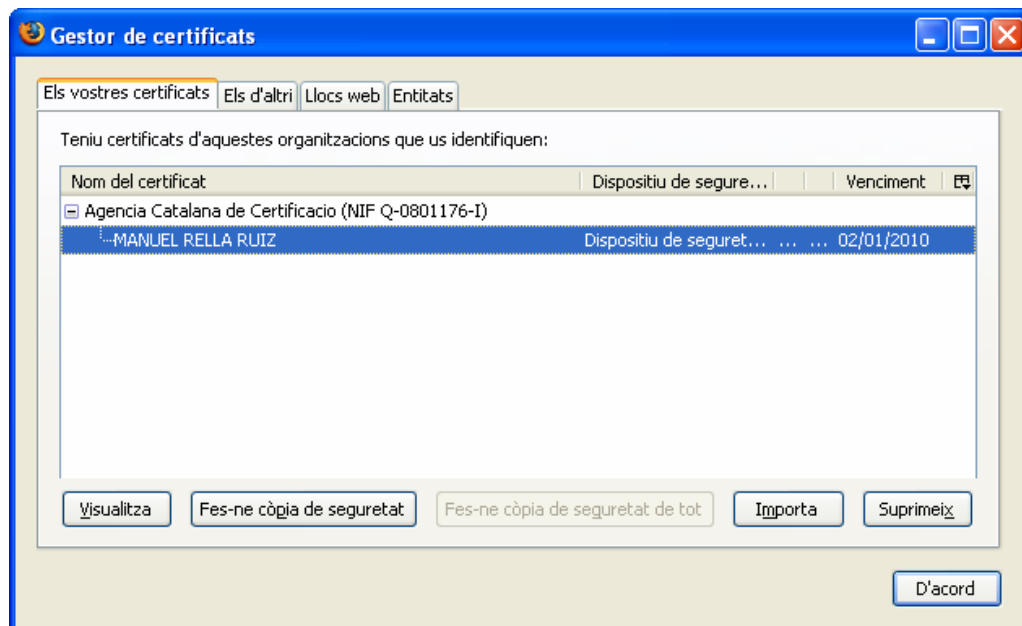
1. Obriu el navegador Firefox i cliqueu l'opció de menú *Eines* → *Opcions*:



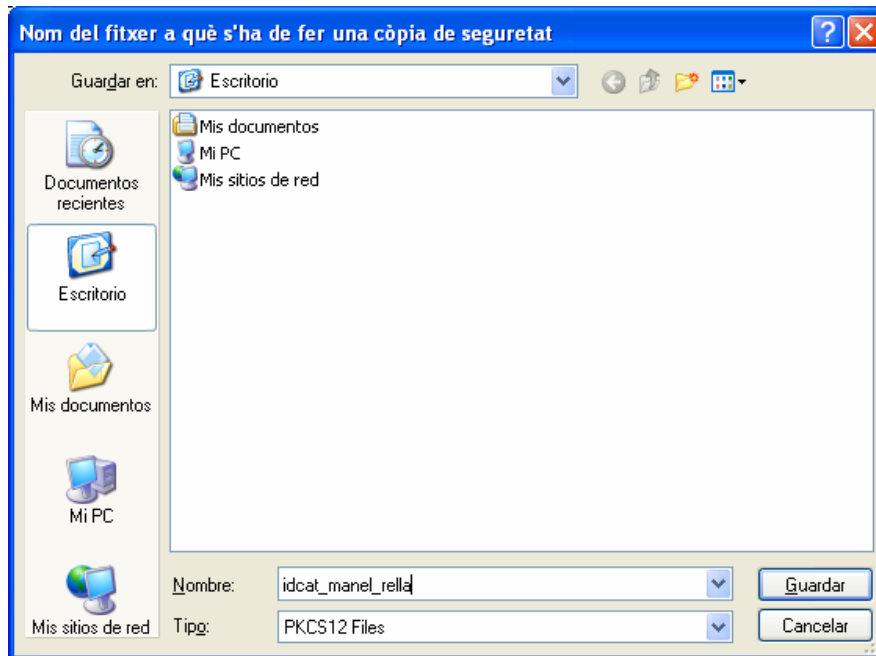
2. Cliqueu sobre la icona d'Avançat i sobre la pestanya de Xifratge. Després cliqueu el botó Visualitza els certificats.



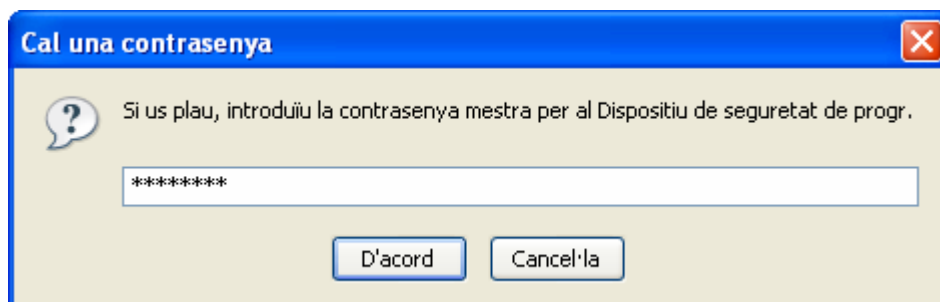
3. Cliqueu sobre el certificat que vulgueu exportar i després premeu el botó Fes-ne còpia de seguretat.



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*:

Trieu una contrasenya per a la còpia de seguretat del certificat

La contrasenya per a la còpia de seguretat del certificat que definiu ací protegeix el fitxer de còpia de seguretat que ara creareu. Heu de definir-la per a seguir amb la còpia de seguretat.

Contrasenya de la còpia de seguretat del certificat:


Contrasenya de la còpia de seguretat del certificat (un altre cop):

Important: si oblideu la contrasenya de la còpia de seguretat del certificat no podreu recuperar-la més endavant. Si us plau, guardeu-la en un lloc segur.

Avaluador de qualitat de la contrasenya

7. El fitxer ja està exportat:

Avis

 Els vostres certificats de seguretat i claus privades s'han desat amb èxit.

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

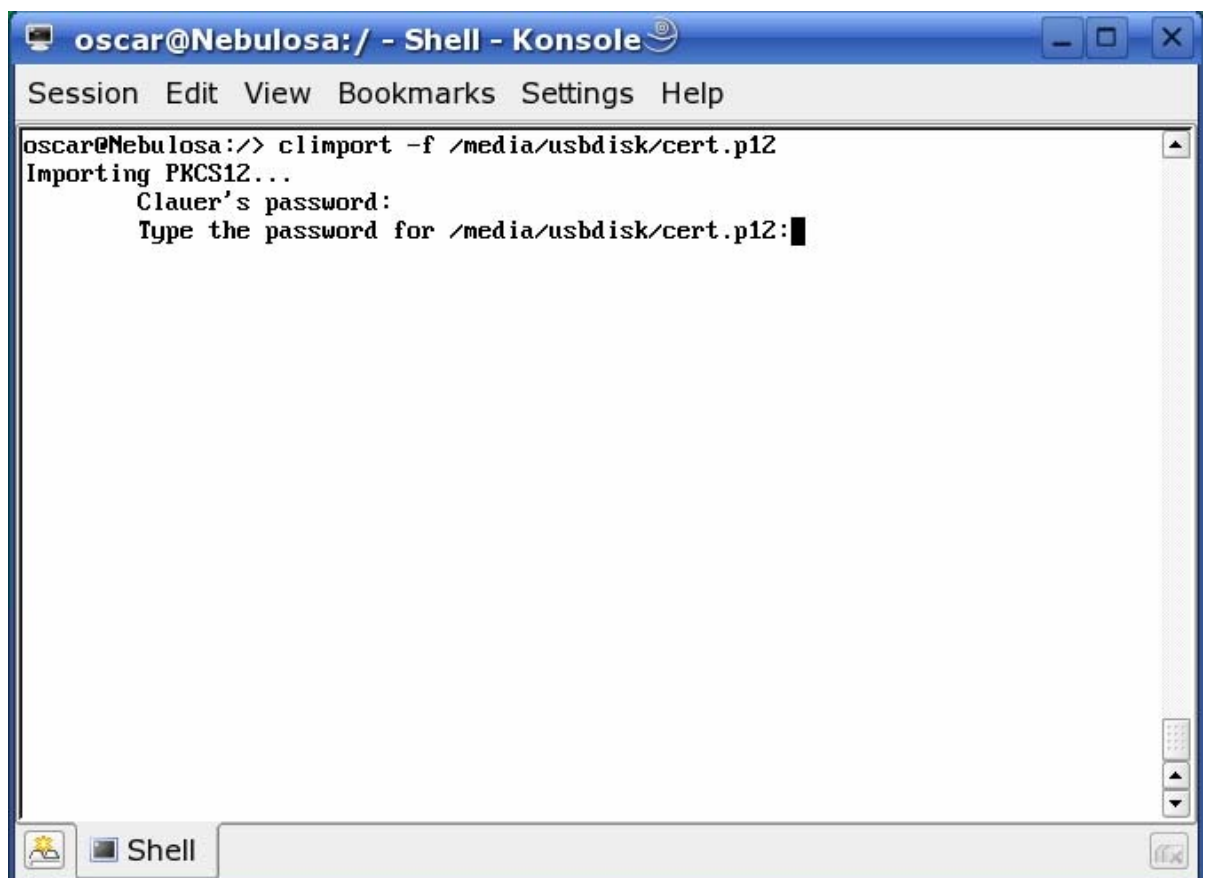
Importar certificats dins del clauer

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.

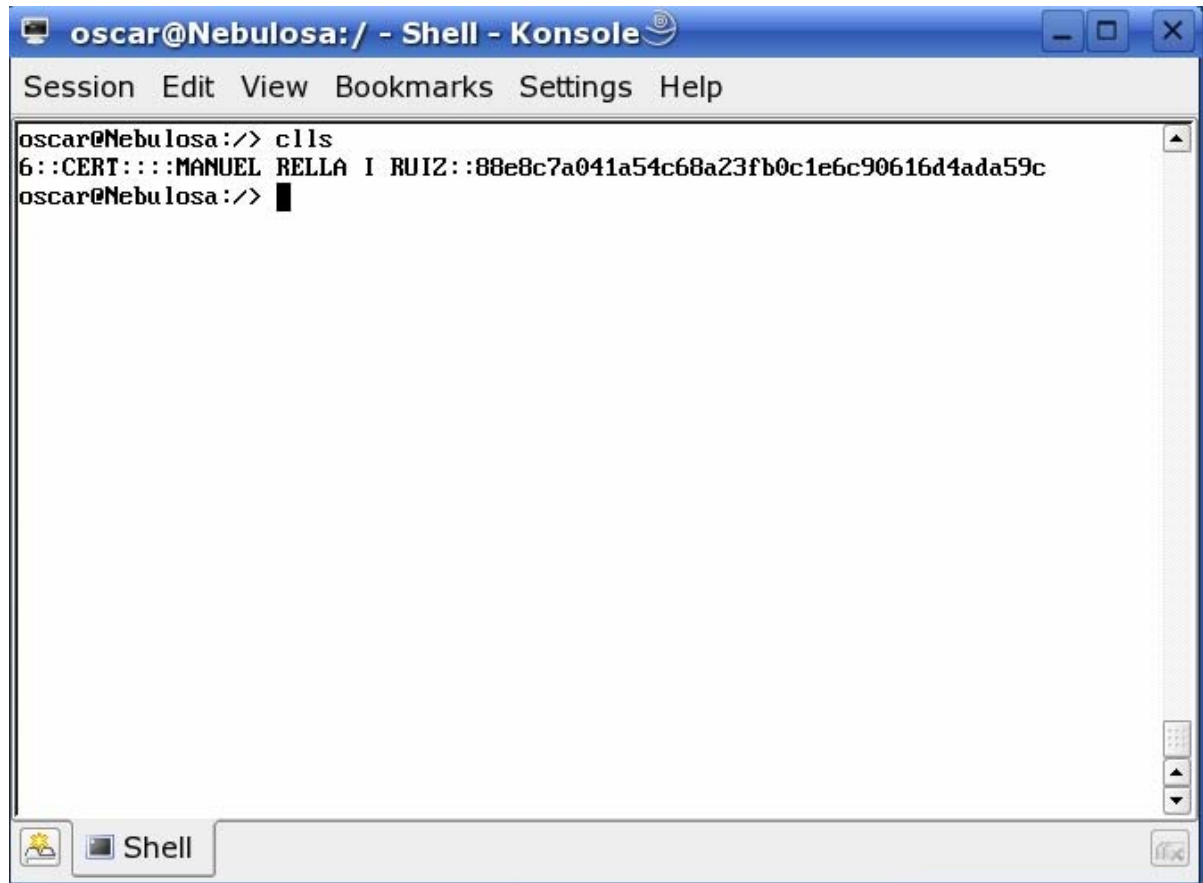
Un cop fet això us demanarà primer el password del clauer i després el password del fitxer .P12



```
oscar@Nebulosa: / - Shell - Konsole
Session Edit View Bookmarks Settings Help
oscar@Nebulosa:~> climport -f /media/usbdisk/cert.p12
Importing PKCS12...
Clauer's password:
Type the password for /media/usbdisk/cert.p12: █
```

Llistar els certificats dins del clauer

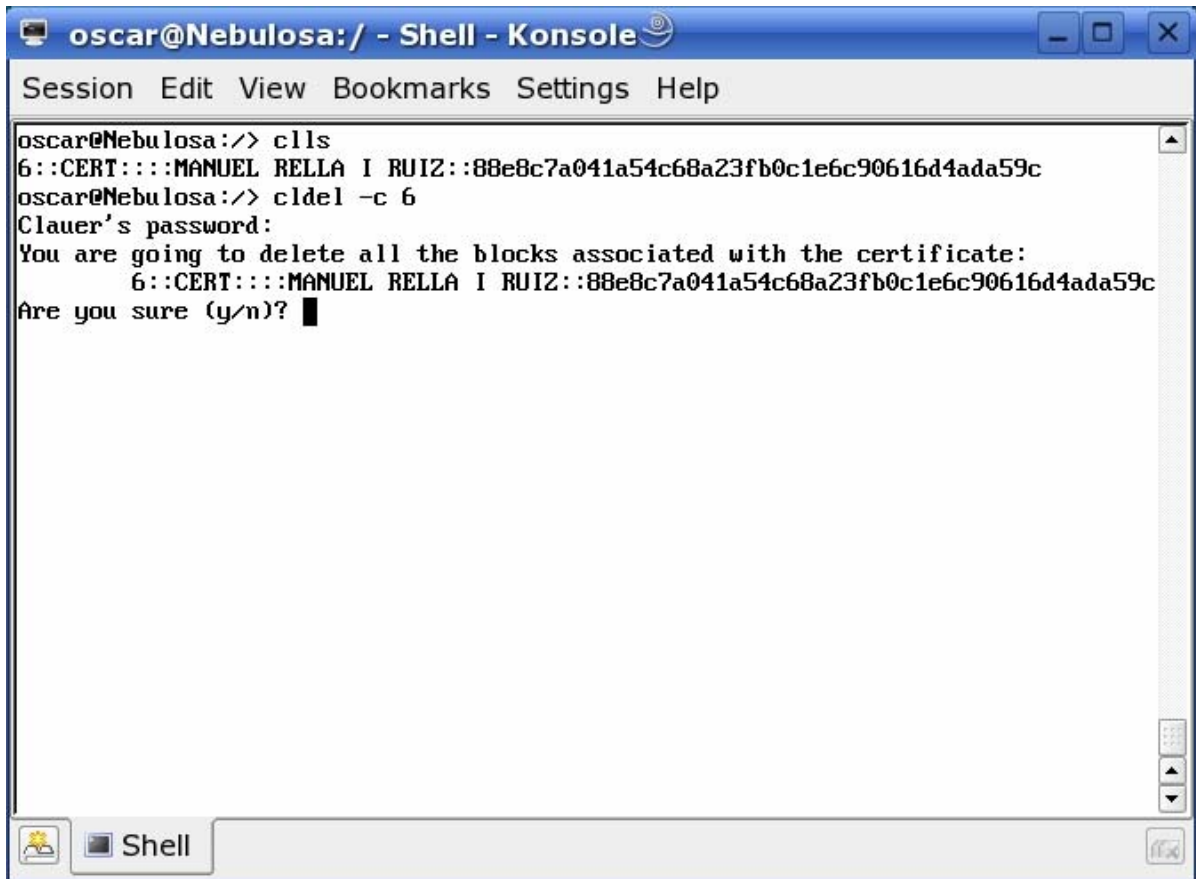
1. Per obtenir un llistat dels certificats instal·lats al clauer caldrà executar la comanda:
c/s



```
oscar@Nebulosa:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
oscar@Nebulosa:~> c/s
6::CERT::::MANUEL BELLA I RUIZ::88e8c7a041a54c68a23fb0c1e6c90616d4ada59c
oscar@Nebulosa:~> █
```


Esborrar certificats dins del clauer

1. Primer caldrà fer un llistat dels certificats amb la comanda: `c/l/s`
2. Amb el número que apareix a la primera columna del llistat feu la invocació a la comanda: `cldel -c <número_del_llistat>`



```
oscar@Nebulosa:~/ - Shell - Konsole
Session Edit View Bookmarks Settings Help
oscar@Nebulosa:~> c/l/s
6::CERT:::MANUEL RELLA I RUIZ::88e8c7a041a54c68a23fb0c1e6c90616d4ada59c
oscar@Nebulosa:~> cldel -c 6
Clauer's password:
You are going to delete all the blocks associated with the certificate:
    6::CERT:::MANUEL RELLA I RUIZ::88e8c7a041a54c68a23fb0c1e6c90616d4ada59c
Are you sure (y/n)? █
```