Agència Catalana de Certificació

Usos del certificat digital amb el navegador Mozilla Firefox 3.6

Control documental

Estat formal	**Elaborat per:** Formació. CATCert	**Aprovat per:** Formació. CATCert
Data de creació	15/06/2010	
Control de versions	**Data:**	15/06/2010
	Descripció:	V1.1 Revisió incorporant indicacions per MAC i Linux
Nivell accés informació	pública	
Títol	Usos del certificat digital amb el navegador Mozilla Firefox 3.6	
Fitxer	Usos del certificat digital amb Firefox v1.1.doc	
Control de còpies	Només les còpies disponibles a la web de CATCert (http://www.catcert.cat) garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.	
Drets d'autor	Aquesta obra està subjecta a una llicència Reconeixement-No comercial-Sense obres derivades 2.5 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.	

Índex

Usos del certificat digital amb el navegador Mozilla Firefox 3.6 1

Control documental 2

Índex 3

1. Introducció 3

1.1 Abast 3

1.2 Contingut 4

1.3 Requisits previs 4

1.4 Verificació dels requisits previs 4

2. Instal·lació de les claus públiques de CATCert 5

2.1 Baixada dels certificats a la màquina local: 5

2.2 Instal·lació de les claus públiques en el Mozilla Firefox 7

3. Càrrega de certificats personals 9

3.1 Introducció 9

3.2 Certificats en software (idCAT) 9

3.3 Certificats en clauer (idCAT) 11

3.3.1 Visualització certificats del clauer 13

3.4 Certificats en targeta (T-CAT) 14

3.4.1 Visualització certificats de la targeta 15

4. Exportació o backup del certificats del repositori 16

5. Ús del certificat en el navegador 19

5.1 Autenticació web en un portal 19

5.2 Avís de pàgina de no confiança 21

1. Introducció

El present document té per objectiu descriure el procés de configuració del navegador Mozilla Firefox 3.6 amb l'objectiu de poder fer ús de certificats digitals de CATCert (Agència Catalana de Certificació).

1.1 Abast

Aquest document va destinat als usuaris del navegador Mozilla Firefox que vulguin utilitzar el certificat digital amb aquest producte.

1.2 Contingut

S'enumeren els passos a seguir per a configurar el navegador. Els diferents punts fan referència als diferents passos que cal seguir i en l'ordre en el que cal executar-los.

1.3 Requisits previs

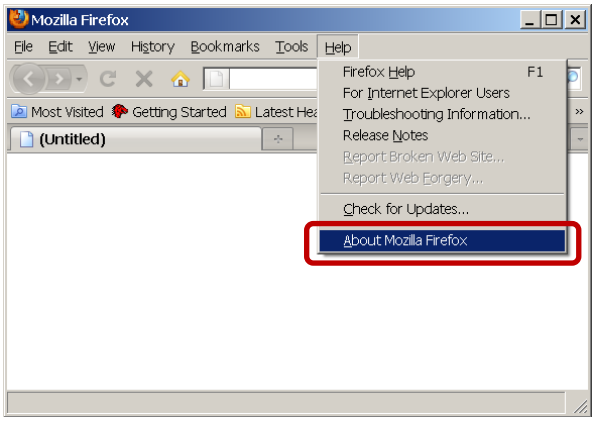
Aquest manual assumeix que l'usuari disposa de:

- **Mozilla Firefox** instal·lat i operatiu en el seu equip.

En cas de no disposar-ho, si us plau, contacteu amb el vostre administrador del sistema o seguiu les passes e indicacions de la web de Mozilla (http://www.mozilla.org/).

1.4 Verificació dels requisits previs

Per verificar que es disposa del Mozilla Firefox:



1. Obrir el programari des de Inici-> Programes-> Mozilla Firefox-> Mozilla Firefox

2. Help -> About Mozilla Firefox

Figura 1

I es pot veure la versió 3.6.+

Figura 2

2. Instal·lació de les claus públiques de CATCert.

2.1 Baixada dels certificats a la màquina local:

Per poder utilitzar els certificats i que no surtin errors de confiança, s'ha d'indicar al programari que es confia en els prestadors de certificació. Això, es fa mitjançant la càrrega de les claus públiques del prestador en el repositori de certificats del programari.

Adquirir les claus públiques de CATCert

Les claus es poden baixar des de la pàgina de baixada de claus públiques del web de CATCert. L'enllaç a ella es troba en la pàgina principal de CATCert.

Figura 3

Cal seguir l'assistent que trobareu al peu de la pàgina i baixar cadascuna de les claus en disc. L'adreça directa és:

http://www.catcert.net/web/cat/descarrega_claus/totes_01.jsp

Baixarem les claus tal i com indica l'assistent.

Figura 4

Al seleccionar el botó de "Baixeu-la" hem de seleccionar l'opció desar a disc.

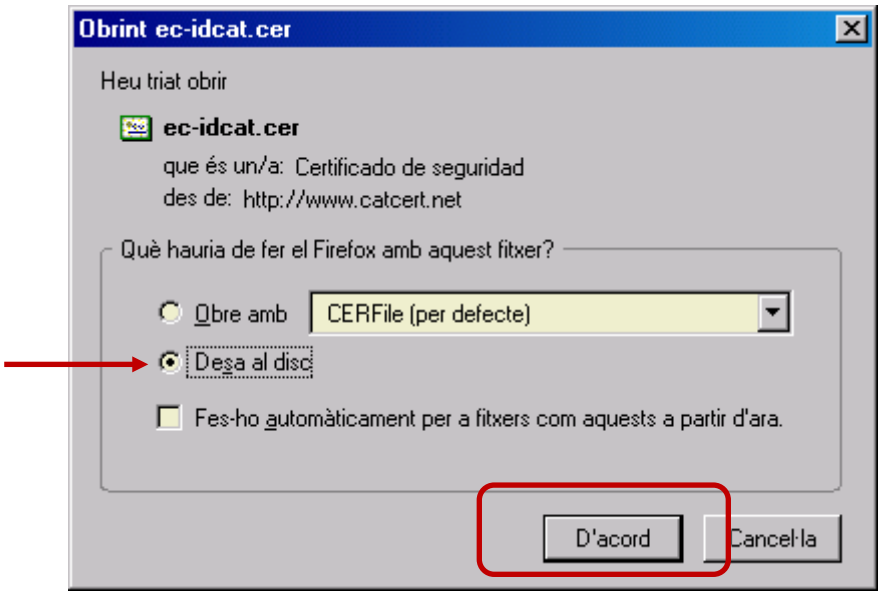
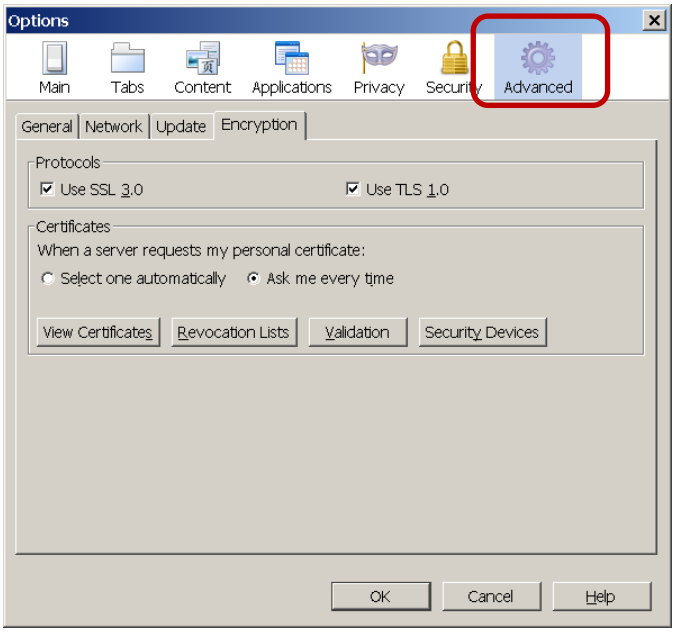


Figura 5

Repetim l'operació per les 9 claus públiques (o certificats de CA) que formen la jerarquia de CATCert.

2.2 Instal·lació de les claus públiques en el Mozilla Firefox

Obertura del gestor de certificats del Mozilla Firefox



1. Obrir el navegador Mozilla Firefox.

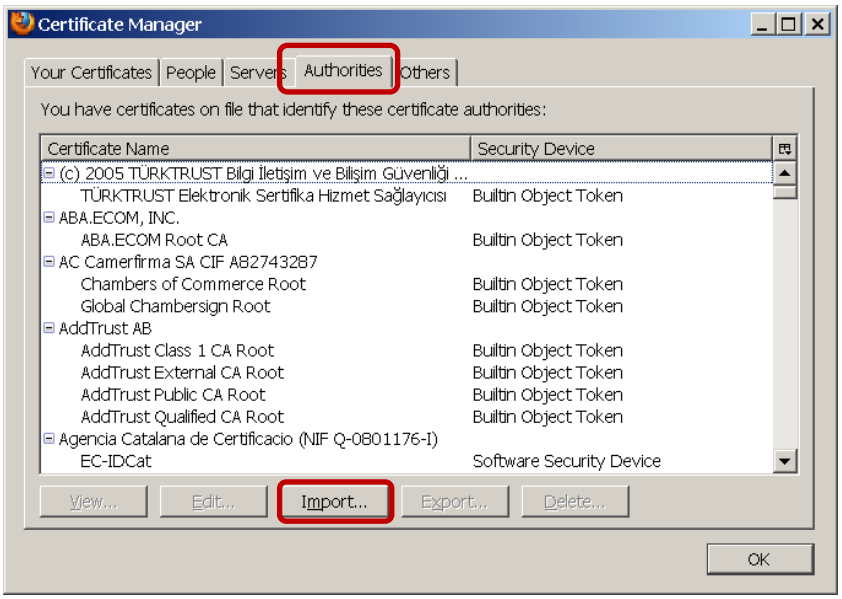
2. Anar a la finestra d'Opcions: a "Tools->Options"

2. Opció "Avanced"

3. Desplegable "Encryption", fer clic al botó "View Certificates".

Figura 6

Ara procedirem a col·locar els certificats públics de CATCert a la pestanya "Authorities" de la finestra del gestor de certificats.



Un cop seleccionada la pestanya, fem clic a "Import":

Figura 7

Anem al directori on s'han desat els certificats descarregats amb anterioritat i escollim tots els certificats a importar.

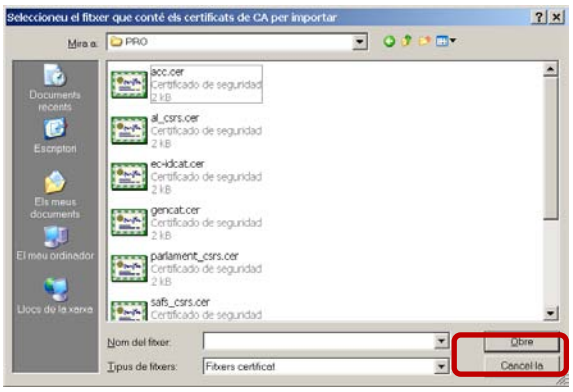
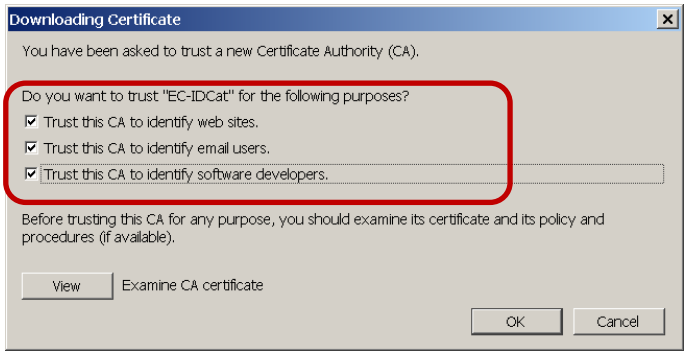


Figura 8



Per a cada certificat a importar, marquem totes les opcions de confiança:

Figura 9

En acabar aquest procés, el gestor de certificats del ThunderBird, hauria de contenir (com a mínim) tots els certificats de les entitats de la jerarquia de certificació des de la que s'ha emès el seu certificat després de la importació.

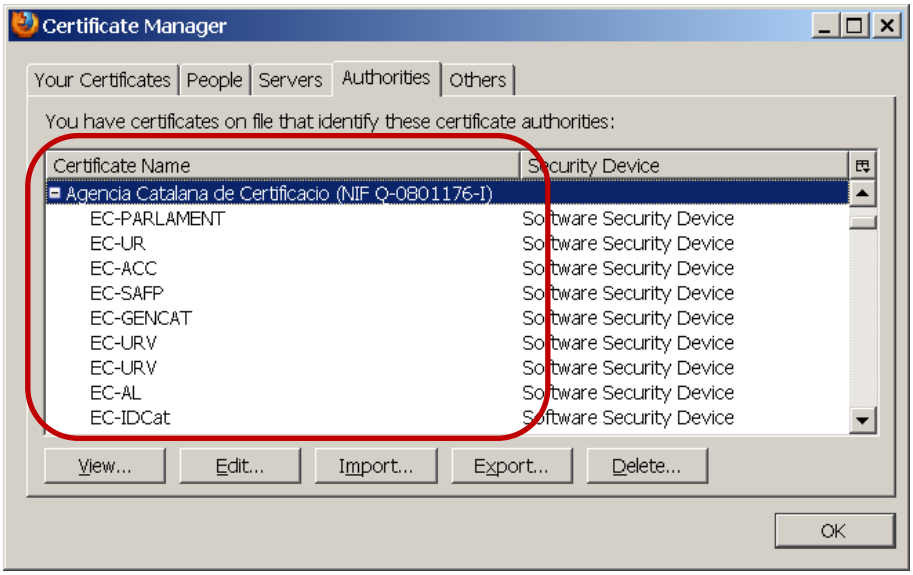


Figura 10

3. Càrrega de certificats personals

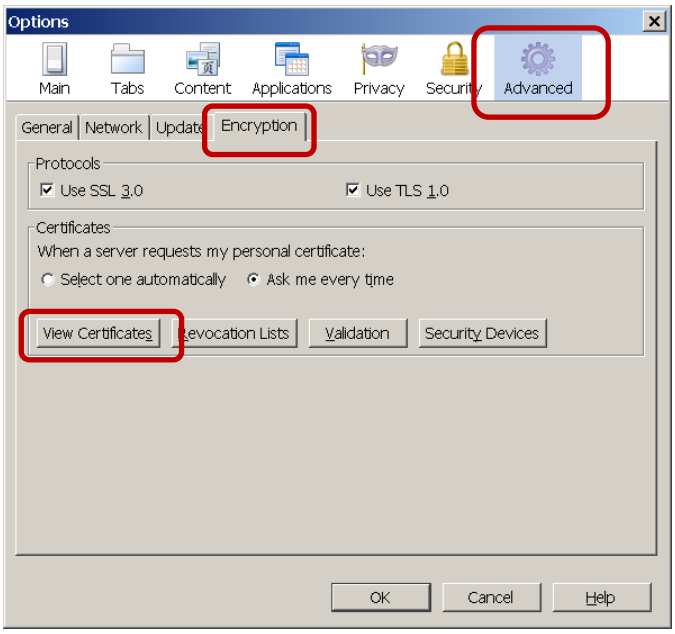
3.1 Introducció

Per tal de realitzat operacions amb el certificat personal, hem de també carregar el certificat personal en el repositori del Thunderbird. Aquesta acció pot ser diferent si tenim un certificat de software (per exemple el idCAT) o bé el tenim en un dispositiu segur criptogràfic (la TCAT) .

Aquesta acció només s'ha de fer un cop.

3.2 Certificats en software (idCAT)

El certificat de ciutadà idCAT es pot subministrar en software, o pot estar en clauer idCAT i ser exportats amb la darrera versió del programari del clauer (disponible sempre a la web http://www.idcat.cat) en un fitxer de software (fitxer .P12 o .PFX)



Per a fer-ho, cal que anem a "Tools->Options", opció "Avanced", etiqueta "Encryption" i fem clic al botó "View Certificates".

Figura 11

Ara fem clic al botó "Import"

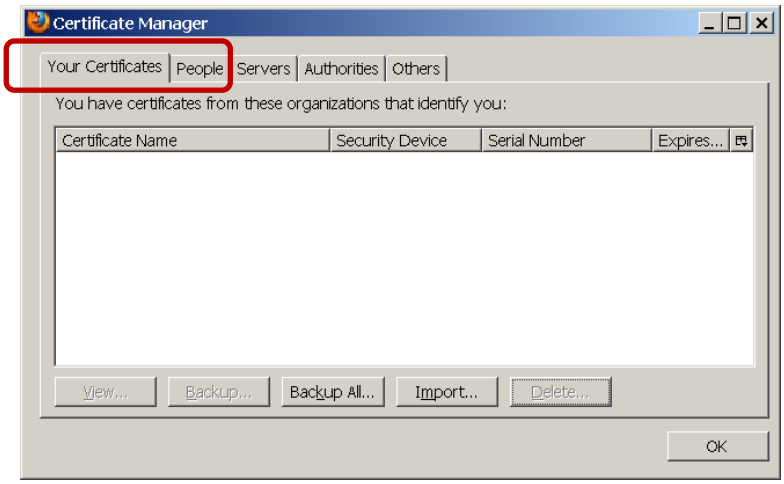


Figura 12

Anem a buscar el fitxer on està el certificat i la clau privada (tenen l' extensió P12 o PFX) i posem la paraula de pas que el protegeix.

Figura 13

Al fer clic en "OK", si la paraula de pas és correcta, ens indicarà que la importació s'ha fet correctament.

El resultat és que hem de poder veure el certificat i la clau privada en el gestor de certificats recollits com certificats en dispositiu de programari software.

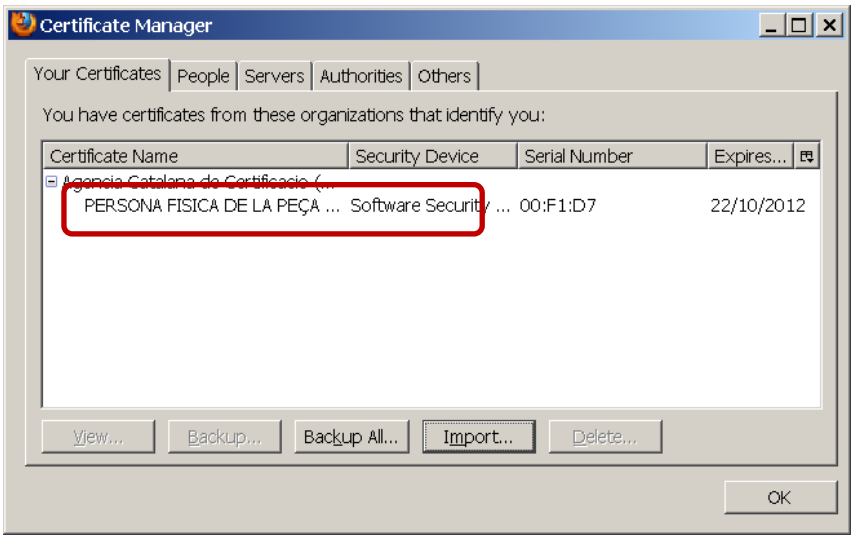


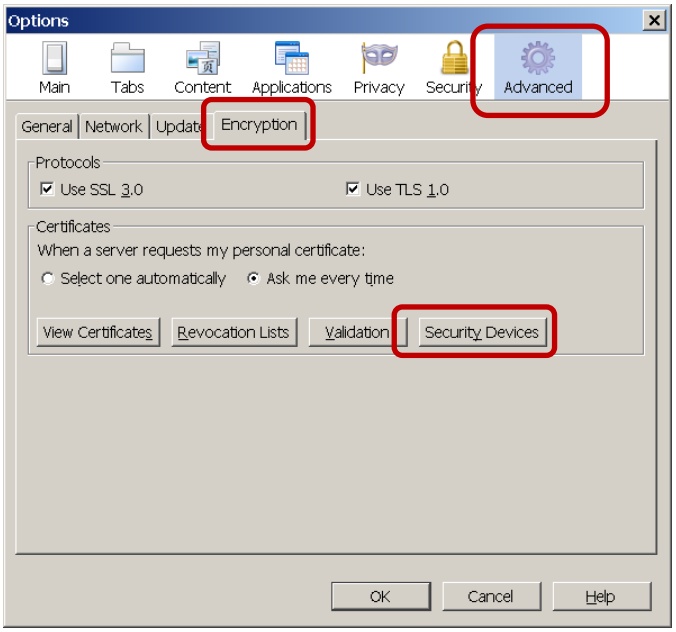
Figura 14

3.3 Certificats en clauer (idCAT)

Per tal que el gestor de certificats del Thunderbird pugui accedir als certificats del clauer com a dispositiu de seguretat hem d'indicar el driver o la dll.

Nota:

Pel correcte ús del clauer, s'ha d'instal·lar primer el programari propi del clauer segons el sistema operatiu (Windows, Linux o MAC) disponible al web d'idCAT http://www.idcat.cat



Per a fer-ho, cal que anem a "Tools->Options", opció "Avanced", etiqueta "Encryption" i fem clic al botó "Security Devices".

Figura 15

Un cop a la finestra d'Administrador de dispositius de seguretat, fem clic al botó "**Load**".

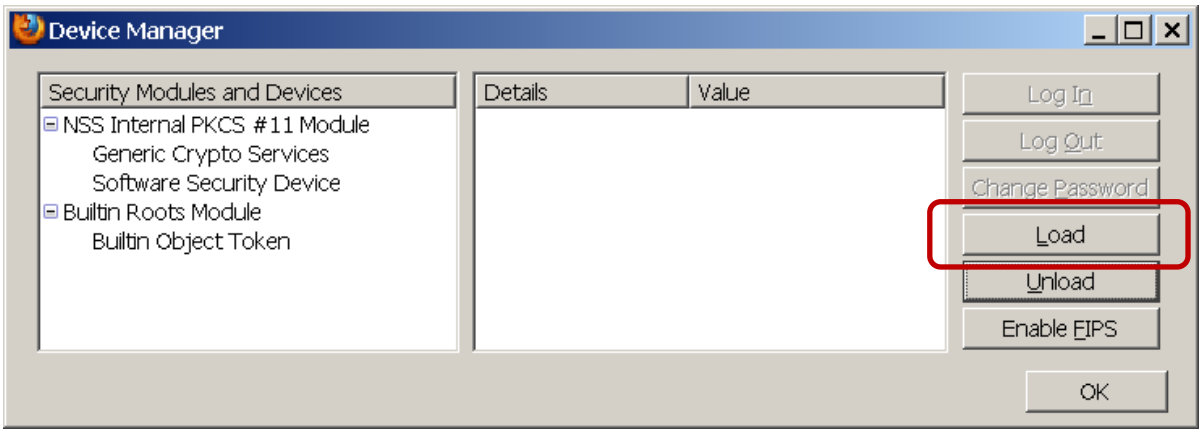


Figura 16

Donem nom "Clauer idCAT" al dispositiu i anem a la carpeta de system32 a seleccionar el fitxer : "C:\WINDOWS\system32\pkcs11-win.dll".

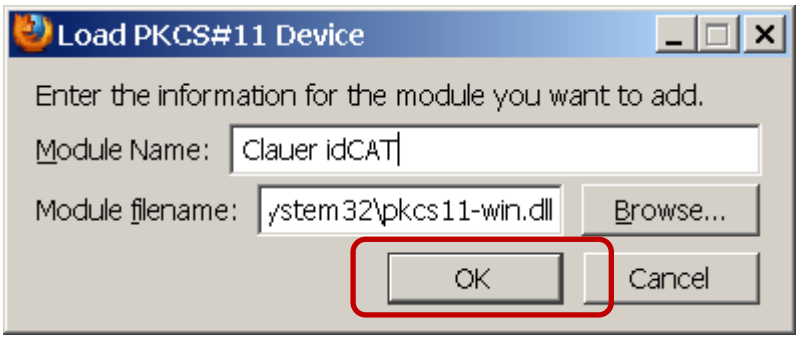
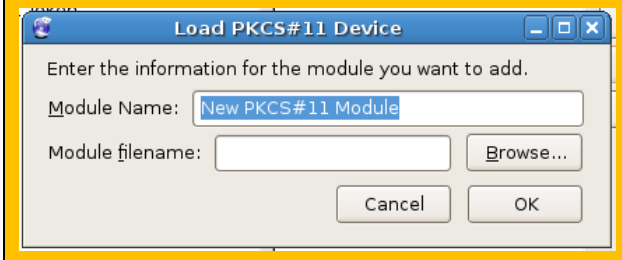


Figura 17

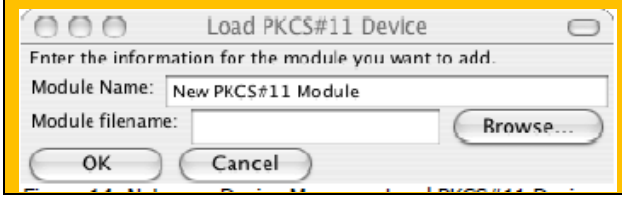
Fem clic en el botó “OK” .

Nota:

En cas de Linux, la llibreria és /usr/local/lib/libpkcs11.so



En cas de Mac OS X, la llibreria és /sw/lib/libpkcs11.dylib



La finestra de l’administrador de dispositius criptogràfics hauria de quedar com es mostra a baix:

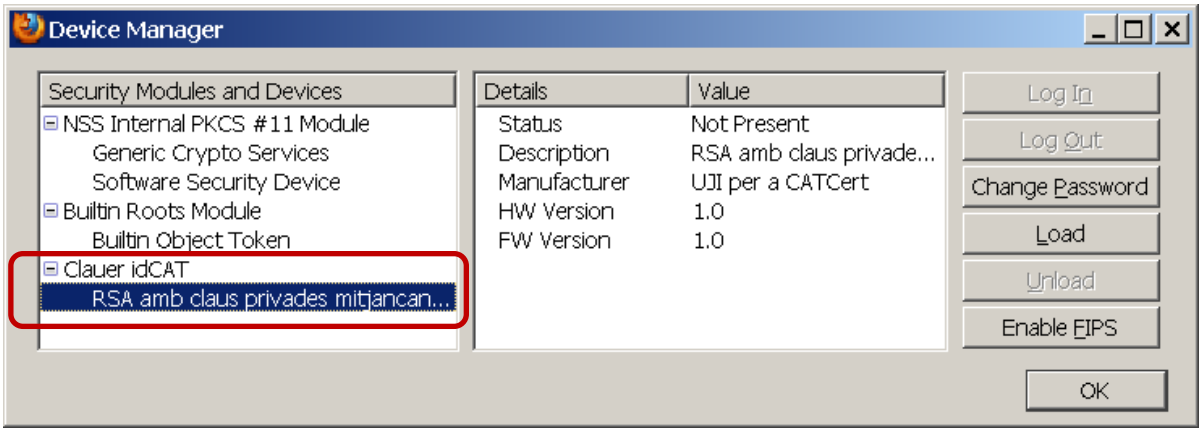


Figura 18

3.3.1 Visualització certificats del clauer

Un cop hem configurat el clauer com a Dispositiu de Seguretat i amb el clauer insertat, anem a "Eines->Opcions", opció "Avançat" i fem clic a "Visualitzar Certificats".

Ens sol·licitarà el PIN d'accés al clauer:

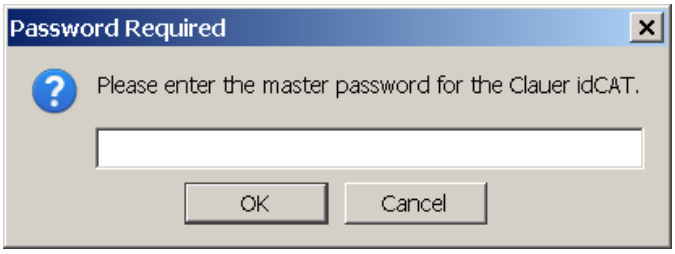


Figura 19

S'hauria de mostrar la finestra de l'Administrador de Certificats amb els seus certificats que tinguem dintre del clauer:

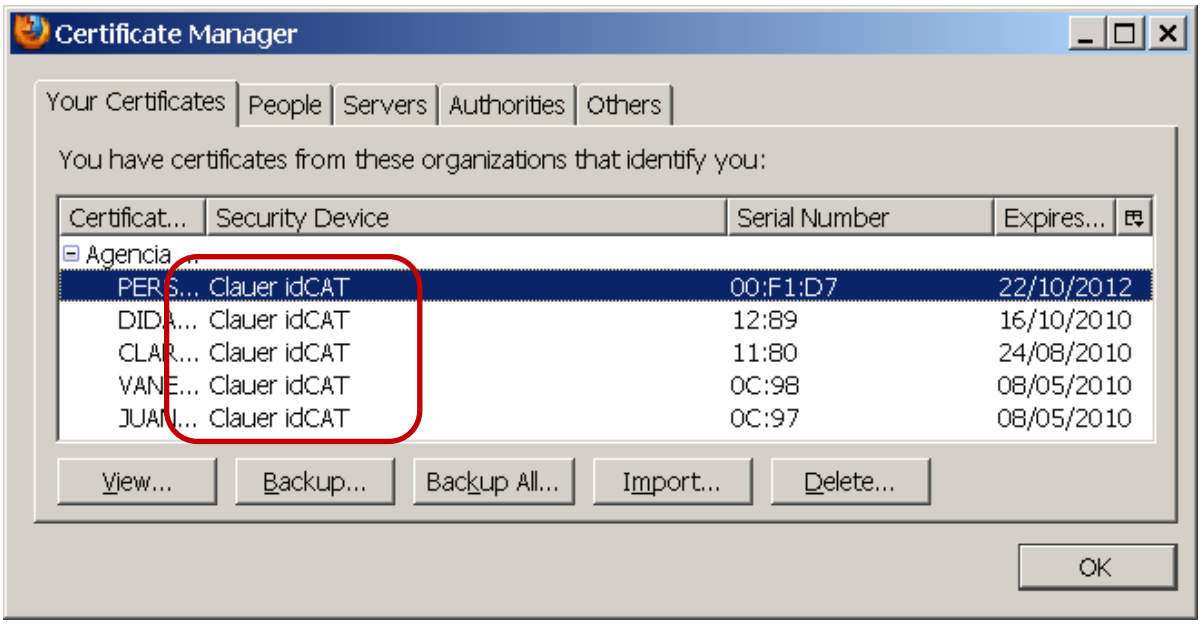


Figura 20

Nota:

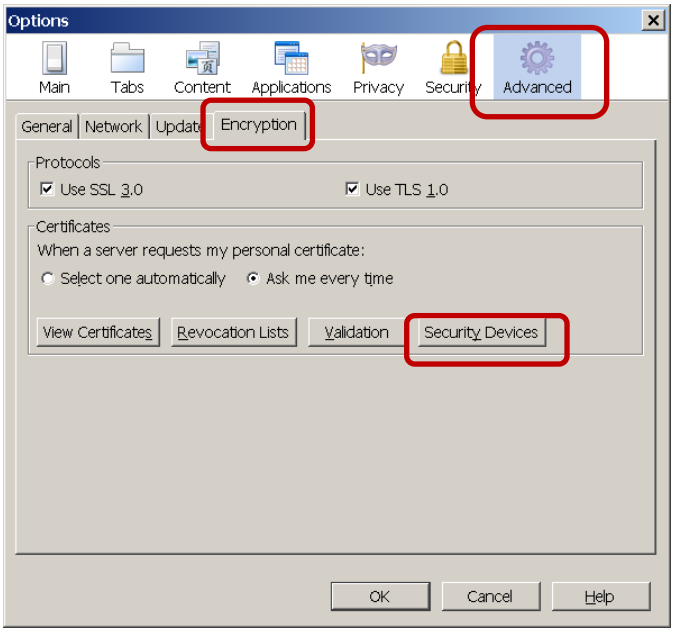
Encara que es disposi de clauer, per facilitar-ne l'ús diari en l'equip local o bé per si hi ha problemes amb llibreries d'ús del mateix, també es pot "exportar" el certificat i la clau privada del clauer en un fitxer P12 i fer la instal·lació en software seguint les indicacions del punt anterior.

3.4 Certificats en targeta (T-CAT)

Per tal que el gestor de certificats del ThunderBird pugui accedir als certificats de la targeta, cal configurar el lector de targetes criptogràfiques com a dispositiu criptogràfic de seguretat en ell.

Nota:

Pel correcte ús de la targeta, s'ha d'instal·lar primer el programari propi de la targeta segons el sistema operatiu (Windows, Linux o MAC). Veure indicacions del fabricant.



Per a fer-ho, cal que anem a "Tools->Options", opció "Avanced", etiqueta "Encryption" i fem clic al botó "Security Devices".

Figura 21

Un cop a la finestra d'Administrador de dispositius de seguretat, fem clic al botó "**Load**".

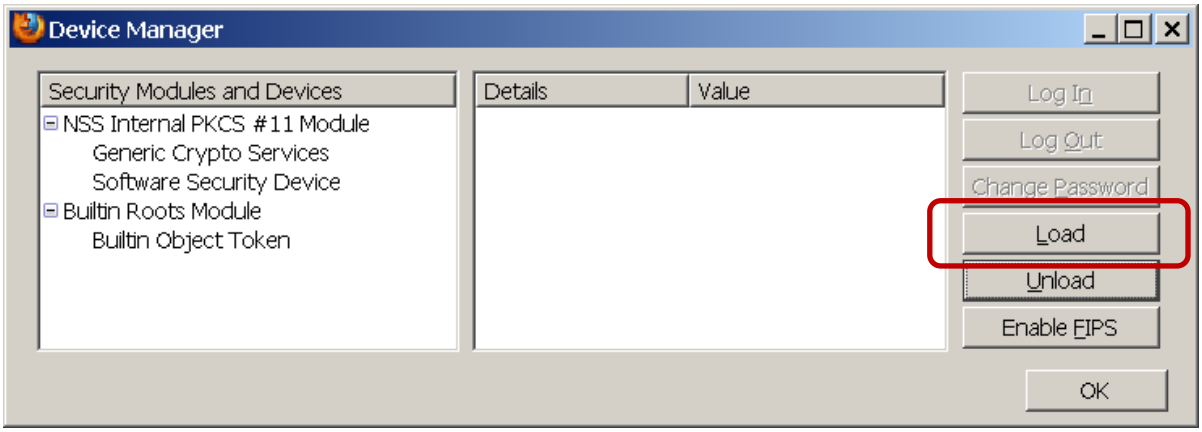


Figura 22

Donem nom "CATCert" al dispositiu i anem a la carpeta de system32 a seleccionar el fitxer: "C:\WINDOWS\system32\aetpkss1.dll".

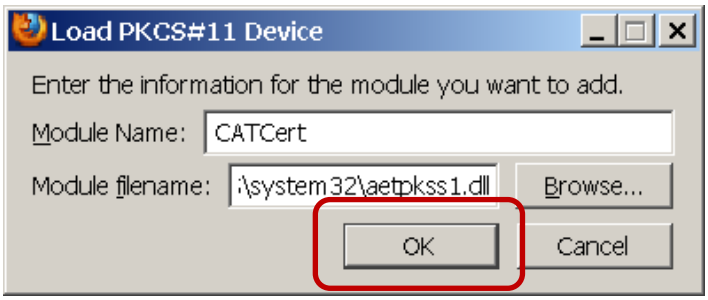
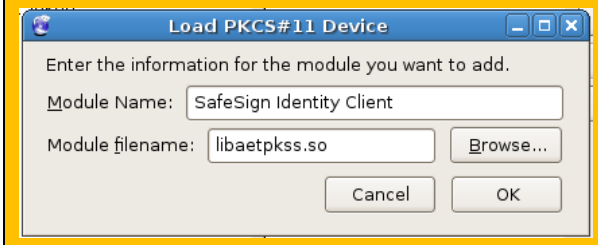


Figura 23

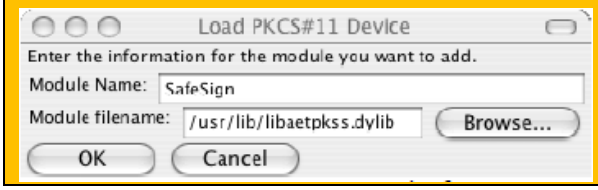
Fem clic en el botó "**OK**" .

Nota:

En cas de Linux, la llibreria és libaetpkss.so



En cas de Mac OS X, la llibreria és /sw/lib/libaetpkss.dylib



La finestra de l'**Administrador de dispositius criptogràfics** hauria de quedar com es mostra a baix:

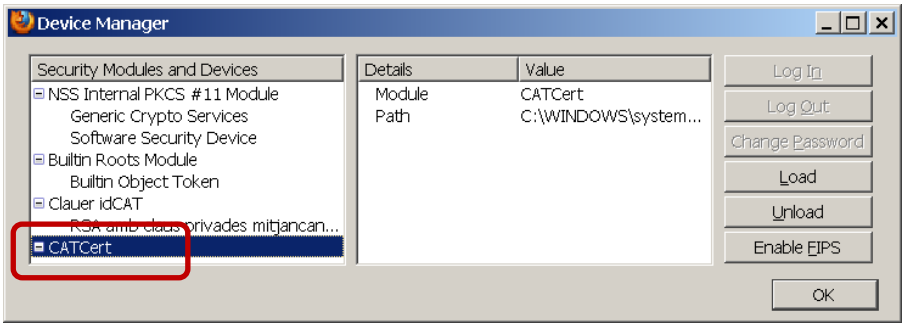


Figura 24

3.4.1 Visualització certificats de la targeta

Un cop hem configurat el lector com a Dispositiu criptogràfic de Seguretat i amb la targeta insertada, anem a "Eines->Opcions", opció "Avançat" i fem clic a "Visualitzar Certificats".

Ens sol·licitarà el PIN d'accés a la targeta:

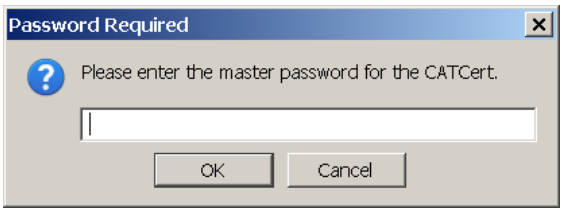


Figura 25

S'hauria de mostrar la finestra de l'Administrador de Certificats amb els seus certificats de Signatura (CPISR-1) i xifrat (CPX-1) tal i com es mostra en l'exemple a continuació:

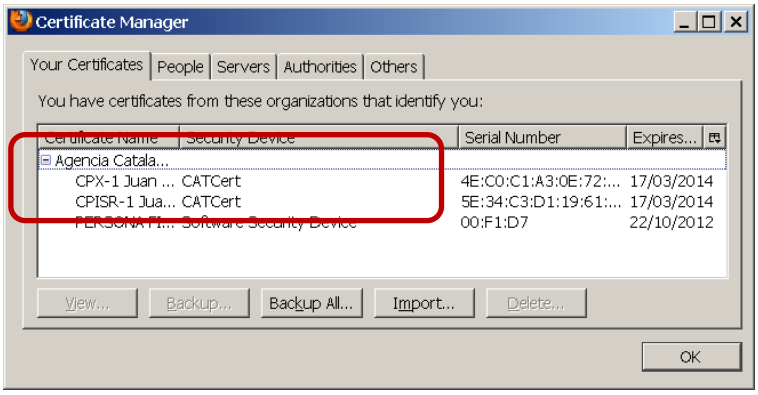
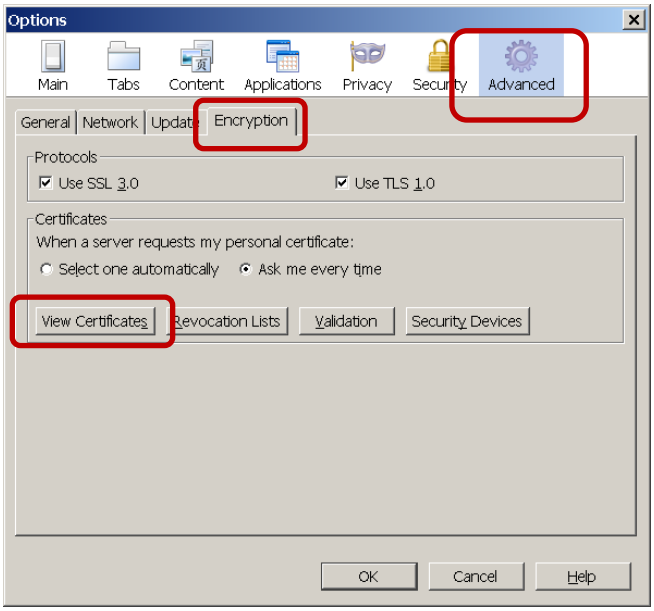


Figura 26

4. Exportació o backup del certificats del repositori

En determinats casos, pot interessar la exportació d'un certificat – i també de la seva clau privada- com a mesura de còpia de seguretat.



Per a fer-ho, cal que anem a "Tools->Options", opció "Avanced", etiqueta "Encryption" i fem clic al botó "View Certificates".

Figura 27

Aquí es pot veure el gestor de certificats amb els certificats classificats en diferents tipus (propis,de gent, de servidors, d'autoritats de confiança o altres respectivament.

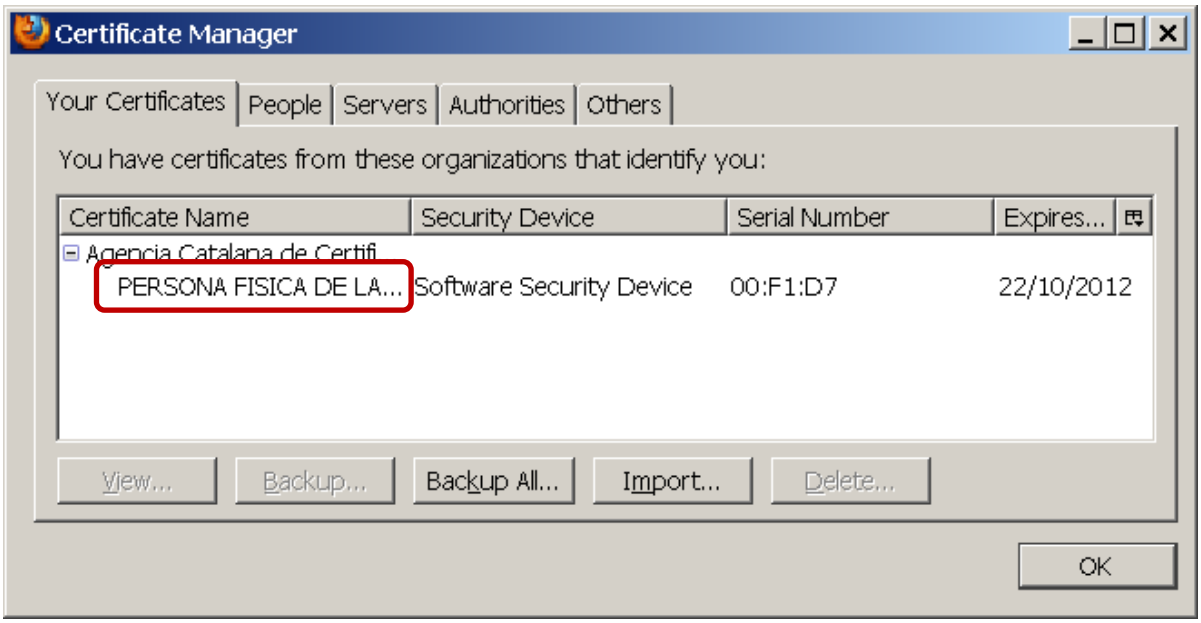


Figura 28

Podem seleccionar un certificat fent un clic a sobre, i s'activarà l'opció de "Backup".

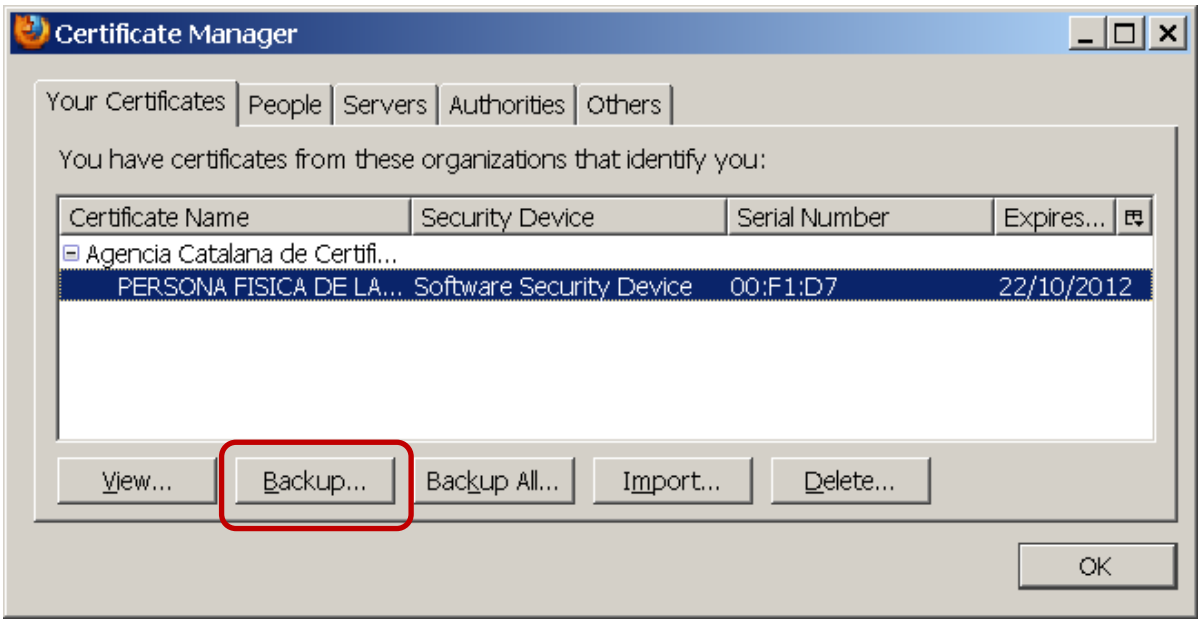


Figura 29

Si és un certificat propi, la exportació ens indicarà on volem desar el certificat juntament amb la clau privada tot creant un fitxer "P12".

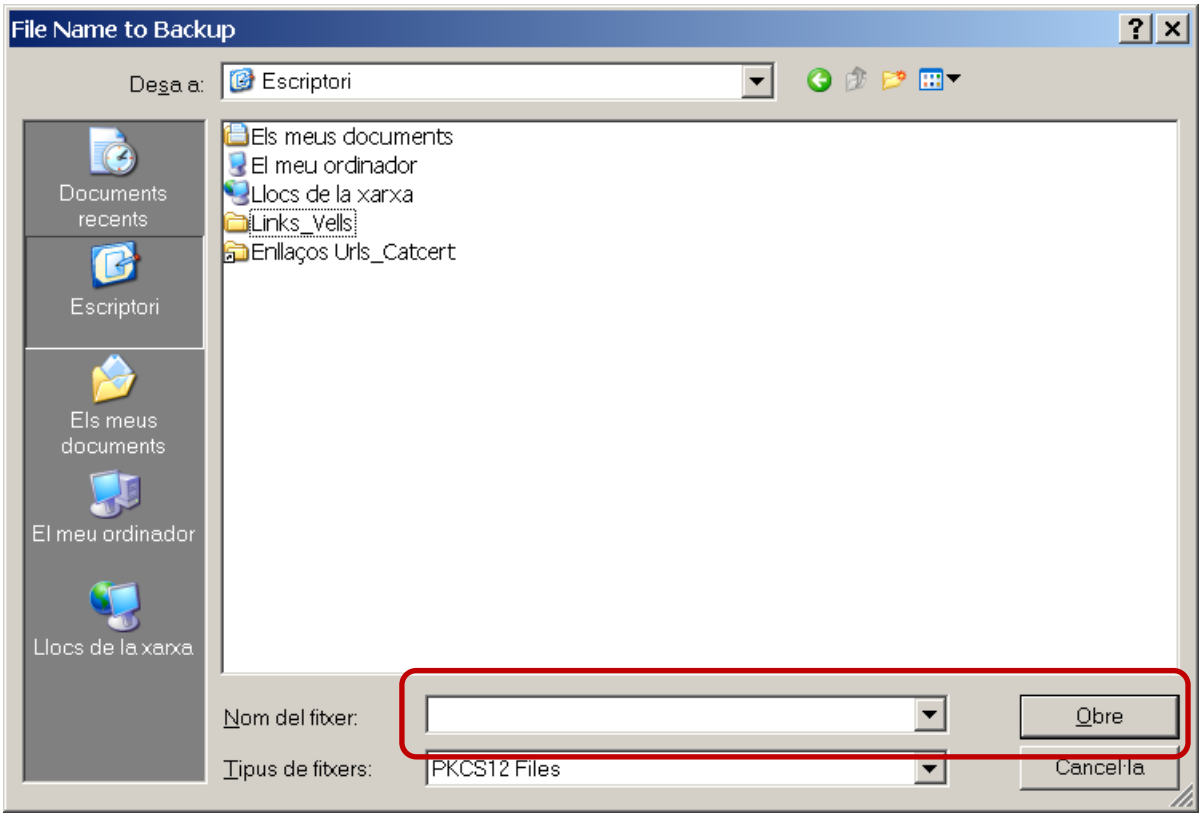


Figura 30

Després de posar el nom del fitxer i fer clic en "Obre", indica que hem de protegir el fitxer amb una paraula de pas.

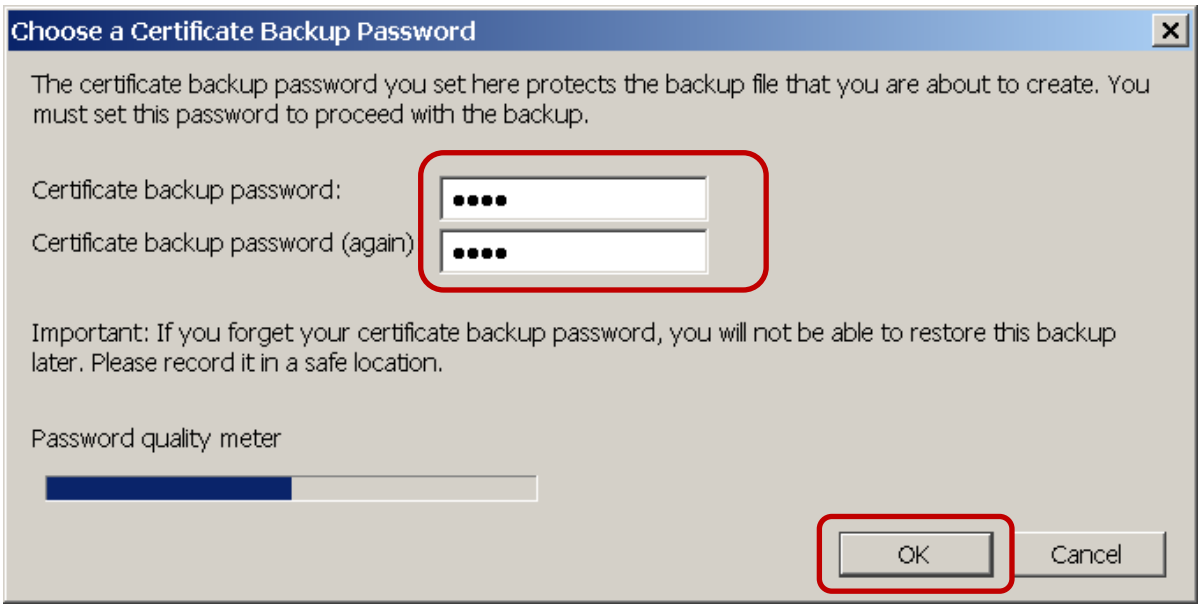


Figura 31

I finalment, al fer clic en "**OK**" ens indica que la exportació s'ha realitzat correctament.

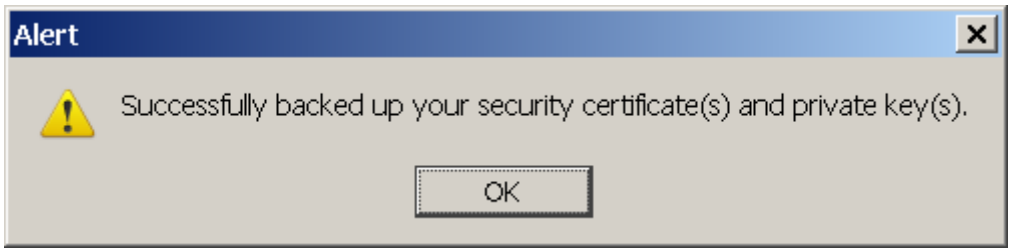


Figura 32

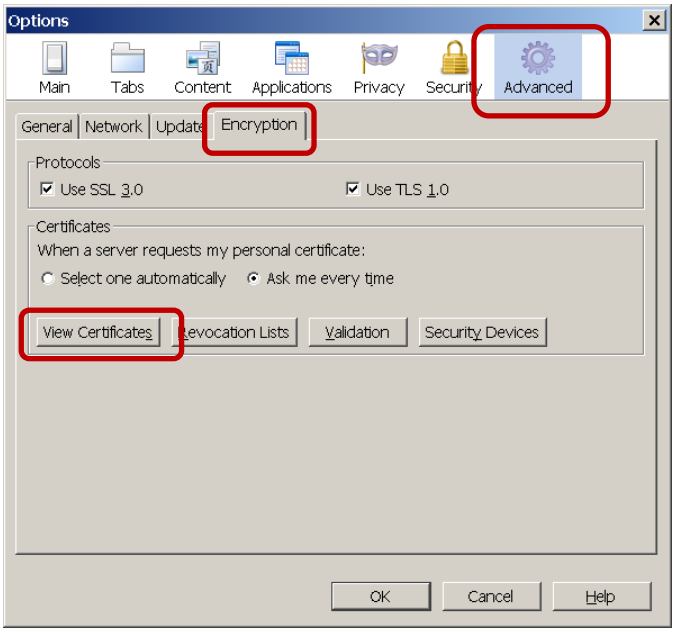
5. Ús del certificat en el navegador

5.1 Autenticació web en un portal

Per fer ús del certificat personal, aquest ha de ser primer de tot visible en el magatzem de certificats del navegador tal i com s'ha indicat anteriorment.

Nota:

Si el certificat és en clauer o en targeta, aquest té que està connectat en l'equip



Per a fer-ho, cal que anem a "Tools->Options", opció "Avanced", etiqueta "Encryption" i fem clic al botó "View Certificates".

Figura 33

Aquí es pot veure el gestor de certificats propis "Your Certificates".

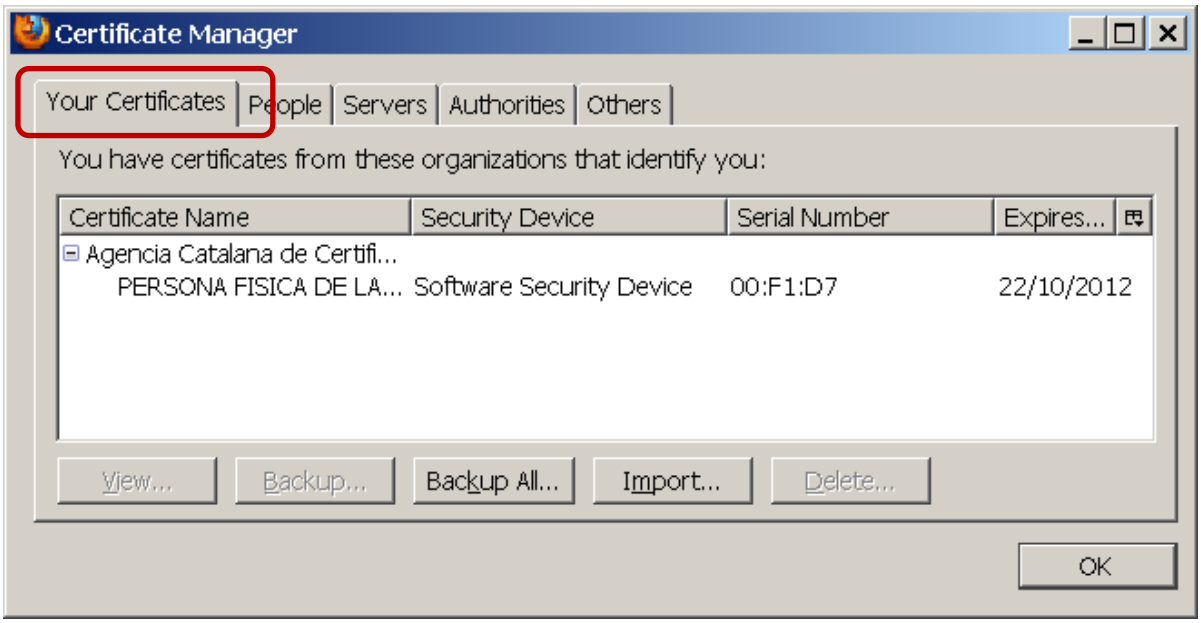


Figura 34

A partir d'aquí, quan s'entra en un portal que requereixi d'autenticació amb certificat digital, el propi navegador ens pregunta en una finestra quin certificat –dels certificats disponibles- s'ha d'utilitzar. En el següent exemple s'entra en la web https://www.eacat.cat/group

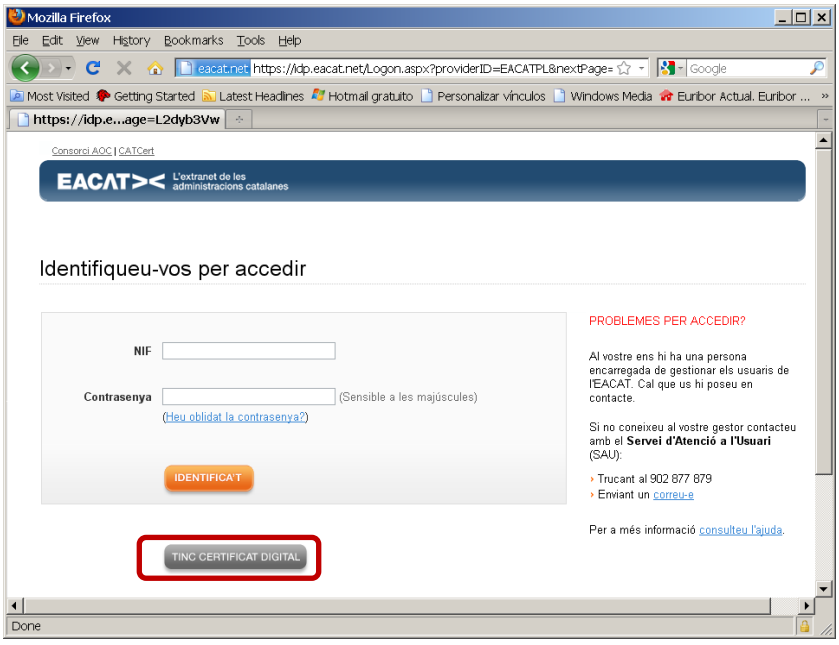


Figura 35

Es selecciona el login mitjançant certificat digital amb "**Tinc Certificat Digital**"

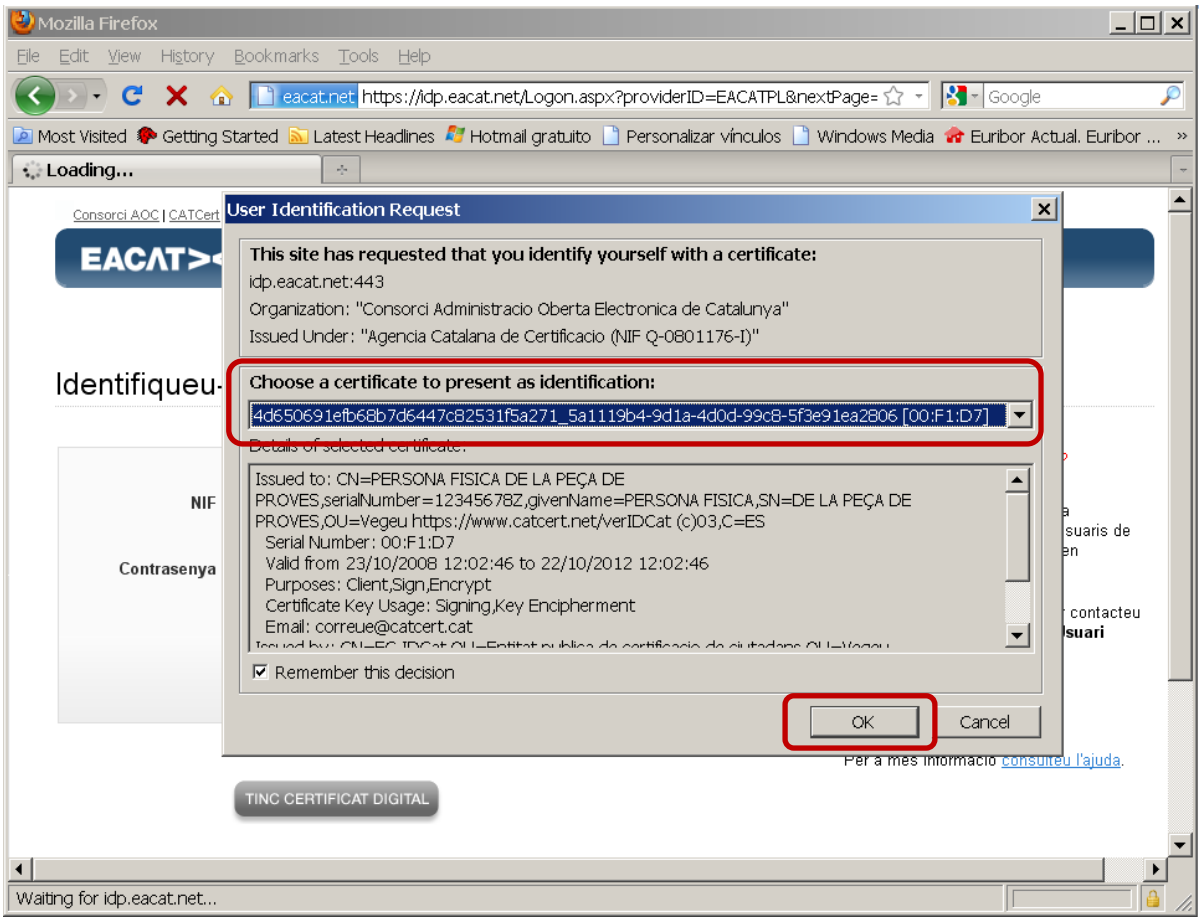


Figura 36

Es selecciona el certificat personal utilitzant el desplegable i es fa clic en “OK” per donar la identitat al portal i accedir si l’usuari existeix o el certificat és vàlid.

5.2 Avís de pàgina de no confiança

Un escenari que ens podem trobar és quan entrem a una web segura i el certificat del portal no ha estat emès per una autoritat de certificació que el navegador en tingui les claus públiques com entitat de confiança.

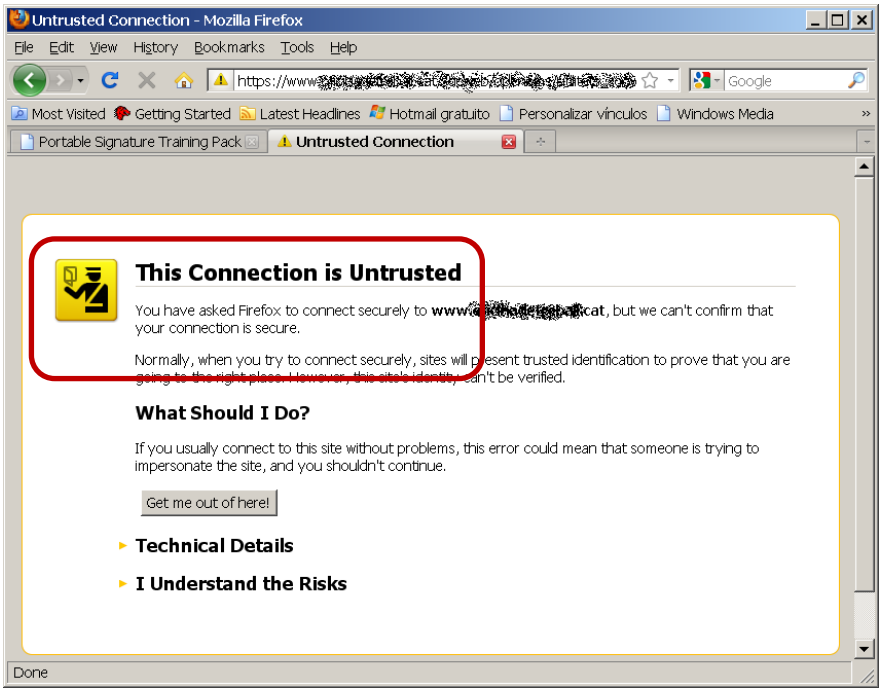


Figura 37

En aquests cas es pot afegir una excepció, fent clic en "**Add Exception**"

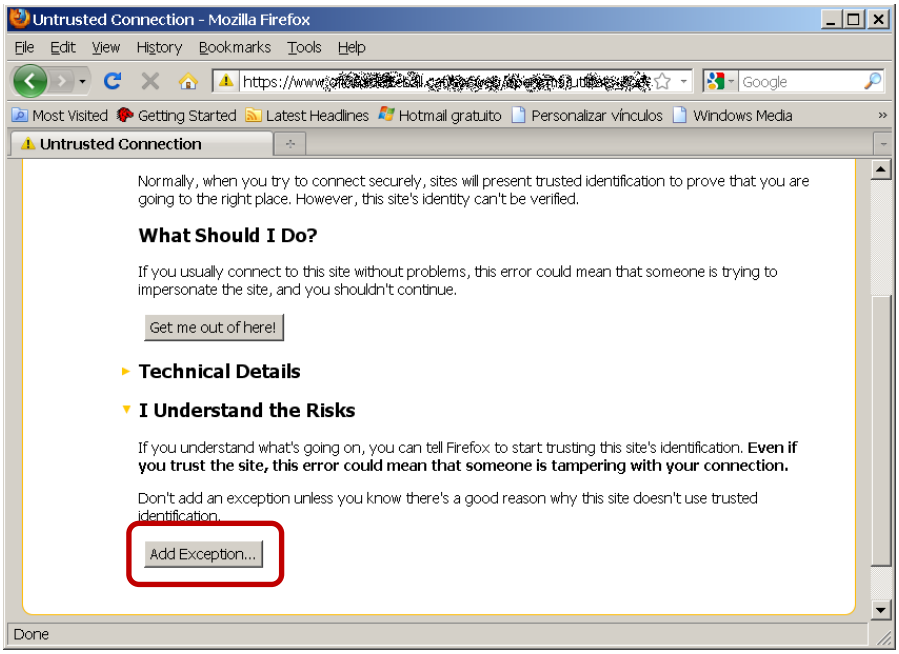


Figura 38

S'ha d'indicar "Get Certificate" i observar qui ha generat el certificat

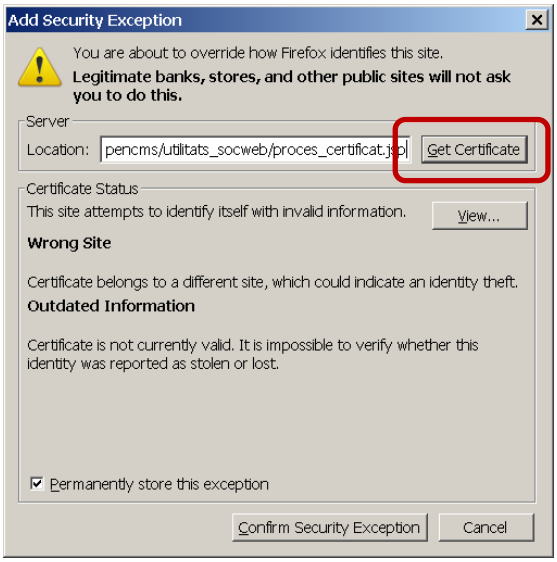


Figura 38

A partir d'aquí, es pot indicar que creem l'excepció o bé cancel·lar-ho i no entrarem en el portal.