Agència Catalana de Certificació

Usos del certificat digital amb el navegador Internet Explorer

Control documental

Estat formal	**Elaborat per:** CATCert	**Aprovat per:** Formació. CATCert
Data de creació	21/06/2010	
Control de versions	**Data:**	23/03/2011
	Descripció:	V2.2 Actualitzar la instal·lació de claus públiques
Nivell accés informació	pública	
Títol	Usos del certificat digital amb el navegador Internet Explorer	
Fitxer	Usos del certificat digital amb Internet Explorer v.2.2.docx	
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		

Índex

1. Introducció

El present document té per objectiu descriure el procés de configuració del navegador Internet Explorer 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 Internet Explorer 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:

- **Equip de Windows amb Internet Explorer** operatiu en el seu equip.

En cas de no disposar-ho, si us plau, contacteu amb el vostre administrador del sistema.

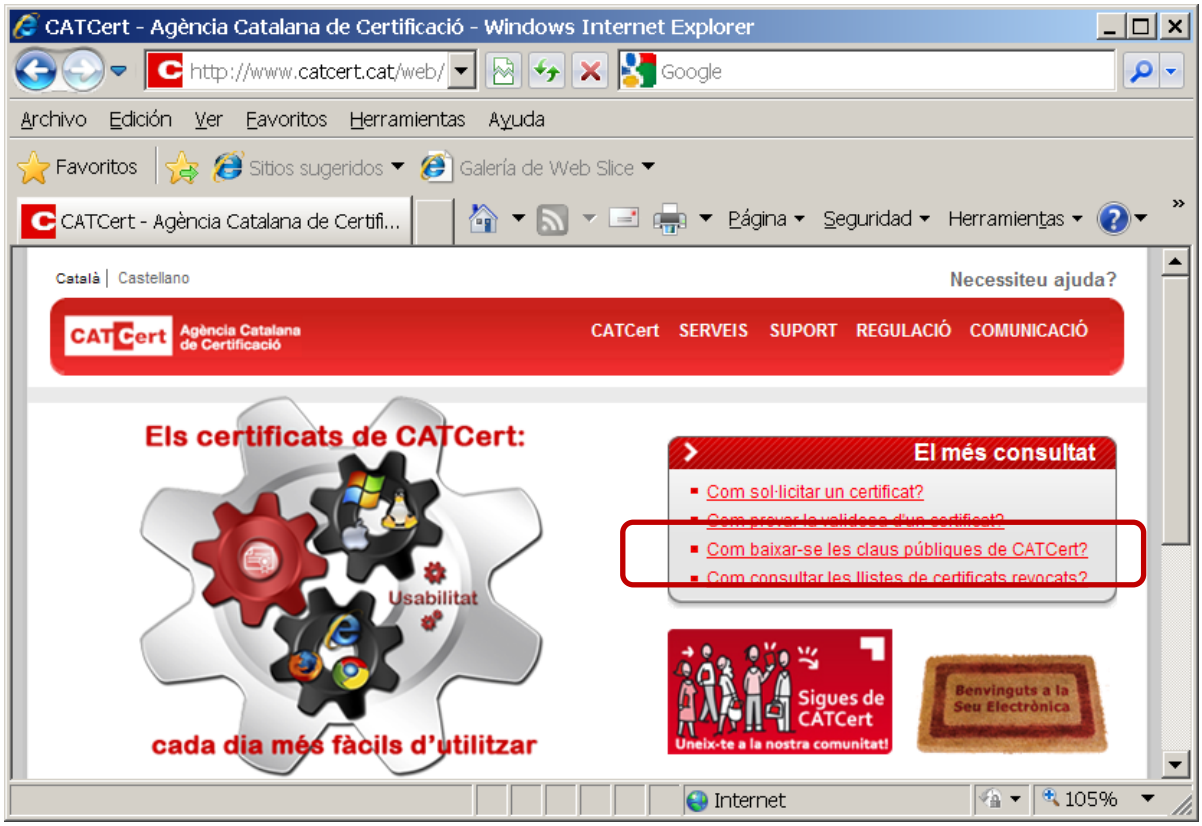
2. Instal·lació de les claus públiques de CATCert.

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 (magatzem) de certificats del programari.

2.1.1 Adquirir les claus públiques de CATCert

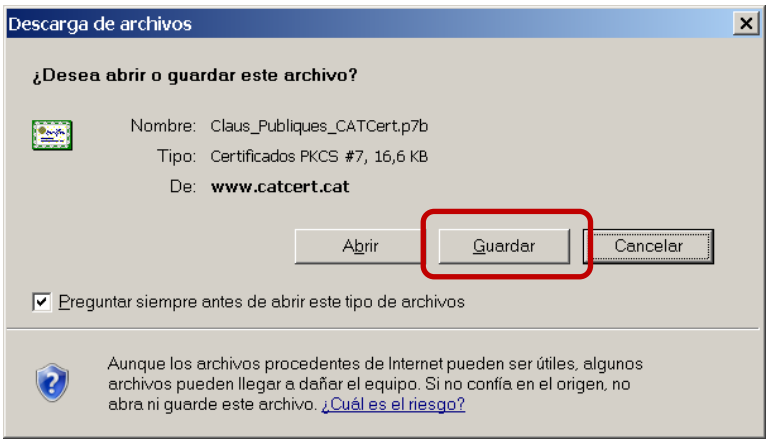
Les claus es poden baixar des de la pàgina de baixada de claus públiques del web de CATCert. L'enllaç a ella es troba en la pàgina principal de CATCert.



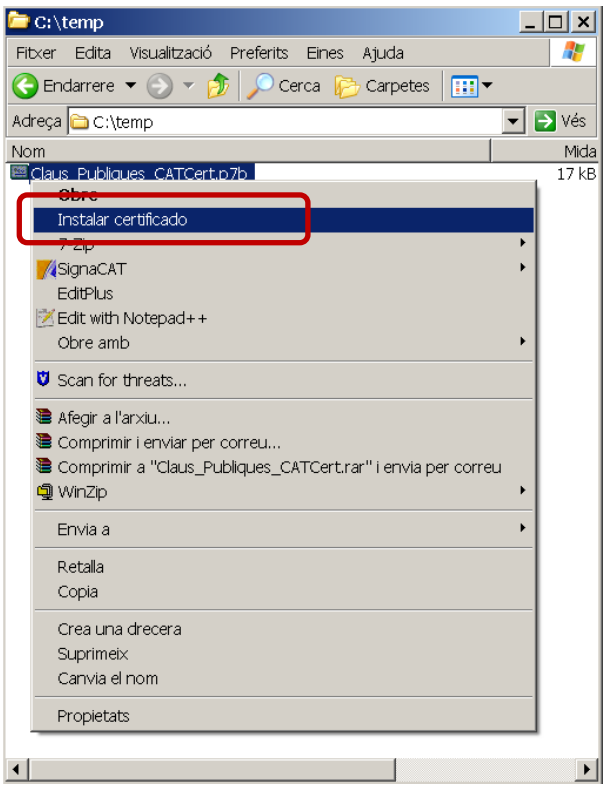
Ara podem instal·lar totes les claus públiques de CATCert en un sol clic. L'adreça directa és: http://www.catcert.cat/descarrega/Claus_Publiques_CATCert.p7b

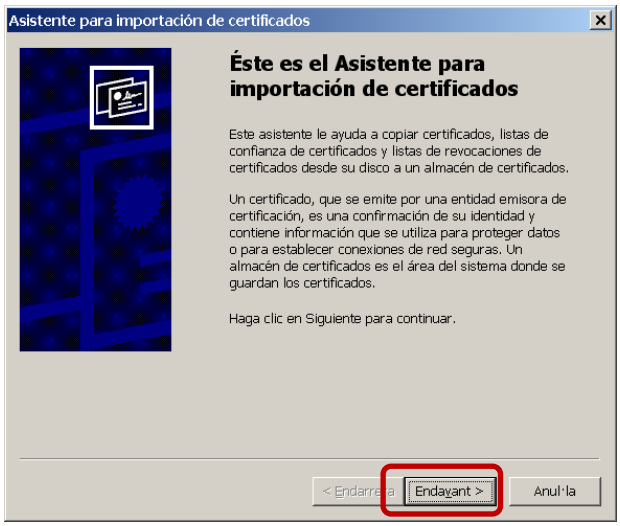
Baixarem el fitxer.

Al seleccionar el botó de "**Baixeu-la**", ens pregunta que volem fer i hem de seleccionar l'opció "**Guardar**".

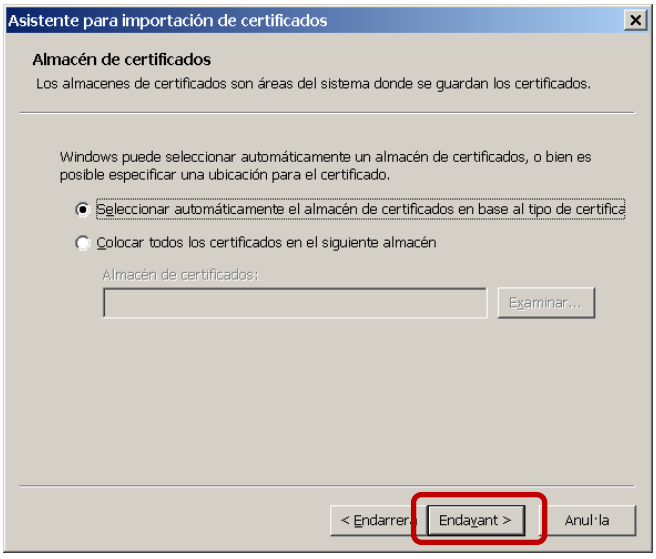


Un cop s'ha baixat el fitxer, fem clic a sobre amb el botó dret i seleccionem l'opció "**Instalar certificado**" per iniciar l'assistent.

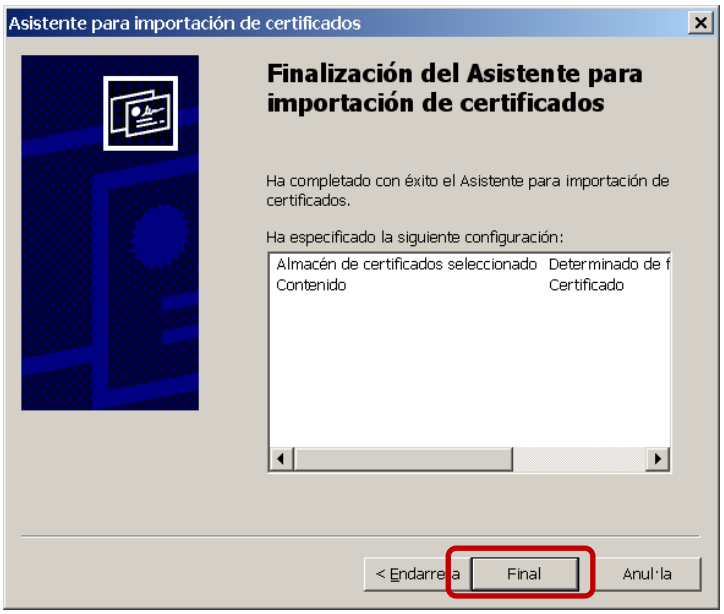




Aquest assistent ens ajuda a la incorporació del certificat al repositori. Es fa clic en el botó d'**Endavant** i el sistema pregunta en quina ubicació el volem posar.



Es torna a fer clic en "**Endavant**" i després en "**Final**".

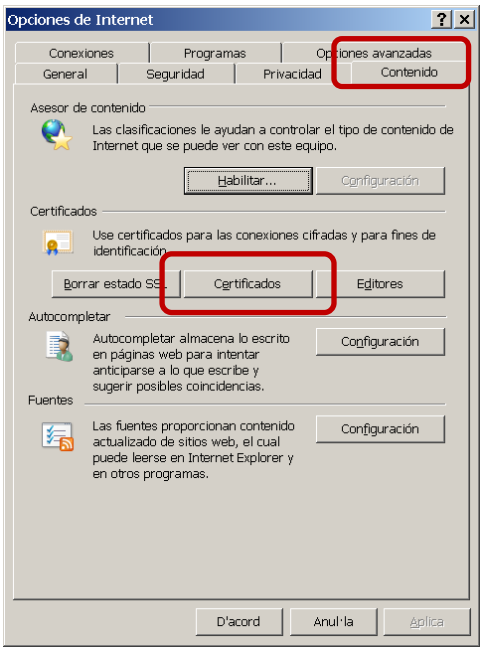


Al finalitzar aquest procés, hi ha una finestra que informa de la importació amb èxit del certificat i fem clic a "D'acord".

2.1.2 Verificació de les claus públiques instal·lades

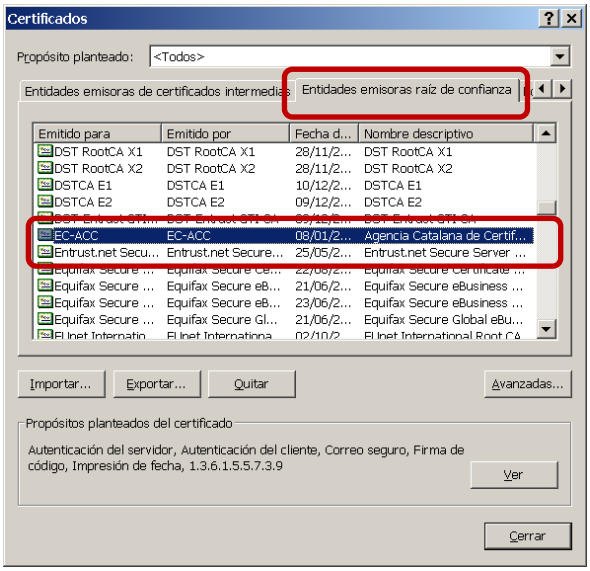
Per verificar que tenim les claus públiques instal·lades s'ha d'anar al gestor de certificats de l'aplicatiu que estem utilitzant i veure el conjunt de certificats de la jerarquia de CATCert.

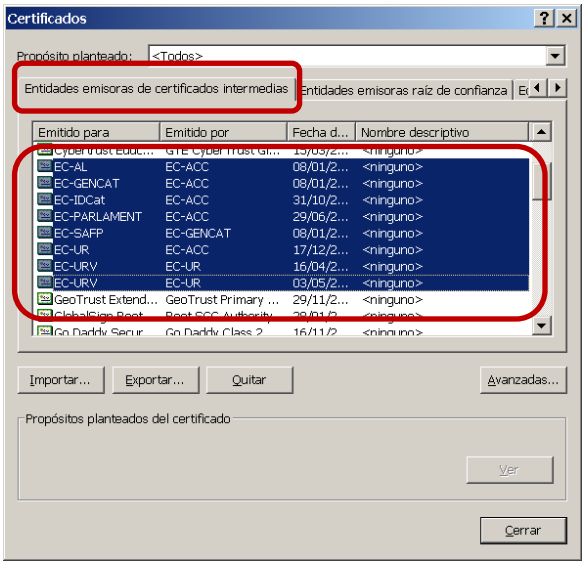
En cas d'Internet Explorer s'utilitza el gestor de certificats de Windows. Obrim Internet Explorer i anem a "**Eines ➔ Opcions d'Internet**"



Dins de "**Continguts**" hi ha un apartat de certificats. Es fa clic en el botó "**Certificados**".

S'ha de fer dos verificacions en llocs diferents ja que se separa la clau pública arrel de CATCert (EC-ACC), de les intermitjes. La clau arrel es trobarà a la pestanya "Entitats emissores arrel de confiança".





Les claus intermitjes es trobaran a la pestanya "**Entitats emissores de certificats intermitges**", tot corresponent-se amb la jerarquia de certificació de CATCert (EC-IDCat, EC-....).

2.2 Sol·licitud d'un certificat idCAT

El certificat idCAT és un certificat digital personal que emet CATCert (amb col·laboració d'entitats de registre ubicades a ajuntaments, consells comarcals, Departaments de la Generalitat, etc.) a tot ciutadà que requereixi un per interactuar amb l'administració.

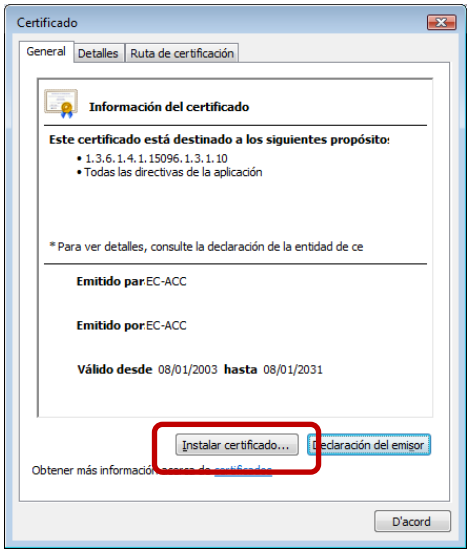
Per fer la sol·licitud s'ha de seguir les indicacions de la web http://www.idcat.cat

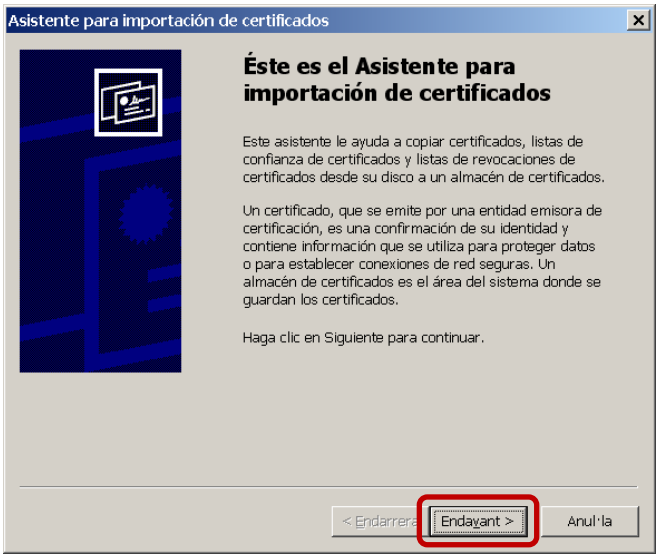
2.3 Importació/Exportació del certificat personal en programari

Importació

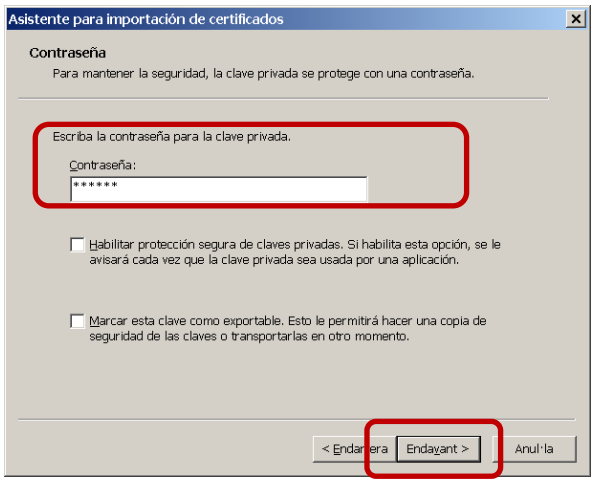
Els certificats digitals personals en software solen estar desats en fitxers amb extensió .CER o .CRT i en cas de portar també la clau privada el fitxer contenidor té per extensió .P12 o .PFX.

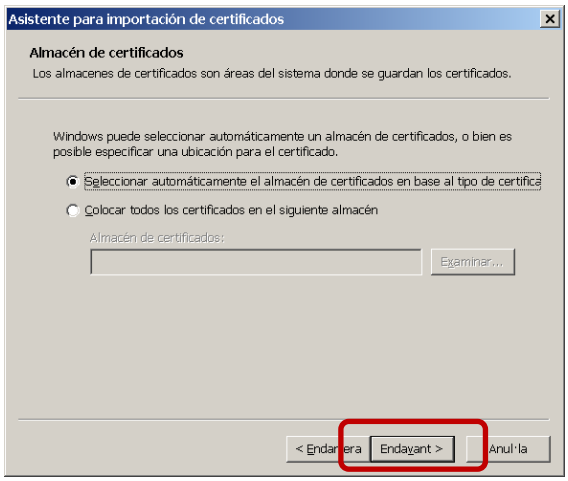
Per importar un certificat digital en Windows simplement s'ha de fer doble clic sobre el fitxer i l'aplicatiu el mostrarà o iniciarà l'assistent.





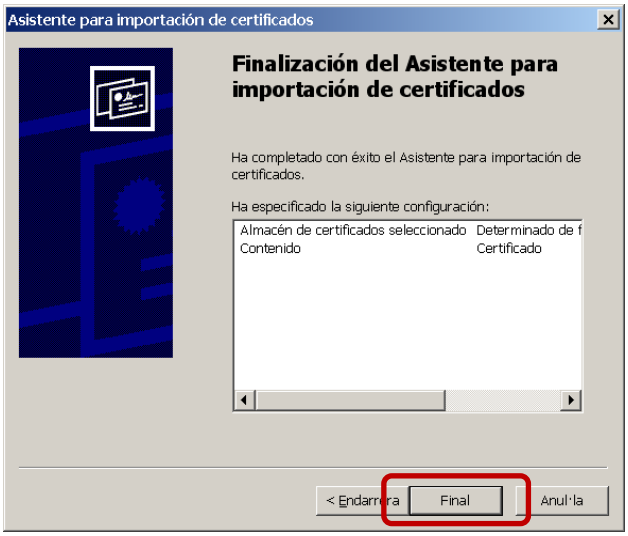
Tot seguit es pot visualitzar el certificat i clicant l'opció "**Instalar certificado**" s'inicia l'assistent, el qual permet incorporar el certificat al magatzem. En el cas d'importar un fitxer .P12 o .PFX es demana confirmació del fitxer. Després cal clicar "**Endavant**" per accedir a la finestra que sol·licita la paraula de pas que protegeix la clau privada:





Un cop introduïda la paraula de pas, l'assistent dóna l'opció de protegir l'ús del certificat amb una nova paraula de pas i/o permetre que, en un futur, s'exporti la clau. Es clica el botó "Endavant" i el sistema pregunta la ubicació a la qual volem posar.

Després cal clicar el botó "**Endavant**" i per acabar, el botó "**Final**".

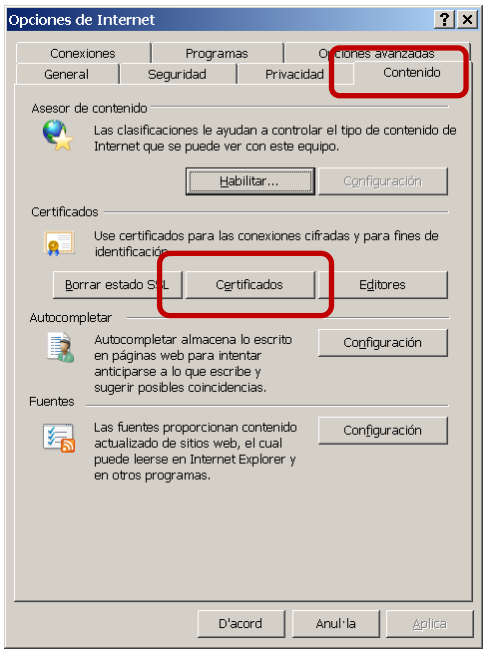


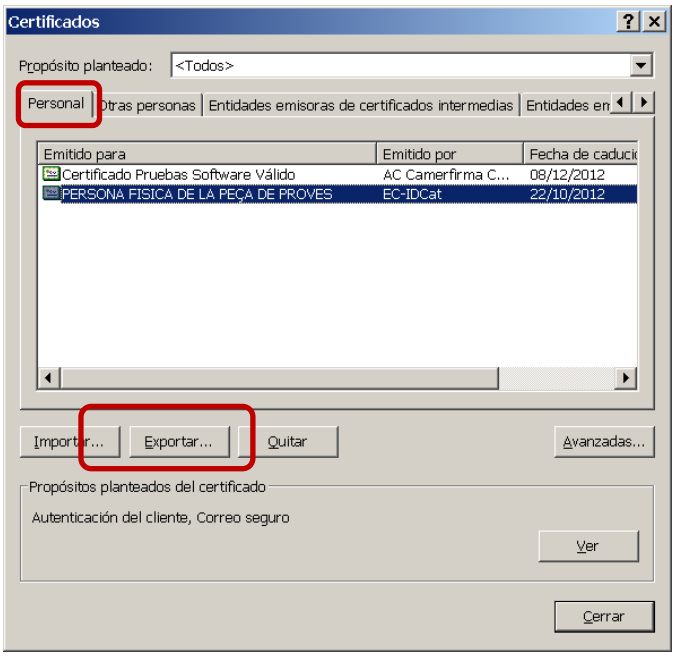
En finalitzar aquest procés, hi ha una finestra que informa de la importació amb èxit del certificat.

Exportació

Per exportar un certificat cal entrar, primer, en el magatzem/gestor de certificats de l'aplicatiu.

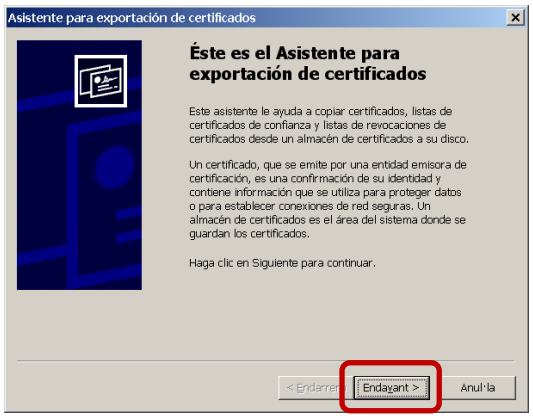
En cas d'Internet Explorer s'utilitza el gestor de certificats de Windows. Cal anar a Internet Explorer i després a "**Herramientas→ Opciones de Internet**"

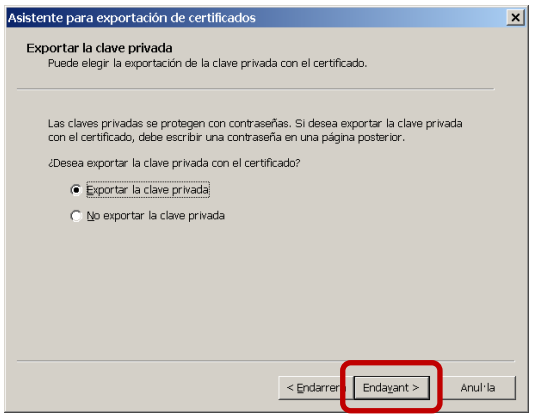




En la pestanya "**Contenido**" dins l' apartat de certificats, cal clicar el botó "**Certificados**".

En la pestanya "**Personal**" cal seleccionar el certificat a exportar i clicar el botó "**Exportar**" per tal que s'iniciï l'assistent que permet fer l'exportació.



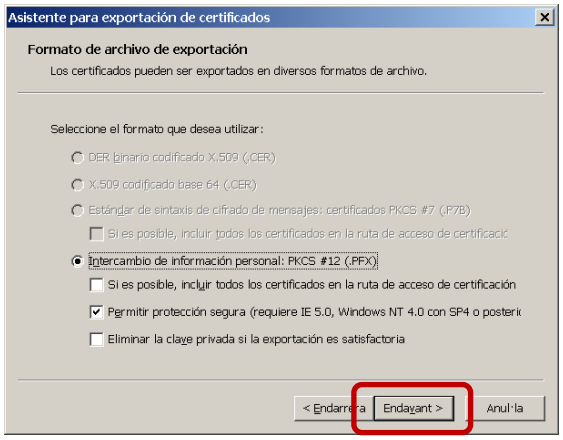


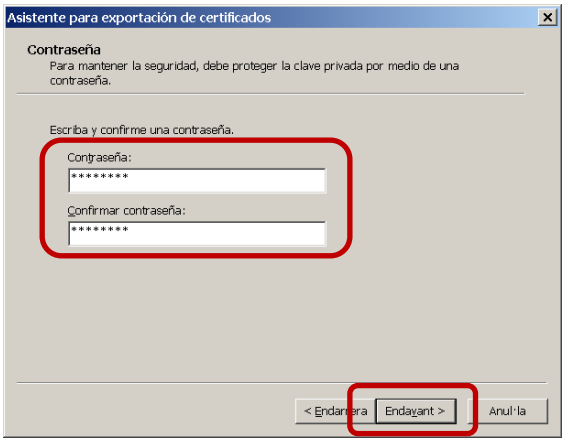
Un cop fet això, cal clicar el botó "**Endavant**" dues vegades.

Si el certificat seleccionat disposa de clau privada exportable dintre del gestor de certificats, l'assistent dóna l'opció d'exportar-la, tot creant un .P12, o bé exportant el certificat sol per generar un .CER o .CRT. Cal seleccionar permesa o que més interessi, i clicar després el botó "**Endavant**".

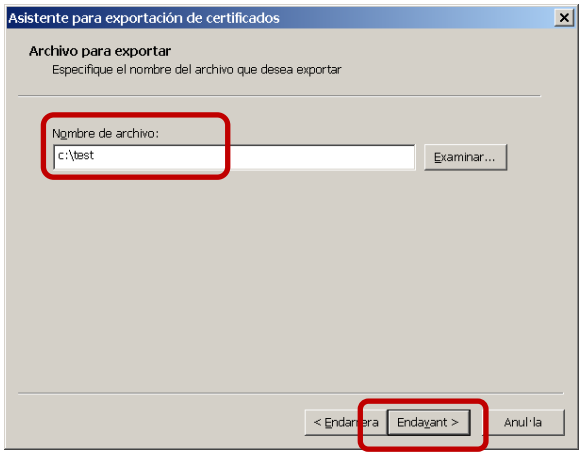
Exportació amb clau privada (P12)

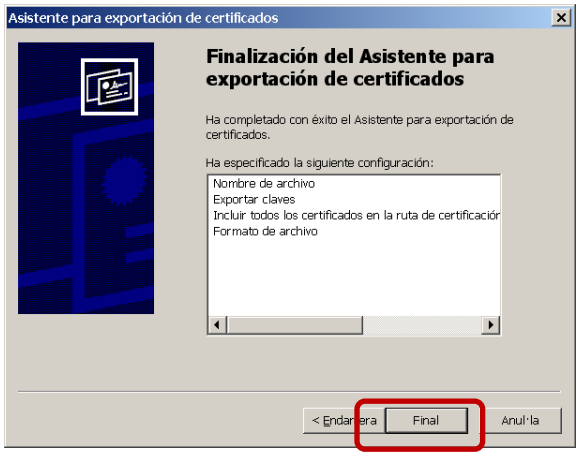
Si se selecciona l'opció d'exportació de la clau privada, preguntarà en quin format es vol desar. Llavors cal seleccionar "**Endavant**" i indicar la paraula de pas amb què es protegirà.





Després cal clicar el botó "**Endavant**".

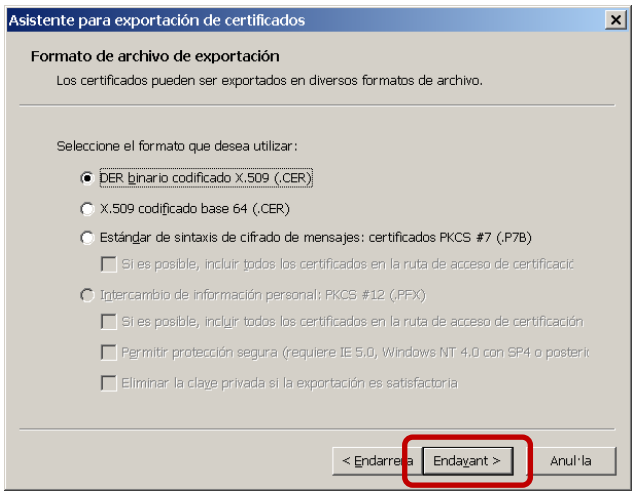




En aquest punt cal introduir el nom del fitxer i clicar el botó "**Endavant**". Un cop finalitzat el procediment, al clicar el botó "**Final**" apareixerà una finestra confirmant l'èxit de l'operació.

Exportació sense clau privada (CER)

En cas de no poder o no seleccionar la clau privada, la finestra de l'assistent per a exportar certificats pregunta quin format es vol utilitzar. Es deixa per defecte i es clica el botó "**Endavant**".



S'indica un nom de fitxer i es clica al botó "Endavant" seguint els mateixos passos que en l'exportació amb clau privada.

2.4 Autenticació amb certificats

L'autenticació amb certificats digitals es pot fer de dues direccions, per una banda es pot fer l'autenticació del servidor o portal al qual es connecta un usuari i, per l'altra, l'autenticació de l'usuari davant el portal. Així l'usuari sap del segur que està connectat a una web real i el portal sap quin usuari està connectat.

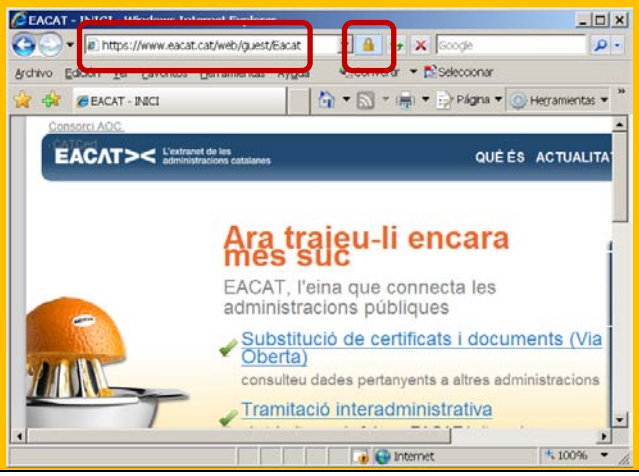
Autenticació de servidor/portal web

Aquest mecanisme està integrat totalment en qualsevol navegador i es pot apreciar normalment tenint en compte dos punts:

- Per un costat, l'adreça del web a visitar comença amb HTTP**S**://.....
- Per altra banda, el navegador activarà internament un protocol (anomenat SSL) i que farà aparèixer un cadenat que fa constar que és un web segur.

Exemple:

La web https://www.eacat.cat/web/guest/Eacat

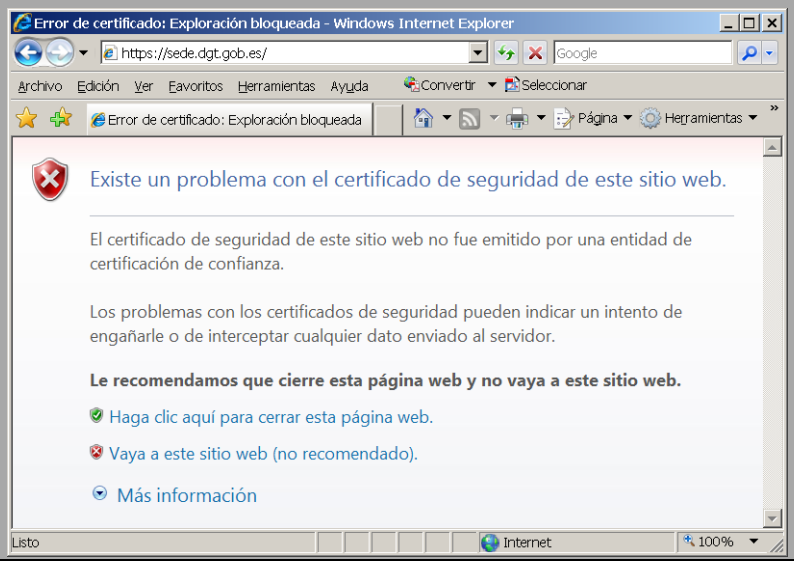


Nota:

Un error freqüent, dels que es poden apreciar, és quan l'aplicatiu no disposa de les claus públiques de l'emissor del certificat i el navegador no sap si confiar o no en el certificat en aquest cas i li pregunta a l'usuari que ha de fer. En cas de confiar en el certificat cal d'indicar que es faci una excepció o bé carregar les claus públiques del emissor.

Exemple:

https://sede.dgt.gob.es/



Autenticació d'usuari

L'autenticació amb certificat és un requisit que ha de demanar el portal web segur (SSL) per entrar a un enllaç o en seleccionar una acció, tot i que no tots els portals SSL estan preparats o demanen autenticació d'usuari.

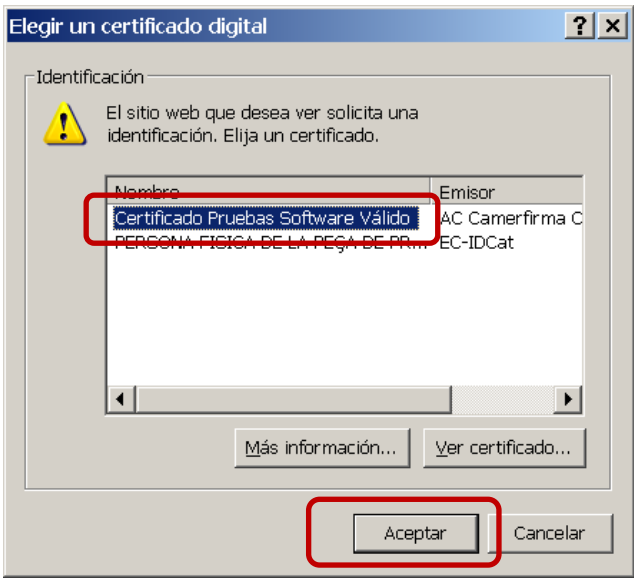
L'usuari només pot utilitzar els certificats que el gestor de certificats de l'aplicatiu indiqui que té disponibles. En cas de disposar el certificat en targeta o dispositiu USB, l'usuari els ha de connectar en l'equip i haver configurat prèviament els controladors/drivers, així com el gestor de certificats per poder accedir i fer ús dels certificats (veure **Guies ràpides** de la pàgina web de CATCert).

Nota:

Els portals web poden filtrar els certificats que tenim i només mostrar uns quants com a vàlids pel tràmit o per l'acció que volem fer – per exemple acceptar només els d'un prestador determinat o els d'una funcionalitat determinada –.

Exemple: El web de http://www.ingdirect.es per entrar amb certificat, només accepta els certificats d'e-DNI i encara que tinguem d'altres, no ens permet l'accés:

Quan l'usuari entri en un portal o enllaç web o cliqui i se li demani autenticació, apareix una finestra on ha de seleccionar el certificat que vol utilitzar –si en té varis disponibles -:



Un cop seleccionat el certificat a utilitzar, es clica al botó “Aceptar” i llavors el portal rebrà aquell certificat per la identificació.

Òbviament, no per identificar-nos en un portal amb un certificat seleccionat, la resposta del portal serà sempre la de benvinguda o l’esperada per l’usuari, ja que potser –encara que sigui un certificat vàlid – que aquell usuari no estigui identificat o el portal no en té dades (per exemple si entrem a la DGT – Direcció General de Trànsit – a l’opció de veure els punts disponibles del carnet de conduir i no tenim carnet de conduir, la resposta serà que no troba informació o a l’usuari).

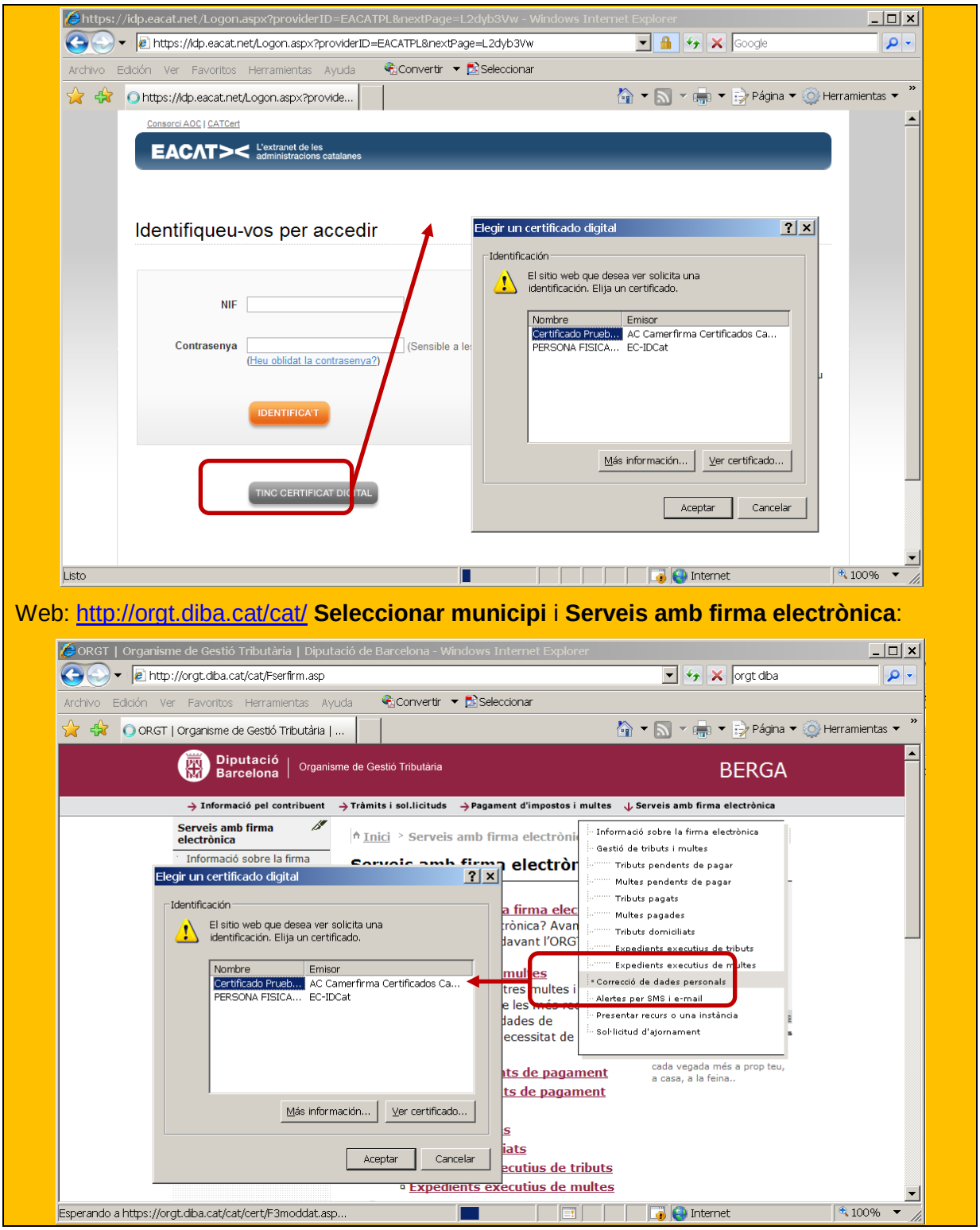
Important:

Un cop autenticats en un portal web, el navegador pot mantenir la informació del mateix mentre no es tanqui la finestra o sessió. Això fa que si tornem a entrar en la mateixa web no ens demanarà de nou quin certificat volem utilitzar per autenticar-nos i, per tant, ens hem d’assegurar de tancar la finestra al finalitzar la comunicació.

Exemple:

A continuació recollim dos webs d’exemple:

Web: https://www.eacat.cat/web/guest/Eacat Botó “**Accediu**” i botó “**Tinc certificat digital**”:



Web: http://orgt.diba.cat/cat/ **Seleccionar municipi** i **Serveis amb firma electrònica**:

3. Annex

3.1 Gestió de testimonis

Si es disposa de la targeta criptogràfica T-CAT, també s'ha d'aprendre el correcte ús de la Utilitat de gestió de testimonis.

Gestor del Testimoni

El gestor del testimoni és un programari per gestionar les targetes criptogràfiques i està associat al model del lector de targetes.

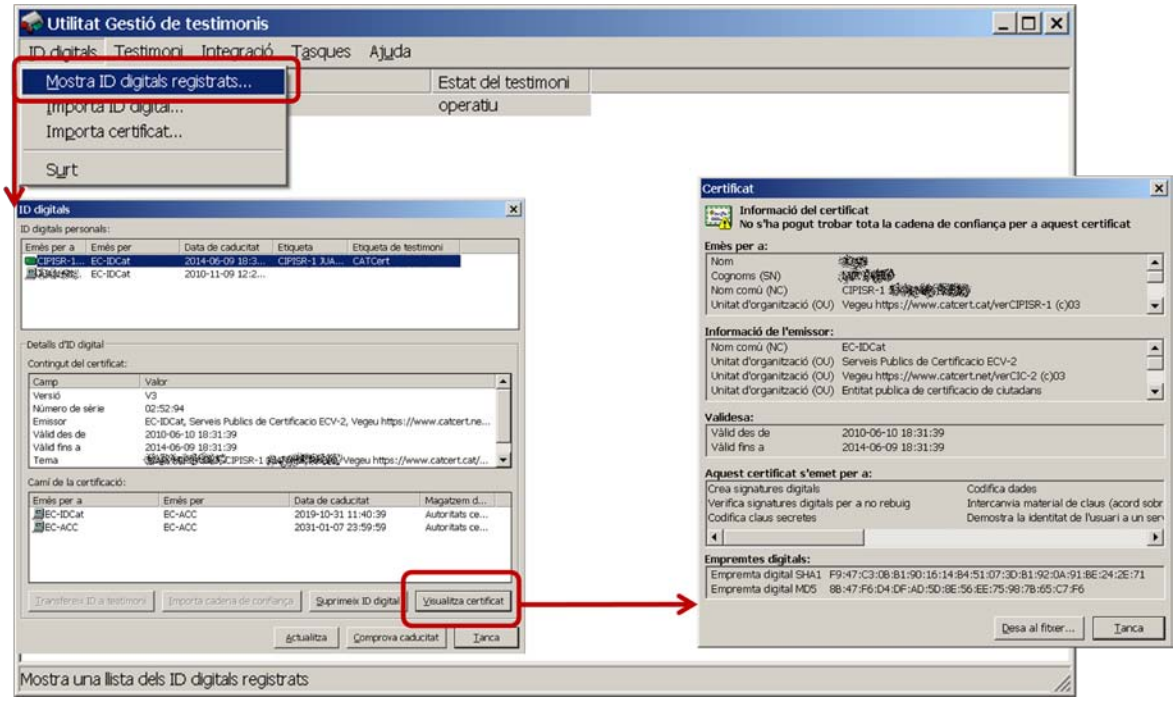
A continuació es recullen les operacions més comunes que podem fer amb el gestor de testimonis:

- Certificats de la targeta
- Canviar el NIP/PUK
- Desbloqueig del NIP

Per iniciar el gestor del testimoni normalment anirem per **Inici**-> **Programes** -> **CATCert** -> **Gestor de testimonis**, o bé, des d'un accés directe creat en l'escriptori.

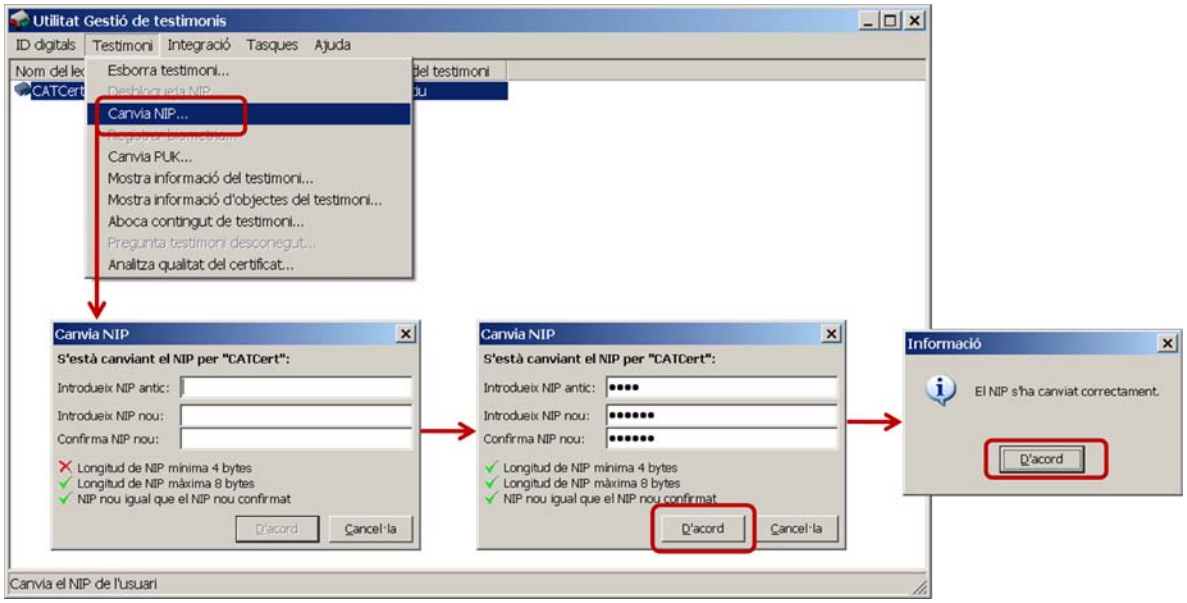
Certificats de la targeta

S'obre el menú "**ID digitals** -> **Mostra ID digitals registrats**". Es pot veure els certificats que hi ha a la targeta. Llavors, quan es selecciona un certificat es poden veure les dades del mateix i exportar-lo:



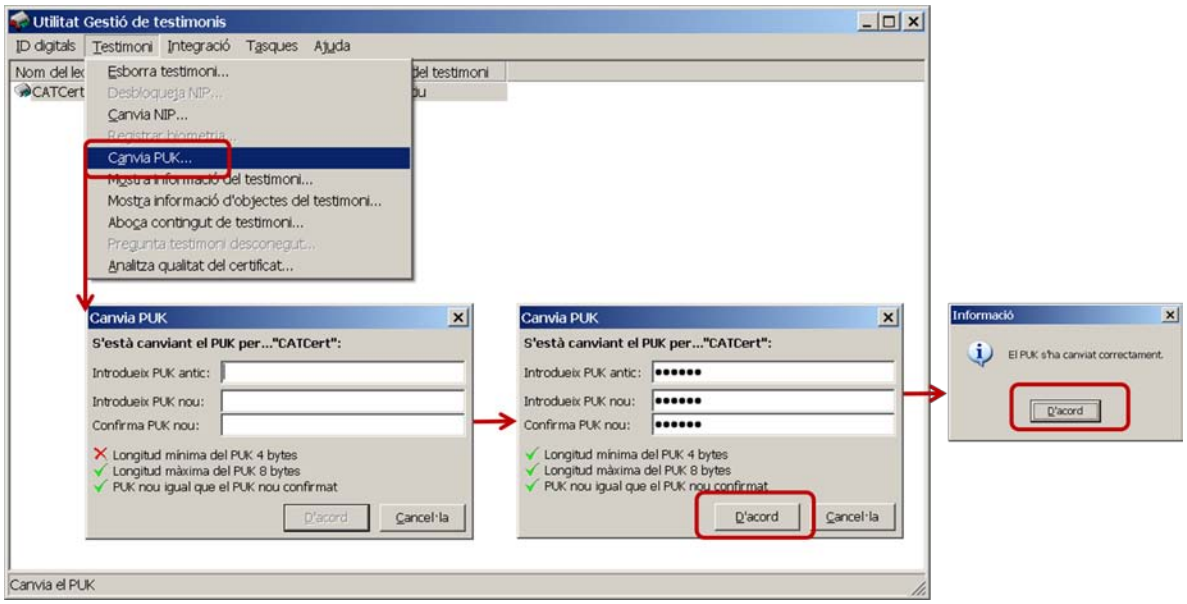
Canvi de NIP

Obrir l'opció de "**Testimoni** -> **Canvia NIP**". S'obre la finestra i s'indica el NIP – o PIN - (número d'identificació personal) antic i dos cops el NIP nou. Al clicar al botó "**D'acord**" es confirma que l'acció s'ha realitzat amb èxit:



Canvi de PUK

Obrir l'opció de "**Testimoni**" -> "**Canvia PUK**". S'obre la finestra i s'indica el PUK antic i dos cops el PUK nou. Es clica al botó "**D'acord**" i es confirma que l'acció s'ha realitzat amb èxit:



Desbloqueig de NIP

Obrir l'opció de "**Testimoni** -> **Desbloqueja NIP**" (aquesta opció només s'activa si el NIP està bloquejat). S'entra el PUK antic i dos cops un NIP nou. Es clica al botó "**D'acord**" i es confirma que l'acció s'ha realitzat amb èxit: