Agència Catalana de Certificació

Usos del certificat digital amb el navegador Google Chrome

Control documental

Estat formal	**Elaborat per:** CATCert	**Aprovat per:** Formació. CATCert
Data de creació	05/06/2010	
Control de versions	**Data:**	05/06/2010
	Descripció:	V2.0 Revisat
Nivell accés informació	pública	
Títol	Usos del certificat digital amb el navegador Google Chrome	
Fitxer	Usos del certificat digital amb Google Chrome v.2.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

1. Introducció

El present document té per objectiu descriure el procés de configuració del navegador Google Chrome 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 Google Chrome 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 Google Chrome** 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 magatzem 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.

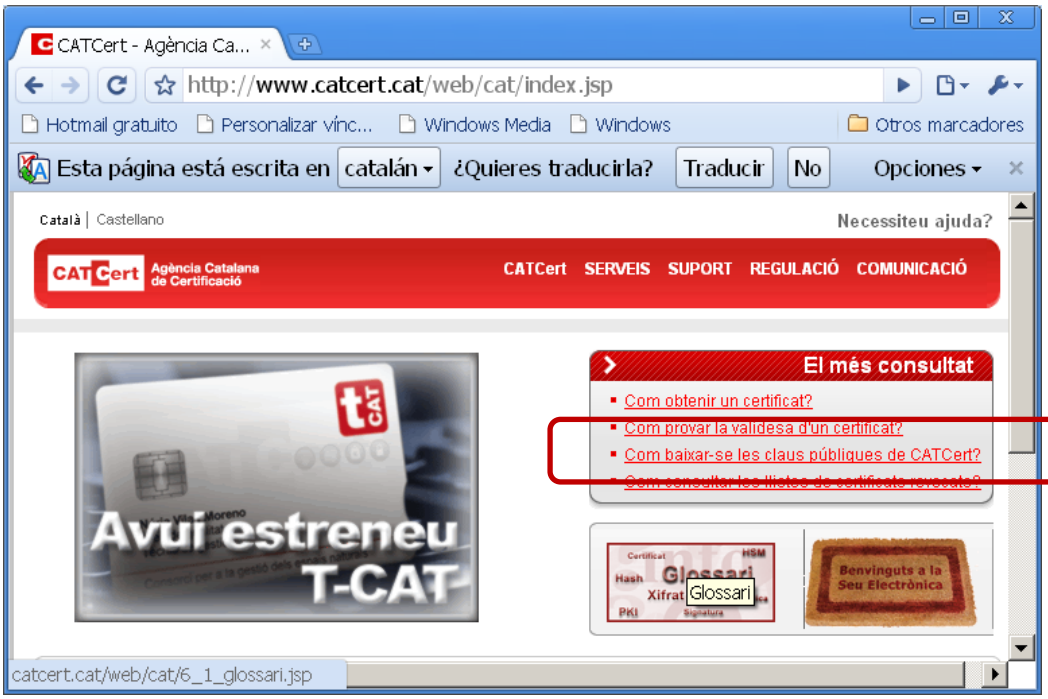


Figura 1

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

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

Baixarem les claus tal i com indica l'assistent.

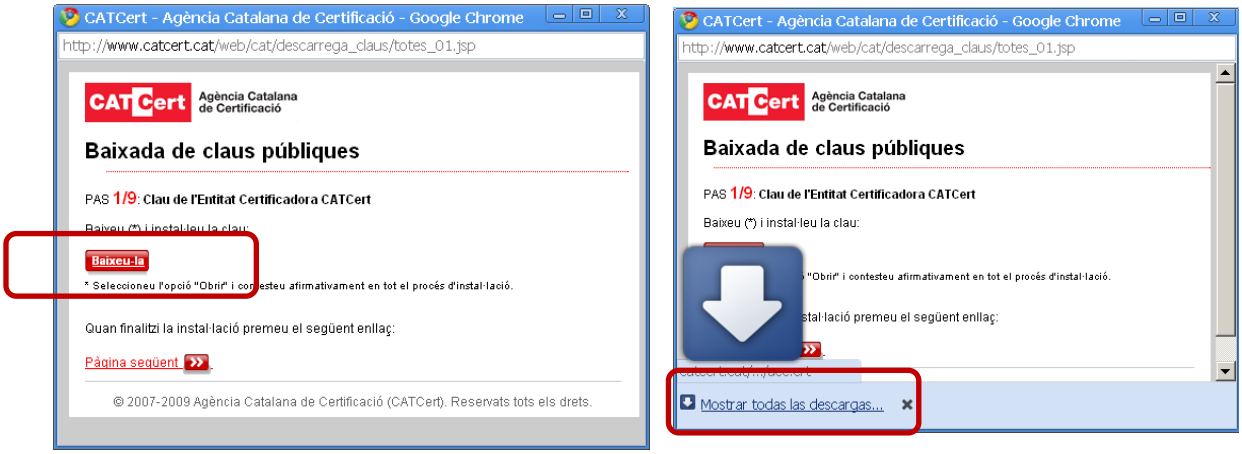


Figura 2

Al seleccionar el botó de “Baixeu-la”, s’apunta el fitxer en el gestor de descàrregues i anem a “Mostrar todas las descargas...” .

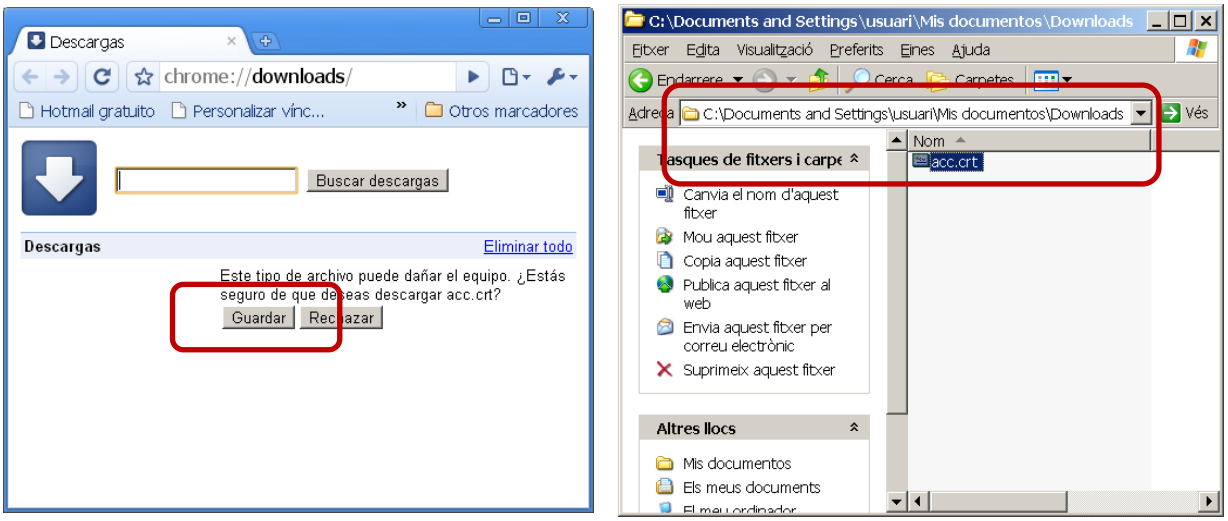


Figura 3

Es selecciona “Guardar”, i en el directori de descàrregues podem veure la clau pública. Fem doble-clic en el fitxer per obrir-lo.

2.2 Instal·lació dels certificats

Instal·lació de les claus públiques

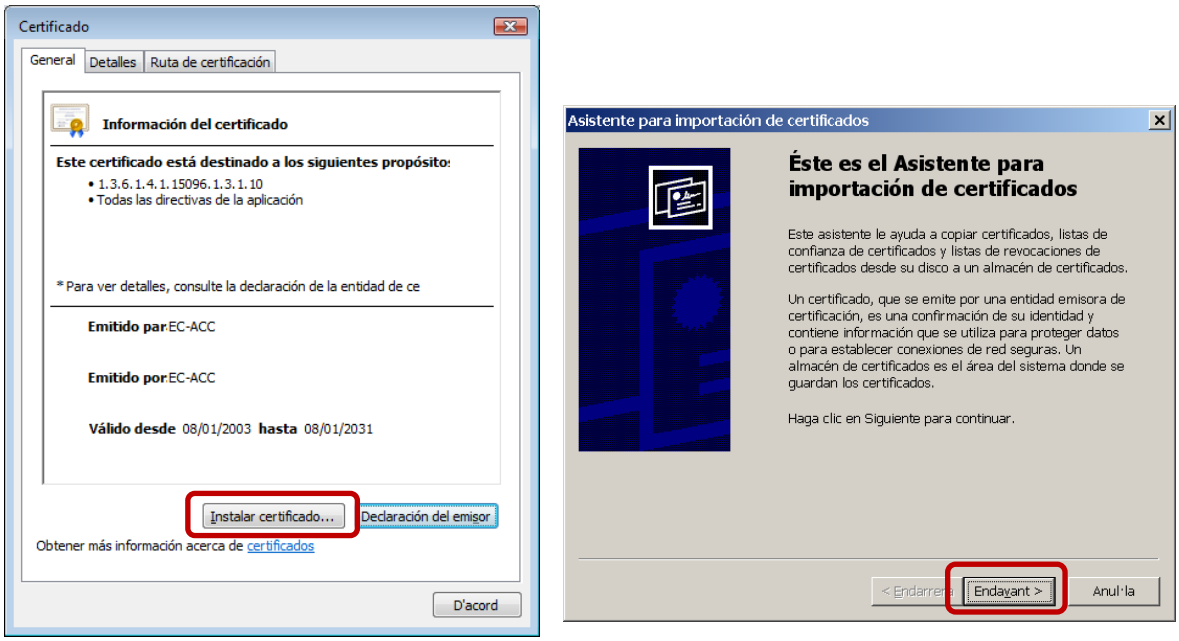


Figura 4

Ara es pot visualitzar el certificat que s'ha baixat i s'ha d'instal·lar, fent clic en l'opció "Instalar certificado" per iniciar l'assistent.

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

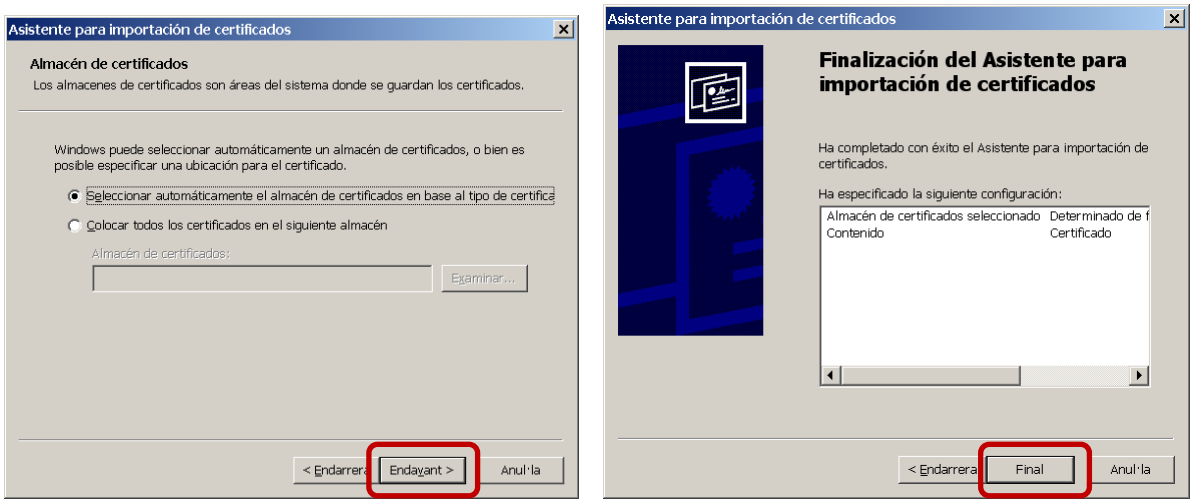


Figura 5

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

En acabar aquest procés, hi ha una finestra que informa de la importació amb èxit del certificat i s'ha de repetir el procediment pels altres certificats que hi ha a la web, fent clic en l'opció "Pàgina següent".

Figura 6

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 (Internet Explorer, Mozilla, Adobe...) i veure el conjunt de certificats de la jerarquia de CATCert.

En cas de Google Chrome utilitza el gestor de certificats de Windows. Obrim el Google Chrome i anem a la pestanya de configuració "Opciones"

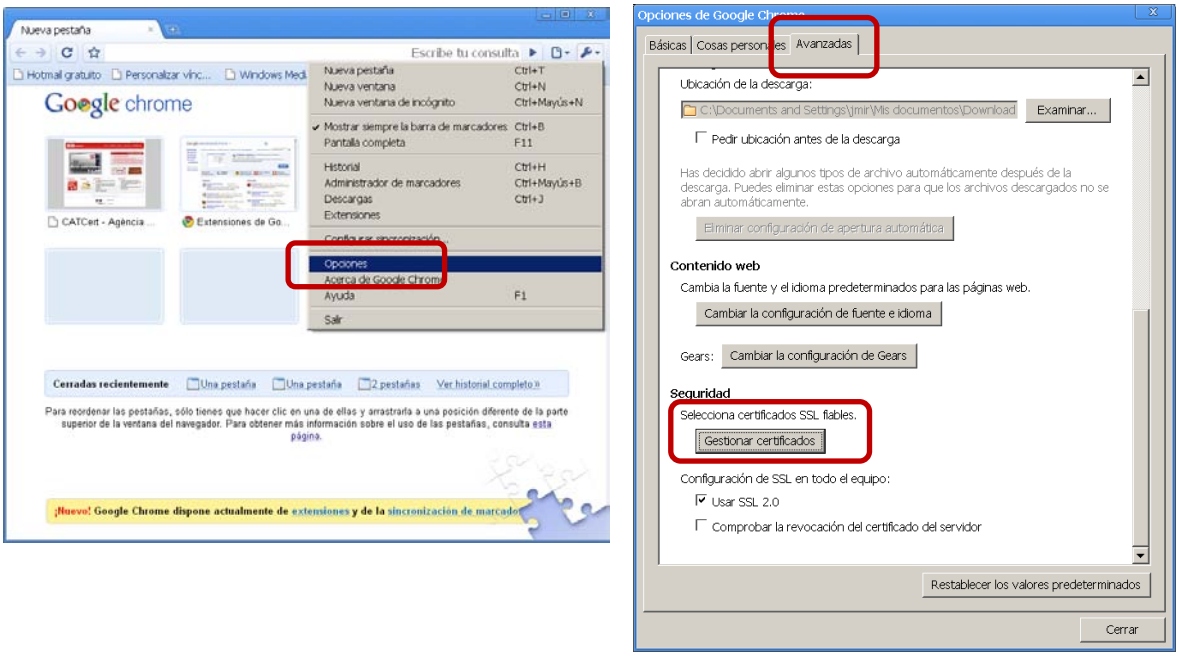


Figura 7

En la pestanya de “Avanzadas” hi ha un apartat de certificats. Es fa clic en el botó “Gestionar certificados”.

En el cas de Google Chrome s’han de fer dos verificacions en llocs diferents ja que es separa la clau pública arrel de CATCert (EC-ACC) de les intermèdies. La clau arrel l’hem de trobar a la pestanya “Entidades emisoras raíz de confianza”.

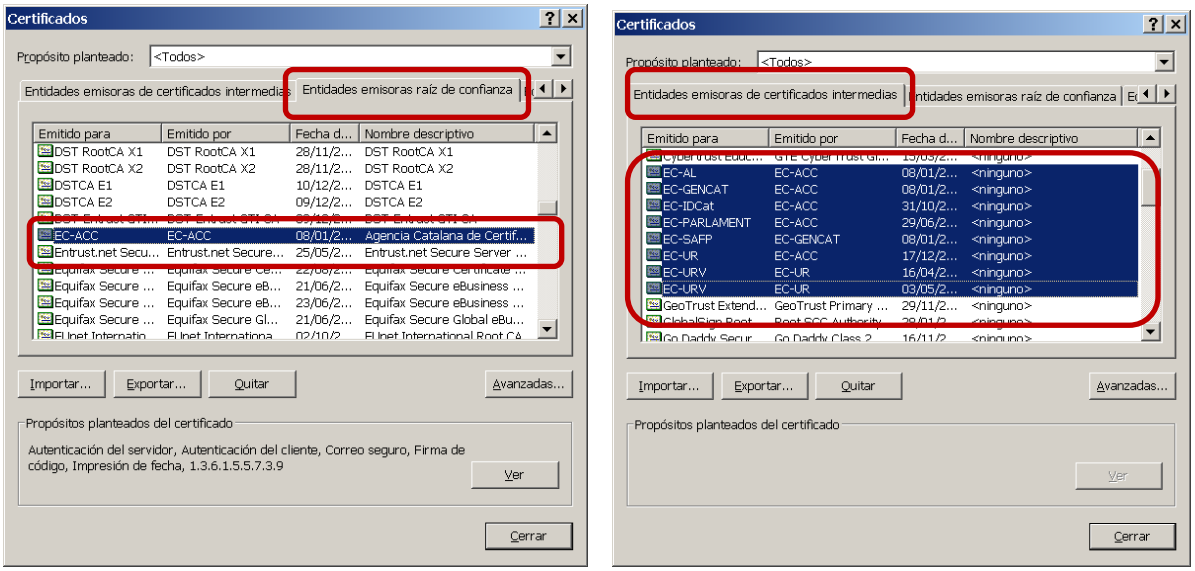


Figura 8

Les intermèdies es poden veure a la pestanya “Entidades emisoras de certificados intermedias”, i en aquest cas corresponen a la jerarquia de CATCert (EC-idCAT, EC-....).

2.3 Sol·licitar un certificat idCAT

El certificat idCAT és un certificat digital personal que emet de forma gratuïta CATCert a tot ciutadà que en 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

2.4 Importar/Exportar el certificats personals en software

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 ens el mostrarà o iniciarà l’assistent.

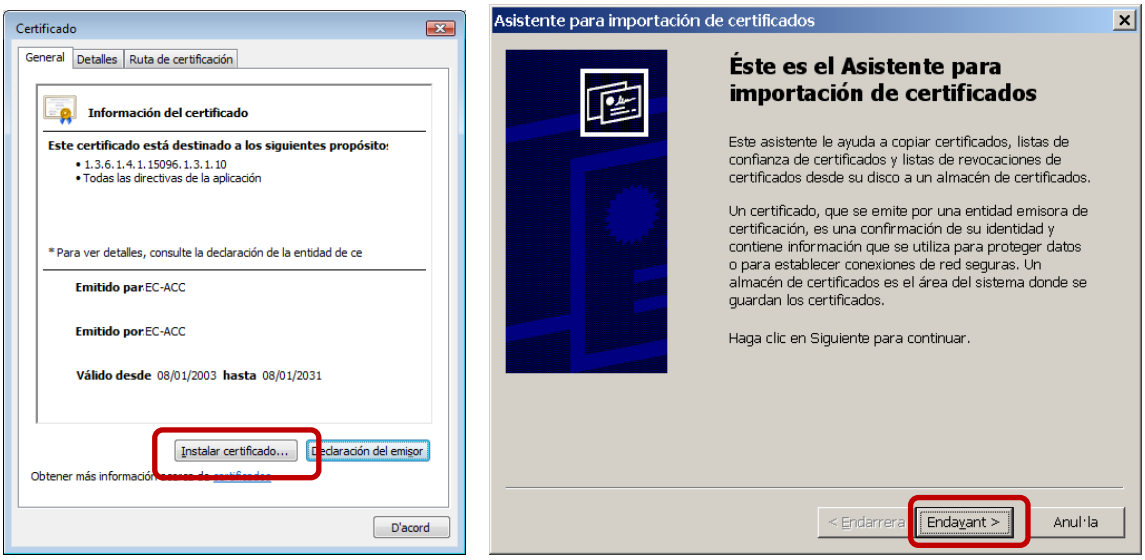


Figura 9

Ara es pot visualitzar el certificat i es fa clic en l'opció "Instalar certificado" per iniciar l'assistent.

Aquest assistent ens ajuda a la incorporació del certificat al magatzem. En el cas d'importar un fitxer .P12 o .PFX ens demana confirmació del fitxer i fem clic en "Endavant" per després sol·licitar la paraula de pas que protegeix la clau privada.

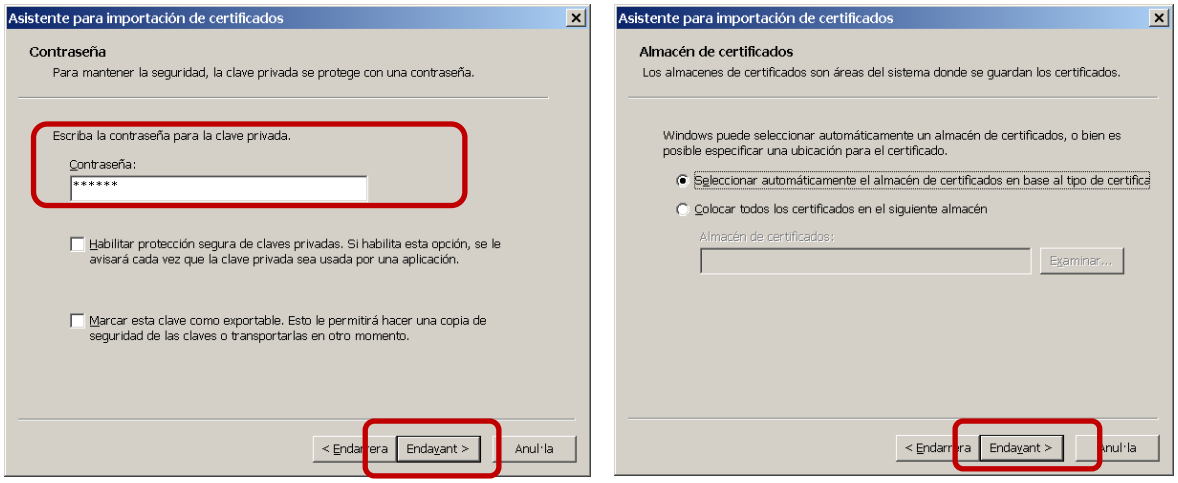


Figura 10

En aquest cas s'ha d'introduir la paraula de pas. L'assistent també dóna l'opció de protegir-ne l'ús amb una nova paraula de pas i/o si volem permetre que en un futur s'exporti la clau. Es fa clic en el botó "Endavant" i el sistema pregunta en quina ubicació el volem posar.

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

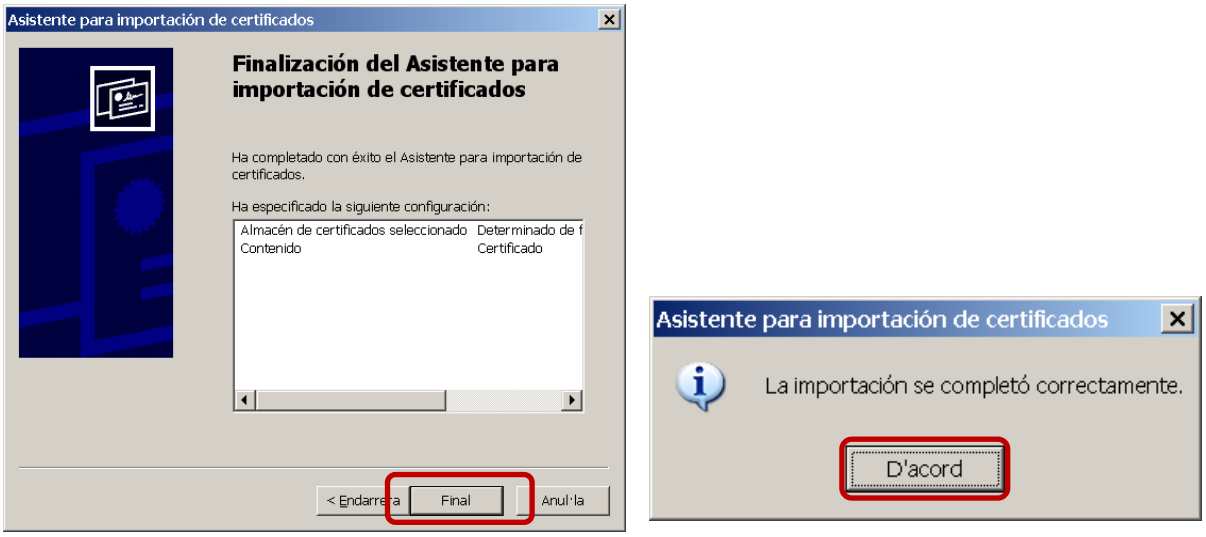


Figura 11

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

Exportació

Per fer exportacions s'ha d'entrar primer en el magatzem/gestor de certificats de l'aplicatiu.

En cas de Google Chrome utilitza el gestor de certificats de Windows. Obrim el Google Chrome i anem a la pestanya de configuració "Opciones"

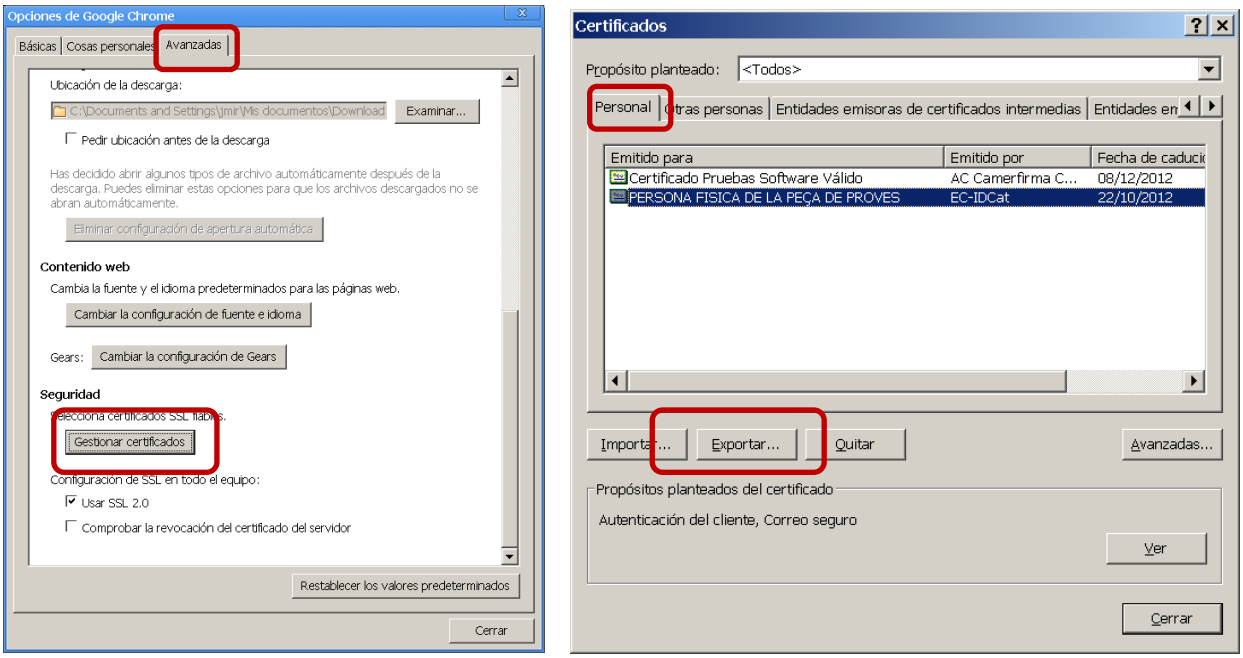


Figura 12

En la pestanya de “Avanzadas” hi ha un apartat de certificats. Es fa clic en el botó “Gestionar certificados”.

En la pestanya de “Personal” seleccionem el certificat a exportar i fem clic a “Exportar”.

S’inicia l’assistent per fer l’exportació.

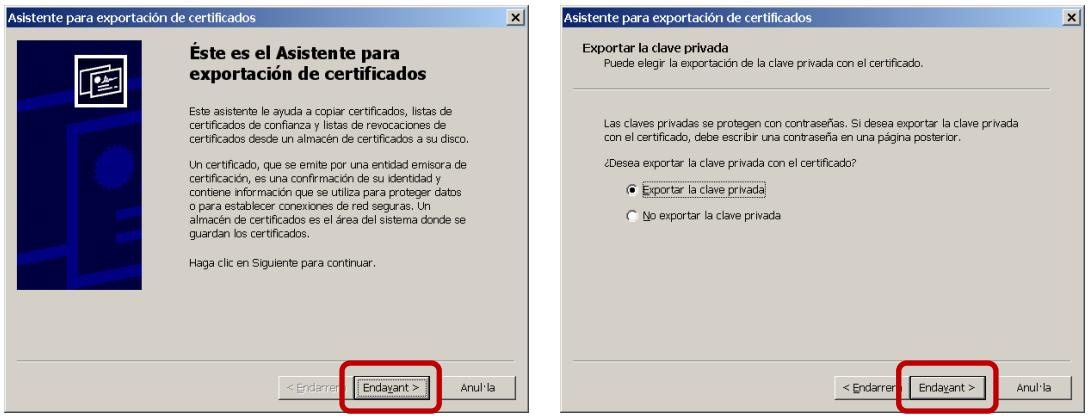


Figura 13

Fem clic en “Endavant”.

Si el certificat seleccionat disposa de clau privada exportable dintre del gestor de certificats, l’assistent ens dóna l’opció d’exportar-la (tot creant un .P12) o bé exportant el certificat sol (per generar un .CER o .CRT). Seleccionem l’opció que ens deixi o que ens interessi i fem clic en “Endavant”.

Exportació amb clau privada (P12)

Si es selecciona l’exportació de la clau privada, preguntarà en quin format es vol desar. Es selecciona “Endavant” i s’indica dos cops la paraula de pas amb que es protegirà.

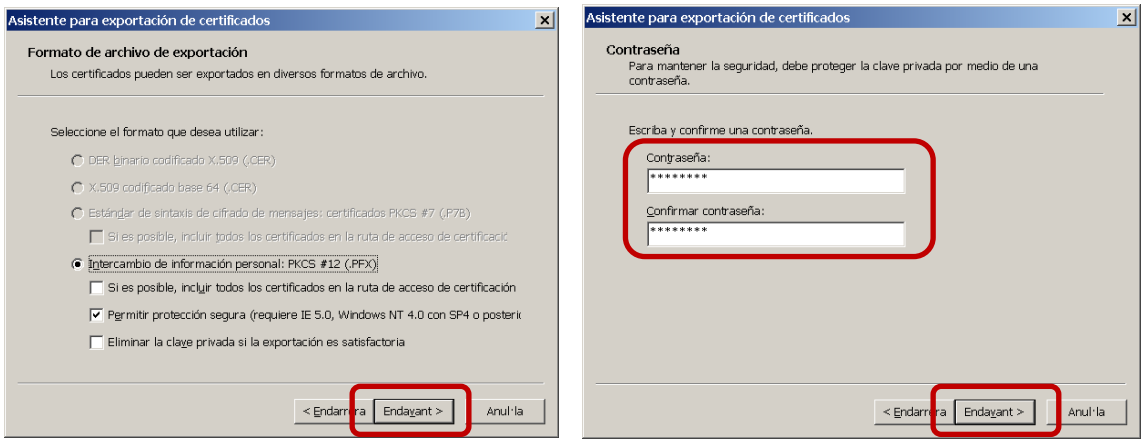


Figura 14

Es fa clic en “Endavant”

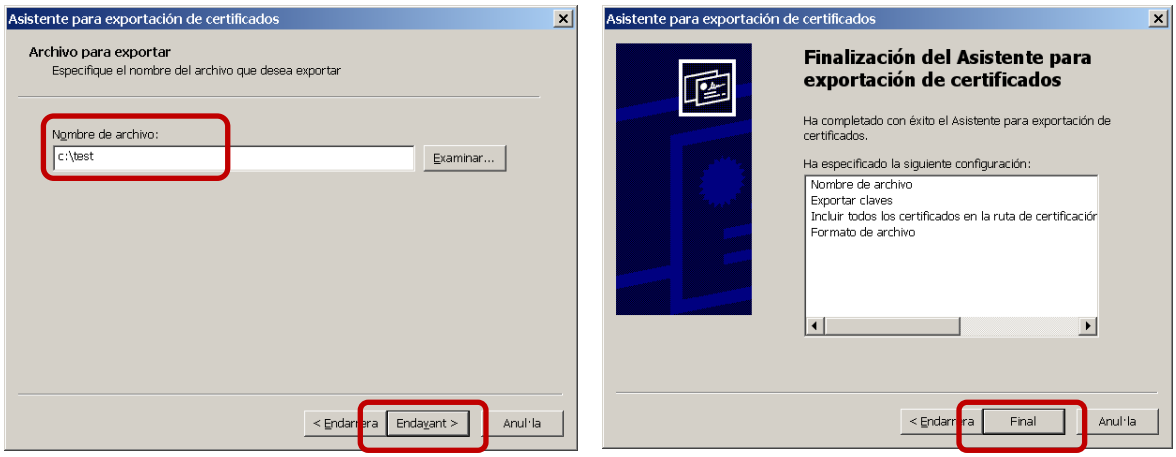


Figura 15

S'introdueix el nom del fitxer i es fa clic en "Endavant". Finalitza el procediment al fer clic en "Final" i una finestra confirma l'èxit de l'operació.

Exportació sense clau privada (CER)

En cas de no poder o no seleccionar la clau privada, pregunta quin format es vol utilitzar. Es deixa per defecte i es fa clic en "Endavant".

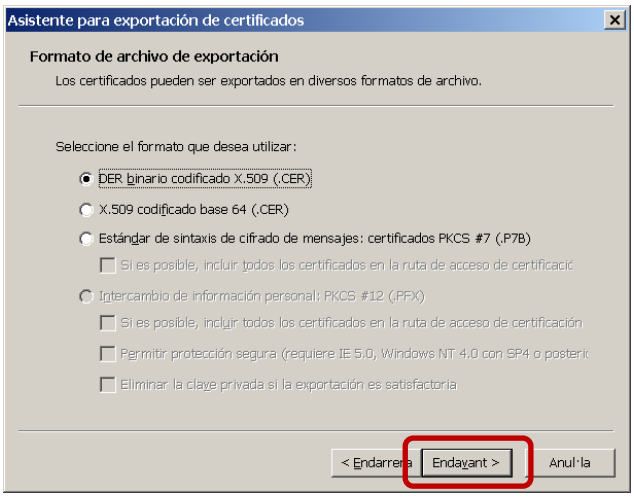


Figura 16

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

2.5 Autenticació amb certificats

L'autenticació amb certificats digitals es pot fer en dos vies, per una banda l'autenticació del servidor o portal on es connecta un usuari, i l'autenticació de l'usuari davant el portal.

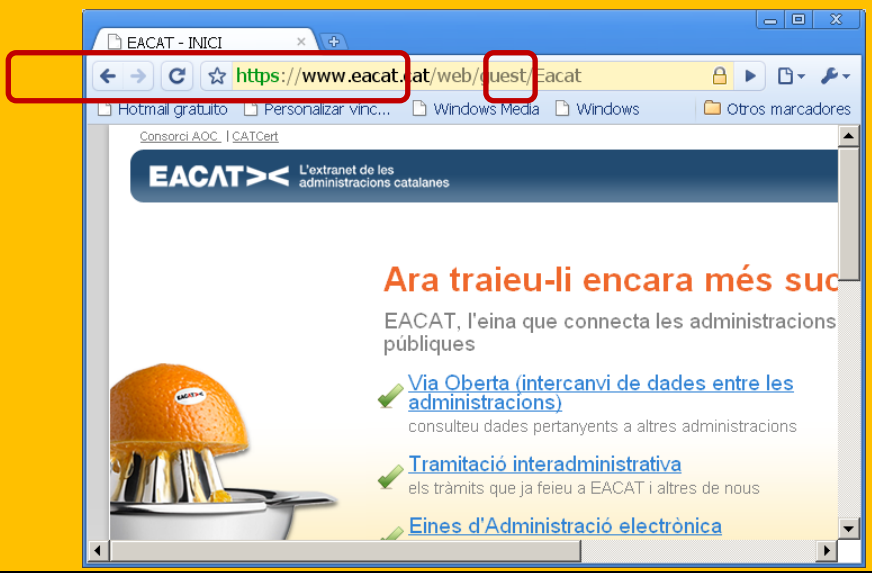
Autenticació de servidor/portal web

Aquest mecanisme està integrat totalment en qualsevol navegador i es pot apreciar normalment amb dues formes:

- Per un costat l'adreça de la web a visitar comença amb HTTP**S**://.....
- Per altre banda el navegador activarà internament un protocol (anomenat SSL) i fa aparèixer un cadenat en referència a que és una web segura.

Exemple:

Entreu a la web https://www.eacat.cat/web/guest/Eacat

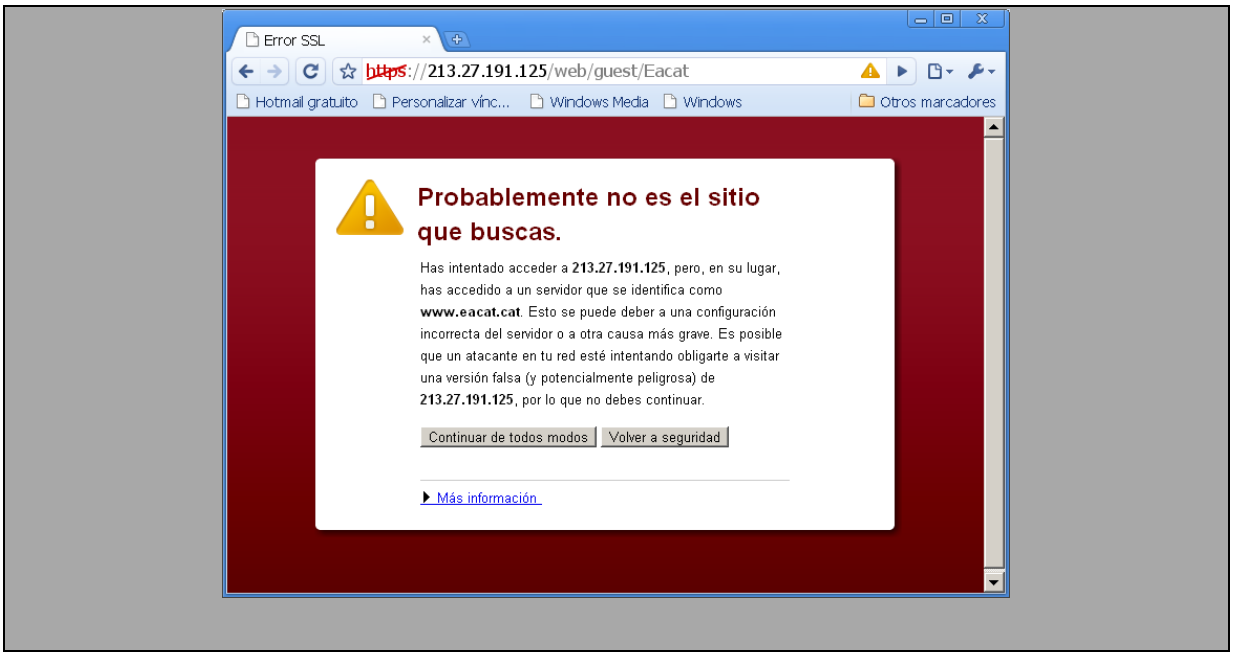


Nota:

Un error freqüent que es pot apreciar és quan l'aplicatiu no disposa de les claus públiques del emissor del certificat i per tant el navegador no sap si confiar o no en el certificat o si el nom (adreça url) del portal no coincideix amb el del certificat, el navegador li pregunta a l'usuari que ha de fer. El cas de confiar en el certificat hem d'indicar que es faci una excepció o bé carregar les claus públiques del emissor.

Exemple:

https://213.27.191.125/web/guest/Eacat



Autenticació d'usuari

L'autenticació amb certificat per part de l'usuari és un requeriment que ha de demanar el portal web segur (SSL) a l'entrar en un enllaç o al seleccionar una acció. 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 d'ús 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: La web de http://www.ingdirect.es per entrar amb certificat, només accepta els certificats de e-DNI i encara que tinguem d'altres, no ens permet l'accés.

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

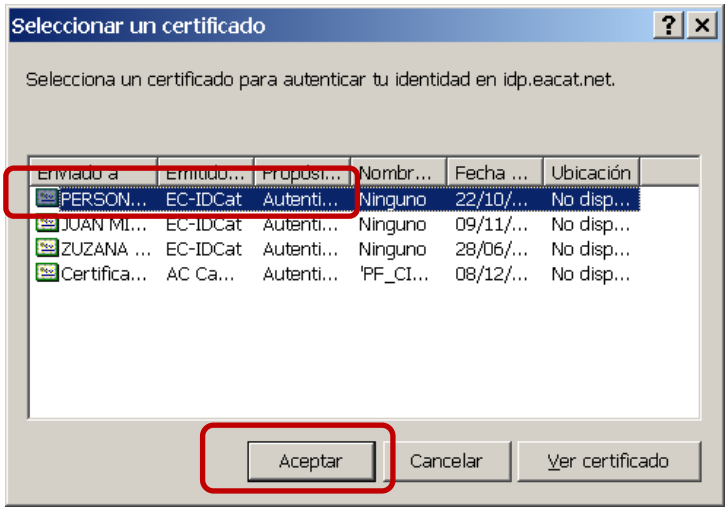


Figura 17

Un cop seleccionat el certificat a utilitzar, es fa clic en "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 – aquell usuari no està 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).

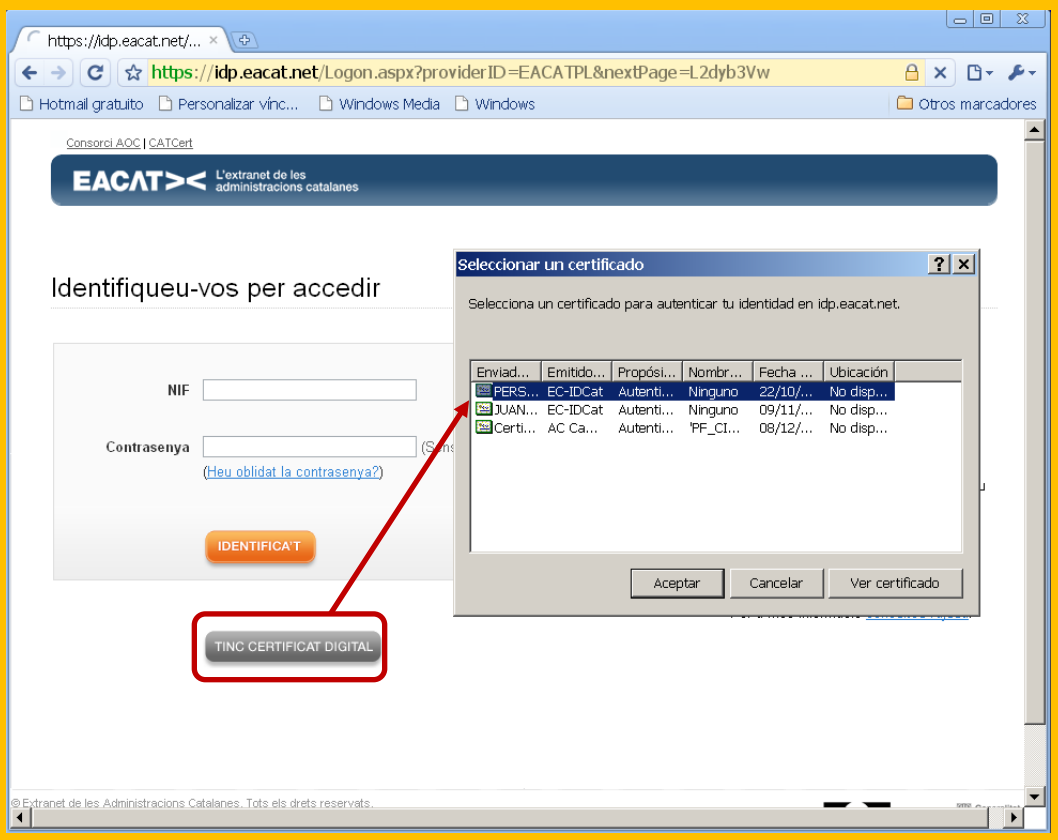
Important:

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.

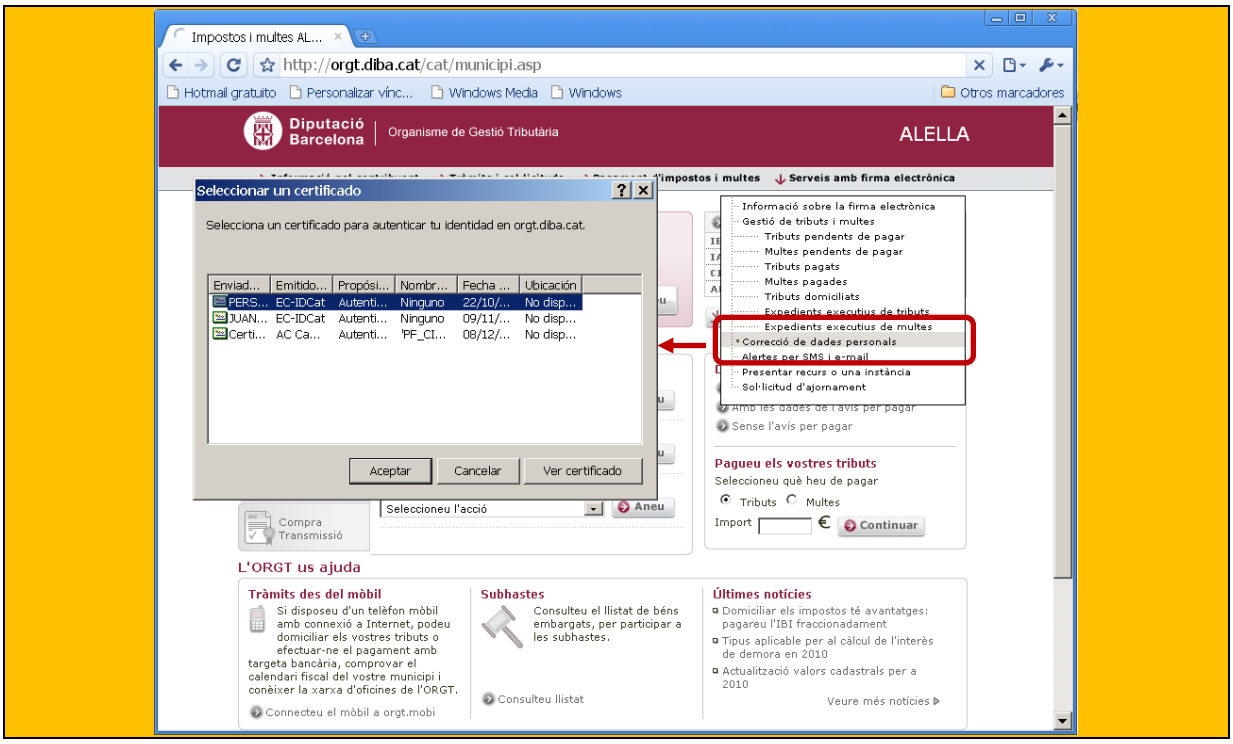
Exemple:

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 Senyals d'advertència

Els senyals que s'indiquen a continuació adverteixen de possibles perills en un lloc web:

- L'advertència "Probablement no és el lloc que buscaves" apareix abans que Google Chrome carregui la pàgina web si l'adreça que s'inclou en el certificat no coincideix amb l'adreça real del lloc web.
- L'advertència "El certificat de seguretat del lloc no és de confiança" apareix si el certificat d'un lloc no l'ha generat una entitat de confiança.
- L'advertència "El certificat de seguretat del lloc ha caducat" o "El certificat de seguretat del servidor encara no és vàlid" apareixen si Google Chrome no disposa d'informació actualitzada sobre la identitat d'un lloc web.
- L'advertència "El certificat de seguretat del servidor està revocat" apareix si el verificador extern del certificat indica que aquest no és vàlid.
- Si es detecta contingut mixt en una pàgina web segura, apareix una icona d'alerta al final la barra d'adreces. Es pot fer clic a la icona per obrir el quadre de diàleg "Informació de seguretat" i accedir a informació addicional. Per obtenir més informació sobre el certificat que ha presentat el lloc web, fes clic al botó **Informació del certificat.**
- La detecció de *phishing* i de codis maliciosos està habilitada per defecte.
    - Si Google Chrome detecta que accedeixes a un lloc web que sembla operar de manera fraudulenta, veuràs l'advertència "S'ha detectat phishing".

- Si detecta que el lloc web de destinació inclou programari enganyós que pretén robar informació personal de l'usuari o utilitzar l'equip per dur a terme accions contra la seva voluntat, es mostra el missatge "Advertència: visitar aquest lloc pot malmetre el teu equip".

3.2 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 asociat al model del lector de targetes.

A continuació es recull 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, per que es tingui un accés directe creat en l'escriptori.

Certificats de la targeta

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

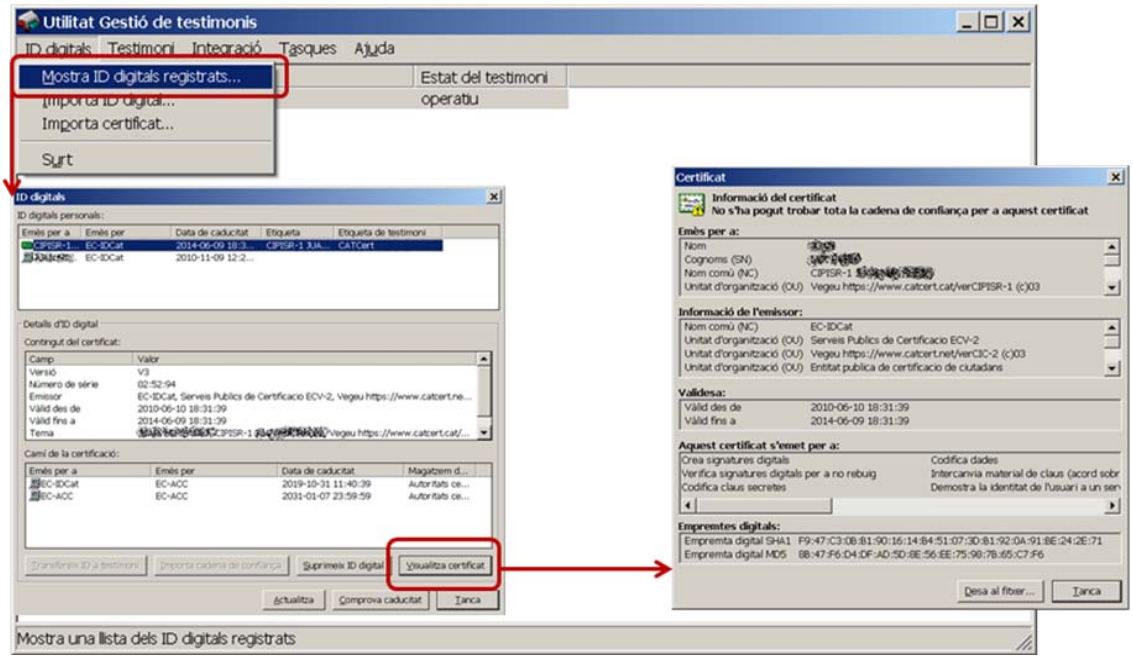


Figura 18

Canvi de NIP

Obrir l'opció de "Testimoni -> Canvia NIP". S'obre la finestra i s'indica el NIP (número d'identificació personal) antic i dos cops el NIP nou. Al fer clic en "D'acord" es confirma que l'acció s'ha realitzat amb èxit.

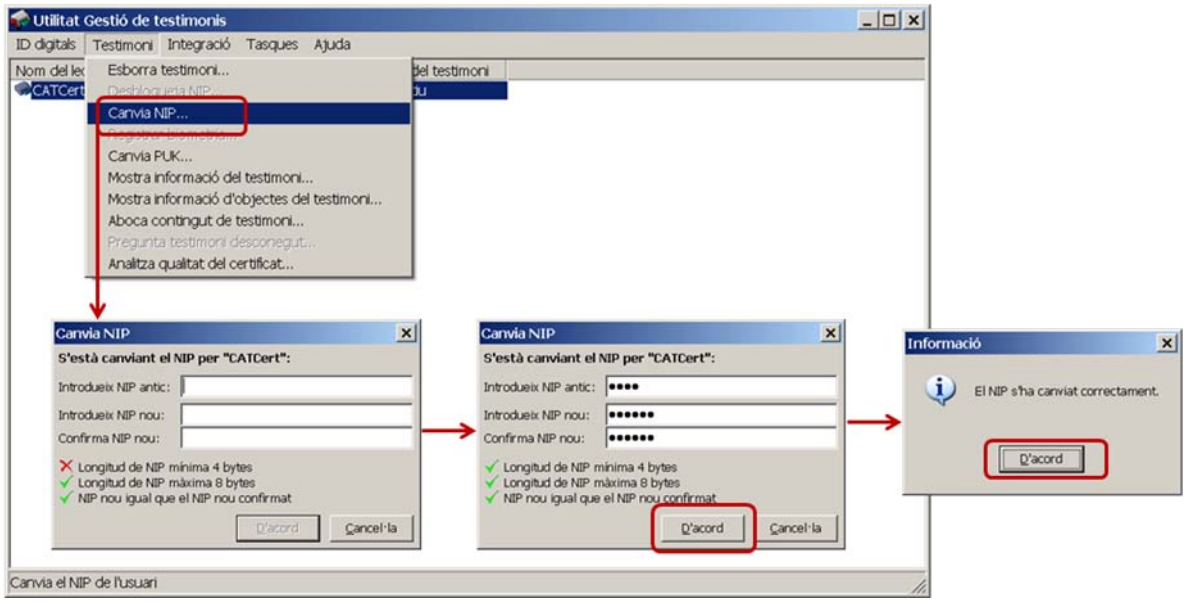


Figura 19

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 fa clic en "D'acord" i es confirma que l'acció s'ha realitzat amb èxit.

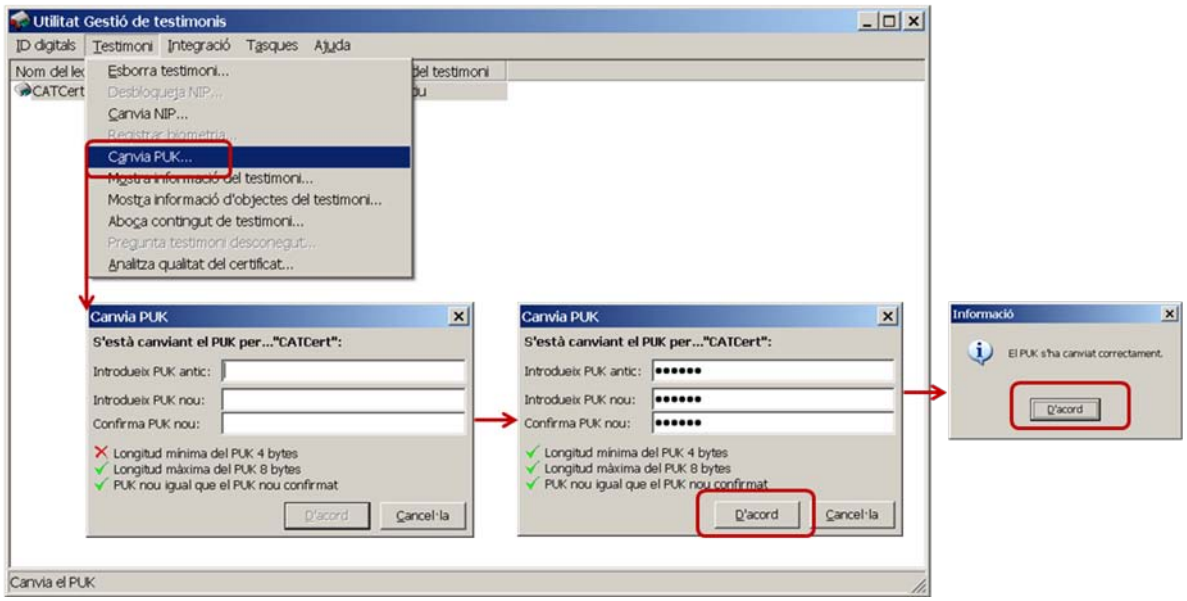


Figura 20

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 fa clic en "D'acord" i es confirma que l'acció s'ha realitzat amb èxit.

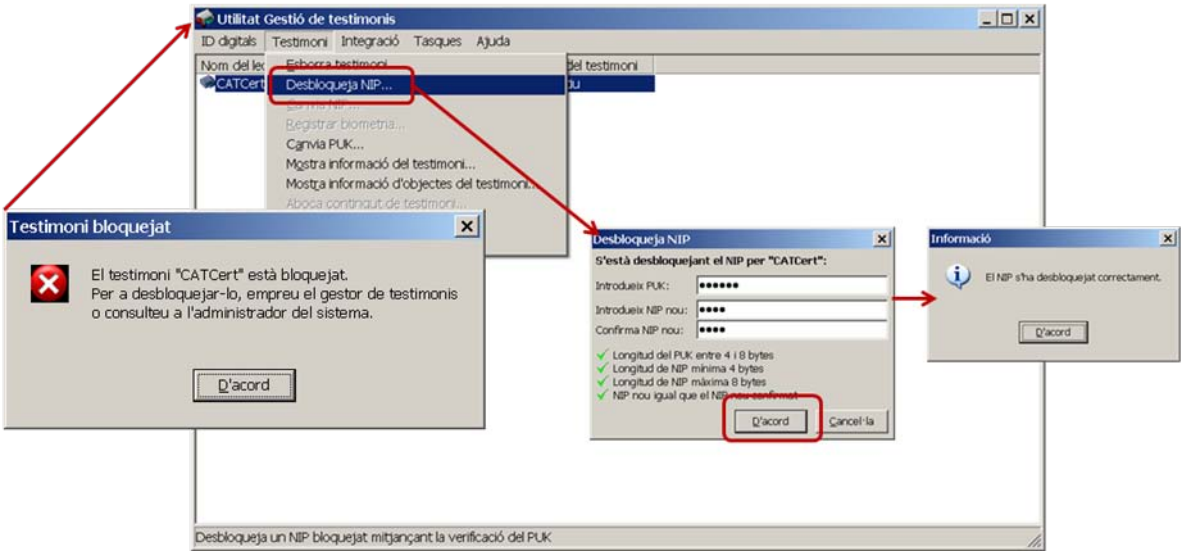


Figura 21