

# Manual de gestió de certificats GICAR

**Data:** Juliol 2009

**Autor:**



## ÍNDEX

---

<b>ÍNDEX.....</b>	<b>2</b>
<b>1. INTRODUCCIÓ .....</b>	<b>3</b>
<b>2. INSTAL·LACIÓ DE CERTIFICATS A L'INTERNET EXPLORER ..</b>	<b>4</b>
<b>3. INSTAL·LACIÓ DE CERTIFICATS AL MOZILLA FIREFOX.....</b>	<b>9</b>
3.1 Instal·lació manual de claus públiques .....	10
3.2 Instal·lació manual dels certificats personals.....	12
3.3 Configuració del dispositiu de seguretat .....	14
<b>4. INSTAL·LACIÓ DES DE LA WEB DE CATCERT .....</b>	<b>16</b>
4.1 Claus públiques .....	16
4.2 Software lector de targetes criptogràfiques.....	17
<b>5. COMPROVAR QUE GICAR ADMET EL CERTIFICAT .....</b>	<b>19</b>
<b>6. POSSIBLES PROBLEMES AMB LA LECTURA DELS CERTIFICATS .....</b>	<b>20</b>



## 1. INTRODUCCIÓ

---

El present document té com a objectiu descriure el procés de configuració dels navegadors d'internet (tant per Internet Explorer com per Mozilla Firefox) per tal de poder accedir als recursos protegits amb GICAR mitjançant l'ús de certificats digitals.

En l'actualitat, GICAR admet certificats de les entitats:

- Agència Catalana de Certificació (CatCert): (T-Cat i Clauers):
  - EC-SAFP.
  - EC-AL
  - EC-UR
  - EC-Parlament
  - EC-IdCat
- Camerfirma
- DNI-E
- Firmaprofesional
- Autoridad de Certificación de la Abogacía
- FNMT-Ceres

Com que les claus públiques de les entitats certificadores en què es confia no venen precarregades en els navegadors, cal fer la seva instal·lació manualment. Aquestes claus són necessàries per a verificar que tots els certificats que arriben als nostres equips informàtics i que utilitzarem per autenticar-nos han estat emesos per alguna de les autoritats de certificació de la jerarquia d'entitats que accepta GICAR.

També es descriurà el procés de configuració dels navegadors per a carregar en ells els certificats digitals que ens identificaran en els formularis d'autenticació, de manera que siguin plenament operatius de cara a la seva utilització en el nostre navegador.

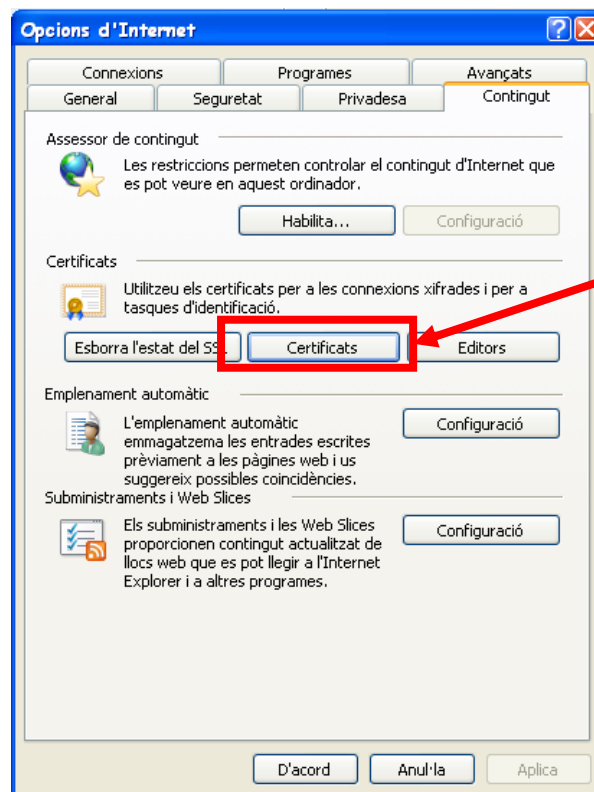
Per altra banda, també s'indicarà quin procediment s'ha de seguir per a instal·lar el lector de targetes per tal que l'usuari pugui fer servir per a autenticar-se certificats del tipus targeta (T-Cat, DNI-E, etc).

## 2. INSTAL·LACIÓ DE CERTIFICATS A L'INTERNET EXPLORER

En aquest apartat es descriuen els passos a seguir per tal d'instal·lar manualment les claus públiques de les entitats certificadores per tal que **Internet Explorer** pugui detectar cadascun dels certificats digitals que podem usar i establir la cadena de confiança que li permeti acceptar-los.

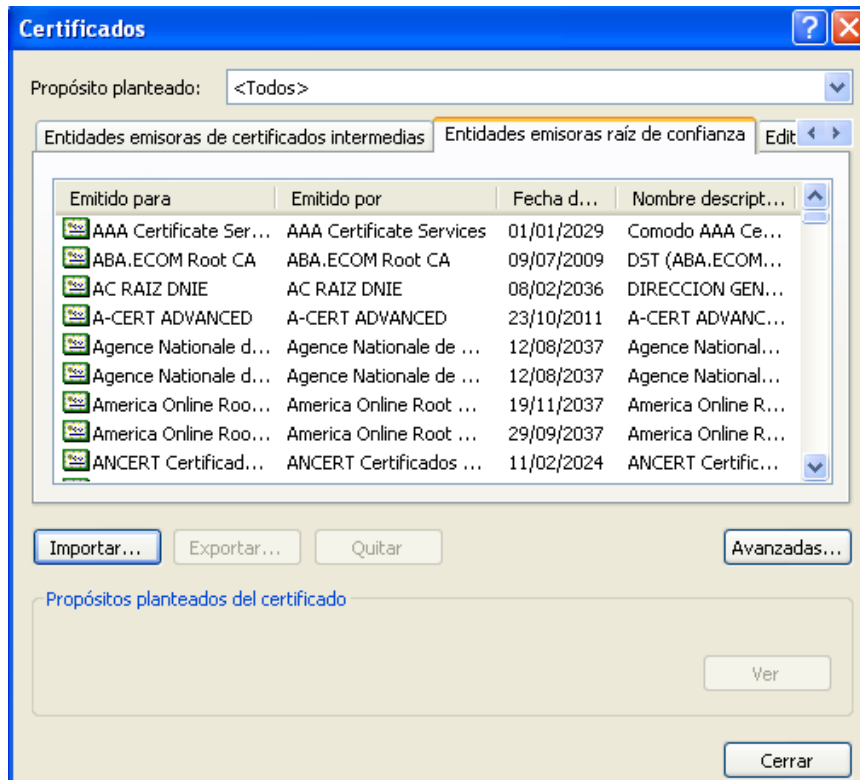
El mateix procediment també es vàlid per tal d'instal·lar manualment certificats digitals personals (del tipus .p12 o .pfx) en el nostre navegador per a que estiguin disponibles per tal que estiguin disponibles a l'hora d'autenticar-se a les aplicacions protegides amb GICAR.

Tota aquesta configuració i instal·lació dels certificats digitals es pot realitzar a partir del menú d' "Opcions d'Internet", situat en la pestanya d' "Eines" en el menú superior del navegador.



Per a realitzar la instal·lació manual d'una clau pública d'una entitat certificadora, caldrà accedir en aquest menú, i en la pestanya "Contingut", tindrem disponible el botó de "Certificats" on podrem veure el següent:

- o *Entitats emissores arrel de confiança*: certificats per tal d'establir la relació de confiança entre el servidor web i l'entitat certificadora que certifica que aquell lloc web és qui diu ser.
- o *Entitats emissores de certificats intermitjers*: per tal d'establir la cadena de confiança amb els certificats que d'aquestes depenen.
- o *Certificats del tipus personal*: d'autenticació d'usuari.

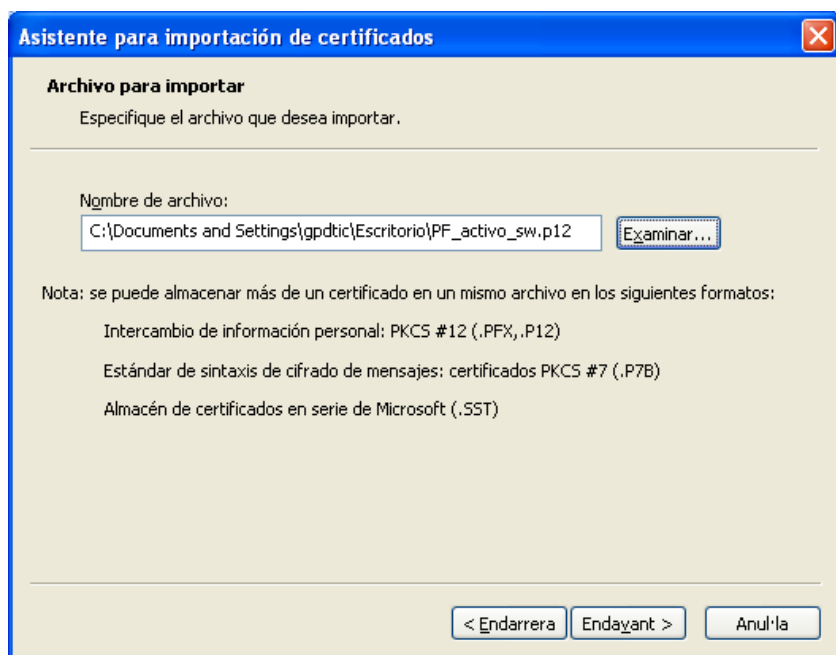


Dins de la nova finestra que s'obre, tenim el llistat de tots els certificats i les claus públiques arrels i intermitjers que pot llegir el navegador.

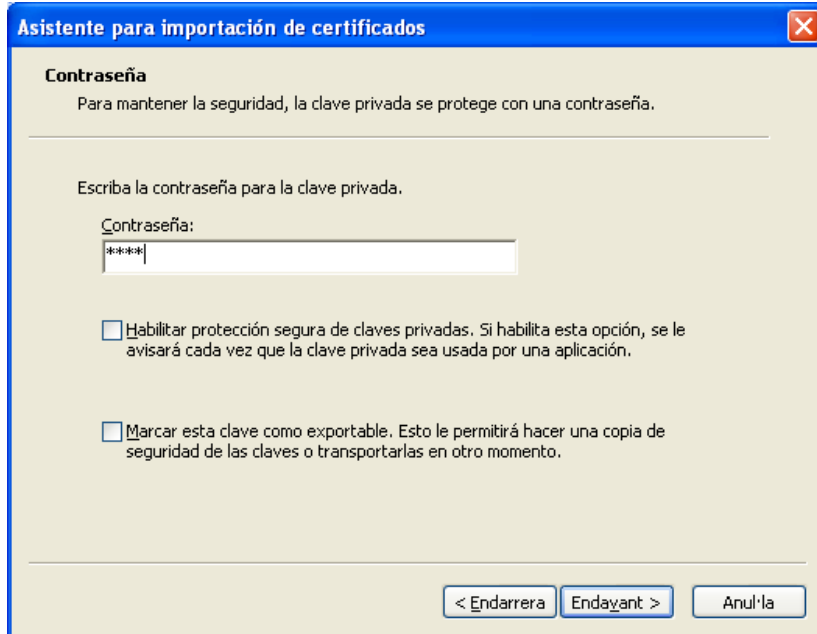
Si pitgem sobre el botó "Importar..." de qualsevol de les pestanyes, accedirem a l'assistent per a la instal·lació de certificats que desitgem associar al nostre navegador.



Posteriorment ens demanarà la ruta d'accés fins a on tenim situat el certificat en qüestió.



En el cas de que estiguem incorporant un certificat personal, com el que es mostra en la captura de pantalla anterior, el navegador ens demanarà la contrasenya associada a aquesta clau privada.



**Asistente para importación de certificados**

**Contraseña**  
Para mantener la seguridad, la clave privada se protege con una contraseña.

Escriba la contraseña para la clave privada.

Contraseña:  
\*\*\*\*\*

Habilitar protección segura de claves privadas. Si habilita esta opción, se le avisará cada vez que la clave privada sea usada por una aplicación.

Marcar esta clave como exportable. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.

< Endarrera   Endavant >   Anul·la

En qualsevol cas, la següent finestra ens demanarà a on volem emmagatzemar la informació referent al certificat. El navegador té una sèrie de carpetes dissenyades específicament per a aquest propòsit, i cadascuna d'elles guarda un tipus diferent de certificat (per exemple, hi ha un magatzem per a certificats del tipus arrel, i n'hi ha pels de tipus personal).

Per defecte, el navegador ja detecta de quin tipus és el nostre certificat i selecciona la carpeta adequada, encara que podem canviar la selecció si ho preferim.



**Asistente para importación de certificados**

**Almacén de certificados**  
Los almacenes de certificados son áreas del sistema donde se guardan los certificados.

Windows puede seleccionar automáticamente un almacén de certificados, o bien es posible especificar una ubicación para el certificado.

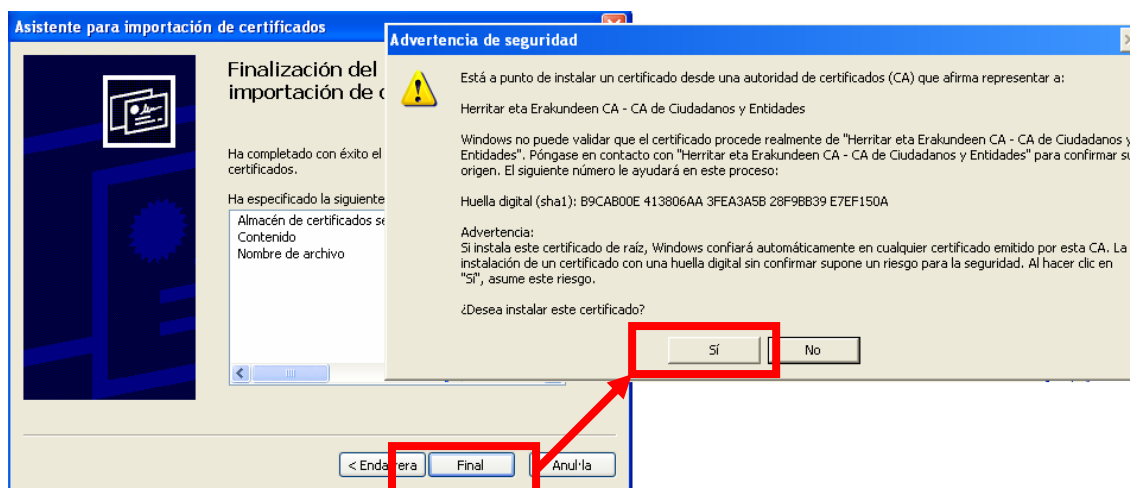
Seleccionar automáticamente el almacén de certificados en base al tipo de certificado

Colocar todos los certificados en el siguiente almacén

Almacén de certificados:  
Entidades emisoras raíz de confianza   Examinar...

< Endarrera   Endavant >   Anul·la

Per a finalitzar, s'obre la finestra final de la importació, a on es mostren totes les dades que hem anat escollint en els passos anteriors. Si estem conformes amb aquestes dades, prement "Final" i, després d'una última confirmació, incorporarem el nostre certificat al llistat de claus disponibles del navegador.

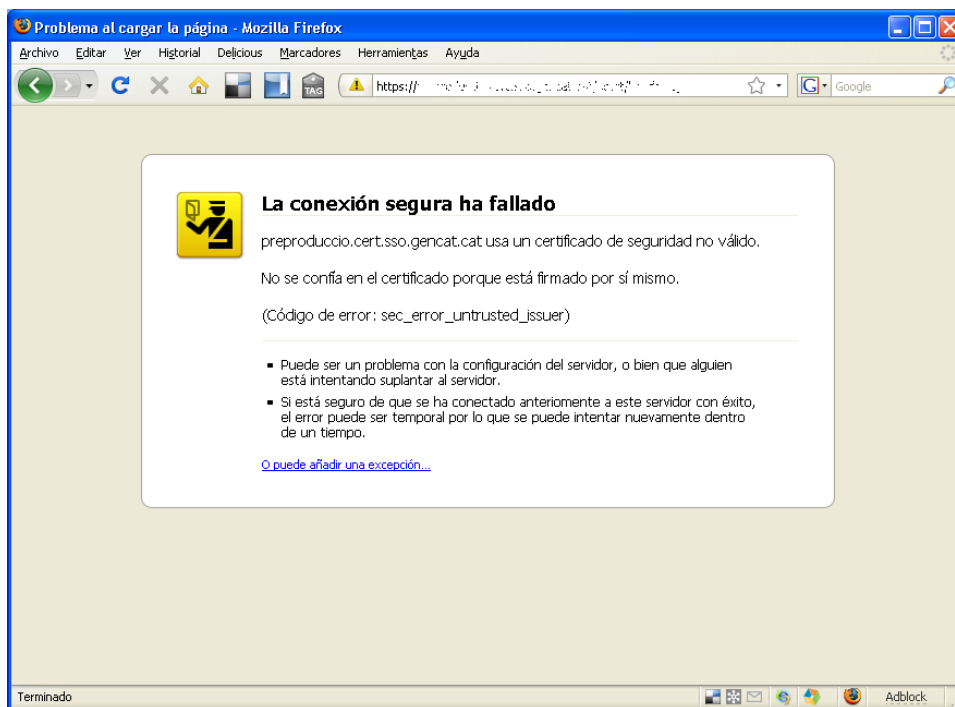




## 3. INSTAL·LACIÓ DE CERTIFICATS AL MOZILLA FIREFOX

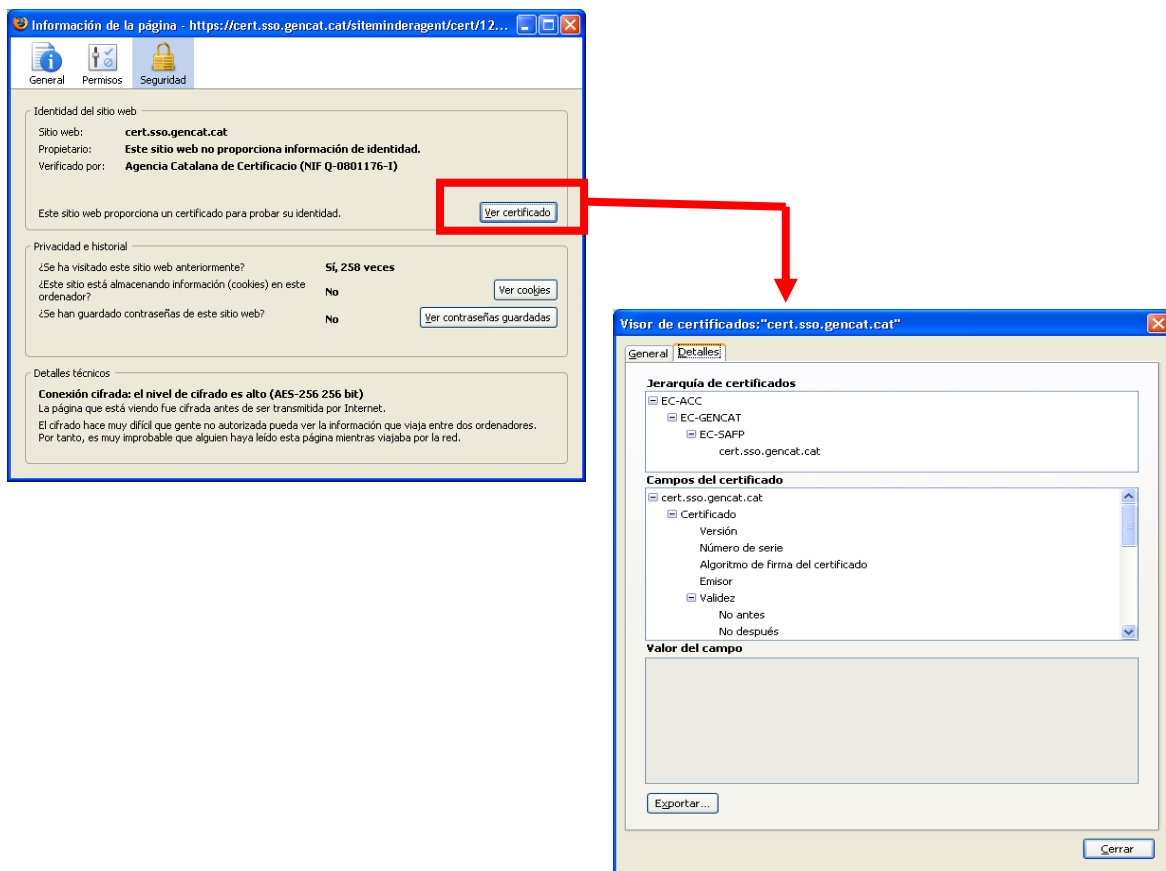
En aquest apartat exposarem com instal·lar i configurar les claus públiques de les entitats certificadores per tal que **Mozilla Firefox** sigui capaç de detectar cadascun dels certificats i establir la cadena de confiança que li permeti acceptar el nostre certificat digital. Posteriorment s'indicarà com incorporar els certificats personals necessaris per a realitzar l'autenticació en les diferents aplicacions que ho requereixin.

En un navegador mal configurat, en intentar accedir a l'aplicació mitjançant l'ús de certificat digital ens donarà un error d' "*Access Forbidden*" o bé ens sortirà un missatge com aquest altre:



Aquest error ve provocat perquè el navegador no confia en el servidor web i, per tant, el que cal fer és establir una relació de confiança entre tots dos elements.

Per fer-ho hem de tenir instal·lada tota la ruta de certificats que usa el servidor en el nostre navegador. La podem conèixer mitjançant l'opció "*Ver información de la página*" del menú que ens sorgirà si pitgem el botó dret del ratolí dins de la pàgina en qüestió.



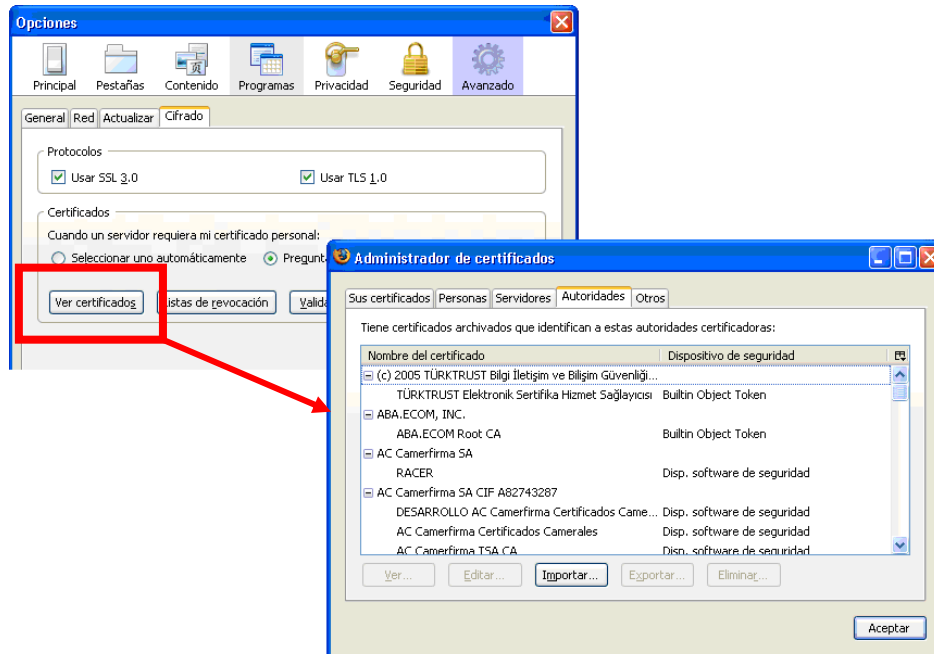
En la última finestra podem comprovar la jerarquia de certificats que usa el servidor. La instal·lació de totes aquestes claus públiques serà necessària per a que el navegador sigui capaç d'interactuar correctament aquest servidor.

També serà necessari tenir instal·lades les claus públiques de la entitat de certificació per tal que el navegador pugui acceptar els certificats d'aquella entitat de certificació.

A continuació es descriu el procés d'instal·lació de claus públiques en el Mozilla Firefox.

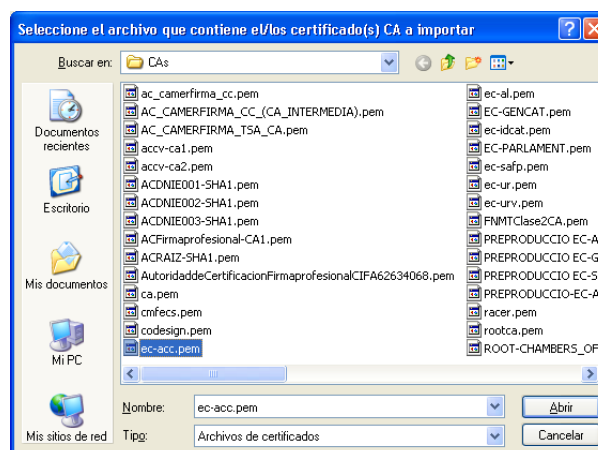
### 3.1 Instal·lació manual de claus públiques

Per a veure el llistat de certificats i de claus públiques associades al nostre navegador, caldrà accedir en el menú *Herramientas > Opciones > Avanzado > Cifrado > Ver certificados*.



En aquesta nova finestra que s'obre, podem consultar totes les dades relacionades amb els certificats instal·lats actualment. En concret, en la pestanya "Sus certificados" estan situats els certificats personals relacionats amb l'usuari, mentre que en la de "Autoridades" tenim col·locades les claus públiques necessàries per a poder confiar en les dades del servidor.

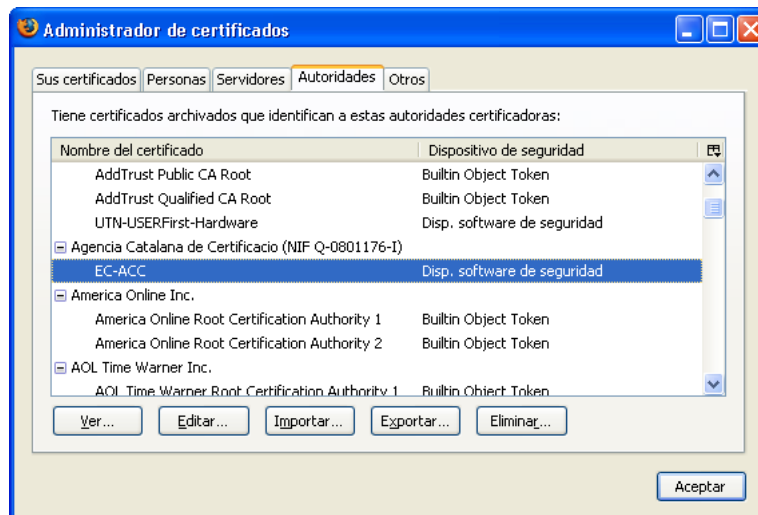
En el cas de voler incorporar una nova autoritat certificadora en el nostre navegador, caldrà pitjar sobre el botó "Importar..." de la pestanya d' "Autoridades" de la finestra anterior. Ens demanarà la situació del certificat que volem introduir.



Un cop seleccionat el certificat adequat, ens preguntarà quin ús li donarem a aquesta clau. En el nostre cas, l'opció recomanada és la primera, la d'identificar servidors web.

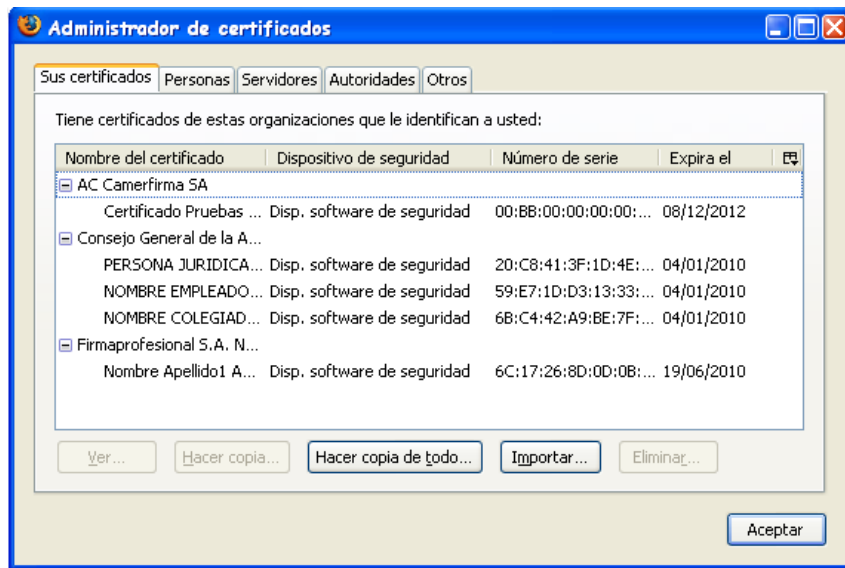


Un cop estiguem conformes amb la seva configuració, aquesta hauria de sortir en el llistat d'autoritats que tenim en el navegador. En qualsevol moment podrem tornar a accedir a la última finestra mitjançant l'ús del botó "Editar..." situat en la part inferior.

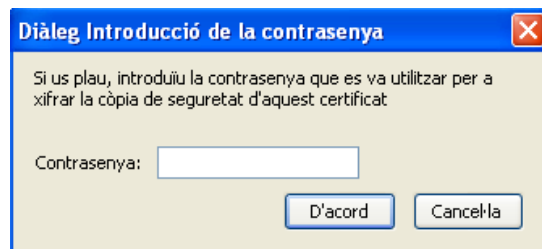


### 3.2 Instal·lació manual dels certificats personals

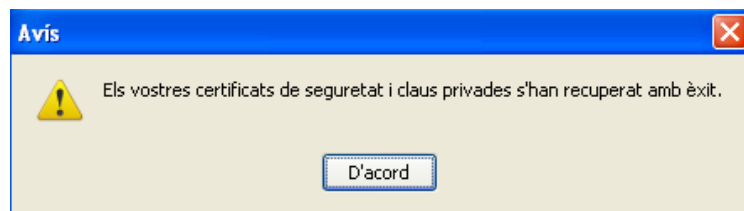
En el mateix menú de l'apartat anterior: Herramientas > Opciones > Avanzado > Cifrado > Ver certificados, tenim la pestanya "Sus certificados" a on estan situats els certificats personals que en aquest moment estan disponibles en el navegador.



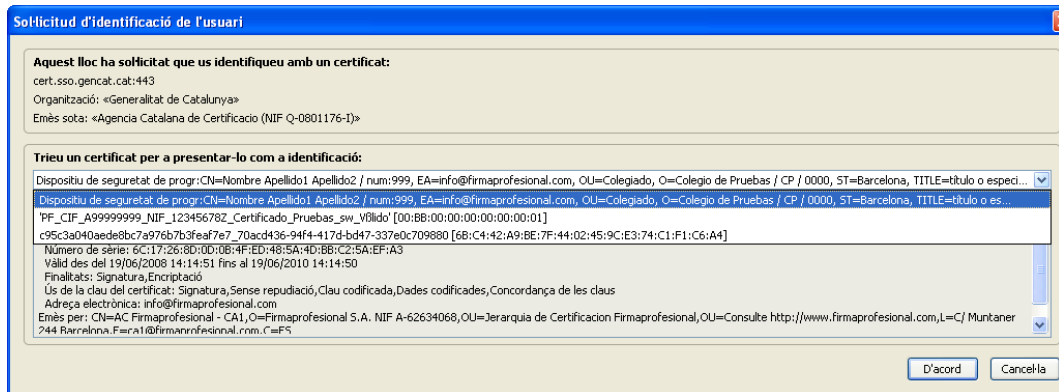
Si volem incorporar-ne un de nou, caldrà pitjar el botó "Importar..." i seleccionar la ruta d'accés fins a trobar el certificat que volem incorporar. Posteriorment ens preguntarà per la PIN / contrasenya associat/da a la clau privada.



Si tot el procés s'ha realitzat de forma correcte ens sortirà un avís confirmant-nos la tasca.



Una vegada associada la clau privada en el nostre navegador, aquesta ha d'aparèixer en el llistat de certificats vist anteriorment, i hauria d'estar disponible en el menú que s'obre al accedir a les aplicacions que requereixin l'ús de certificats en el seu procés d'autenticació.

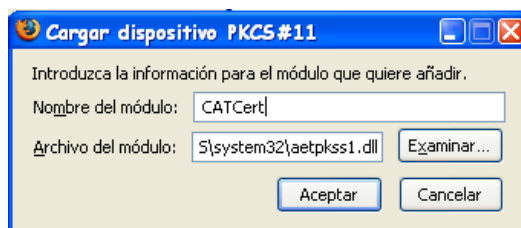


### 3.3 Configuració del dispositiu de seguretat

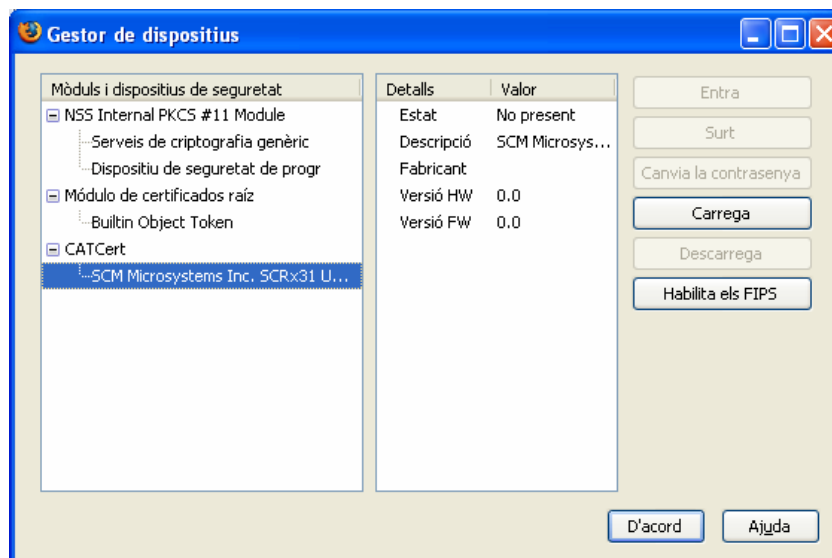
Per tal que el navegador pugui accedir als certificats de targeta de Catcert (T-Cat), cal configurar correctament el lector de targetes criptogràfiques com a dispositiu criptogràfic de seguretat en el Firefox (abans cal instal·lar el software del lector de targetes. Veure apartat 4.2). Aquesta opció està disponible en el menú situat en Herramientas > Opciones > Avanzado > Cifrado > Dispositivos de seguridad.



Si pitgem sobre el botó "Carga" d'aquesta finestra, el navegador ens preguntarà sobre quin dispositiu volem implementar. Cal inserir com a nom de fitxer del mòdul la ruta "C:\WINDOWS\system32\actpkcs1.dll". En el cas de tenir els arxius de Windows en una altre ruta, caldrà inserir sempre la que correspongui.



Si es realitza correctament, el dispositiu hauria de sortir en el llistat del gestor de dispositius.



## 4. INSTAL·LACIÓ DES DE LA WEB DE CATCERT

L'agència catalana de certificació posa a disposició dels usuaris una pàgina web amb tota la informació i tots els arxius necessaris per a poder treballar amb certificats en el nostre navegador web. Aquesta pàgina està situada en la direcció:

<http://www.catcert.cat>

Català | Castellano CAU: 902 901 080 - [info@catcert.cat](mailto:info@catcert.cat)  
[Inici](#) | [Registre](#) | [Suport](#) | [Notícies](#)

**CATCert** Agència Catalana de Certificació CERTIFICATS QUÈ OFERIM ADMINISTRACIÓ EMPRESES PER QUÈ CATCERT

Sol·liciteu ja els **nous certificats** per complir amb la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics.

  
Segell  
electrònic

  
Sistema  
electrònic

  
Sistema  
electrònic

  
Segell  
electrònic

[Procés de sol·licitud del certificat](#) 

**Novetat:**  
[procés de sol·licitud del certificat via web \(eaCat\)](#) 

**Vull obtenir el certificat**

- Certificats Personals
- Certificats d'Entitat
- Certificats de Dispositiu

**AOC**  
Consorci AOC  
El seu objectiu és col·laborar amb les administracions públiques catalanes per millorar els serveis públics amb iniciatives, productes i serveis mitjançant l'ús intensiu de les TIC. CATCert en depèn com a organisme autònom.

**Ciutadania**  
**Garanteix la teva identitat digital**  


**Utilitza el teu certificat**  
Podeu realitzar la declaració de la renda, tant amb l'idCAT com amb la T-CAT.



[> Actualitat](#) [> Destacats](#)

### 4.1 Claus públiques

Per a procedir amb l'instal·lació dels mateixos, cal seguir l'assistent de descàrrega que apareix al seleccionar l'opció de '*baixada de claus públiques*' en la mateixa pàgina principal del portal.

**Baixada de claus públiques**

En aquest apartat trobareu les claus de totes les entitats de certificació de la jerarquia de l'Agència Catalana de Certificació.





Es recomana baixar les claus de totes les entitats de certificació de la jerarquia. Si s'instal·la només les d'una branca de la jerarquia, en el moment que sigui necessari intercanviar informació amb un ens que pertany a una administració d'una altra branca s'haurà de repetir aquest procediment per aquella branca de la jerarquia.

## 4.2 Software lector de targetes criptogràfiques

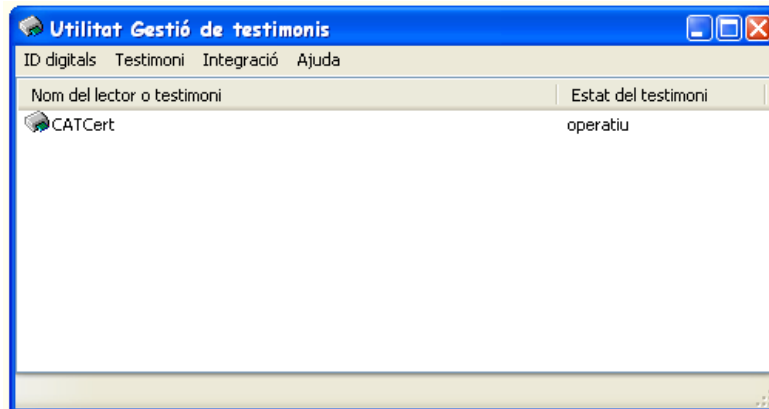
CatCert també posa a la disposició dels usuaris un software per a la gestió del lector de targetes. S'anomena SafeSign i es pot descarregar la última versió des de la mateixa pàgina web, dins de l'apartat de programari:

[http://www.catcert.cat/web/cat/6\\_5\\_programari.jsp](http://www.catcert.cat/web/cat/6_5_programari.jsp)

Durant la realització d'aquest manual, la última versió disponible del gestor es troba en la versió 2.3.2, la qual està comprovada que funciona correctament i sense errors amb totes les funcionalitats que integra GICAR.

Cal tenir en compte de que només es proporciona el software de gestió, per al seu correcte funcionament cal instal·lar primer els drivers corresponents al seu model, que els acostuma a proporcionar el fabricant del dispositiu.

El gestor té una aparença semblant a:



En aquesta pantalla es mostra la informació bàsica sobre el dispositiu i el seu estat. En el cas de voler obtenir més informació sobre aquest o sobre els certificats que conté la targeta criptogràfica que hi ha carregada, sempre es pot comprovar pitjant sobre la corresponent icona. Per exemple, si visualitzem els detalls sobre els certificats carregats obtindrem una finestra com:

**ID digitals**

ID digitals personals:

Emès per a	Emès per	Data de caducitat	Eti...	Etiqueta de testimoni
CPX-1 Alb...	EC-SAFP	2012-07-03 15:50:21	Alb...	
CPISR-1 A...	EC-SAFP	2012-07-03 15:50:21	Alb...	
CPISR-1 P...	EC-SAFP	2012-06-12 10:35:17	OI...	
CPISR-1 P...	EC-SAFP	2012-07-22 09:42:45	OI...	

Detalls d'ID digital

Contingut del certificat:

Camp	Valor
Versió	V3
Número de sèrie	19:0C:33:41:88:8B:CF:5E:48:50:DF:E3:95:1C:41:E1
Emissor	EC-SAFP, Serveis Publics de Certificacio ECV-2, Vegeu https://www.catcert.net/verCIC-2 (c)...
Vàlid des de	2008-06-12 10:35:47
Vàlid fins a	2012-06-12 10:35:17
Tema	Persona Física, de la Peça de Proves, CPISR-1 Persona Física de la Peça de Proves, Vegeu htt...
Clau pública	RSA (1024 bits)

Camí de la certificació:

Emès per a	Emès per	Data de caducitat	Magatzem de c...
EC-SAFP	EC-GENCAT	2019-01-07 23:59:59	Autoritats certif...
EC-GENCAT	EC-ACC	2027-01-07 23:59:59	Autoritats certif...
EC-ACC	EC-ACC	2031-01-07 23:59:59	Autoritats certif...

Des d'aquí es pot visualitzar tota la informació que contenen, comprovar si estan caducats, etc.



## 5. COMPROVAR QUE GICAR ADMET EL CERTIFICAT

---

Per a comprovar la validesa d'un certificat personal, l'equip GICAR posa a disposició dels usuaris una eina web per tal de comprovar si el certificat és bo, si és admès per GICAR, i si és admès per CATCert. Aquesta eina es troba situada en:

**URL:** <https://cert.sso.gencat.cat/acert/header.cgi>

L'aplicació comprova que el certificat sigui vàlid, que no estigui revocat ni que estigui bloquejat per alguna circumstància.

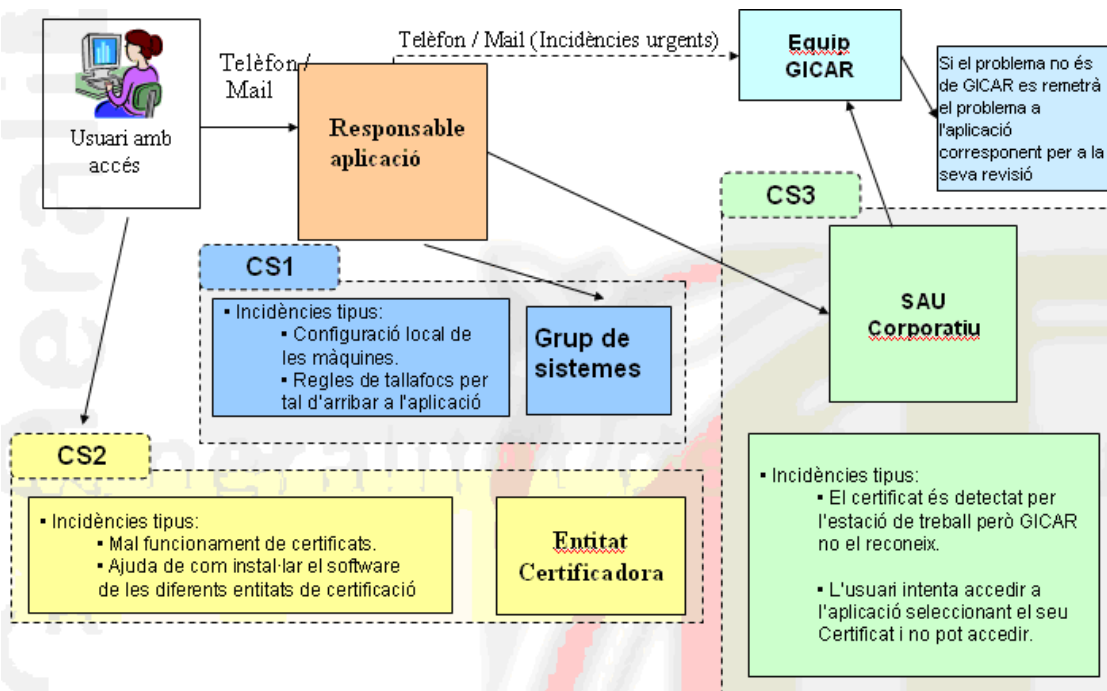
Si el certificat no compleix alguna d'aquestes condicions, l'usuari no podrà accedir a cap aplicació de GICAR i obtindrà un error per part del servidor (error 403 o error 500). Cal notar que també ens retornarà un error si GICAR no detecta correctament el tipus de certificat. En l'actualitat, GICAR admet certificats de les entitats:

- **Agència Catalana de Certificació**
- **Camerfirma**
- **Firmaprofesional**
- **Autoridad de Certificación de la Abogacía**
- **FNMT – Ceres**
- **DNI-E**

Si en canvi, el certificat es vàlid i GICAR el detecta, aquesta aplicació ens retornarà les dades del certificat que hàgim utilitzat.

## 6. POSSIBLES PROBLEMES AMB LA LECTURA DELS CERTIFICATS

En el moment d'accedir en alguna aplicació implementada per GICAR mitjançant un certificat digital, poden donar-se una sèrie de problemes. Els més comuns els podem classificar com:



### 1. La incidència ve provocada pel fet que la màquina de l'usuari no detecta el certificat digital. Això es pot comprovar:

- No li apareix a l'usuari la finestra d'elecció de certificats al autenticar-se.
- L'usuari selecciona el certificat però ja no li demana ni el PIN.
- L'eina de gestió dels certificats no li mostra a l'usuari els ID's registrats.

### En aquests casos s'hauria de validar que:

- La màquina ha d'estar configurada amb el SW de l'entitat certificadora pertinent, per tal de que pugui detectar el certificat. (Incidència de tipus CS1 / CS2).
- El navegador de l'usuari ha de tenir carregades les claus públiques. Aquestes poden ser descarregades des la pàgina web de CATCert, tal i com s'explica en el punt 4 d'aquesta guia. Incidència de tipus CS1.



- Si es tracta d'un certificat d'usuari de tipus software (\*.p12), s'hauria de comprovar que aquest es troba instal·lat en el contenidor personal corresponent al navegador que s'estigui utilitzant (punt 2 i 3.2 d'aquesta guia per a més informació). Incidència de tipus CS1.
- Si el certificat és detectat correctament pel gestor de certificats, però no pel navegador, caldria esborrar la caché i les galetes del navegador, comprovar que les claus públiques necessàries estiguin instal·lades i revisar que la connectivitat entre el client i el servidor estigui operativa. Incidència de tipus CS1.
- Si el certificat no és detectat pel lector de les targetes, revisar la configuració d'aquest. Reinstal·lar els controladors del lector de targetes (Incidència del tipus CS1).

## **2. La màquina detecta el certificat digital, però no s'efectua l'autenticació .**

### **Això es pot comprovar:**

- Se li dóna l'opció d'escollir el certificat al fer l'autenticació però aquesta no tira endavant.

El certificat ha de ser vàlid, no ha d'estar revocat ni ha d'estar bloquejat. Si el certificat té cap d'aquests problemes l'usuari no podrà accedir a l'aplicació. L'equip GICAR posa a la disposició dels usuaris una eina web per a comprovar la validesa dels certificats personals i si es acceptat per les aplicacions, per a més informació remetre al punt 5 d'aquesta guia.

- En el cas de que en invocar l'eina no s'obté cap error, el certificat es vàlid i GICAR el detecta correctament , per tant la incidència no es de GICAR i cal redirigir el problema al responsable de l'aplicació. Incidència de tipus CS1.
- En el cas de que l'eina retorni un error, el certificat en qüestió no es admès per GICAR. Incidència de tipus CS2.

Si després de fer totes les anteriors verificacions l'usuari segueix sense poder accedir a l'aplicació, remetre el problema a l'equip GICAR. Aquest s'enviarà, a través del SAU Corporatiu, a la següent adreça:

- [sau.ctti@gencat.cat](mailto:sau.ctti@gencat.cat) indicant el següent al camp assumpte:  
**\_INNEO\_INC\_ORD\_9.34 GICAR - PRO – INC CERTIFICAT**

En el cas que es tracti d'una incidència de caràcter urgent, contactar directament amb els responsables de la plataforma GICAR.



### **3. Altres incidències:**

- Se li demana el PIN diverses vegades a l'usuari abans d'accedir a l'aplicació. Aquest problema sol ser freqüent quan s'utilitza un controlador del lector de targetes que està desactualitzat. Aquest problema doncs se sol solucionar al instal·lar la versió més nova del lector del token (CS1).