

Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació

# Manual de gestió de certificats GICAR

Data: Juliol 2009 Autor:



## ÍNDEX

ÍNDEX2
1. INTRODUCCIÓ3
2. INSTAL·LACIÓ DE CERTIFICATS A L'INTERNET EXPLORER4
3. INSTAL·LACIÓ DE CERTIFICATS AL MOZILLA FIREFOX9
3.1 Instal·lació manual de claus públiques10
3.2 Instal·lació manual dels certificats personals12
3.3 Configuració del dispositiu de seguretat14
4. INSTAL·LACIÓ DES DE LA WEB DE CATCERT
4.1 Claus públiques
4.2 Software lector de targetes criptogràfiques17
5. COMPROVAR QUE GICAR ADMET EL CERTIFICAT
6. POSSIBLES PROBLEMES AMB LA LECTURA DELS
CERTIFICATS



## 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):
  - o EC-SAFP.
  - o EC-AL
  - o EC-UR
  - o EC-Parlament
  - o 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:





- *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.
- *Entitats emissores de certificats intermitjes*: per tal d'establir la cadena de confiança amb els certificats que d'aquestes depenen.
- o Certificats del tipus personal: d'autenticació d'usuari.

Certificados	?	? 🔀
Propósito planteado: <todos></todos>	~	~
Entidades emisoras de certificados intermedias Entidad	des emisoras raíz de confianza Edit 🔹 🕨	ıíz de confianza Edit 🔹 🔪
Emitido para       Emitido por         MAA Certificate Ser       AAA Certificate Services         ABA.ECOM Root CA       ABA.ECOM Root CA         AC RAIZ DNIE       AC RAIZ DNIE         AC CERT ADVANCED       A-CERT ADVANCED         Agence Nationale d       Agence Nationale de         America Online Roo       America Online Root         America Online Roo       America Online Root	Fecha d         Nombre descript           01/01/2029         Comodo AAA Ce           09/07/2009         DST (ABA.ECOM           08/02/2036         DIRECCION GEN           23/10/2011         A-CERT ADVANC           12/08/2037         Agence National           12/08/2037         Agence National           19/11/2037         America Online R           29/09/2037         America Online R	Nombre descript Comodo AAA Ce DST (ABA.ECOM DIRECCION GEN A-CERT ADVANC Agence National Agence National America Online R America Online R
Importar       Exportar         Quitar         Propósitos planteados del certificado	11/02/2024 ANCERT Certific  Avanzadas Ver	ANCERT Certific

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





Asistente para importación	de certificados	X
	<ul> <li>Éste es el Asistente para importación de certificados, listas de cortificados y listas de revocaciones de certificados desde su disco a un almacén de certificados.</li> <li>Un certificado, que se emite por una entidad emisora de certificación, es una confirmación de su identidad y contiene información que se utiliza para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados.</li> <li>Haga clic en Siguiente para continuar.</li> </ul>	
	< Endarrera Endayant > Anul	la

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

Asistente para importación de certificados
Archivo para importar
Especifique el archivo que desea importar.
Nombre de archivo:
C:\Documents and Settings\gpdtic\Escritorio\PF_activo_sw.p12
Nota: se puede almacenar más de un certificado en un mismo archivo en los siguientes formatos:
Intercambio de información personal: PKCS #12 (.PFX,.P12)
Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
Almacén de certificados en serie de Microsoft (.SST)
· · · · · · · · · · · · · · · · · · ·

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 🛛 🛛 🗙
<b>Contraseña</b> 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 Endayant > 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.	
O Seleccionar automáticamente el almacén de certificados en base al tipo de certificado	
<ul> <li>Colocar todos los certificados en el siguiente almacén</li> </ul>	
Almacén de certificados:	
Entidades emisoras raíz de confianza Examinar	
< Endarrera Endavant > Anu	l·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.

Anistanta para importanión	de contificados		
Asistente para importación	ue certificados	Adverte	ncia de seguridad 🛛 🕺
	Finalización del importación de c	<u>.</u>	Está a punto de instalar un certificado desde una autoridad de certificados (CA) que afirma representar a: Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades
	Ha completado con éxito el certificados.		Windows no puede validar que el certificado procede realmente de "Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades", Póngase en contacto con "Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades" para confirmar su origen. El siguiente número le ayudará en este proceso:
	Ha especificado la siguiente		Huella digital (sha1): B9CAB00E 413806AA 3FEA3A5B 28F9BB39 E7EF150A
	Almacén de certificados se Contenido Nombre de archivo		Advertencia: Si instala este certificado de raíz, Windows confiará automáticamente en cualquier certificado emitido por esta CA. La instalación de un certificado con una huella digital sin confirmar supone un riesgo para la seguridad. Al hacer clic en "Si", asume este riesgo.
			¿Desea instalar este certificado?
	<		Sí No
	< Enda	rera	Final



## 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 pàgina"* del menú que ens sorgirà si pitgem el botó dret del ratolí dins de la pàgina en qüestió.







En la ultima finestra podem comprovar la jerarquia de certificats que usa el servidor. La instal·lació de <u>totes</u> 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 *Herrramientas > 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.



Descargando certificado
Se le ha pedido que confíe en una nueva Autoridad Certificadora (CA).
¿Quiere confiar en "EC-ACC" para los siguientes propósitos?
Confiar en esta CA para identificar sitios web.
Confiar en esta CA para identificar usuarios de correo.
Confiar en esta CA para identificar desarrolladores de software.
Antes de confiar en esta CA para cualquier propósito, debe examinar el certificado, política y procedimientos de la CA (si están disponibles).
Ver Examinar certificado de CA
Aceptar Cancelar

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.

Administrador de certificados		
Sus certificados Personas Servidores Autoridades Otr	ros	
Tiene certificados archivados que identifican a estas aut	oridades certificadoras:	
Nombre del certificado	Dispositivo de seguridad	E.
AddTrust Public CA Root	Builtin Object Token	~
AddTrust Qualified CA Root	Builtin Object Token	
UTN-USERFirst-Hardware	Disp. software de seguridad	
🖃 Agencia Catalana de Certificacio (NIF Q-0801176-I)		
EC-ACC	Disp. software de seguridad	
America Online Inc.		
America Online Root Certification Authority 1	Builtin Object Token	
America Online Root Certification Authority 2	Builtin Object Token	
🖃 AOL Time Warner Inc.		
AOL Time Warner Root Certification Authority 1	Builtin Ohiect Token	×
Ver Editar Importar Expo	ortar Elimina <u>r</u>	
		Aceptar

### 3.2 Instal·lació manual dels certificats personals

En el mateix menú de l'apartat anterior: Herrramientas > 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.



Administrador de certi Sus certificados Personas Ser	ficados vidores Autoridades Otros			
Tiene certificados de estas or	ganizaciones que le identifican	a usted:		
Nombre del certificado	Dispositivo de seguridad	Número de serie	Expira el	E.
🖃 AC Camerfirma SA				
Certificado Pruebas Consejo General de la A	Disp. software de seguridad	00:BB:00:00:00:00:	08/12/2012	
PERSONA JURIDICA	Disp. software de seguridad	20:C8:41:3F:1D:4E:	04/01/2010	
NOMBRE EMPLEADO	Disp. software de seguridad	59:E7:1D:D3:13:33:	04/01/2010	
NOMBRE COLEGIAD Firmaprofesional S.A. N	Disp. software de seguridad	6B:C4:42:A9:BE:7F:	04/01/2010	
Nombre Apellido1 A	Disp. software de seguridad	6C:17:26:8D:0D:0B:	19/06/2010	
Ver Hacer copia	Hacer copia de <u>t</u> odo	Importar Elim	ina <u>r</u>	
			A	ceptar

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.

Diàleg Introdu	cció de la contrasenya 🛛 🛛 🔀
Si us plau, intro xifrar la còpia de	duïu la contrasenya que es va utilitzar per a e seguretat d'aquest certificat
Contrasenya:	
	D'acord Cancel·la

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.



quest lloc ha sol·licitat	ie us identifiqueu amb un certificat:	
ert.sso.gencat.cat:443		
rganització: «Generalitat d	Zatalunya»	
mès sota: «Agencia Catala	de Certificacio (NIF Q-0801176-1)»	
rieu un certificat per a	esentar-lo com a identificació:	
ispositiu de seguretat de p	gr:CN=Nombre Apellido1 Apellido2 / num:999, EA=info@firmaprofesional.com, OU=Colegiado, O=Colegio de Pruebas / CP / 0000, ST=Barcelona, TITLE=	=título o especi.
Dispositiu de seguretat de j	gr:CN=Nombre Apellido1 Apellido2 / num:999, EA=info@firmaprofesional.com, OU=Colegiado, O=Colegio de Pruebas / CP / 0000, ST=Barcelona, TITLE,	=título o es
PF_CIF_A999999999_NIF_:	345678Z_Certificado_Pruebas_sw_VBilido' [00:8B:00:00:00:00:00:00:00]	
:95c3a040aede8bc7a976b	3feaf7e7_70acd436-94f4-417d-bd47-337e0c709880 [6B:C4:42:A9:BE:7F:44:02:45:9C:E3:74:C1:F1:C6:A4]	
Número de sèrie: 6C:17:2	3D:00:08:4F:ED:48:5A:4D:88:C2:5A:EF:A3	
Finalitate: Signatura Encri	14:51 mms al 19/06/2010 14:14:50	
Ús de la clau del certificat:	curo ginatura, Sense repudiació, Clau codificada, Dades codificades, Concordança de les claus	
Adreça electrònica: info@	naprofesional.com	
més per: CN=AC Firmapro	sional - CA1, O=Firmaprofesional S.A. NIF A-62634068, OU=Jerarquia de Certificacion Firmaprofesional, OU=Consulte http://www.firmaprofesional.com, L	.=C/ Muntaner

### 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.

Detalles	Valor	Iniciar sesión
		Terminar sesión
		⊆ambiar contraseña
		⊆argar
		Descargar
		Habilitar <u>F</u> IPS
	Detalles	Detalles Valor

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\aetpkss1.dll*". En el cas de tenir els arxius de Windows en una altre ruta, caldrà inserir sempre la que correspongui.





🖲 Cargar dispositivo PKC5#11				
Introduzca la información para el módulo que quiere añadir.				
No <u>m</u> bre del módulo:	CATCert			
<u>A</u> rchivo del módulo:	S\system32\aetpkss1.dll	E <u>x</u> aminar		
	Aceptar	Cancelar		

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

🕹 Gestor de dispositius			
<ul> <li>Gestor de dispositius</li> <li>Mòduls i dispositius de seguretat</li> <li>NSS Internal PKCS #11 Module</li> <li>Serveis de criptografia genèric</li> <li>Dispositiu de seguretat de progr</li> <li>Módulo de certificados raíz</li> <li>Builtin Object Token</li> <li>CATCert</li> </ul>	Detalls Estat Descripció Fabricant Versió HW Versió FW	Valor No present SCM Microsys 0.0 0.0	Entra Surt Canvia la contrasenya Carrega Descarrega Habilita els FIP5
		(	D'acord Ajuda



## 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 Inici | Registre | Suport | Notícies CERTIFICATS QUÈ OFERIM ADMINISTRACIÓ EMPRESES PER QUÈ CATCERT CAT Cert Agència Catala de Certificació Sol·liciteu ja els <mark>nous certificats</mark> per complir amb la Llei 11/2007 d'accés electrònic dels ciutadans als serveis Procés de sol·licitud del certificat $\rightarrow$ públics. <u>Novetat:</u> procés de sol·licitud del certificat via web (eaCat) Vull obtenir el certificat Certificats Personals Certificats d'Entitat Certificats de Dispositiu Ciutadania <u>Utilitza el teu certificat</u> Consorci AOC A**O**C El seu objectiu és col·laborar amb les administracions públiques Podeu realitzar la declaració de la renda, tant amb l'idCAT com amb la T-CAT . Administració Oberta de Catalumea catalanes per millorar els serveis Renda públics amb iniciatives, productes i serveis mitjançant l'ús intensiu de les TIC. CATCert en 200 depèn com a organisme autònom >> 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.







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

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:

😡 Utilitat Gestió de testimonis	
ID digitals Testimoni Integració Ajuda	
Nom del lector o testimoni	Estat del testimoni
GCATCert	operatiu
	.:

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:						
Emèspera E	Emès per	Data de caducita	it Eti	Etiqueta de te	estimoni	
🛄 CPX-1 Alb E	C-SAFP	2012-07-03 15:5	D:21 Alb			
🛄 CPISR-1 A E	C-SAFP	2012-07-03 15:5	D:21 Alb			
CPISR-1 P E	C-SAFP	2012-06-12 10:3	5:17 OI			
CPISR-1 P E	C-SAFP	2012-07-22 09:4	2:45 OI			
- Detalls d'ID digital -						
Contingut del certil	ficat:					
Camp	Valo	r				
Versió Número de sèrie Emissor Vàlid des de Vàlid fins a Tema Clau pública	V3 19:0 EC-5 2008 2012 Pers RSA	C:33:41:88:88:CF:5E: AFP, Serveis Publics de I-06-12 10:35:47 -06-12 10:35:17 ona Física, de la Peça d (1024 bits)	18:50:DF:E3:9 Certificacio EC e Proves, CPIS	i:1C:41:E1 V-2, Vegeu https R-1 Persona Físic	s://www.catcert.r ca de la Peça de P	net/verCIC-2 (c) Proves, Vegeu htt
Camí de la certifica	ició:					
Emès per a		Emès per		Data de caducital	t	Magatzem de c
EC-SAFP		EC-GENCAT	2	2019-01-07 23:59:59		Autoritats certif
EC-GENCAT		EC-ACC	2	2027-01-07 23:59:59		Autoritats certif
EC-ACC		EC-ACC	2	2031-01-07 23:59:59		Autoritats certif
	Transfereix ID a	Importa	cadena de con	fiança Supri	meix ID digital	Visualitza certificat
				Actualitza	Comprova cad	ucitat Tanca

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).
- 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 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).