

Revocació del certificat idCAT

Control documental

| | | |
|--------------------------------|--|---|
| Estat formal | Elaborat per: Àrea de Qualitat i Procediments | Aprovat per: Emma Suevos i Guillaumet |
| Data de creació | 28/09/2006 | |
| Control de versions | Data: | 28/09/2009 |
| | Descripció: | Actualització del document |
| Nivell accés informació | pública | |
| Títol | Revocació del certificat idCAT | |
| Fitxer | revocacio_20090929.doc | |
| Control de còpies | Només les còpies disponibles a M:\NouPrometeo\Departaments\QualitatProcediments\Projectes_externs_E0527\idCAT\documentacio_servei\Procediments_idCAT\PO_ER_idCAT\2009 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

| | |
|---|-----------|
| Revocació del certificat idCAT..... | 1 |
| Control documental..... | 2 |
| Índex..... | 3 |
| 1. Introducció..... | 4 |
| 2. Definició de Rols..... | 5 |
| 2.1 Rol d'Operador d'Entitat de Registre idCAT | 5 |
| 2.2 Rol de Responsable del Servei d'Entitat de Registre idCAT | 5 |
| 2.3 Rol de subscriptor | 5 |
| 2.4 Operativa..... | 6 |
| 2.4.1 Cerca del certificat a revocar | 9 |
| 2.4.2 Arxiu de la sol·licitud de revocació del certificat..... | 18 |
| Annex 1: Sol·licitud de Revocació del certificat idCAT | 20 |

1. Introducció

El present document recull un esbós dels passos que s'han de seguir, de forma obligatòria, quan es realitzi la revocació d'un certificat digital idCAT.

La revocació consisteix en deixar sense efecte un certificat. Aquesta revocació és a instància de part i ha de sol·licitar-se a una Entitat de Registre idCAT. La revocació és un estat definitiu.

El tipus de certificat que es podrà revocar seguint el procediment aquí descrit serà el CPIXSA-2 Individual (Certificat Personal d'Identificació, Xifrat i Signatura Avançada de classe 2), anomenat certificat idCAT.

El procediment s'ha estructurat seguint una lògica seqüencial en el temps de les accions a portar a terme pels rols que intervenen en el procediment de revocació d'un certificat. Aquest rols són els següents:

- Rol d'Operador d'Entitat de Registre idCAT (OER)
- Rol de Responsable de Servei d'Entitat de Registre idCAT

D'altra banda, per a portar a terme el procediment de revocació de certificats CPIXSA-2, s'hauran d'establir les mesures necessàries per a complir amb allò establert a la Llei 59/2003, de 19 de desembre, sobre signatura electrònica.

Totes les accions relacionades amb aquest procediment hauran de ser registrades, establint-se les mesures de protecció adients. Per tal d'assegurar la integritat de les operacions registrades, cada una d'elles s'emmagatzema a la base de dades juntament amb la signatura de la mateixa, portada a terme per l'operador que va gestionar l'operació. Aquesta tasca la durà a terme directament l'Agència Catalana de Certificació – CATCert.

2. Definició de Rols

En les següents seccions s'especifiquen les funcions i responsabilitats assignades al rol d'Operador d'Entitat de Registre idCAT i al rol de Responsable d'Entitat de Registre idCAT, així com també l'operativa amb l'aplicació web per a garantir la seguretat, la integritat i la confidencialitat de la informació tractada.

2.1 Rol d'Operador d'Entitat de Registre idCAT

El rol d'Operador d'Entitat de Registre idCAT, en el procediment de revocació d'un certificat digital CPIXSA-2, té com a missió atendre les peticions de revocació que es realitzin quan el subscriptor d'un certificat digital acudeixi personalment a l'Entitat de Registre idCAT sol·licitant la revocació del seu certificat digital idCAT.

En el cas que el mateix OER tingui assignada la funció d'emmagatzemar la documentació associada a la revocació dels certificats, haurà d'assegurar que la documentació estigui arxivada d'acord amb les directrius establertes per CATCert. Si aquesta funció d'arxiu la realitza una altra persona, l'OER haurà d'assegurar que la documentació arribi a la persona encarregada de l'arxiu.

En ambdós casos, la documentació associada a la revocació de certificats digitals s'ha de conservar en l'arxiu de l'ens durant 15 anys, segons recull *l'article 20.1.f de la Llei 59/2003, de 19 de desembre, sobre signatura electrònica*.

2.2 Rol de Responsable del Servei d'Entitat de Registre idCAT

El rol de Responsable del Servei de l'Entitat de Registre idCAT té com a missió vetllar pel bon funcionament de l'Entitat de Registre idCAT. Amb aquest fi ha d'aplicar o fer aplicar els procediments d'arxiu, seguretat física i seguretat lògica que regulen el servei.

A més d'això, ha de fer d'enllaç entre l'Entitat de Registre idCAT i CATCert. Per a fer-ho, comunica via correu electrònic a info@idcat.cat o al 902 90 10 80 les possibles anomalies o incidències de l'emissió o gestió dels certificats.

Per últim, el Responsable del Servei de l'Entitat de Registre idCAT és l'encarregat de designar els Operadors de l'Entitat de Registre que prestaran el servei idCAT.

2.3 Rol de subscriptor

Són susceptibles de ser subscriptors del certificat idCAT totes aquelles persones físiques que necessiten relacionar-se amb les Administracions públiques locals, autonòmiques o estatals.

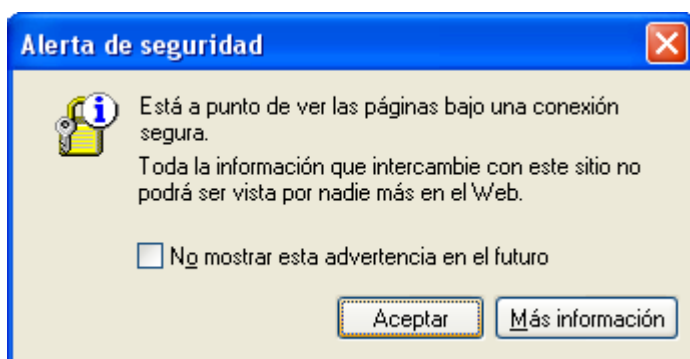
2.4 Operativa

Quan el subscriptor es persona a l'Entitat de Registre idCAT per a procedir a revocar el seu certificat digital, l'Operador d'Entitat de Registre idCAT accedirà a l'aplicació web a través de la URL següent: <https://www.idcat.cat:4443>.

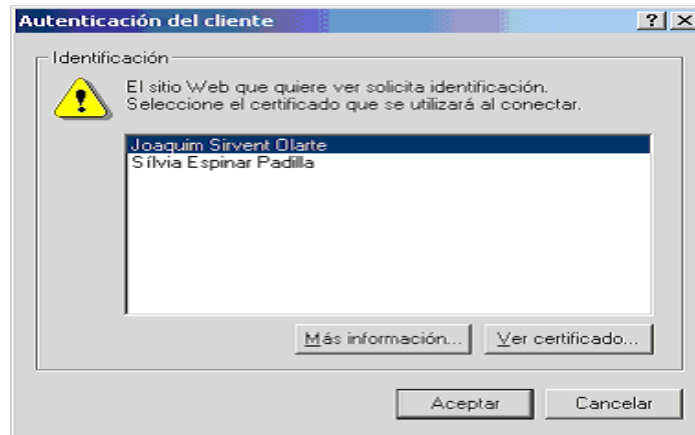
El subscriptor del certificat que es pretén revocar haurà de personar-se a l'Entitat de Registre idCAT aportant el document acreditatiu de la seva identitat (NIF -DNI amb lletra-, NIE, passaport o DNI d'altres països) i fotocòpia del mateix.

Per a poder accedir a l'aplicació web, l'Operador d'Entitat de Registre idCAT necessitarà disposar d'un certificat CIPISR amb funcions d'Operador d'Entitat de Registre que li haurà subministrat l'Agència Catalana de Certificació – CATCert després de verificar els coneixements i rebre la informació suficient i adequada per actuar com a tal.

Aquest Operador introduirà la targeta dins el lector de targetes criptogràfiques i, en el moment d'accedir a la web, haurà d'escollir el seu certificat d'operador i "**Aceptar**" en la finestra d'autenticació (fig. 2).



(fig. 1)

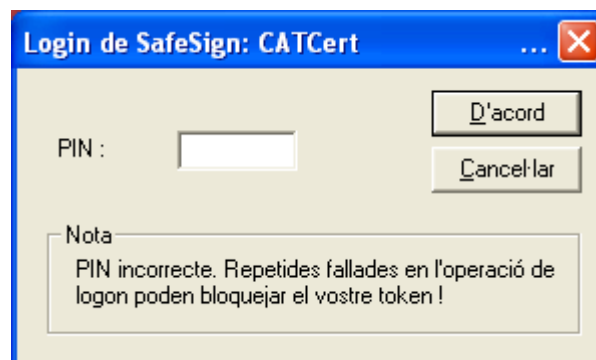


(fig. 2)

En el moment d'accedir a l'aplicació haurà d'introduir el PIN del certificat d'Operador d'Entitat de Registre idCAT (fig. 3) de manera que si no és correcte, no es permetrà l'accés a aquesta (fig. 4).



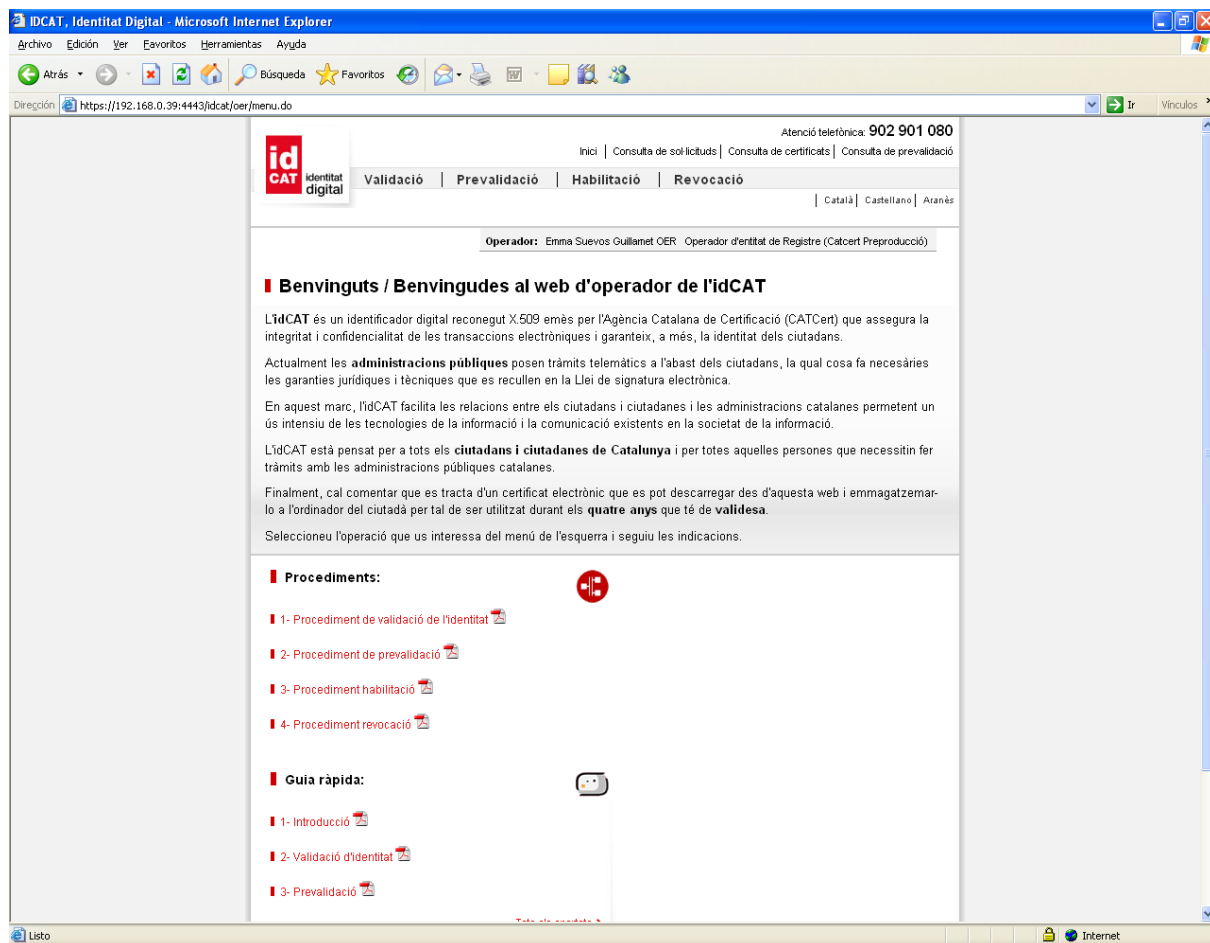
(fig. 3)



(fig. 4)

NOTA: Missatge d'error indicant que el PIN del certificat d'Operador d'Entitat de Registre idCAT no ha estat introduït correctament. Després d'introduir de forma incorrecta el PIN 3 vegades, és necessari desbloquejar el PIN mitjançant el PUK amb l'aplicació de Gestió de testimonis. Després d'introduir el PUK de forma incorrecta, es bloqueja la targeta d'operador.

Si l'Operador d'Entitat de Registre idCAT introdueix el PIN del seu certificat CIPISR-1 correctament, accedirà a la pantalla inicial de l'aplicació web (fig. 5), des d'on tindrà accés a diverses funcionalitats, entre elles, la de revocació de certificats. La connexió establerta serà una connexió segura mitjançant protocol SSL versió 3.

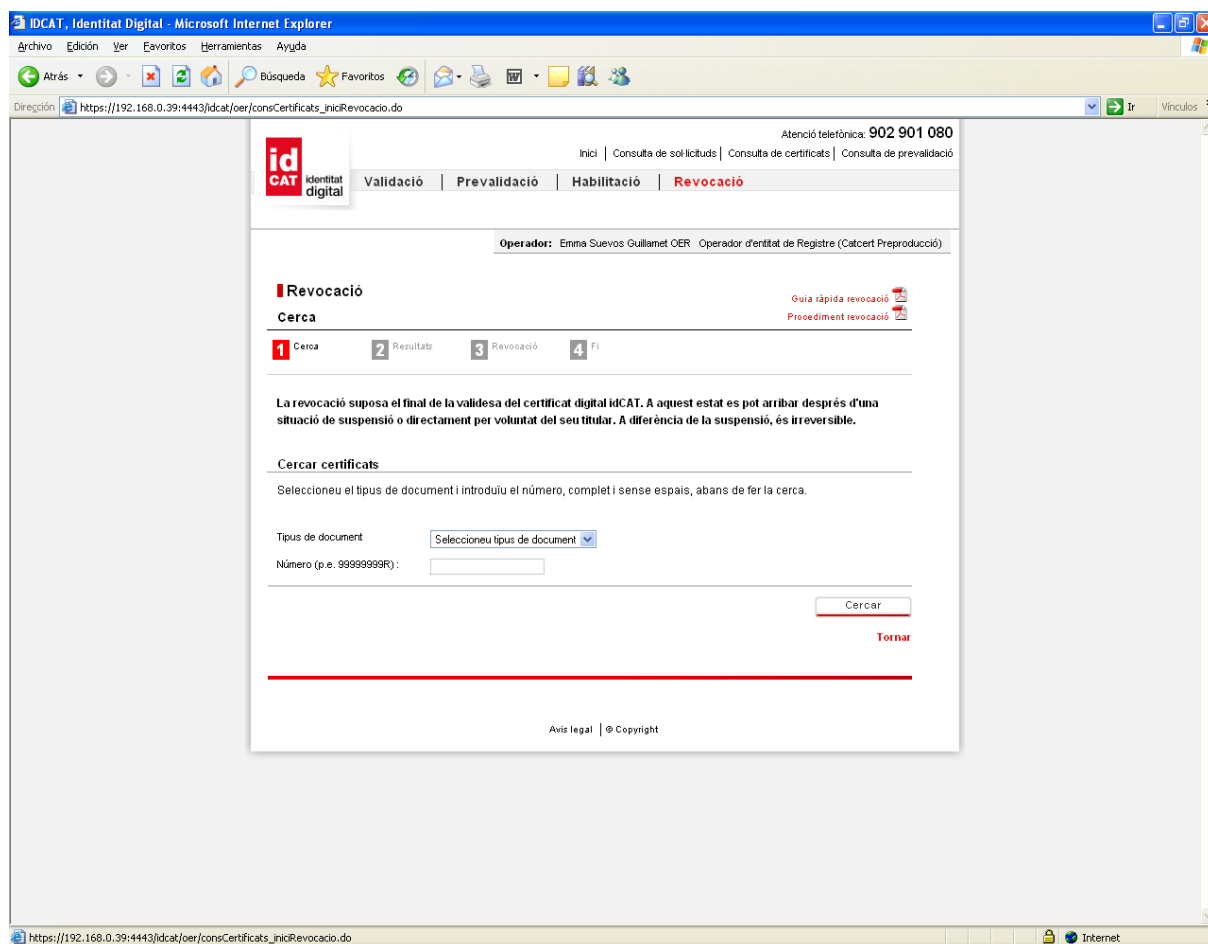


(fig. 5)

Per tal de gestionar una petició de revocació, l'operador ha de seguir els següents passos:

2.4.1 Cerca del certificat a revocar

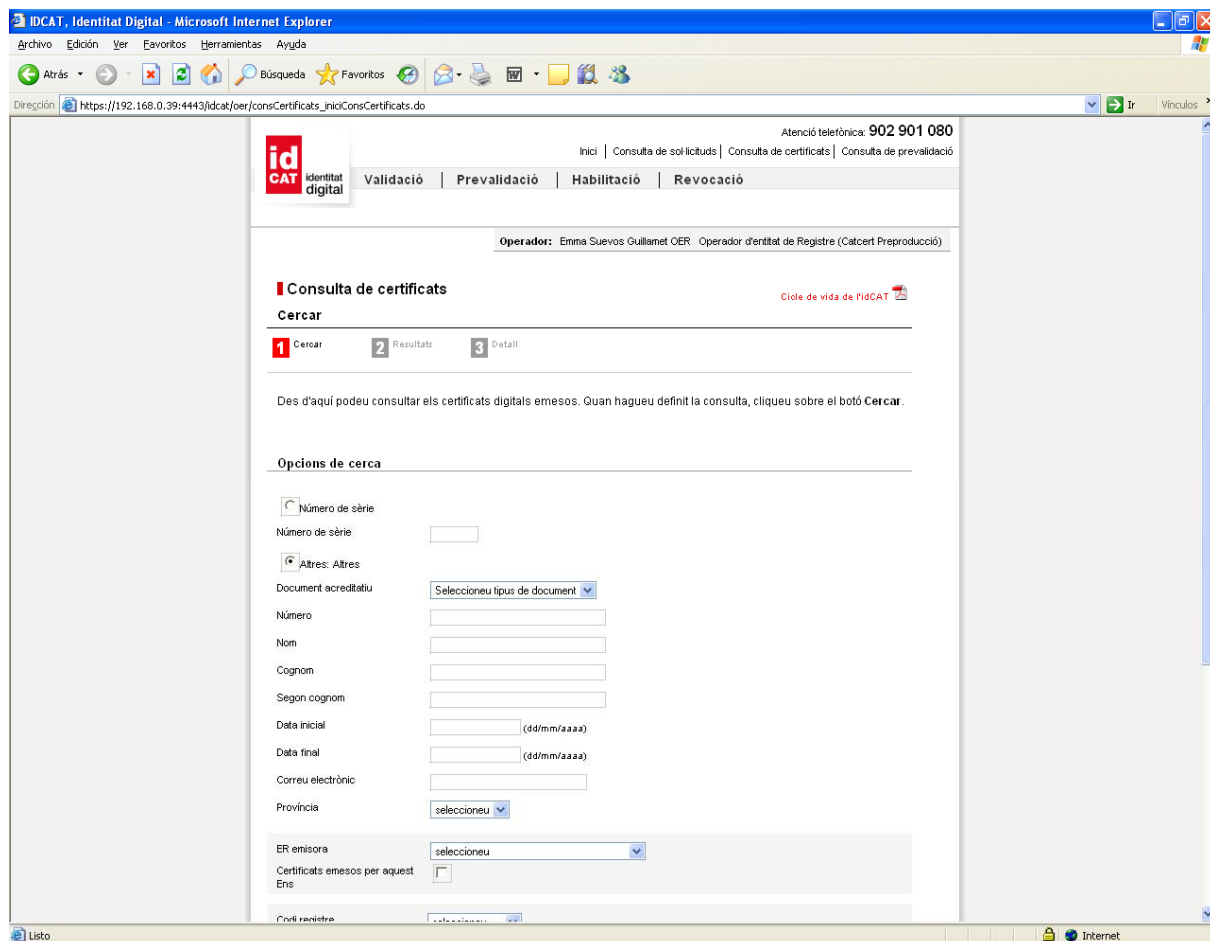
L'Operador ha d'accedir a l'enllaç Revocació que es troba al marge superior de la pàgina web (fig. 6).



(fig. 6)

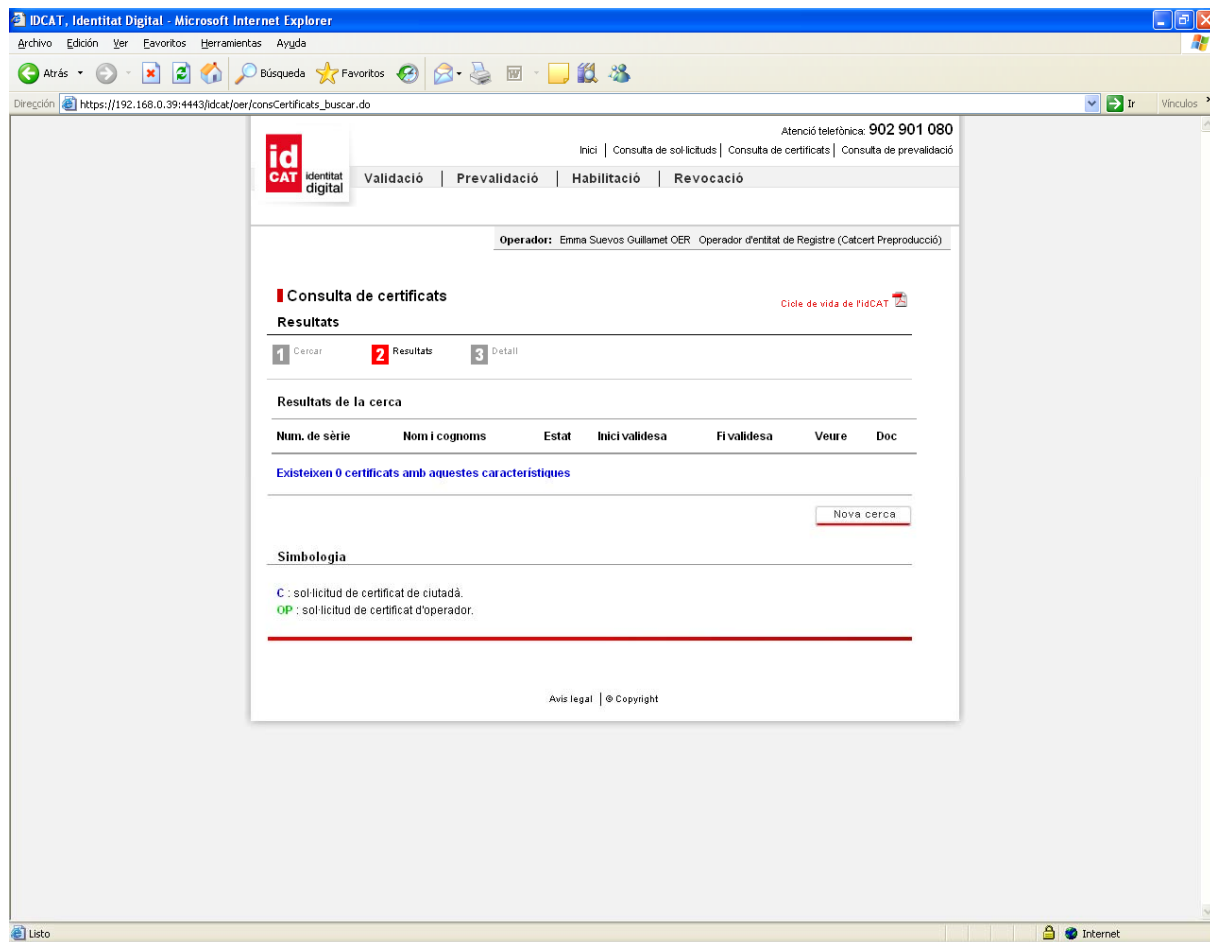
En aquesta pantalla, l'Operador d'Entitat de Registre idCAT podrà buscar el certificat que es vol revocar a partir del document identificatiu que el subscriptor ha fet servir en el moment de fer la sol·licitud del certificat digital. Com a documents identificatius es permet seleccionar el NIF -DNI amb lletra-, el NIE, el passaport o el DNI d'altres països. Un cop seleccionat el tipus de document, s'ha d'introduir el número de document i accedir a l'enllaç Cercar.

Per altra banda, existeix una altra forma de cercar el certificat que volem revocar, clicant en el menú de la part superior de la web **Consulta de certificats**, que ens farà accedir a una pàgina on podrem indicar dades addicionals per filtrar entre tots els certificats (fig. 7).



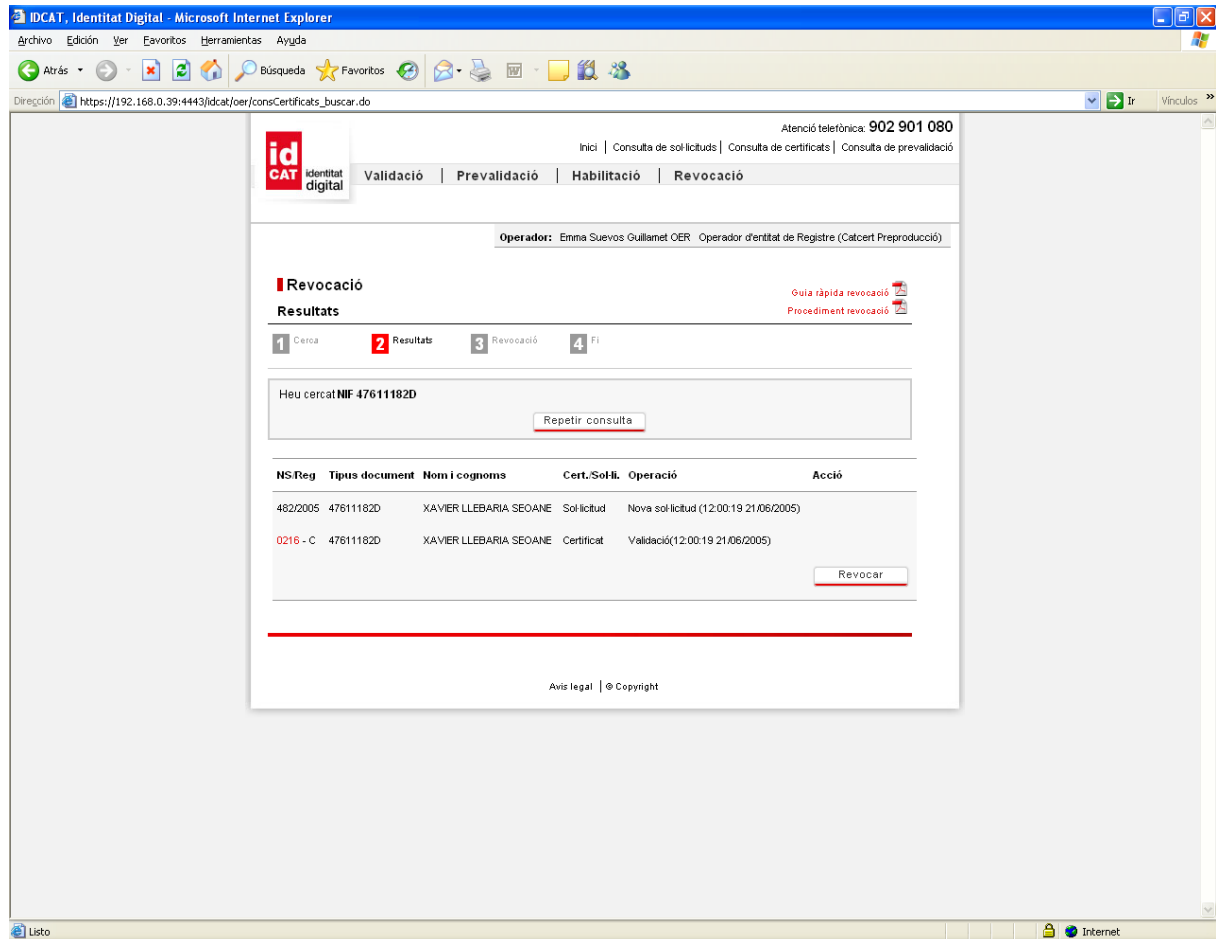
(fig. 7)

Si la cerca no troba cap certificat amb el document acreditatiu indicat, ens mostrarà el següent comentari (fig. 8).



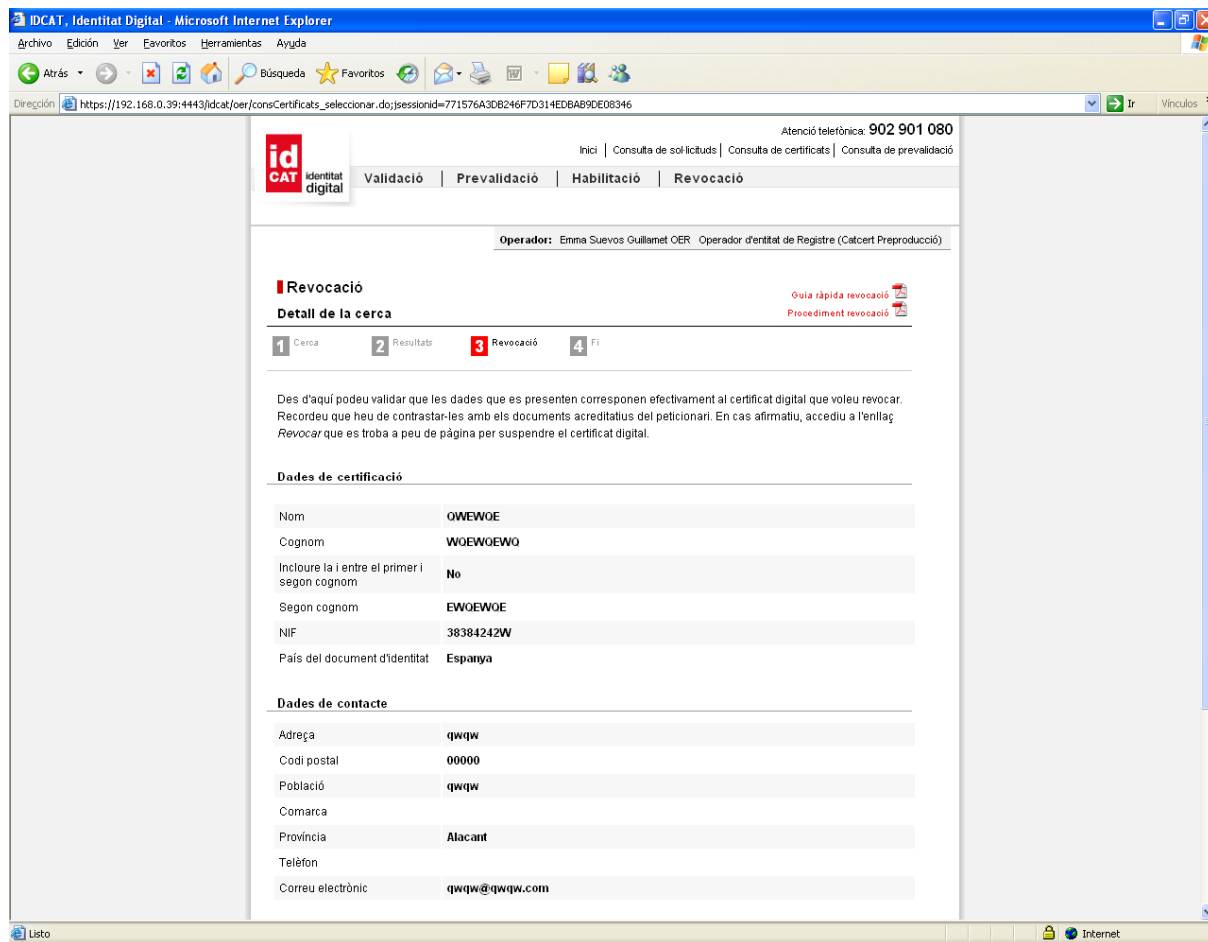
(fig. 8)

Si el número de document s'ha introduït correctament i existeix un certificat que coincideixi amb les dades identificatives, s'accedeix a la pàgina de resultats de la cerca. Accedirem als certificats clicant sobre **Revocar** o sobre el **número de registre** (fig. 9).



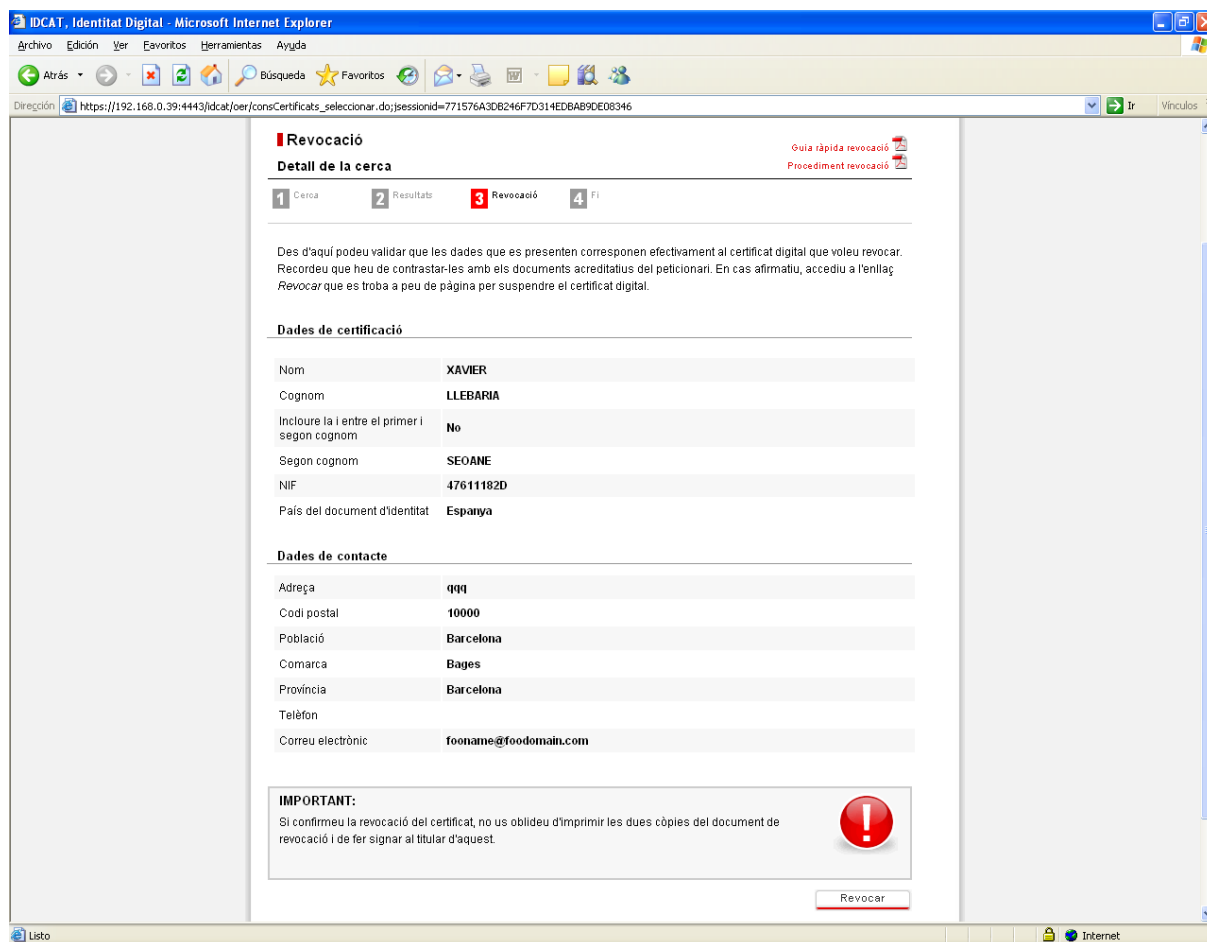
(fig. 9)

Per accedir al contingut del certificat a revocar cal clicar el botó Revocar des del qual s'accedeix a la següent pantalla (fig. 10):



(fig. 10)

Un cop verificades les dades del ciutadà (fig. 11) clicarem **Revocar**, i abans de confirmar la revocació haurem d'escollir el motiu de la mateixa (fig. 12).

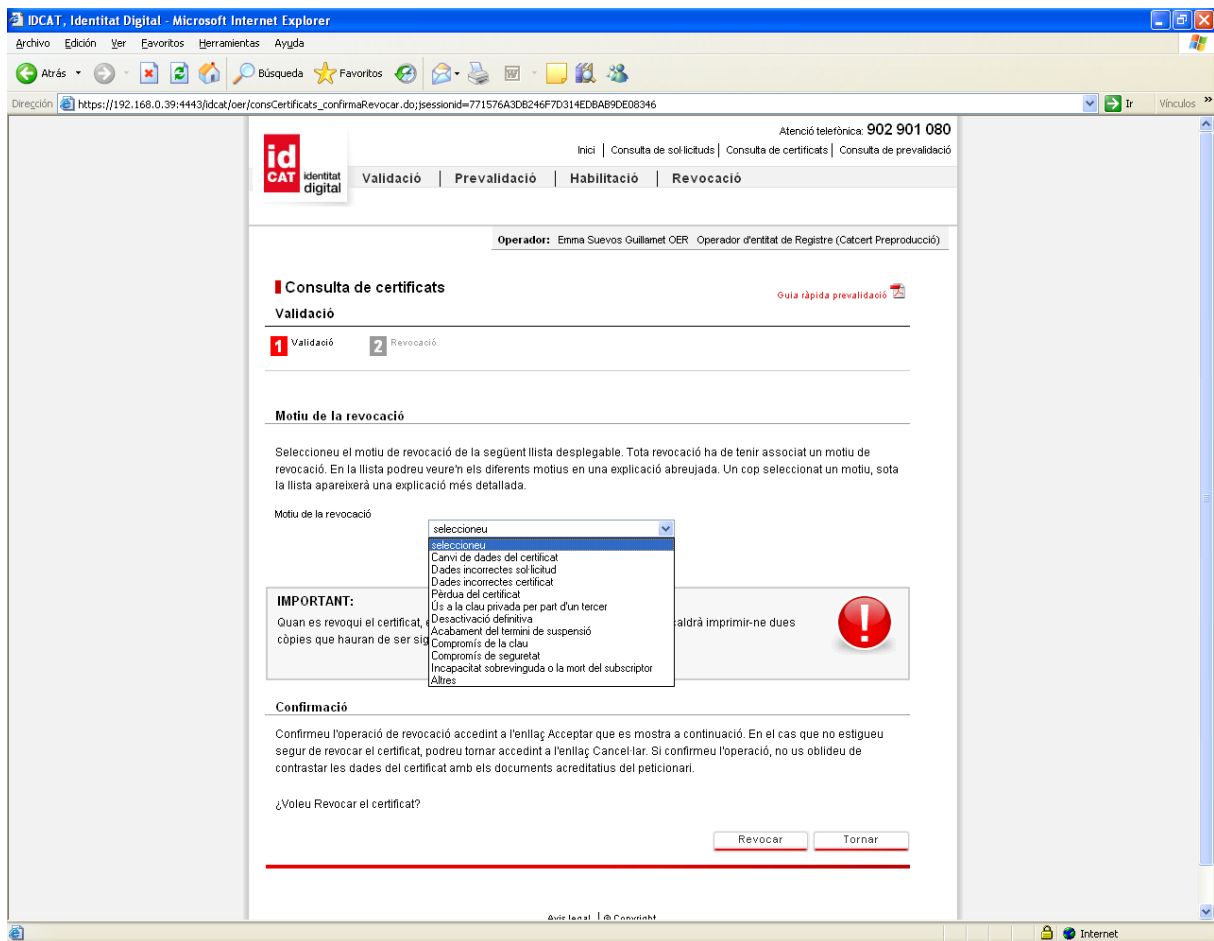


(fig. 11)

Els motius pels quals un subscriptor pot voler revocar el seu certificat són els següents (fig.12):

- Canvi de dades del certificat: Quan el subscriptor ha canviat alguna de les dades que apareixen al certificat i el vol revocar per tal de fer una sol·licitud amb les noves dades.
- Dades incorrectes a la sol·licitud: Quan el subscriptor vol obtenir un altre certificat personal perquè va introduir dades incorrectes al fer la sol·licitud del seu certificat.
- Dades incorrectes al seu certificat: Quan el subscriptor detecta alguna dada que no és correcta.
- Pèrdua del certificat: El subscriptor ha perdut el seu certificat que estava emmagatzemat en un suport electrònic i no el localitza, o es trobava emmagatzemat en un ordinador que ha sofert l'eliminació o pèrdua de la informació.
- Ús o compromís de la clau privada per part d'un tercer: El subscriptor sospita que alguna persona podria haver tingut accés al seu ordinador o a un suport electrònic on estava emmagatzemat el certificat, la qual cosa permetria a aquest infiltrat fer un ús il·lícit del certificat

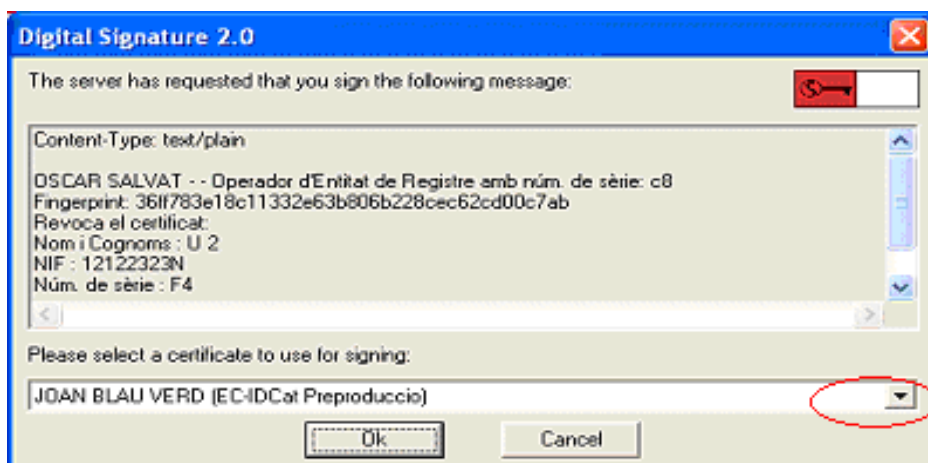
- Desactivació definitiva: El subscriptor no vol tornar a fer servir mai més el certificat, de manera que opta per la seva desactivació definitiva.
- Acabament del termini de suspensió: Durant el període de suspensió el subscriptor pot demanar la revocació del certificat si té la certesa que no el podrà recuperar.
- Defunció o incapacitat sobrevinguda.
- Oblit de les claus d'accés al dispositiu (PIN i PUK).
- Error en la generació del certificat.



(fig. 12)

Quan haguem escollit el motiu de la revocació, podem confirmar la revocació clicant de nou **Revocar**.

En aquest moment, l'aplicació sol·licitarà el certificat CIPISR-2 de l'Operador d'Entitat de Registre idCAT i haureu de seleccionar el certificat corresponent (fig. 13).



(fig. 13)

NOTA: Recordeu que si no us apareix el vostre certificat per defecte heu d'obrir el desplegable i seleccionar-lo. Després de comprovar que és el vostre, cliqueu el botó "OK".

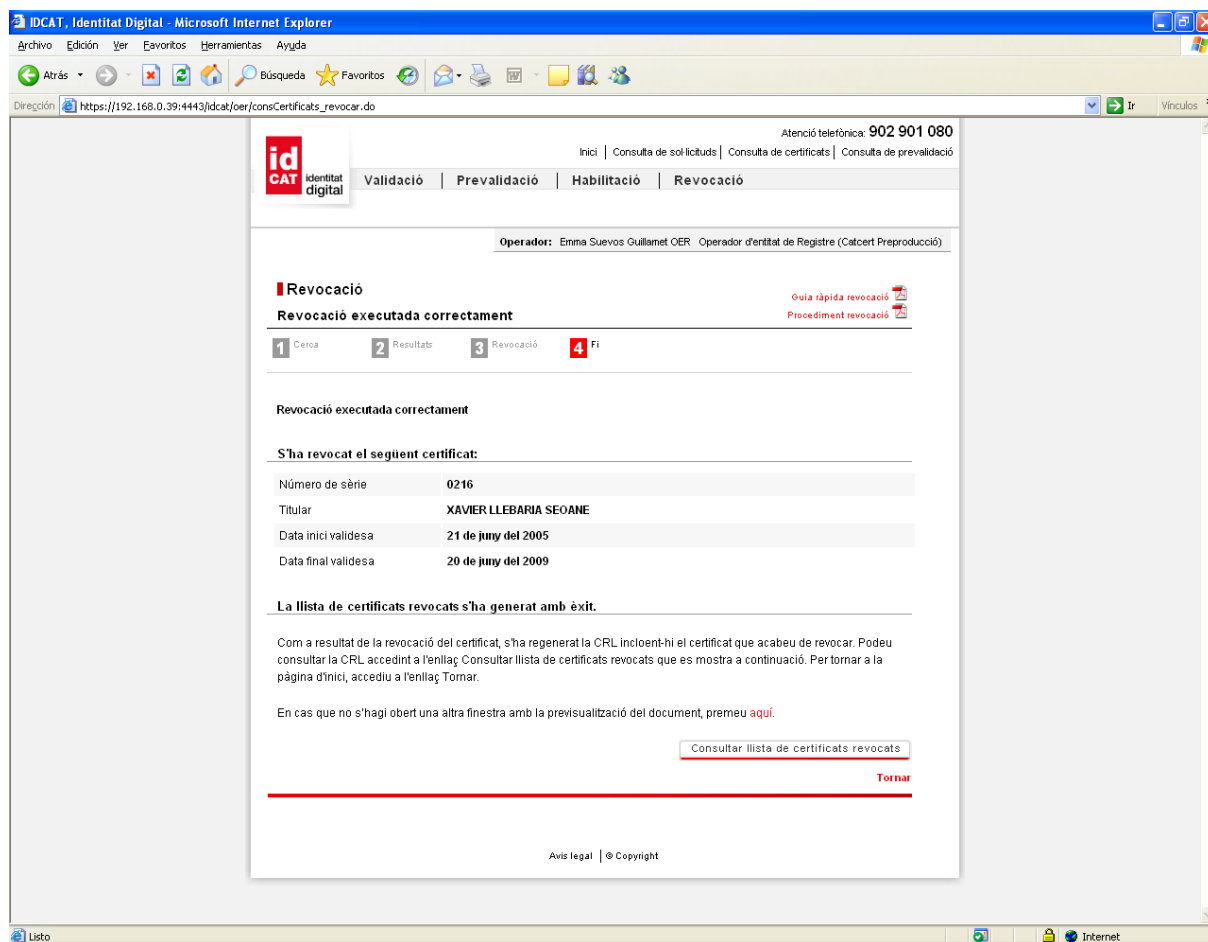
Introduïu el vostre PIN i cliqueu el botó "D'acord". (fig. 14)



(fig. 14)

NOTA: Recordeu que en aquest procés es porta a terme la signatura digital del formulari de confirmació de revocació, de manera que és imprescindible que la targeta d'OER estigui introduïda al lector de targetes.

Un cop signada l'operació per part de l'operador, automàticament el sistema ens mostrarà una nova plana amb la confirmació de l'operació.



(fig. 15)

A més, es genera el document de revocació, del qual n'haurem d'imprimir dues còpies (Annex 1). Aquest document tindrà la capçalera de l'Entitat de Registre idCAT, que haurà de ser signada pel subscriptor. A més, aquest document s'ha de registrar d'entrada en el registre general i corporatiu de l'organisme i segellar amb indicació de les següents dades: especificació del registre de què es tracti, el número d'entrada assignat al document i la data i hora d'alta al registre, o si, com a l'Annex 1 teniu activada en la vostra entitat de registre l'opció del registre auxiliar, aquest us apareixerà automàticament. Una còpia d'aquest document, juntament amb la fotocòpia compulsada del document d'identificació del ciutadà, l'haureu d'arxivar i conservar correctament durant 15 anys a l'arxiu de l'ens, segons recull l'article 20.1.f de la Llei 59/2003, de 19 de desembre, sobre signatura electrònica.

En el cas que l'operador tingui els elements emergents bloquejats, no s'obrirà el document de Sol·licitud d'habilitació per defecte. Per tal de visualitzar-lo, pot desbloquejar-los o clicar el missatge "Aquí" que apareix a la figura 15.

A partir d'aquest moment, aquest certificat ja no podrà ser utilitzat i la llista de certificats revocats (CRL) s'actualitzarà, afegint-hi el número de sèrie del certificat que acaba de ser revocat. A més, aquesta llista podrà ser descarregada a través de l'enllaç que es mostra en la pantalla **Consultar Llista de Certificats Revocats**.

Les CRL s'emeten periòdicament (amb una freqüència de dues vegades al dia) i s'actualitzen cada cop que hi ha una habilitació, suspensió i/o revocació i s'emmagatzemen en una taula de base de dades de forma automàtica. L'únic rol que disposa d'accés físic directe a la base de dades és l'administrador del sistema.

A més, s'enviarà automàticament un correu electrònic al subscriptor del certificat revocat, confirmant la revocació.

Una vegada que un certificat és revocat no podrà tornar a utilitzar-se mai més, per la qual cosa en el cas que el subscriptor volgués tornar a disposar d'un certificat digital CPIXSA-2, hauria de tornar a sol·licitar-ne un de nou.

2.4.2 Arxiu de la sol·licitud de revocació del certificat

L'Entitat de Registre idCAT haurà d'organitzar i emmagatzemar tota la documentació que es generi quan el subscriptor d'un certificat digital sol·licita la seva revocació, i aquesta documentació haurà de custodiar-se en l'arxiu de l'ens durant 15 anys, a comptar a partir de la data de revocació del certificat.

La documentació que s'haurà de conservar és la fotocòpia compulsada del document identificatiu i una còpia signada i registrada del document de confirmació de revocació del certificat.

El subscriptor del certificat pot presentar la sol·licitud de revocació a una Entitat de Registre idCAT diferent a la qual es va dirigir quan va presentar la sol·licitud de validació. Per a assegurar l'arxiu correcte de les sol·licituds de revocació, l'Entitat de Registre idCAT ha d'obrir un expedient de revocacions, independent del d'obtenció de certificats anual i ordenat pel número de registre d'entrada de la sol·licitud. Quan la carpeta tingui un gruix excessiu s'haurà de partir en tants volums com siguin necessaris per evitar manipulacions incorrectes (per exemple, en el volum 1 trobarem les habilitacions de certificats de l'1 a la 25, i en el segon, de la 26 a la 50).

Els expedients han d'anar retolats de manera uniforme, amb una informació mínima. Les dades que han de constar a la caràtula de la carpeta d'expedient són:

- **Número expedient:** codi alfanumèric que identifica de manera individualitzada l'expedient. Es recomana obrir un expedient per cada 25 operacions del mateix tipus, és a dir, un expedient a cada 25 revocacions, i així en endavant, degudament numerats. P.e.: REV_01_2009 (amb les primeres 25 habilitacions del 2009).

- **Data d'obertura de l'expedient:** només hi constarà l'any.
- **Data de tancament de l'expedient:** només hi constarà l'any.
- **Codi de classificació:** Codi que identifica la sèrie documental a la qual pertany l'expedient. Aquesta nova entrada s'haurà d'afegir al quadre de classificació de la documentació administrativa de la institució. L'actualització del quadre és responsabilitat de l'arxiver de la institució, però pot demanar assessorament a l'arxiver de CATCert a l'hora de definir la nova entrada.
- **Títol:** Paraula, frase que dona el nom precís a l'expedient, atenent al seu contingut essencial. En aquest cas, el títol genèric que s'utilitzarà serà: *Revocacions certificats idCAT*.
- **Nom del productor:** Identificar el productor de l'expedient; el nom abreujat de la unitat administrativa que gestiona l'expedient. Aquesta dada és útil en els casos d'un ens que té diverses ER idCAT.

Annex 1: Sol·licitud de Revocació del certificat idCAT

| | |
|----------------------------|----------------------------|
| Espai pel logotip de l'ERC | Ref.: <codi de referència> |
|----------------------------|----------------------------|

Sol·licitud de revocació del certificat idCAT

<Nom i Cognoms>, amb <Document acreditatiu> <número>, amb domicili a <adreça: carrer, avinguda o plaça, número, pis i porta> de <Localitat> (<codi postal>),

Exposa:

Que per mitjà del present document, i en relació amb el procediment de revocació del certificat idCAT de l'Agència Catalana de Certificació – CATCert, compareix davant d'aquesta oficina.

Que el motiu de revocació del certificat idCAT del que és subscriptor és el marcat a la següent llista:

| | |
|--------------------------|--|
| <input type="checkbox"/> | Canvi de les dades contingudes al certificat (p.e. canvi de correu-e) |
| <input type="checkbox"/> | Descobriments de dades incorrectes a la sol·licitud (p.e. error ortogràfic) |
| <input type="checkbox"/> | Descobriments de dades incorrectes al certificat (p.e. error ortogràfic) |
| <input type="checkbox"/> | Pèrdua o inutilització del dispositiu criptogràfic o del certificat |
| <input type="checkbox"/> | Ús o accés a la clau privada del certificat per part d'un tercer (p.e. compromís de la clau privada per manca de diligència a la custòdia) |
| <input type="checkbox"/> | Desactivació definitiva, per la simple voluntat |
| <input type="checkbox"/> | Acabament del termini de suspensió |
| <input type="checkbox"/> | Compromís o sospita del compromís de la clau o del certificat |
| <input type="checkbox"/> | Compromís de seguretat |
| <input type="checkbox"/> | Incapacitat sobrevinguda o la mort del subscriptor |

| | |
|--------------------------|--|
| <input type="checkbox"/> | Oblit de les claus d'accés al dispositiu (PIN i PUK) |
| <input type="checkbox"/> | Revocació d'ofici per error en la generació del certificat |
| <input type="checkbox"/> | Altres |

Sol·licita:

Que sigui emesa copia compulsada del meu **<document acreditatiu>** **<número>** que lliura personalment, per tal de ser incorporada, junt a la sol·licitud, al corresponent expedient.

Que en virtut de tot l'anterior, s'accepti la documentació presentada, i en cas de compliment de tot allò que antecedeix, es revoqui el certificat idCAT d'acord amb les *Condicions Generals d'Emissió dels Certificats idCAT* i la *Declaració de Pràctiques de Certificació*, amb les quals manifesta la seva conformitat i pot consultar-ne el contingut a **www.catcert.cat/registre**.

Número de sèrie: **<número de sèrie del certificat>**

<Localitat>, **<data de la sol·licitud>**

<Espai per a la signatura>

<Nom i Cognoms del subscriptor>

*** La revocació és un estat definitiu del certificat**

Per qualsevol consulta, posi's en contacte amb el centre d'atenció a l'usuari per correu-e electrònic a **info@idcat.cat**.

<NOM DE L'ERC>. Entitat de registre idCAT