Consorci
Administració Oberta
de Catalunya

Usos del certificat digital amb dispositius mòbils iPhone/iPad

Generalitat
de Catalunya

LOCALRET

1 Introducció

El present document té per objectiu descriure el procés de configuració d'un dispositiu iPhone o iPad per poder fer ús dels certificats digitals del Consorci Administració Oberta de Catalunya (Consorci AOC).

1.1 Abast

Aquest document va destinat als usuaris d'iPhone o iPad que vulguin utilitzar el certificat digital amb aquest dispositiu.

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 què cal executar-los.

1.3 Requisits previs

Aquest manual assumeix que l'usuari disposa de:

- iPhone amb sistema operatiu 7.1.2 o superior amb connectivitat a Internet.

O bé

- iPad amb sistema operatiu 7.1.2 o superior amb connectivitat a Internet.

2 Baixada i instal·lació de les claus públiques del Consorci AOC

Per poder utilitzar els certificats i que no apareguin errors de confiança, s'ha d'indicar al dispositiu 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 dispositiu mòbil.

2.1 Obtenir les claus públiques del Consorci AOC

Les claus es poden baixar des de la pàgina de baixada de claus públiques del web del Consorci AOC. S'hi pot accedir mitjançant la pàgina principal del Consorci AOC (http://www.aoc.cat), fent clic a "CATCert" i després a la pestanya "Claus", o accedint directament a http://www.aoc.cat/Inici/SERVEIS/Signatura-electronica-i-seguretat/CATCert/Claus.

Figura 1

Figura 2

Cal seleccionar les claus públiques de les Entitats Certificadores corresponents.

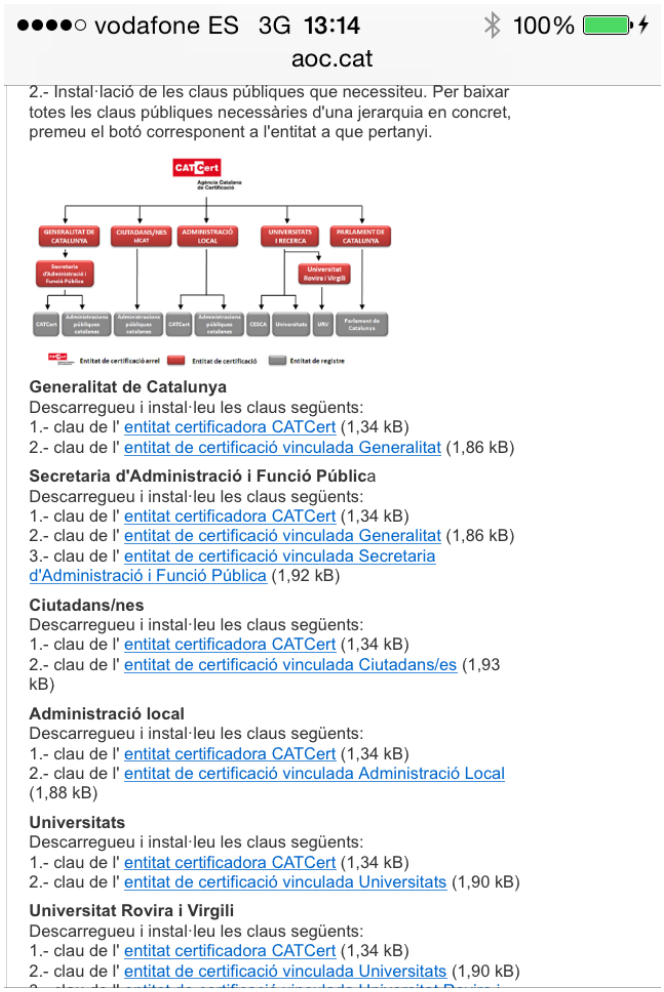

Figura 3

Al seleccionar una entitat, es descarrega el certificat i tenim l'opció d'instal·lar-lo com un perfil.

2.2 Instal·lació de les claus públiques (Perfils)

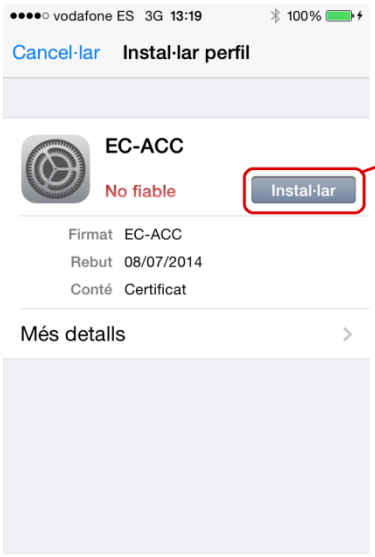

Figura 4

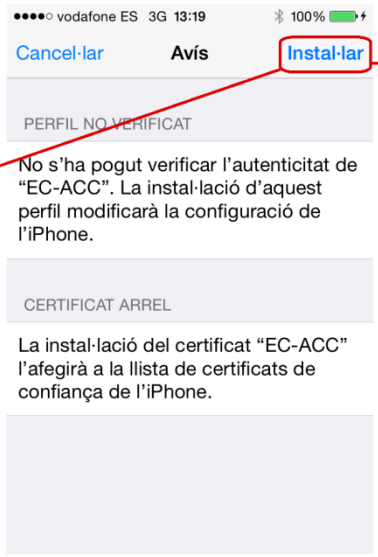

Figura 5

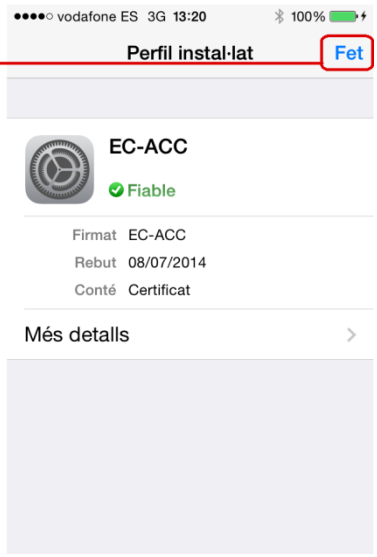

Figura 6

Per poder visualitzar el certificat que s'ha baixat i s'ha d'instal·lar, fem clic a l'opció "Instal·lar" per iniciar l'assistent (Figura 4), que ens mostra l'avís que s'afegirà com a certificat arrel de confiança de l'iPhone / iPad. Al fer clic en el botó "Instal·lar" (Figura 5) ens informa que la instal·lació s'ha realitzat correctament i que ara ja serà de confiança ("Fiable") (Figura 6). Quan fem clic en el botó "Fet" el procés haurà finalitzat.

2.3 Verificació de les claus públiques instal·lades

Per verificar que disposem de les claus públiques instal·lades s'ha d'anar a "Configuració" -> "General" i l'opció de "Perfils". Aquí podem veure els certificats instal·lats.

3 Importació de certificats personals en programari

Els certificats digitals personals en programari estan desats en fitxers amb extensió .P12 o .PFX. Per importar el certificat digital en l'iPhone o l'iPad cal accedir a aquest fitxer des del propi dispositiu. Una manera fàcil és enviar el fitxer .P12 o .PFX per correu electrònic (Figura 7) o qualsevol via que permeti descarregar o accedir al certificat a través del navegador Safari (per exemple, Dropbox, Google Drive o gestors de correu amb accés web).

Figura 7

Un cop obrim el fitxer s'activa l'assistent d'instal·lar un perfil:

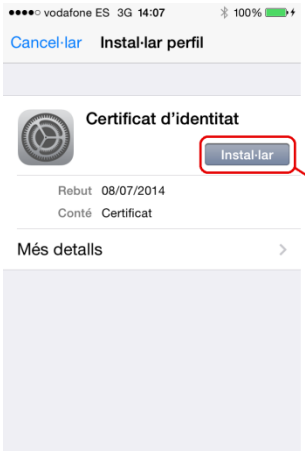

Figura 8

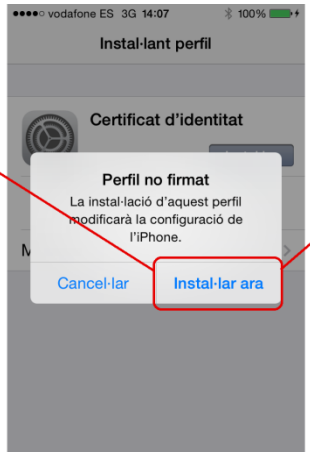

Figura 9

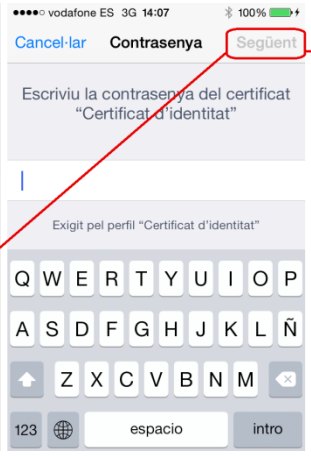

Figura 10

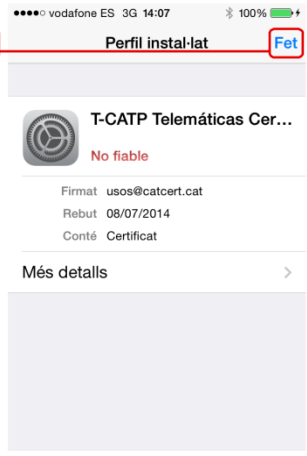

Figura 11

Seleccionem "Instal·lar" i ens notifica que això modificarà la configuració de l'iPhone. Fem clic a "Instal·lar ara" i ens demana que escrivim la paraula de pas que protegeix el certificat en programari. Un cop introduïda correctament, el sistema ens confirma que el perfil s'ha instal·lat correctament.

4 Autenticació amb certificats

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

4.1 Autenticació de servidor/portal web

Aquest mecanisme està integrat totalment en qualsevol navegador i es pot visualitzar normalment de dues formes:

- Per un costat, l'adreça de la web a visitar comença amb HTTPS://.....
- Per altra banda, el navegador activarà internament un protocol (anomenat SSL) que fa aparèixer un cadenat al costat de l'adreça, que indica que es tracta d'una web segura.

Exemple

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

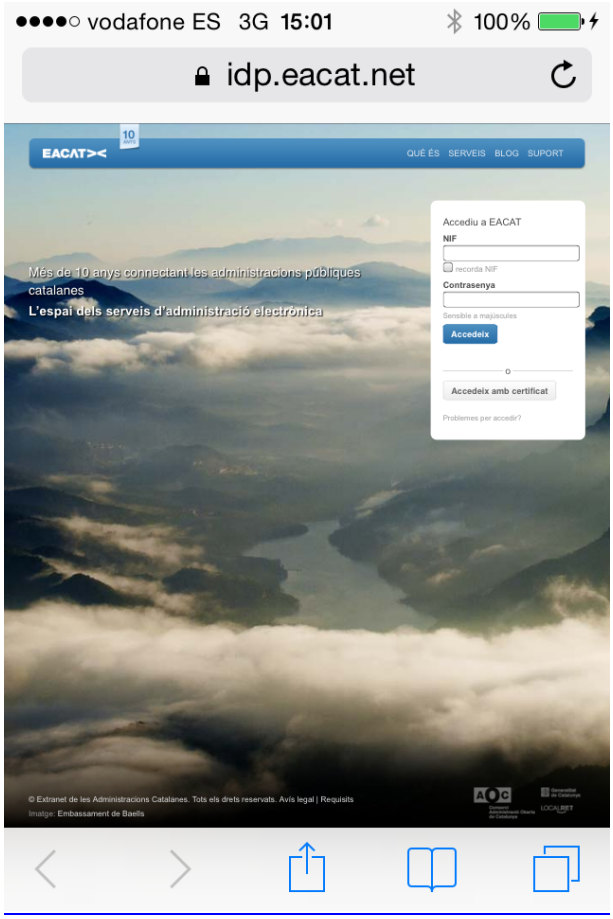

Figura 12

Nota:

Un error freqüent que es pot apreciar és quan el navegador no disposa de les claus públiques de l'emissor del certificat, i per tant, el navegador no reconeix l'entitat que va emetre el certificat. Aleshores pregunta a l'usuari si vol abandonar la navegació o confia en el lloc web. En aquest cas caldrà carregar les claus públiques de l'emissor o bé indicar que es vol continuar.
També es pot donar el cas que el nom (adreça URL) del portal no coincideixi amb el que consta en el certificat. El navegador també demanaria a l'usuari si vol abandonar la navegació o confia en el lloc web. En aquest cas, caldria indicar que es vol continuar.

Exemple:

https://213.27.191.125/web/guest/Eacat

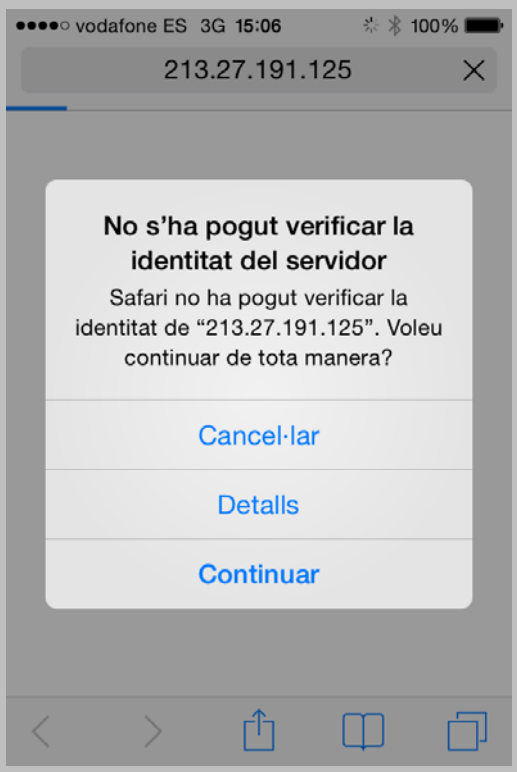

Figura 13

4.2 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 amb certificat. L'usuari només pot utilitzar els certificats que el gestor de certificats indiqui que té disponibles.

Nota:

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

Exemple:

El web de http://www.ingdirect.es només accepta els certificats d'e-DNI i no permet l'accés amb d'altres certificats.

Figura 14

Quan l'usuari entra en un portal o enllaç web o fa un clic i se li demana autenticació, apareix una finestra indicant que es requereix l'ús de certificat digital.

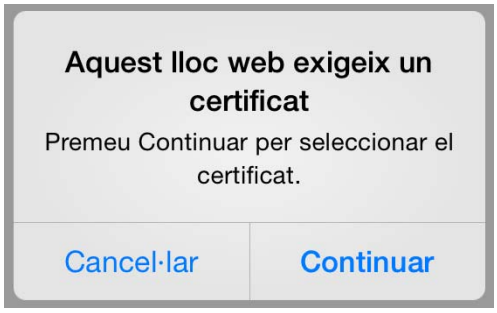

Figura 15

En aquest punt, s'ha de seleccionar el certificat que es vol utilitzar, si en tenim diversos disponibles.

Figura 16

Un cop seleccionat el certificat a utilitzar, el portal rebrà aquell certificat per la nostra identificació. Cal tenir present que, pel fet de tenir certificat digital, no tenim accés a tots els portals que permeten la identificació amb aquest sistema ja que, per exemple, encara que tinguem un certificat vàlid, si l'usuari no està identificat o el portal no en té dades, la resposta serà que no troba informació o a l'usuari (això passa, 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).

4.3 Altres usos

L'iPhone i l'iPad disposen d'altres funcionalitats on es poden utilitzar els certificats personals carregats, com són:

- Creació de VPN amb autenticació de certificat
- Connexió a xarxa Wifi amb certificat