Ajuntament de L'Hospitalet
Àrea de Qualitat Urbana
Servei de Sistemes d'Informació Territorial

SOLUCIÓ

AL FUNCIONAMENT INCORRECTE

DE L'APP L'H BEN FET

SOBRE ALGUNES VERSIONS ANTIGUES

DE IOS

Índex

Problema detectat 3
Problema 3
Possible causa 3
Renovació de certificats 3
Explicació 3
Quins són els actors en la comunicació en el cas de l'*app* L'H Ben Fet? 3
Què és un certificat? 3
Les autoritats de certificació 3
Establiment d'un canal de comunicació cibersegur 4
Els certificats renovats 4
Possible solució 4
Instal·lació de certificat des d'una autoritat de certificació reconeguda 4
Mètode per solucionar el funcionament incorrecte 5
Pas 1 5
Pas 2 5
Pas 3 6
Pas 4 7

Problema detectat

Problema

Alguns dels dispositius mòbils (*mòbil*, a partir d'ara) amb sistema operatiu iOS, desenvolupat pel fabricant *Apple*, no executen bé el programa informàtic per a mòbils (*app*, a partir d'ara) **L'H Ben Fet** v.2.0. De fet, alguns, quan l'inicien, des d'un temps enrere, resten en un estat d'esperar que sembla que l'*app* no fa res.

Possible causa

Renovació de certificats

La causa més probable d'aquest comportament és el nou certificat digital (*certificat*, a partir d'ara) instal·lat al servidor municipal al febrer de 2026, al qual, l'*app* accedeix a l'inici del seu funcionament.

Explicació

Quins són els actors en la comunicació en el cas de l'*app* L'H Ben Fet?

Quan una *app* funciona en un mòbil, habitualment es comunica digitalment amb uns altres programes informàtics que funcionen en una altra màquina, el servidor. En el cas de l'*app* **L'H Ben Fet**, o la seva nova versió **L'H A Punt**, els actors principals en l'acte de comunicació són:

- La mateixa *app* **L'H Ben Fet**.
- El servidor municipal; és a dir, els programes informàtics que estan funcionant als ordinadors que representen l'Ajuntament de l'Hospitalet.

Ambdós poden actuar d'**emissor** o de **receptor** en la comunicació bidireccional que mantenen. És a dir, unes vegades, l'*app* actua com a emissora, perquè envia informació al servidor municipal, que actua com a receptor; i, d'altres, l'*app* actua com a receptora de la informació que li envia el servidor municipal, que actua com a emissor.

Què és un certificat?

Sense ànim de ser estrictament precisos, podem afirmar que un **certificat** és un document digital —és a dir, un fitxer digital— que està emmagatzemat en algun lloc (*instal·lat* , a partir d'ara), que serveix per garantir la correcta identitat dels actors, ja sigui de l'emissor, ja sigui del receptor, ja sigui d'ambdós, i que la comunicació sigui segura, per exemple, mitjançant el xifratge dels missatges intercanviats.

Els certificats tenen data de caducitat —és a dir, no són vàlids per sempre— i són emesos per **entitats** o **empreses certificadores** (*autoritat de certificació*, a partir d'ara). A aquests certificats, de vegades, li diem **certificats arrels**.

Les autoritats de certificació

D'autoritats de certificació n'hi ha moltes, però han de ser reconegudes —és a dir, han de tenir la confiança— pels programes informàtics que utilitzen els seus certificats. Els sistemes operatius no deixen de ser programes informàtics, sobre els quals, s'executen altres programes, com les *app*s.

Algunes de les autoritats de certificació reconegudes són: *DigiCert*, *Sectigo*, *GlobalSign*, *Let's Encrypt*, *Entrust* o altres autoritats de certificació europees, com la *FNMT* (o *Fàbrica Nacional de Moneda y Timbre*), *CATCert* (de l'Agència Catalana de Certificació), *DNI Electrónico* (de la Dirección General de la Policía)... També *Apple Root Certification Authority* (per al cas del sistema operatiu iOS que utilitzen els mòbils iPhone d'Apple)

Per al cas d'un mòbil amb una versió del sistema operatiu Android determinada, es pot consultar les autoritats de certificació reconegudes seguint la següent cadena Ajustos → Seguretat i privacitat → Més opcions de seguretat, tot tenint en compte que cada implementació d'Android pot mostrar aquesta informació de diverses maneres.

Establiment d'un canal de comunicació cibersegur

A l'iniciar-se l'*app*, la primera cosa que aquesta realitza és intentar obrir un espai de comunicació (*canal*, a partir d'ara) que estigui protegit front a accessos no autoritzats, per evitar danys o atacs digitals (*canal cibersegur*, a partir d'ara).

Mitjançant els seus propis certificats, l'*app* accedeix als certificats del servidor. Si el reconeixement i confiança són correctes, l'*app* s'inicia correctament i pot començar a funcionar. Si no, no.

Un mòbil que funciona sobre un sistema operatiu que compta amb una llista d'autoritats de certificació que no contempla la que ha emès els certificats instal·lats al servidor municipal, molt probablement, no podrà establir un canal de comunicació cibersegur quan l'*app* s'inicia.

Els certificats renovats

Quan un certificat caduca, s'ha de renovar. Per aquesta raó, el febrer de 2026, al servidor municipal s'hi van renovar els certificats caducats que hi estaven instal·lats.

Algunes versions d'iOS antigues no reconeixen l'autoritat de certificació que ha emès el nou certificat que té instal·lat el servidor municipal. Això passa, per exemple, amb les versions anteriors a la 17, simplement, perquè aquesta versió del sistema operatiu iOS és anterior a la data d'emissió del certificat esmentat.

Possible solució

Instal·lació de certificat des d'una autoritat de certificació reconeguda

A més de la possibilitat més evident —fer-se amb un mòbil més modern o que compti amb un sistema operatiu que tingui preinstal·lada una llista d'autoritats de certificació que inclogui la que ha emès els certificats utilitzats al servidor municipal—, una possible solució consisteix en instal·lar un determinat certificat al mòbil sobre el qual no funciona l'*app*: el certificat **Sectigo Public Server Authentication Root R46**.

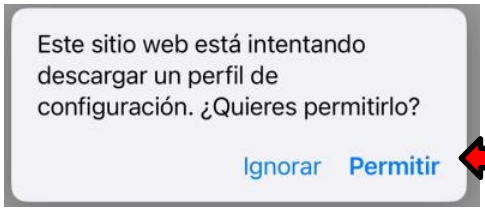
Aquest certificat ja ve integrat al sistema operatiu iOS 17.4 (https://support.apple.com/es-es/121728). En dispositius anteriors és el mateix usuari qui ha d'instal·lar l'esmentat certificat perquè la connexió als servidors de l'Ajuntament de l'Hospitalet pugui verificar-se i acreditar-se com a segura.

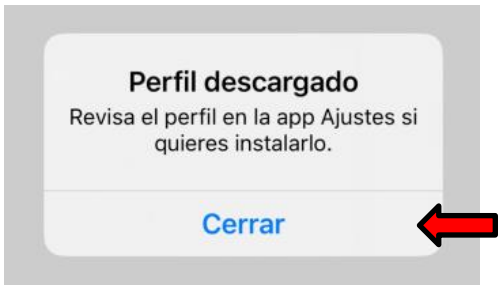
Mètode per solucionar el funcionament incorrecte

Pas 1

Descarregui el certificat des de la web de Sectigo:

http://crt.sectigo.com/SectigoPublicServerAuthenticationRootR46.crt

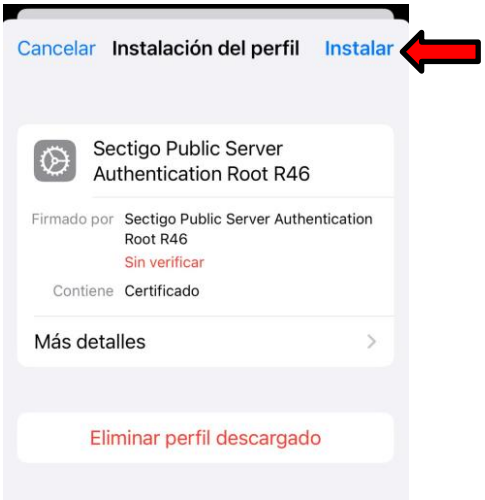




Pas 2

Vagi a la secció **Ajustes** del seu mòbil on hauria d'aparèixer l'opció **Perfil descarregat**.

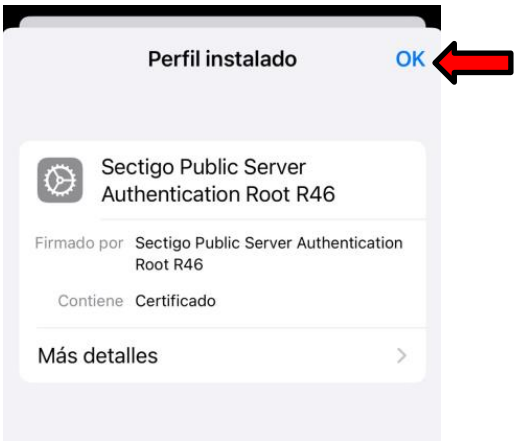
Al clicar li proposarà la instal·lació del certificat **Sectigo Public Server Authentication Root R46**.



Seleccioni **Instal·lar**.

Apareixerà un missatge que informa que s'afegirà el certificat a la llista de certificats de confiança i que deu activar-lo, quan estigui instal·lat, perquè comenci a funcionar.

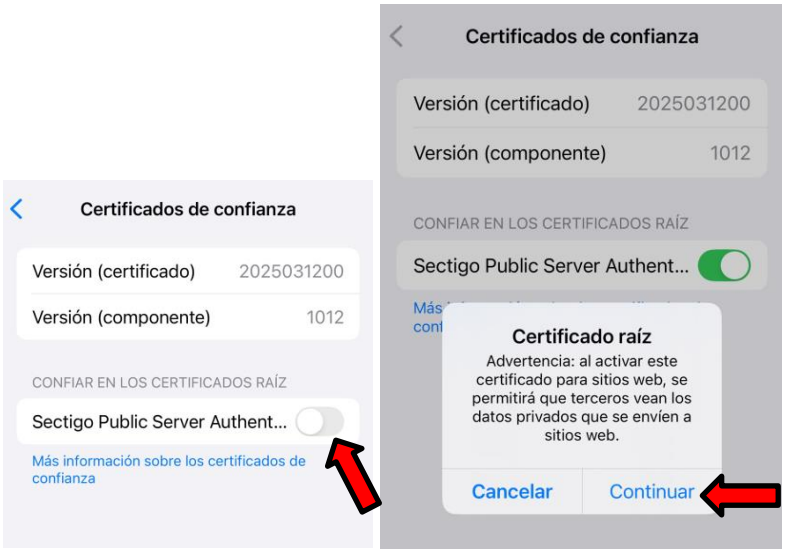
El procés d'instal·lació finalitzarà quan aparegui el missatge **Perfil instal·lat**.



Pas 3

Activi el certificat perquè comenci a funcionar. Per fer-ho, vagi a **Ajustos** → **General** i accedeixi a la secció **Certificats de confiança**.

Finalment, activi el certificat **Sectigo Public Server Authentication Root R46**.



Pas 4

Provi de nou l'*app* i verifiqui si funciona.

En mòbils amb la versió 16 d'iOS, en concret, al model iPhone 8, aquest mètode ha estat provat amb èxit.