

Manual d'instal·lació del Certificat de Dispositiu Servidor (CDS) i les claus públiques al servidor web Iplanet

Control documental

Estat formal	Elaborat per: Àrea Alcaide	Aprovat per: Francesc Ferré
Data de creació	28/01/2008	
Control de versions	Data:	28/01/2008
	Descripció:	Creació del document
Nivell accés informació	pública	
Títol	Manual de gestió del certificat de servidor a l'Apache HTTP Server.	
Fitxer	Installacio_CDS_i_Claus_Públiques_Iplanet_v1.0.doc	
Control de còpies	Només les còpies disponibles a Ubicació de les còpies controlades 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/ o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.	

Introducció

En aquest manual es descriu el procediment a seguir per configurar el servidor web Apache per admetre transmissions segures d'informació sota SSL/TLS.

El Certificat de Dispositiu Servidor (CDS) conté informació sobre les claus públiques que cal instal·lar. Per tant, s'ha de tenir en compte que no només cal instal·lar el CDS, sinó també els certificats de les Entitats de Certificació intermèdies i arrel de CATCert que han intervingut en l'emissió del CDS, és a dir, tots els certificats de la cadena de certificació. Això és necessari ja que, en la majoria dels casos, els clients no tindran instal·lats en els seus navegadors els certificats de les Entitats de Certificació intermèdies de CATCert, però sí tindran instal·lat el certificat arrel (instal·lat per defecte en Windows XP SP2 i Windows Vista), i, aleshores, el propi protocol de comunicacions SSL/TLS s'encarrega d'enviar al client el CDS juntament amb els altres certificats de la cadena de certificació.

Exemples:

- a) Quan s'instal·la un CDS emès a una administració local catalana, a més d'instal·lar el propi CDS, cal també instal·lar el certificat EC-AL i EC-ACC.
- b) Quan s'instal·la un CDS emès a un departament de la Generalitat, a més d'instal·lar el propi CDS, cal també instal·lar els certificats EC-SAFP, EC-GENCAT i EC-ACC.
- c) Quan s'instal·la un CDS emès a una universitat catalana, a més d'instal·lar el propi CDS, cal també instal·lar els certificats EC-UR i EC-ACC, i en el específic de la Universitat Rovira i Virgili, caldria instal·lar addicionalment el certificat EC-URV.

Instal·lació del Certificat de Dispositiu Servidor (CDS)

Per instal·lar el certificat de dispositiu servidor, cal seguir els següents passos:

Es selecciona *Install Certificate* (del menú del marge esquerre)

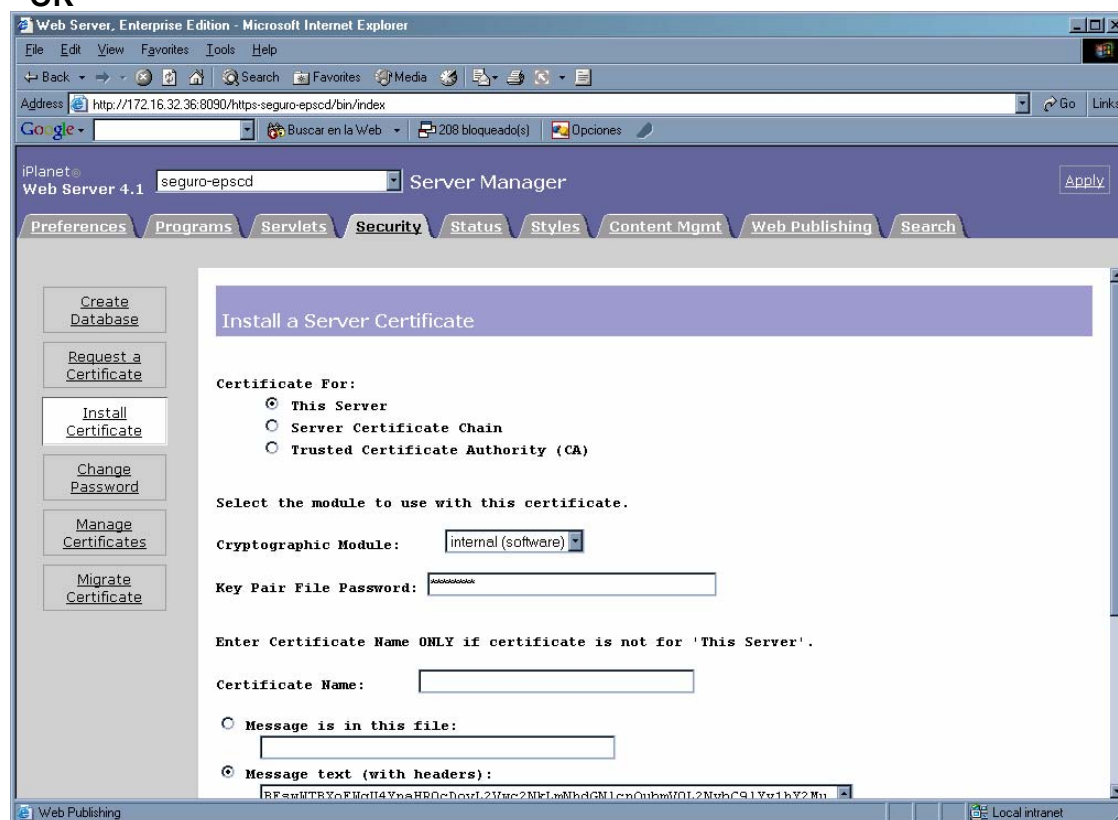
S'omplen els camps que ens demanen tal i com es mostra a la següent captura de pantalla:

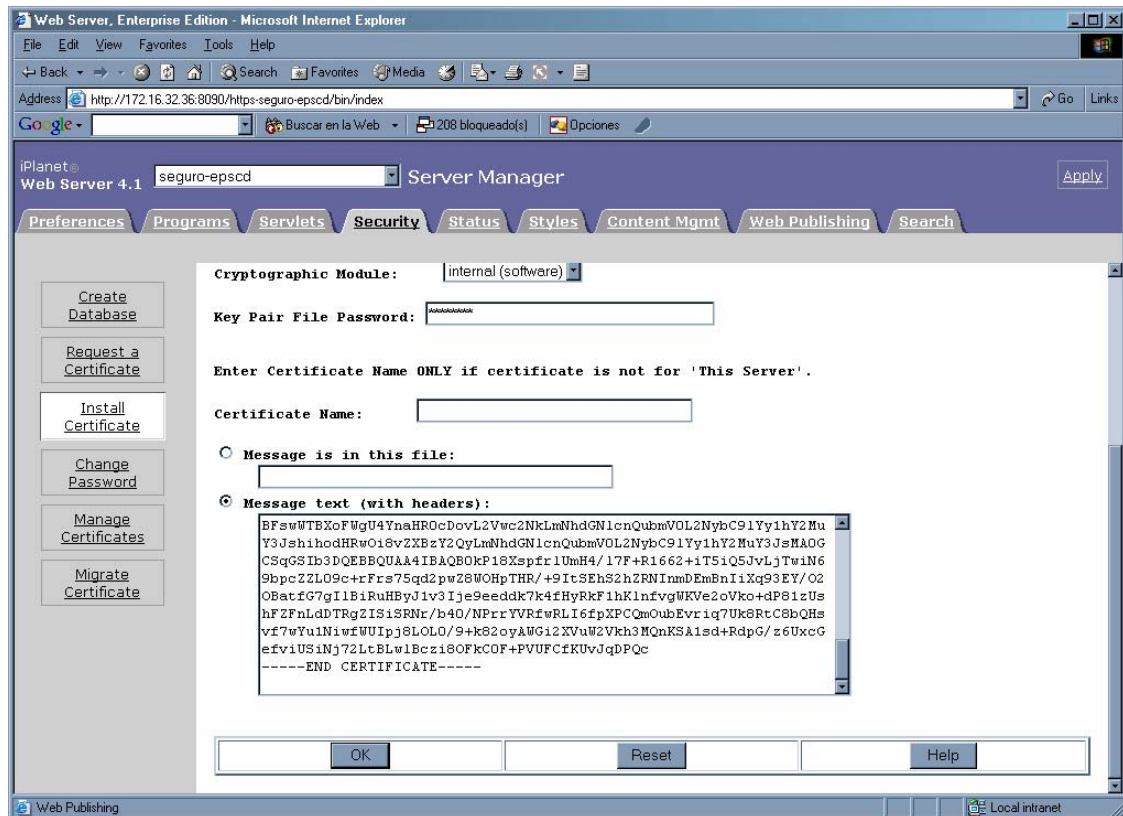
* **This server**

* **Key Pair File Password** : *****

* **Message text (with headers)** : Hem d'engaxar el certificat en BASE 64 que ha enviat CATCert

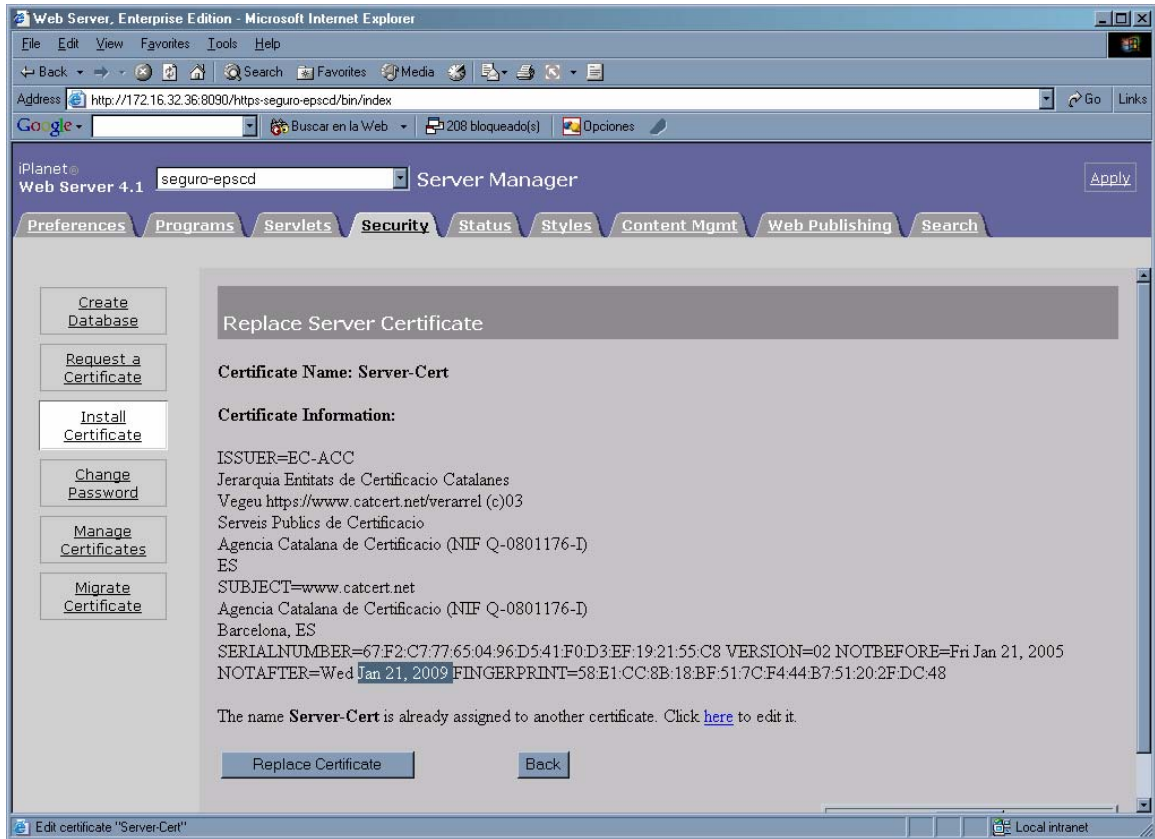
* **OK**



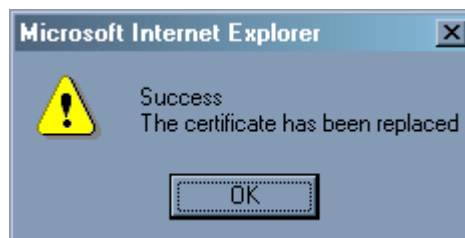
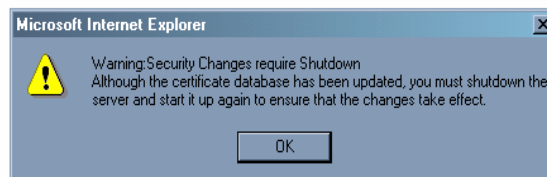


La següent captura de pantalla ens mostra les dades del nou certificat i si estem d'acord i tot és correcte s'ha de reemplaçar el certificat.

Per exemple, es mostra la nova data de caducitat (21 January 2009)



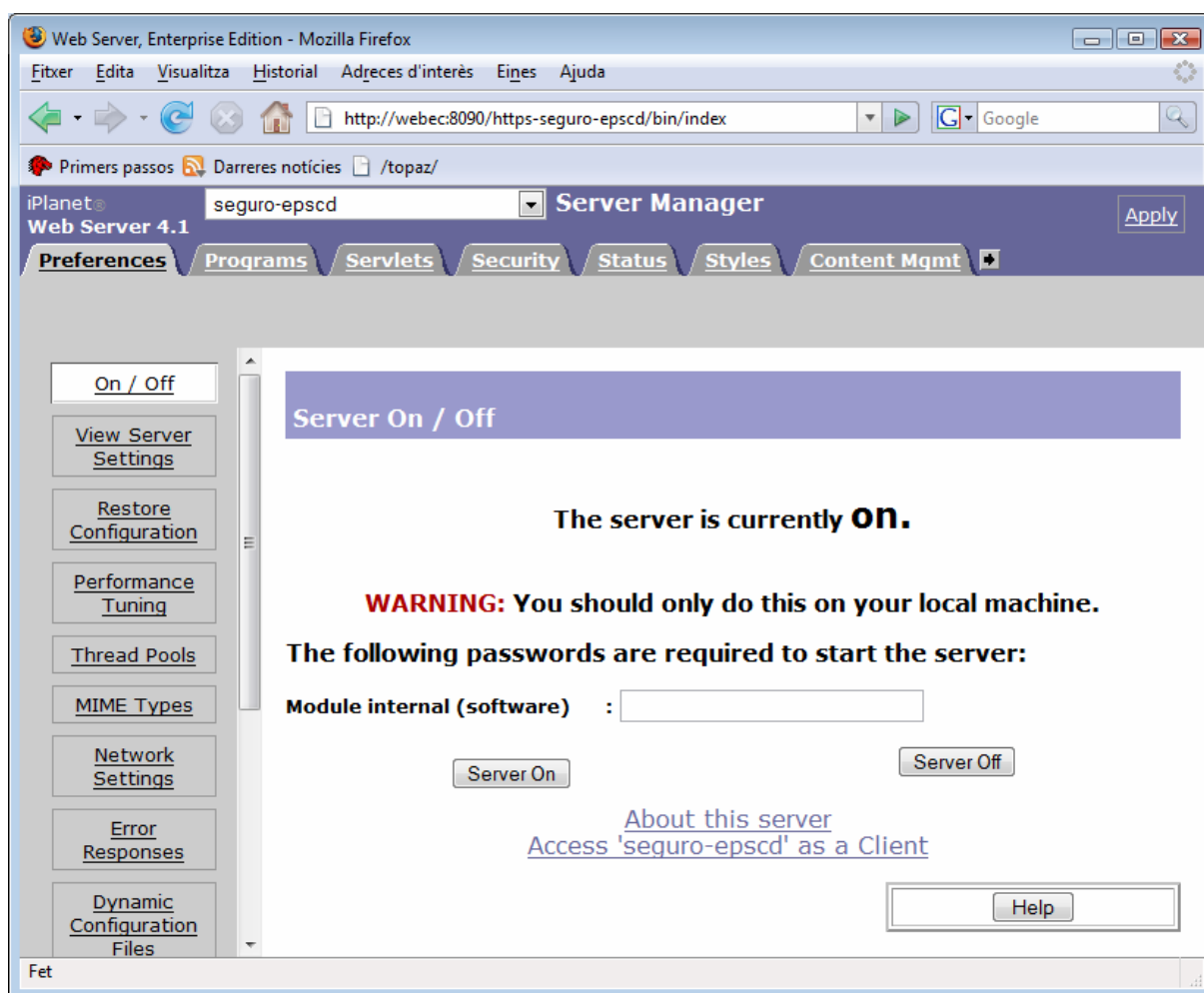
A continuació es mostra les pantalles finals. Informant de que s'ha de reiniciar el servidor per a que el certificat es carregui.



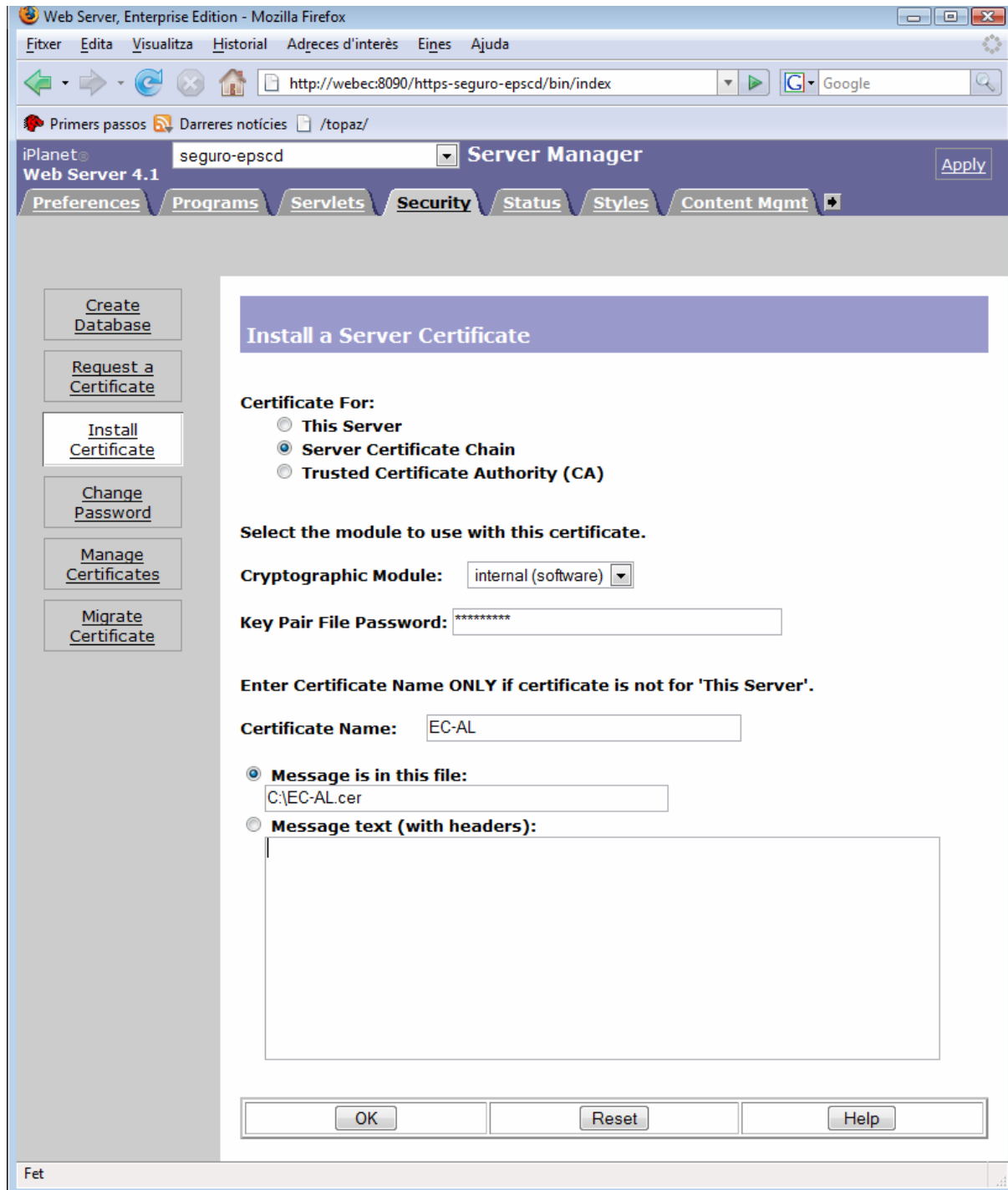
Instal·lació de les claus públiques

Des de la pàgina inicial de la consola d'administració de l'iPlanet, seleccionem la instància de *Servidor* a administrar i fem clic a *Manage*.

A continuació es mostra una pantalla semblant a la que s'ha de veure per a comprovar que tot és correcte.



Anar a la pestanya security i a la opció Install Certificate. Configurar les diferents opcions que es mostren a la captura de pantalla següent:



Repetir el procés per cada certificat de la jerarquia emissora del certificat de servidor CDS a instal·lar.