

# Manual de gestió del certificat de servidor a l'IIS

## Control documental

<b>Estat formal</b>	<b>Elaborat per:</b>  Àrea Alcaide	<b>Aprovat per:</b>  Francesc Ferré
<b>Data de creació</b>	28/01/2008	
<b>Control de versions</b>	<b>Data:</b>	28/01/2008
	<b>Descripció:</b>	Creació del document
<b>Nivell accés informació</b>	pública	
<b>Títol</b>	Manual de gestió del certificat de servidor a l'IIS	
<b>Fitxer</b>	20080128_Gestio_certificats_CDS_IIS.doc	
<b>Control de còpies</b>	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.	
<b>Drets d'autor</b>	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 <a href="http://creativecommons.org/licenses/by-nc-nd/2.5/es/">http://creativecommons.org/licenses/by-nc-nd/2.5/es/</a> o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.	

## Índex

---

<b>Manual de gestió del certificat de servidor a l'IIS.....</b>	<b>1</b>
<b>Control documental.....</b>	<b>2</b>
<b>Índex.....</b>	<b>3</b>
<b>1. Objecte.....</b>	<b>4</b>
<b>2. Generació del CSR.....</b>	<b>5</b>
<b>3. Instal·lació de les claus públiques.....</b>	<b>13</b>
<b>4. Instal·lació del certificat.....</b>	<b>16</b>

## 1. Objecte

L'objectiu del present document és el de descriure les instruccions necessàries per tal de portar a terme les següents tasques relatives a la gestió d'un CDS (Certificat de Dispositiu Segur) al servidor web Apache:

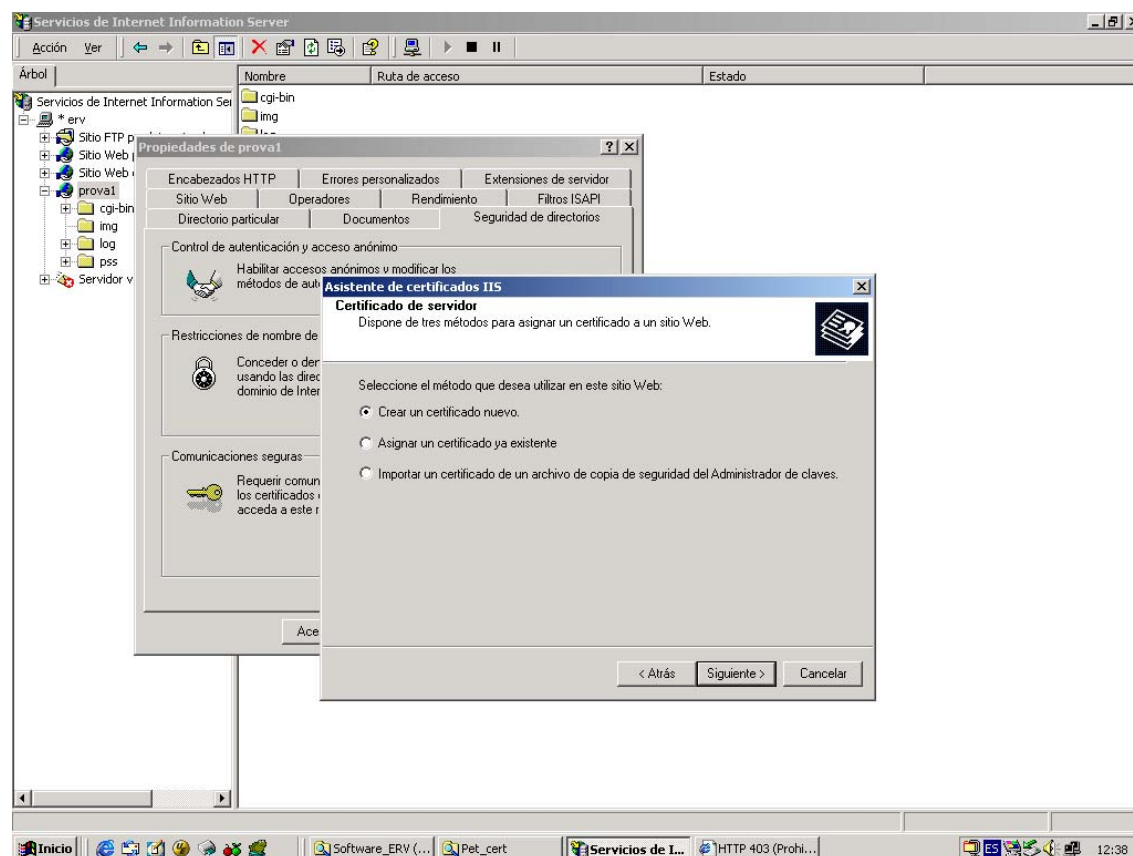
- Generar una sol·licitud de CDS (CSR: Certificate Signing Request).
- Instal·lar el CDS al servidor.
- Instal·lar les claus públiques de les entitats de certificació al servidor.

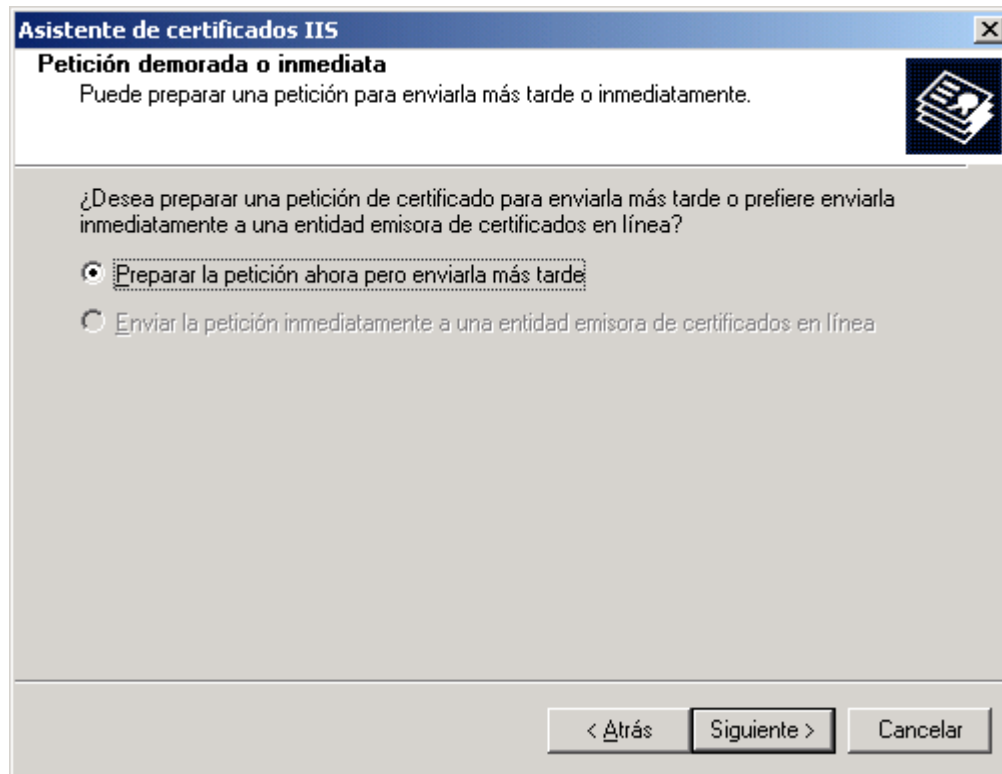
## 2. Generació del CSR

Aquest és un exemple de generació del arxiu "CSR" de petició d'un certificat. Les captures de pantalles s'han fet durant una prova feta per un MS IIS del entorn de preproducció de CATCERT.

Cal que seguiu les següents passes:

- Seleccionar *Herramientas de administración (Administrative Tools)*
- Iniciar *Internet Servicios de Internet (Services Manager)*
- Obrir la finestra de propietats de la web per a la qual se sol·licitarà el CRS (click botó dret > propietats)
- Situar-se a la pestanya *Seguridad de directorios (Directory Security)*
- A la secció *Comunicaciones seguras (Secure Communications)* premeu el botó *Certificado de servidor (Server certificate)*. A continuació s'iniciarà un assistent que us guiarà. Seguiu aquestes opcions:





El nom pel certificat que us demanarà a continuació no afecta al certificat; només és per a la vostra informació, per a que sigui fàcilment identificable.

**Asistente de certificados IIS**

**Nombre y configuración de seguridad**

Su nuevo certificado debe tener un nombre y una longitud en bits determinada.

Escriba un nombre para el nuevo certificado. El nombre debe ser fácil de usar y recordar.

Nombre:

La longitud en bits de la clave de cifrado determina el nivel de cifrado del certificado. Cuanto mayor sea la longitud, mayor será el nivel de seguridad pero puede hacer que disminuya el rendimiento.

Longitud en bits:

Certificado de Criptografía activada por servidor (S@C) (sólo para las versiones exportadas)

< Atrás    Siguiente >    Cancelar

**Asistente de certificados IIS**

**Información de la organización**

El certificado debe incluir información que permita diferenciar su compañía de otras.

Seleccione o escriba el nombre de su compañía y departamento.

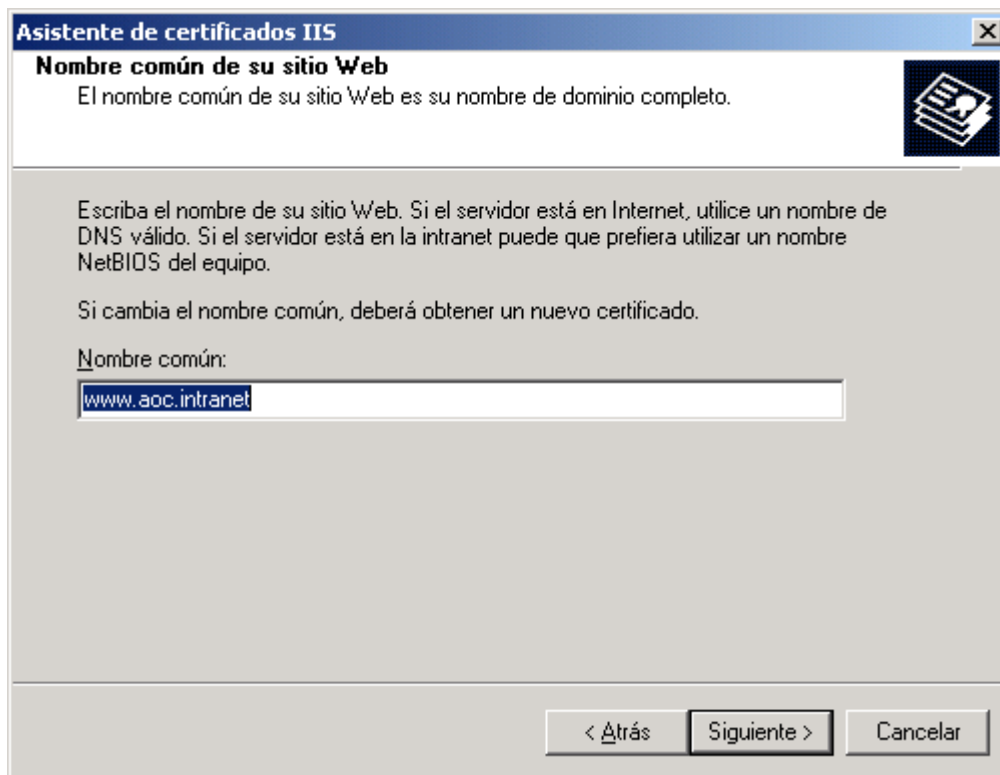
Para obtener más información, consulte el sitio Web de la entidad emisora del certificado.

Organización:

Departamento:

< Atrás    Siguiente >    Cancelar

Ara us demanarà el nom del domini pel que se sol·licita el certificat. Cal assegurar-se de que tot és correcte i que conté un nom de domini principal o subdomini (ex. organitzacio.net, www.organitzacio.com, ...).



**Asistente de certificados IIS**

**Información geográfica**

La entidad emisora de certificados necesita la información geográfica siguiente.

País o región:  
ES [España]

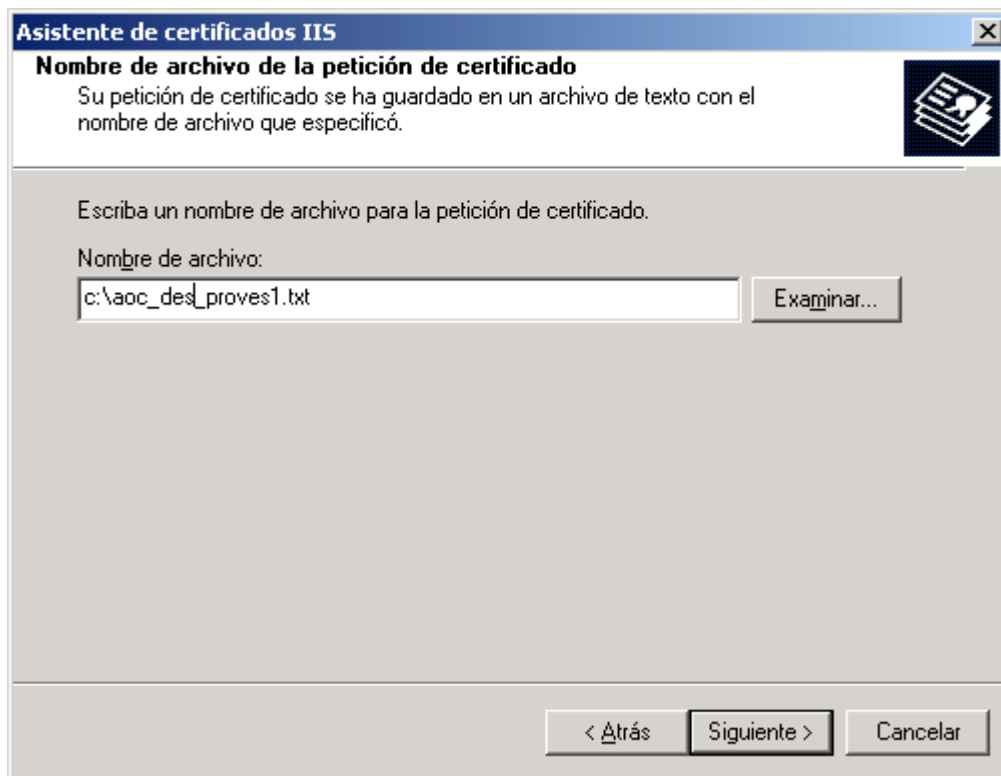
Estado o provincia:  
BARCELONA

Ciudad o localidad:  
BARCELONA

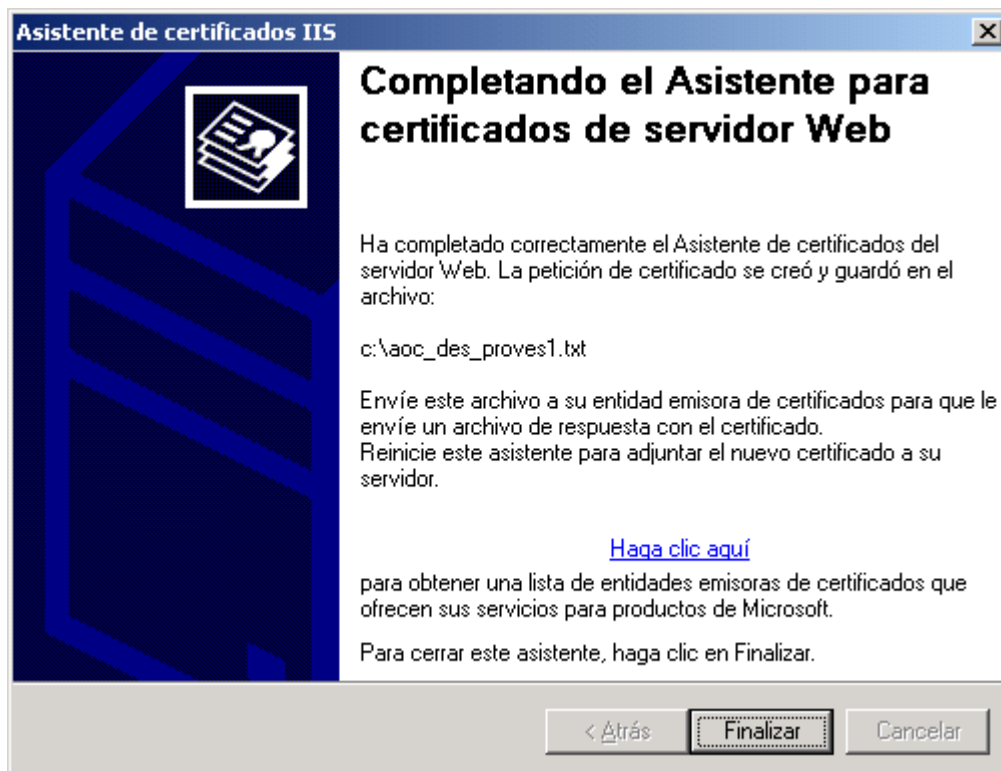
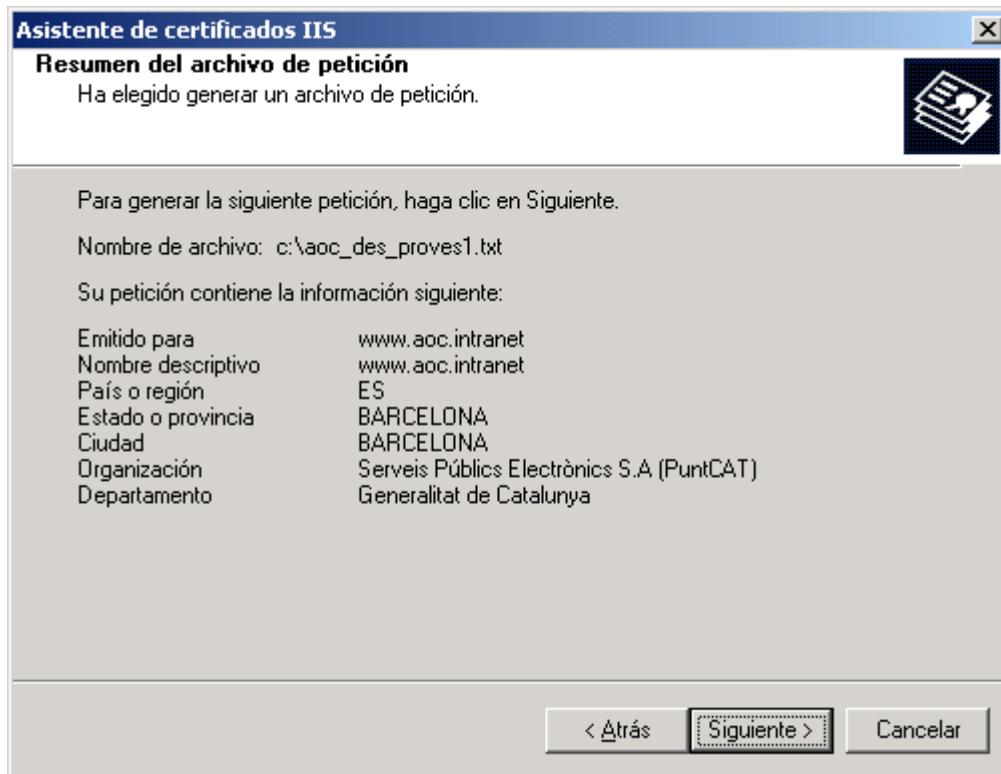
Los nombres de estado, provincia, ciudad y localidad deben ser nombres oficiales completos que no contengan abreviaturas.

< Atrás    Siguiente >    Cancelar

A continuació demanarà el nom i la ruta del fitxer on es vol guardar la petició:



Comproveu que els detalls introduïts son totalment correctes. Si trobeu alguna errada encara podeu tornar enrera per corregir-lo. Si tot és correcte feu click al botó *Siguiete*.



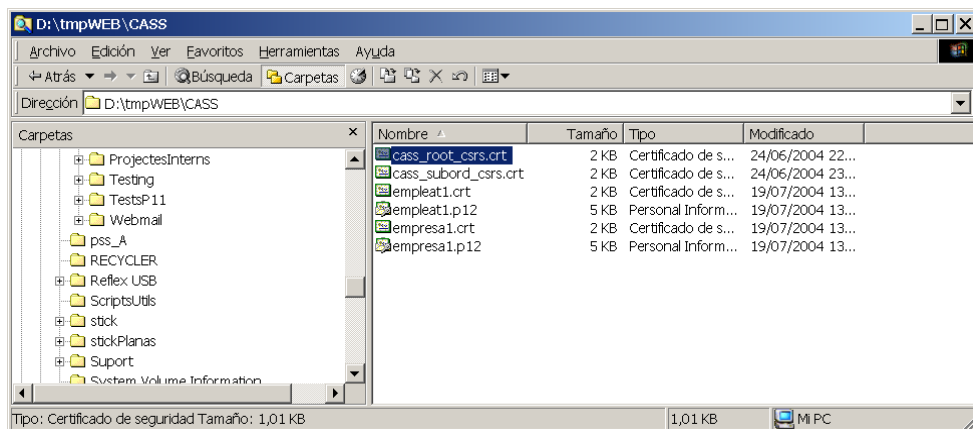
Finalment, caldrà que envieu aquest fitxer adjunt en un missatge de correu-e dirigit a l'adreça: **desenvolupament@catcert.net**

### 3. Instal·lació de les claus públiques

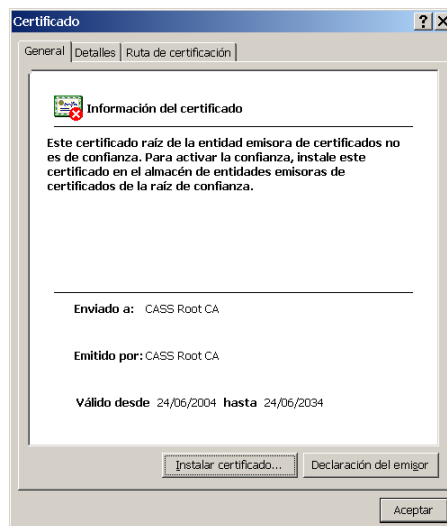
Aquest punt descriu el procediment a seguir per configurar el servidor web IIS (Internet Information Server) per admetre transmissions segures d'informació sota SSL per part d'un client amb un certificat digital vàlid emès per qualsevol entitat de certificació.

El procés d'instal·lació és el següent:

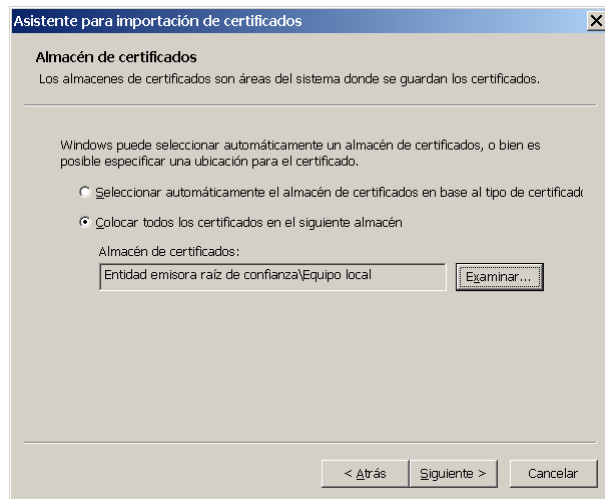
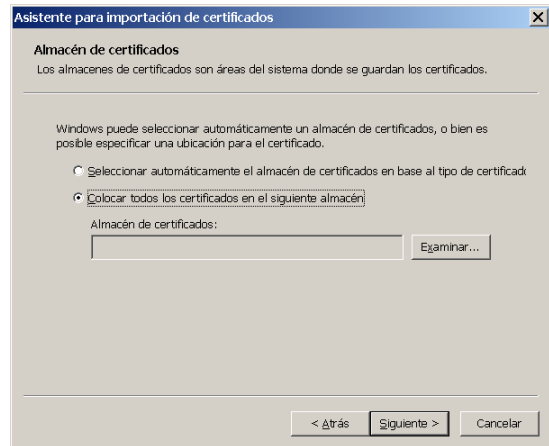
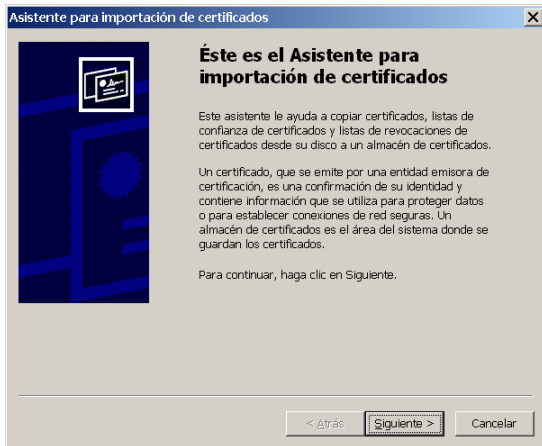
1. Un cop obtinguts els certificats de la jerarquia, és a dir, arrel i subordinades, guardar-los en una carpeta.

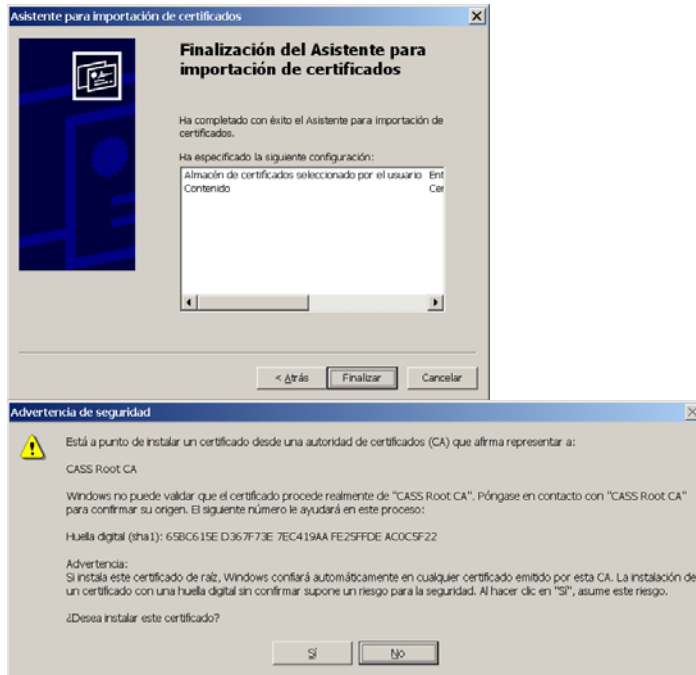


2. Fent doble clic sobre el certificat arrel apareix la informació sobre el certificat.



3. Fer clic sobre la opció "Instalar Certificado..." i continuar amb tal com indiquen les captures següents:





4. Repetir el procés per a tots els certificats de la resta de la jerarquia, tenint en compte sempre el fet de seleccionar el magatzem "Equipo local".

## 4. Instal·lació del certificat

Seguir els mateixos passos que al punt anterior, però amb el certificat de servidor.