

## Manual de càrrega de claus per a servidors IIS

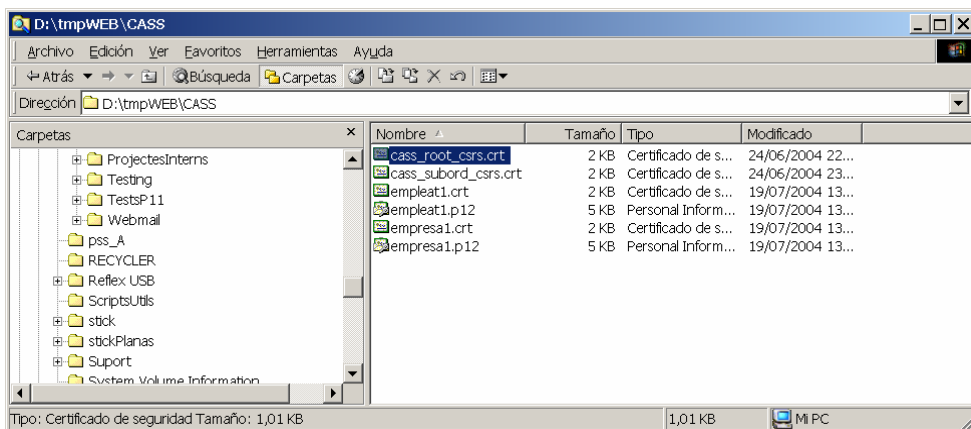
Aquest document descriu el procediment a seguir per configurar el servidor web IIS (Internet Information Server) per admetre transmissions segures d'informació sota SSL per part d'un client amb un certificat digital vàlid emès per qualsevol entitat de certificació.

El procediment consta de dues accions a realitzar sobre el servidor i la configuració de l'IIS. La primera consisteix en la importació dels certificats arrel en el servidor. La segona, en la modificació de les polítiques d'accés d'IIS.

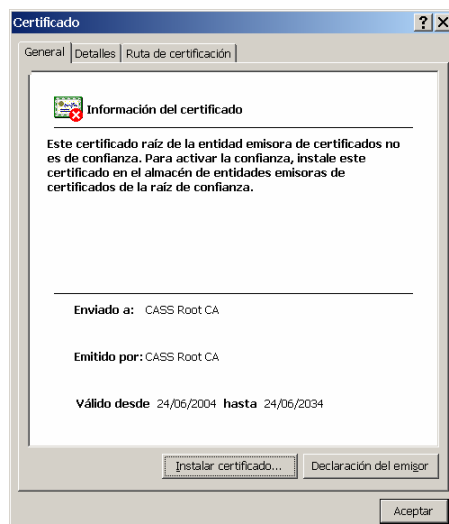
### Instal·lació dels certificats arrel

El procés d'instal·lació és el següent:

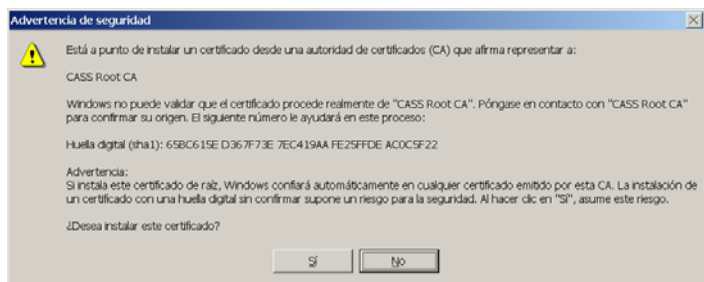
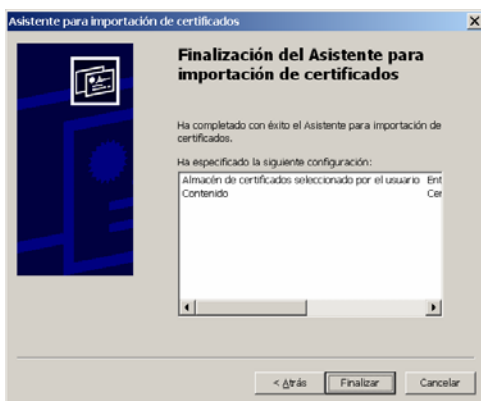
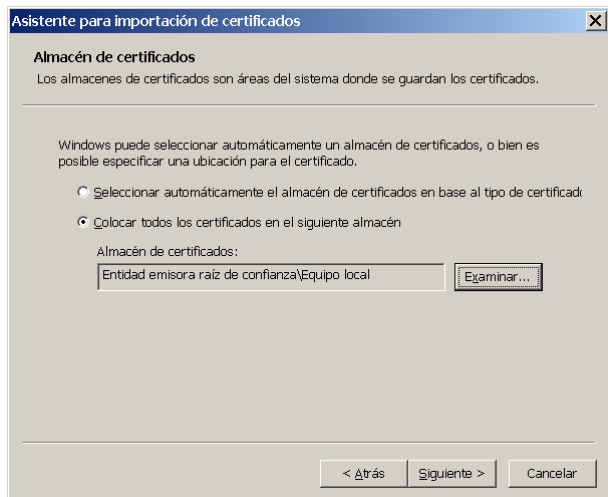
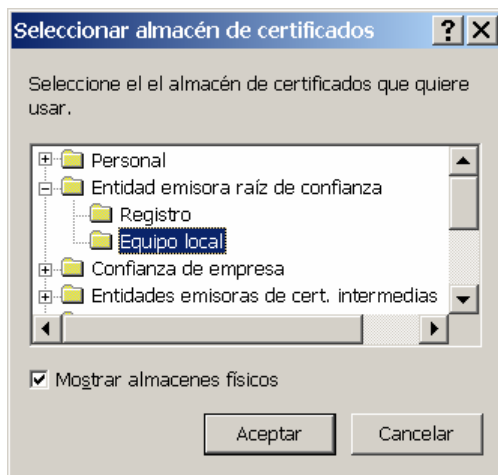
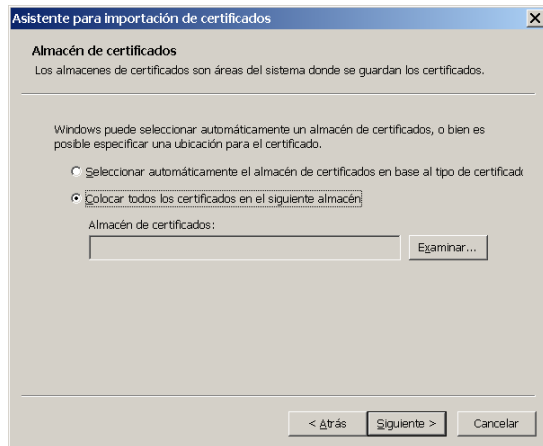
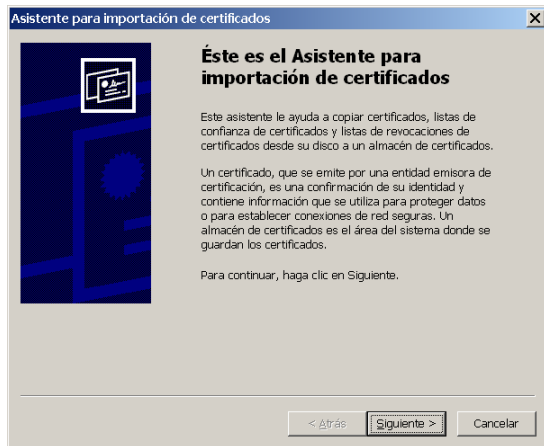
1. Un cop obtinguts els certificats de la jerarquia, és a dir, arrel i subordinades, guardar-los en una carpeta.



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:

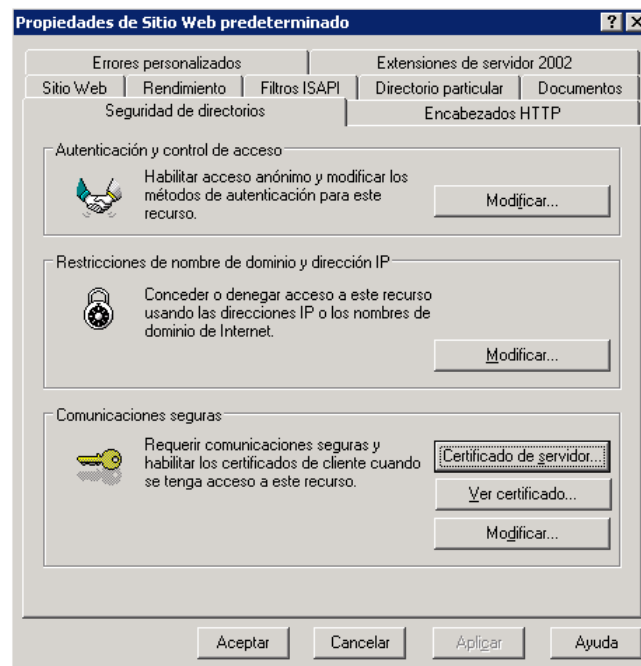


4. Repetir el procés per a tots els certificats de la resta de la jerarquia, tenint en compte sempre el fet de seleccionar el magatzem "Equipo local".

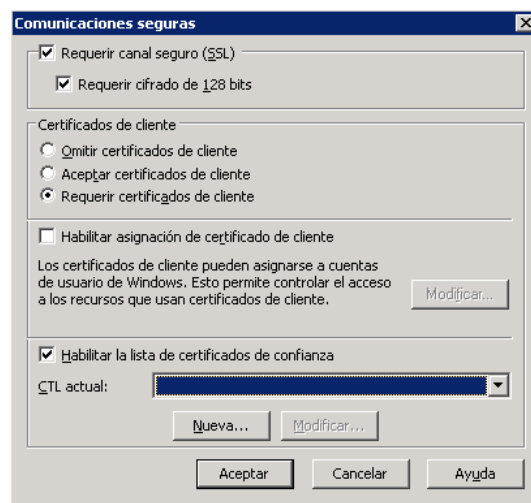
## Configuració de l'autenticació de client a IIS

Un cop carregades les claus públiques, cal configurar la instància de servidor web en la que es desitja activar l'autenticació de client.

1. Per aconseguir-ho cal entrar a les propietats del "Sitio Web", concretament a la pestanya de "Seguridad de directorios".

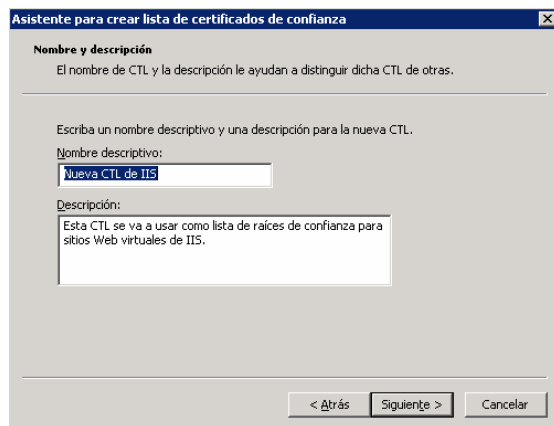
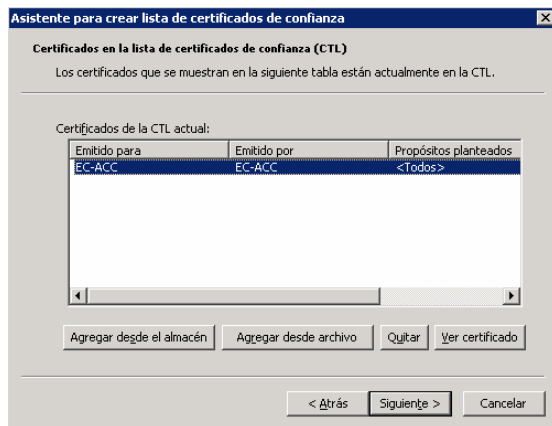
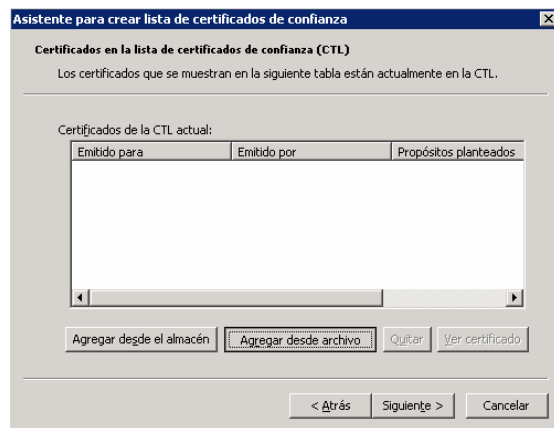
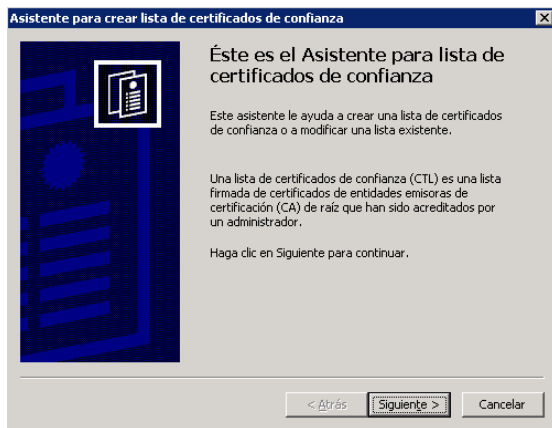


2. Si el certificat està ben instal·lat, dins de l'apartat de "Comunicaciones seguras", el botó "Modificar" estarà activat. Prement-lo podrem modificar els paràmetres de configuració relatius a l'autenticació de client, el canal segur i els certificats de client que seran admesos.



3. Dins de la pantalla de configuració cal marcar les opcions tal com apareixen a la captura superior. Han d'estar activades les opcions de "Requerir canal seguro (SSL)" i que el xifrat sigui de 128

bits. Dins dels certificats de client, activar la opció "Requerir certificados de cliente". I per últim, s'ha d'habilitar una llista de certificats de confiança. Aquesta llista tan sols conté els certificats arrel de les Entitats Certificadores en les que es confia. És molt important haver carregat les claus públiques, ja que si el certificat d'usuari penja d'una Entitat intermitja i IIS no és capaç de reconstruir la cadena l'autenticació fallarà.



En aquest exemple el certificat arrel correspon amb el certificat arrel de CATCert.

