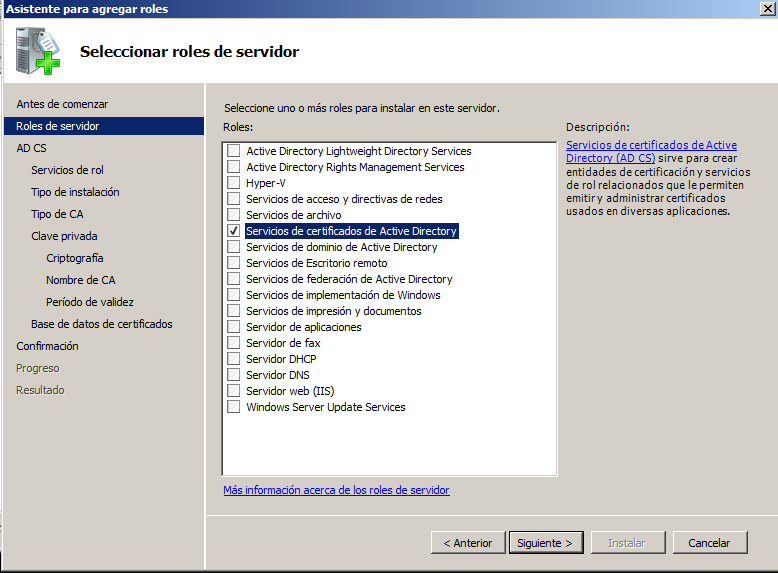
# Identidad digital

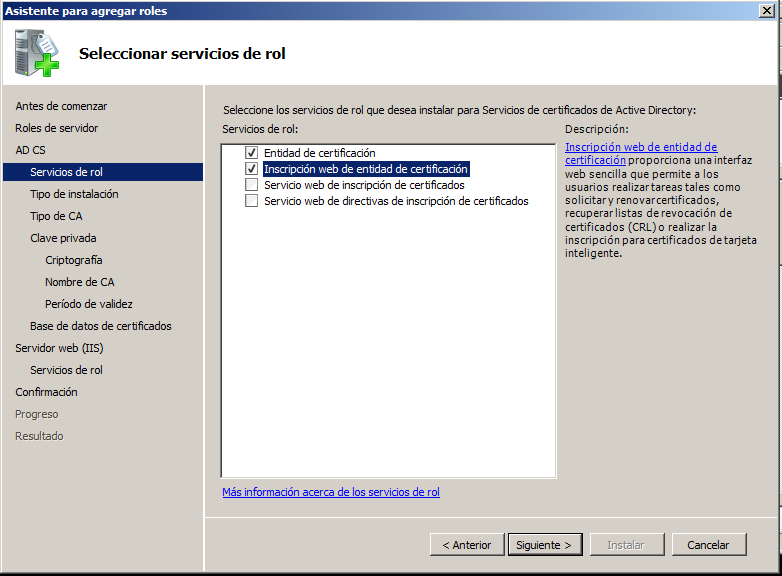
En esta práctica vamos a comprobar el funcionamiento de los certificados digitales para verificar el emisor de los mensajes mediante la firma digital del correo realizada con la clave privada. El receptor deberá tener la clave pública del remitente para poder comprobarlo. También realizaremos el cifrado del mensaje mediante la clave pública del destinatario, que luego podrá descifrar con su clave privada.

Primero instalaremos un servidor de certificados con un windows2008.

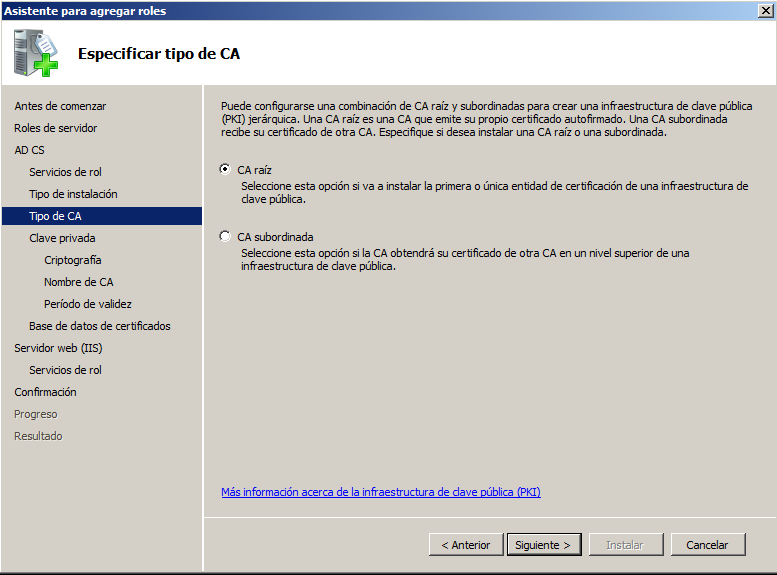
Instalamos servicios de certificados de active directory



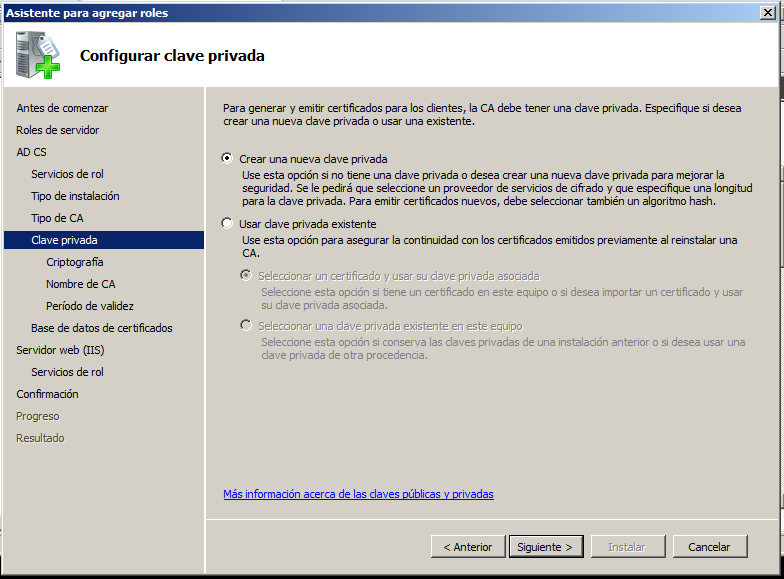
Marcamos la casilla **entidad de certificación** e **inscripción web de entidad de certificación**, esto hará que se instale también el servicio iis



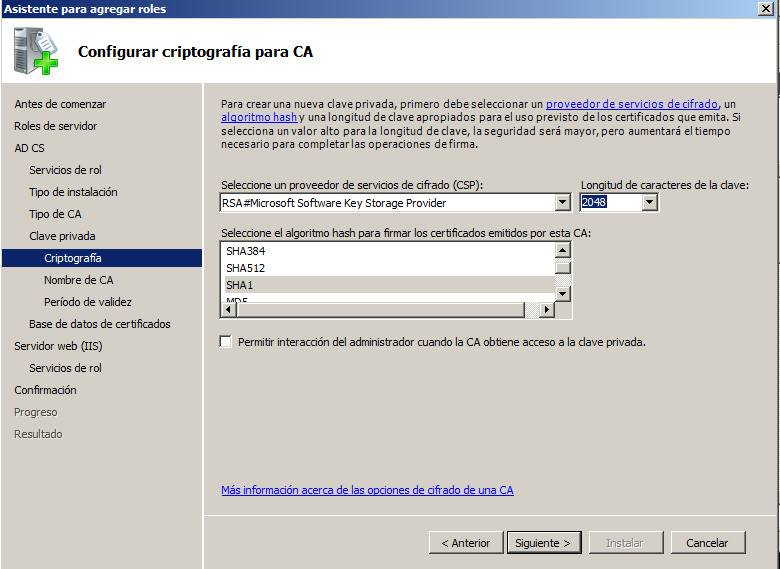
Seleccionaremos entidad certificadora raíz



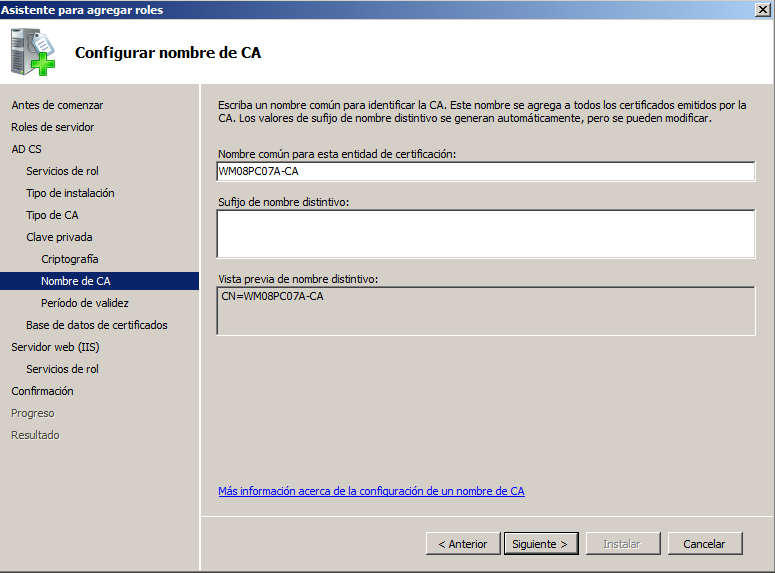
Creamos una nueva clave privada (suponiendo que no la tengamos ya, en ese caso seleccionaríamos usar clave privada existente)



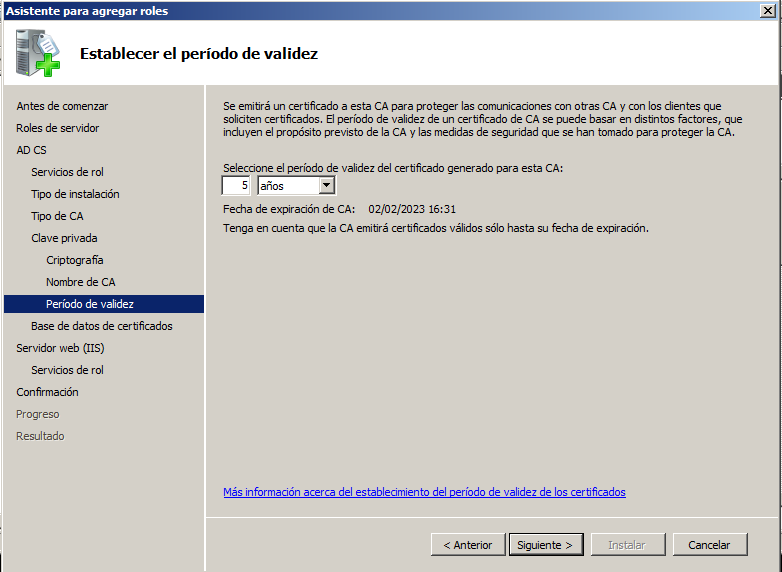
Seleccionamos el algoritmo que queremos utilizar y la longitud de la clave.

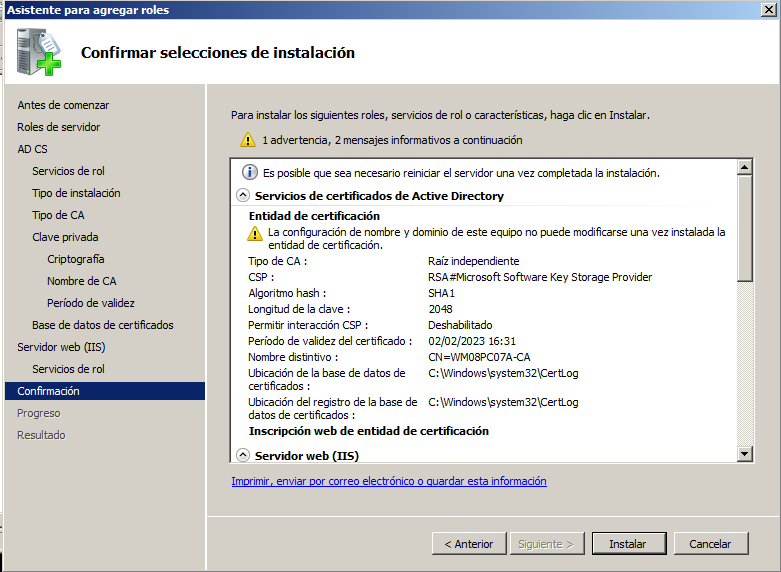


Ponemos el nombre del certificado

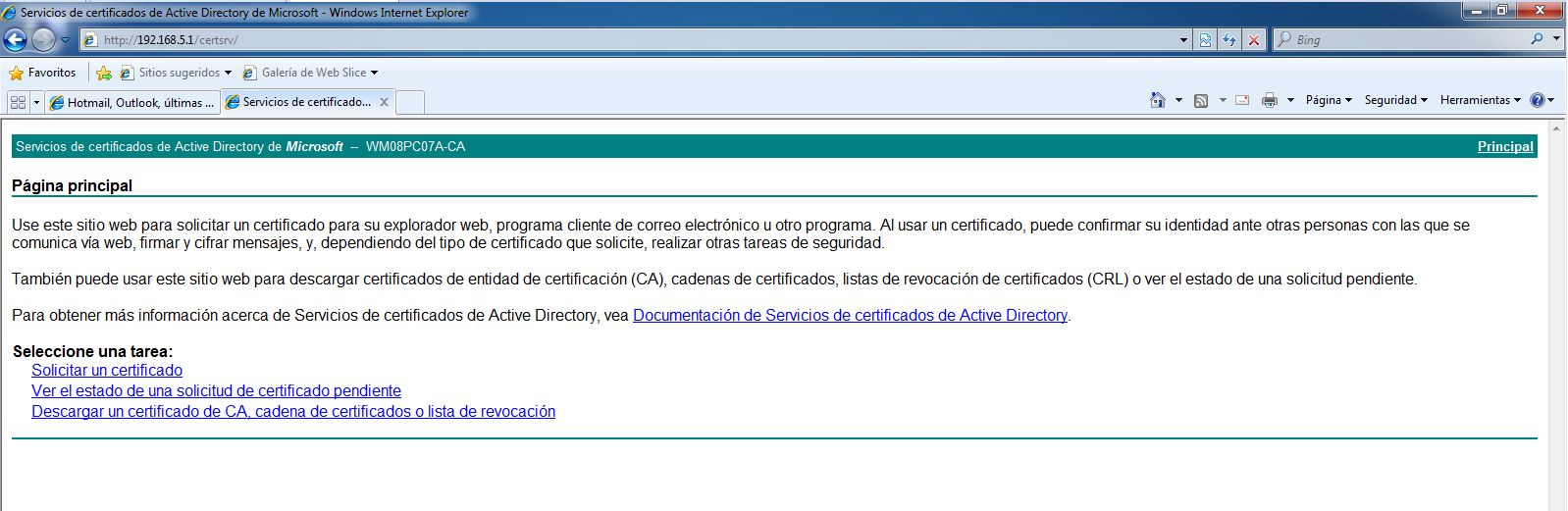


Seleccionamos el tiempo de validez

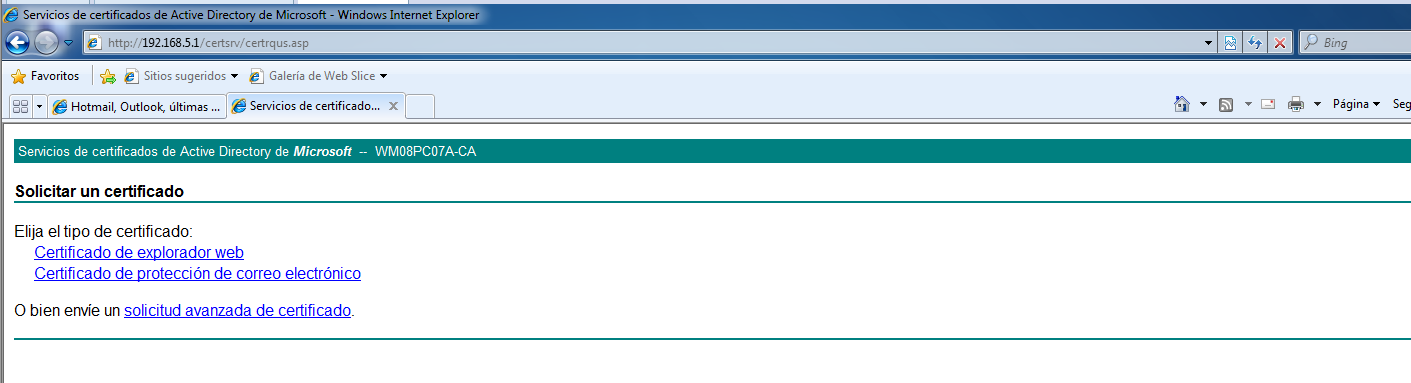


Una vez “configurado” el asistente solo queda instalar. 

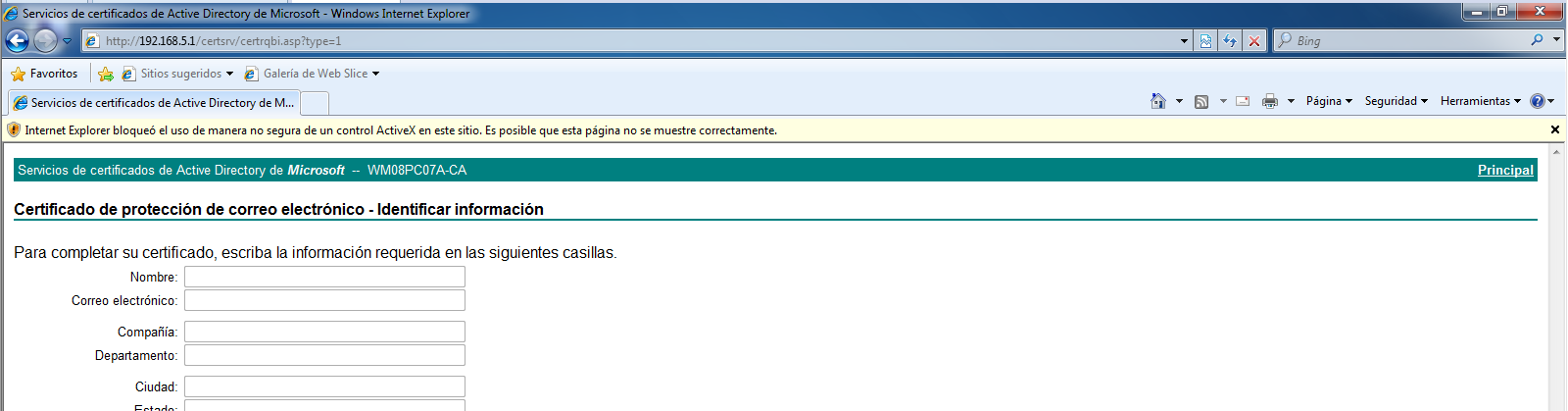
Una vez hecho esto, desde el cliente nos meteremos en la url <https://ipdelservidor/certsrv> para solicitar un certificado



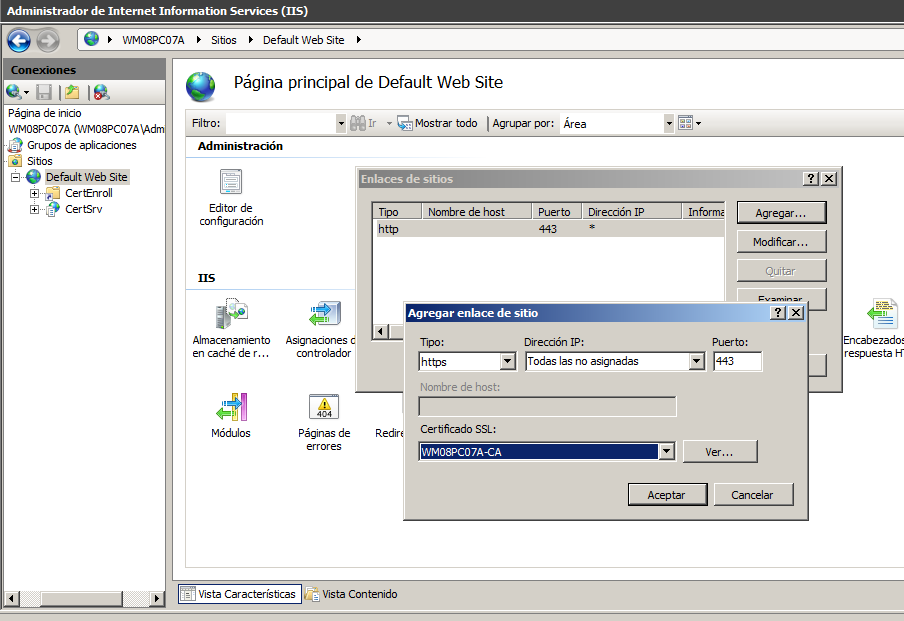
Seleccionaremos **certificado de protección de correo electrónico**



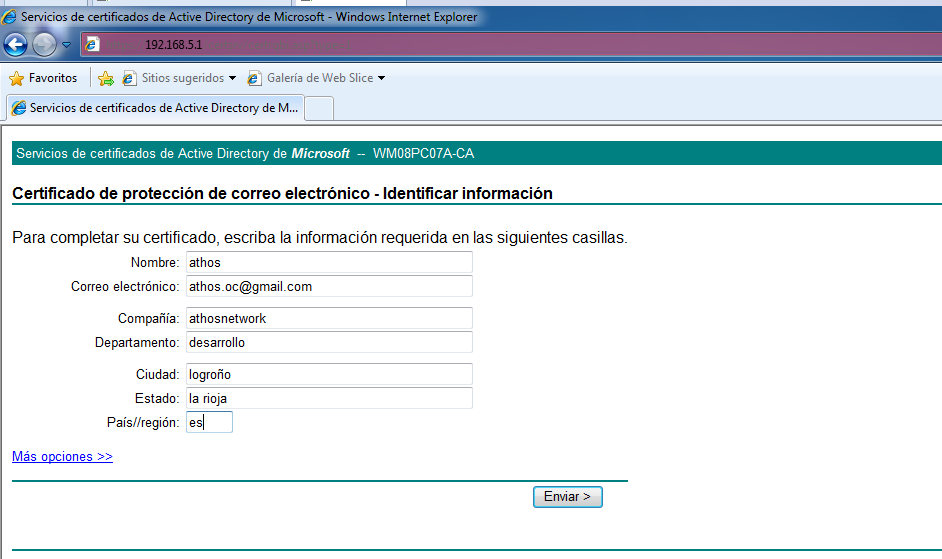
En este ejemplo, hemos entrado a la página por http en lugar de https y no podemos rellenar el formulario para solicitar el certificado, así que tendremos que configurar el iis del servidor para que admita SSL



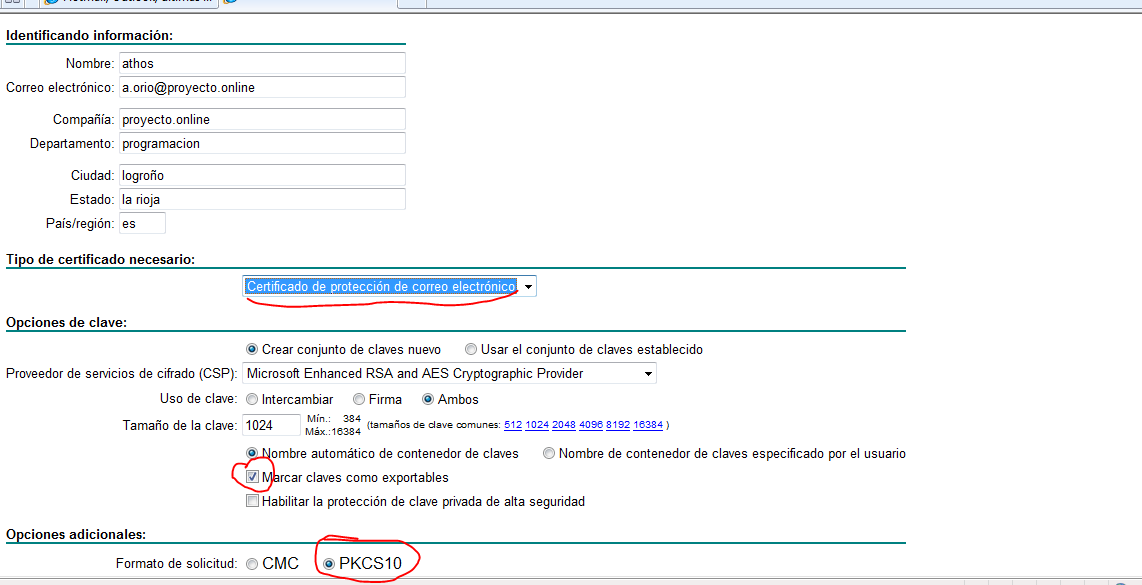
Agregamos un enlace al sitio que administra las solicitudes de certificados



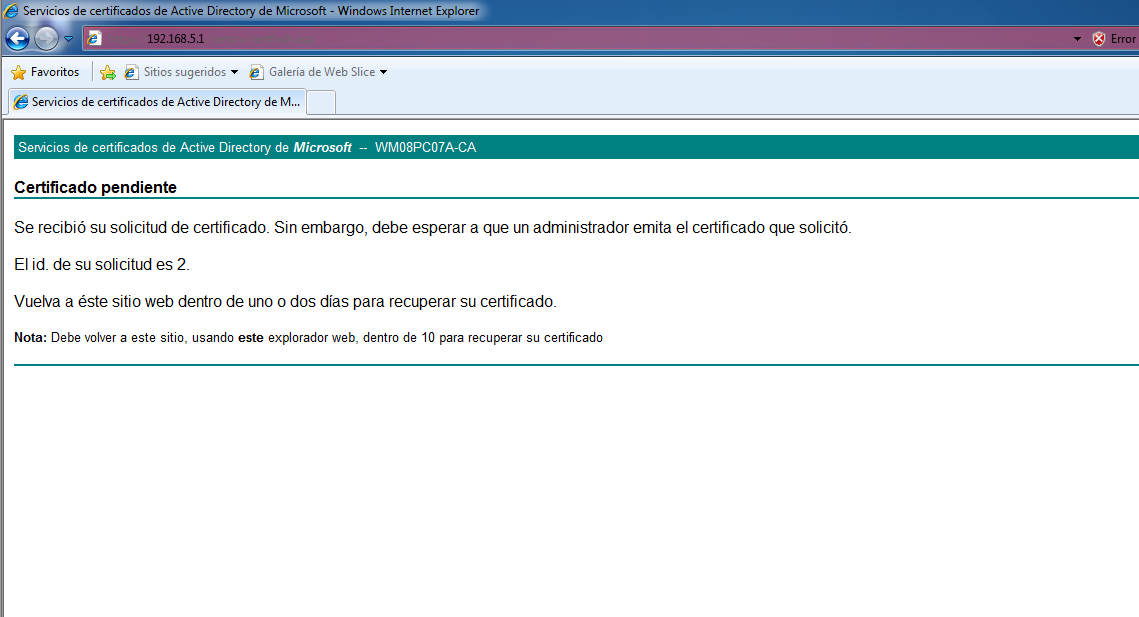
Una vez hecho esto, volvemos a entrar en la url de solicitud de certificados y vemos que ahora deja rellenar el formulario



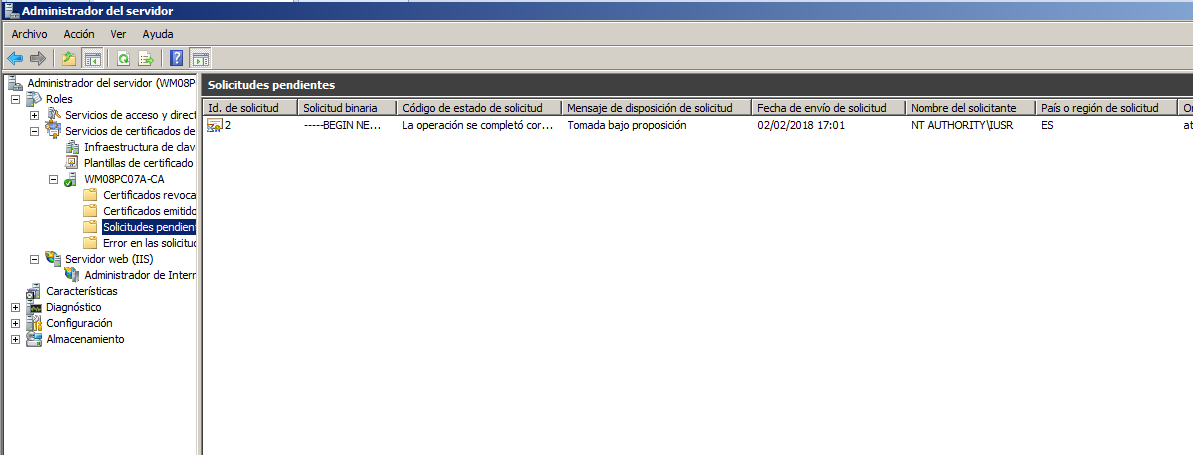
Pincharemos en más opciones para que nos permita seleccionar algunas opciones extra como que se pueda exportar la clave privada del certificado



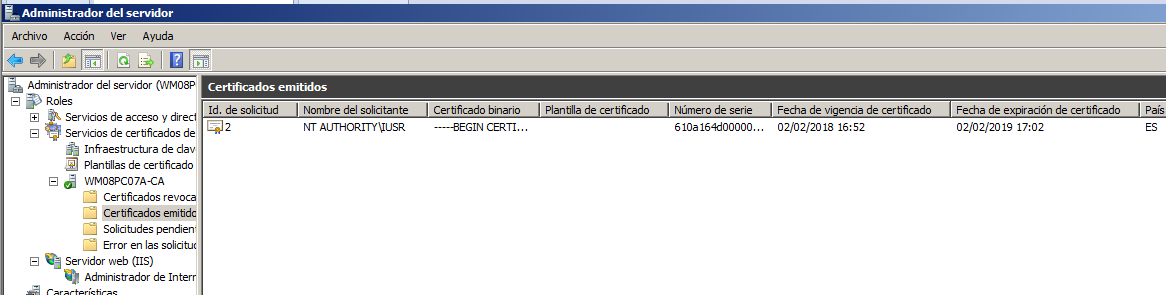
Una vez hecha la solicitud, solo queda esperar a que nos emitan el certificado desde el servidor.



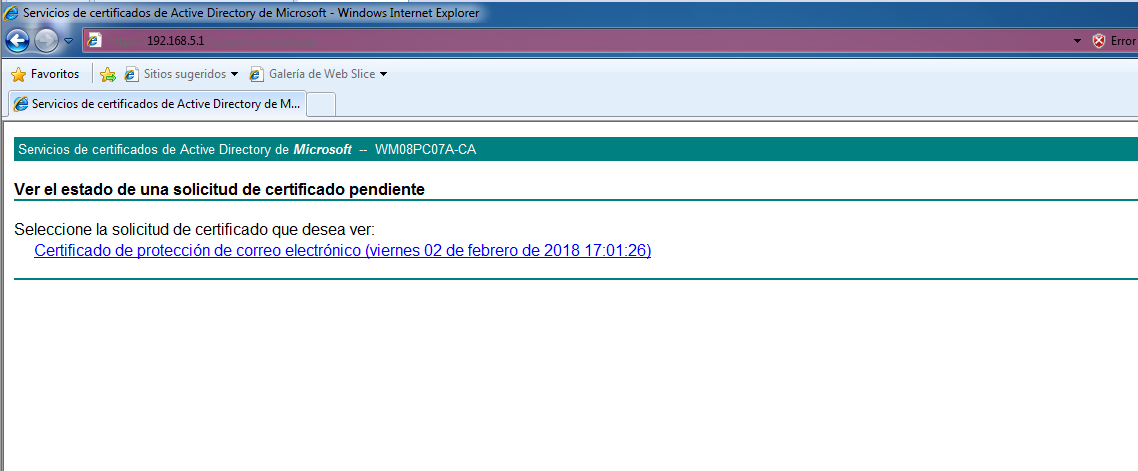
Vamos al servidor a la sección de certificados pendientes



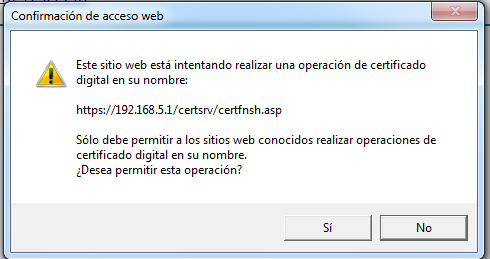
Le damos a emitir y veremos que se ha emitido en la sección correspondiente



Vamos otra vez desde el cliente a la url de los certificados y vamos a ver el estado de nuestro certificado

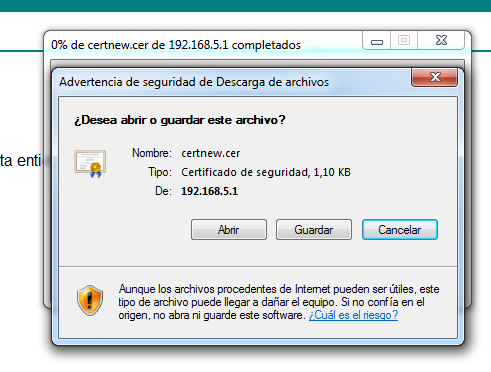


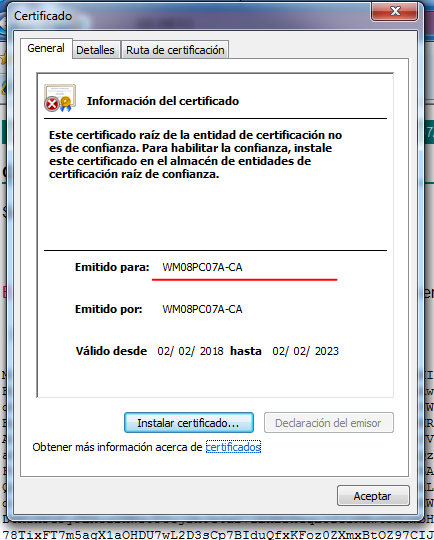
Nos saldrá esta advertencia

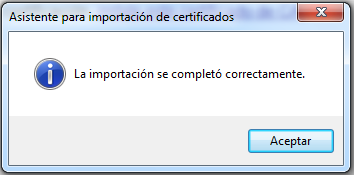


Aceptaremos la operación y nos avisa de que no es una entidad certificadora de confianza ya que no puede verificarse por ningún pki

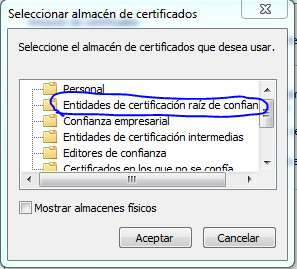




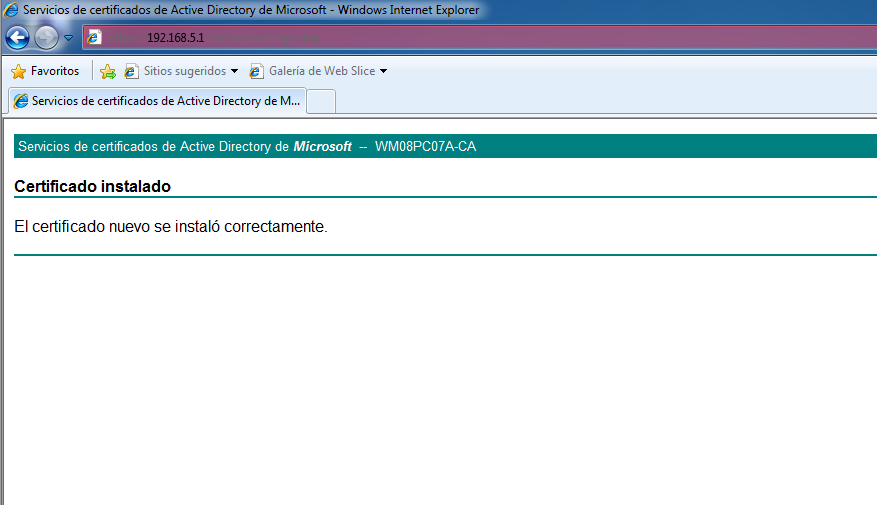




Nota, hay que instalarlo como en la siguiente imagen

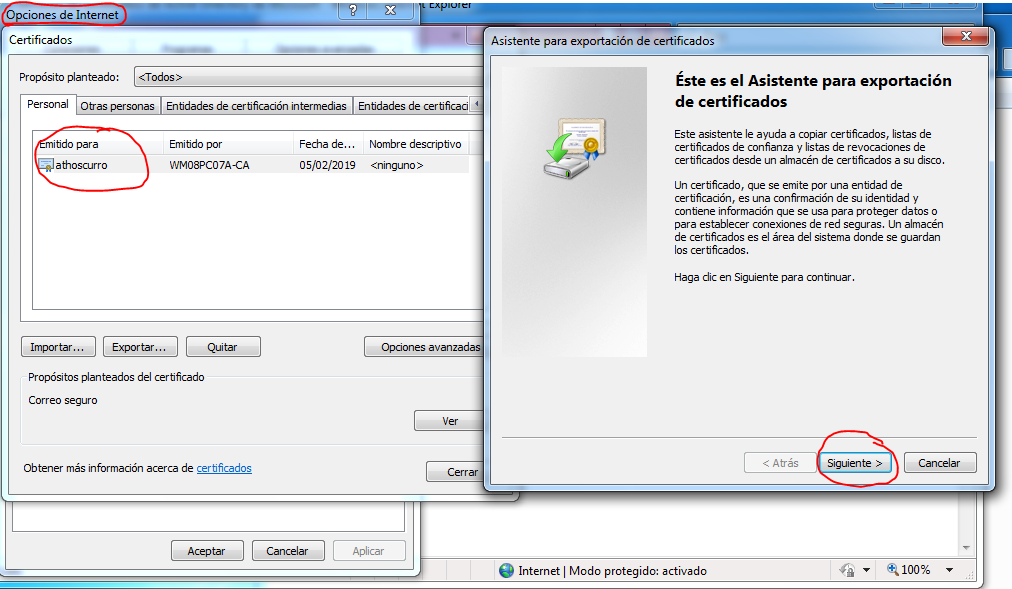


Una vez instalado el certificado de nuestro servidor en el cliente podemos instalar el certificado que este nos emitió.

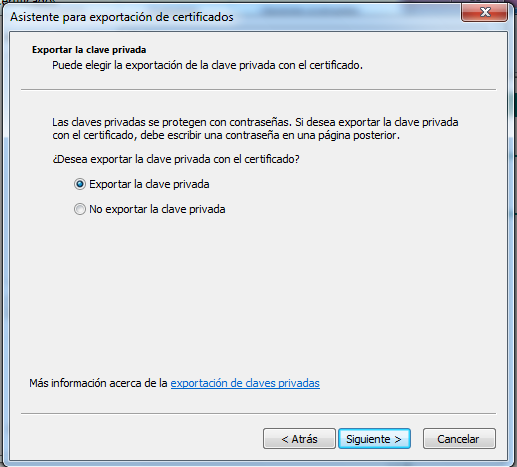


Ahora tendremos que exportarlo, para después instalarlo en nuestro cliente de correo.

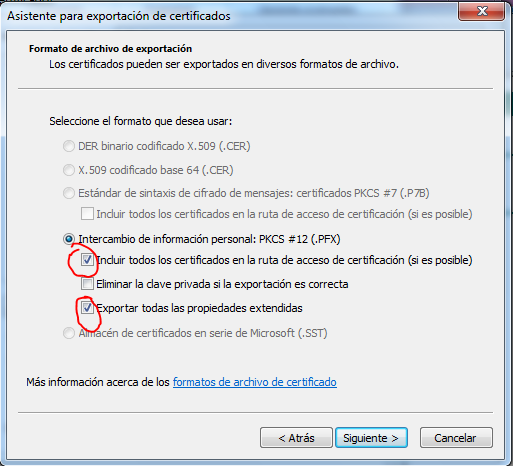
Iremos a opciones de internet, buscaremos la sección de certificados y lo exportaremos.



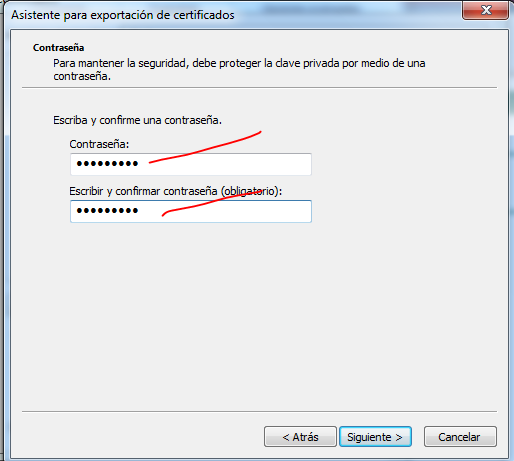
Marcaremos la opción exportar la clave privada, ya que será necesario para poder firmar nuestros mensajes digitalmente.



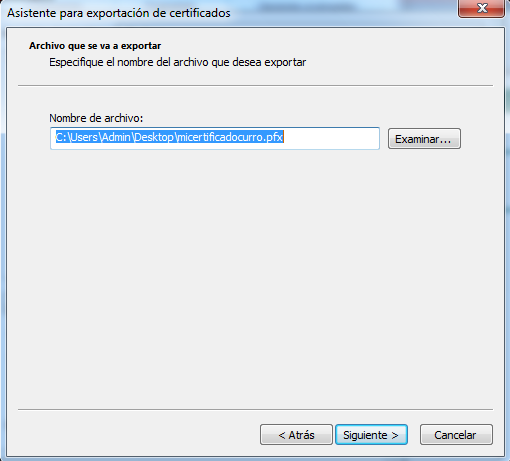
Marcaremos la opción 1 y 3 y continuaremos con el asistente.

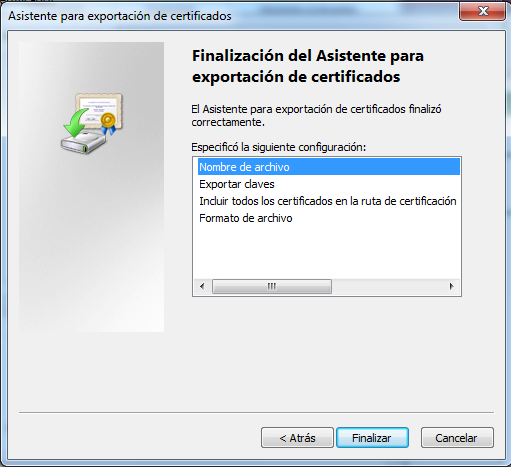


Nos pedirá una contraseña. Esta será necesaria cuando vayamos a importar nuestro certificado en otro sitio.

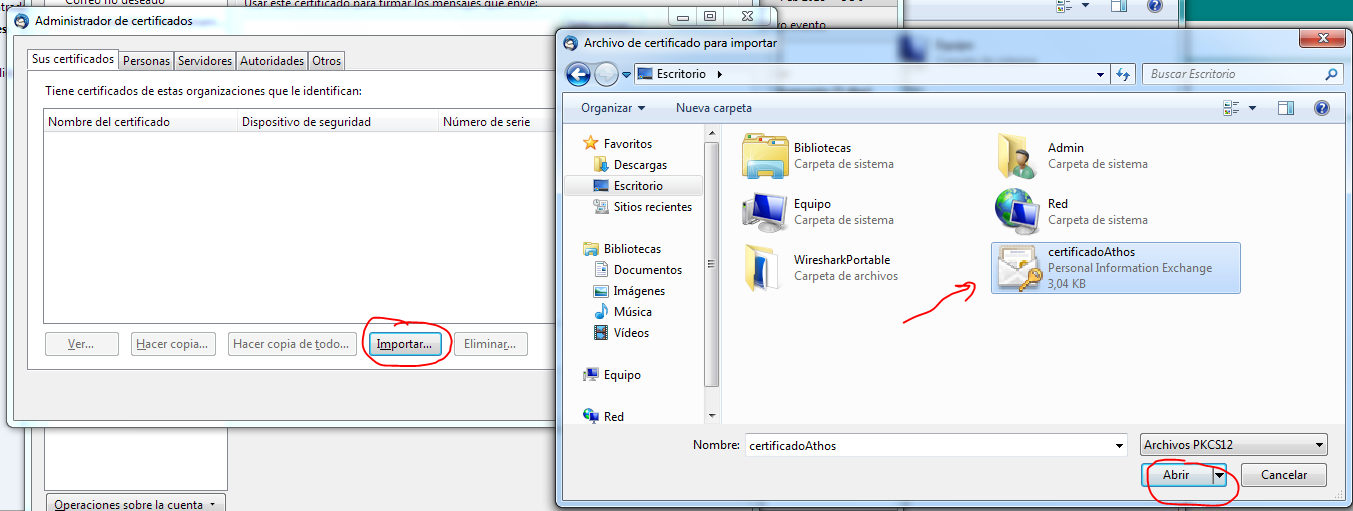


Seleccionaremos la ruta donde queremos que se exporte el certificado

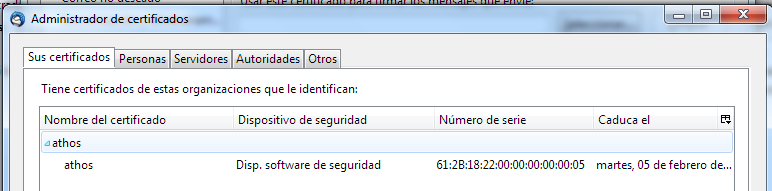




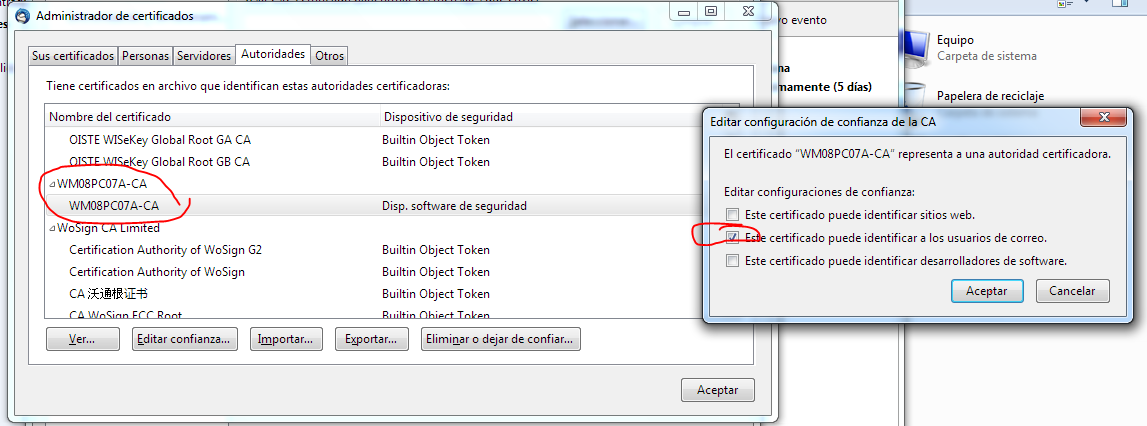
Una vez exportado, tendremos que importarlo en nuestro cliente de correo electrónico. Iremos a la opción seguridad de nuestra cuenta de correo electrónico e importaremos el certificado que acabamos de exportar en los pasos anteriores.



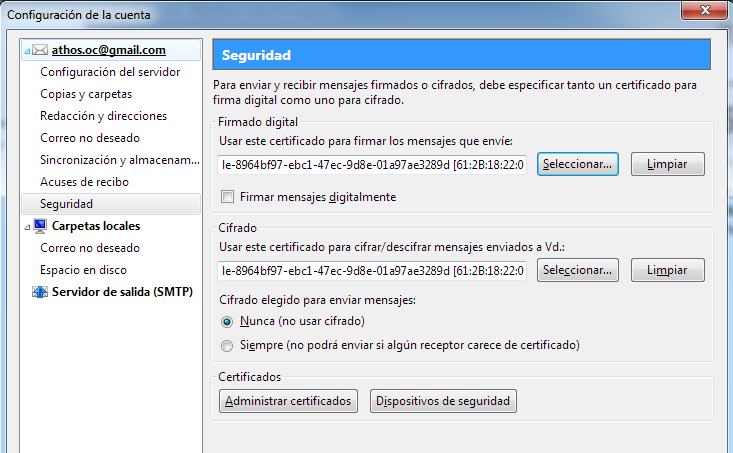
Veremos que se nos añade el certificado en la pestaña *Sus certificados*



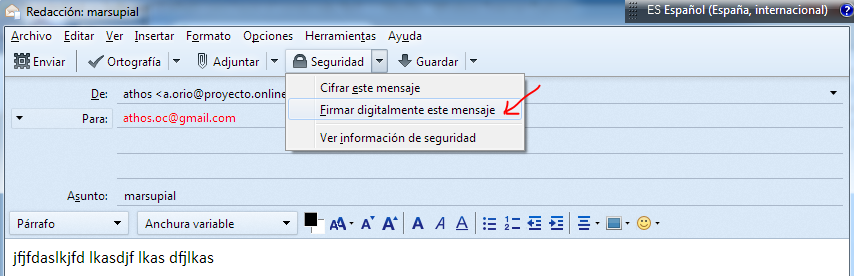
Para que todo esto funcione, tendremos que añadir el certificado de la ca (nuestro servidor 2008) y marcar la segunda opción que nos permitirá firmar nuestros mensaje.



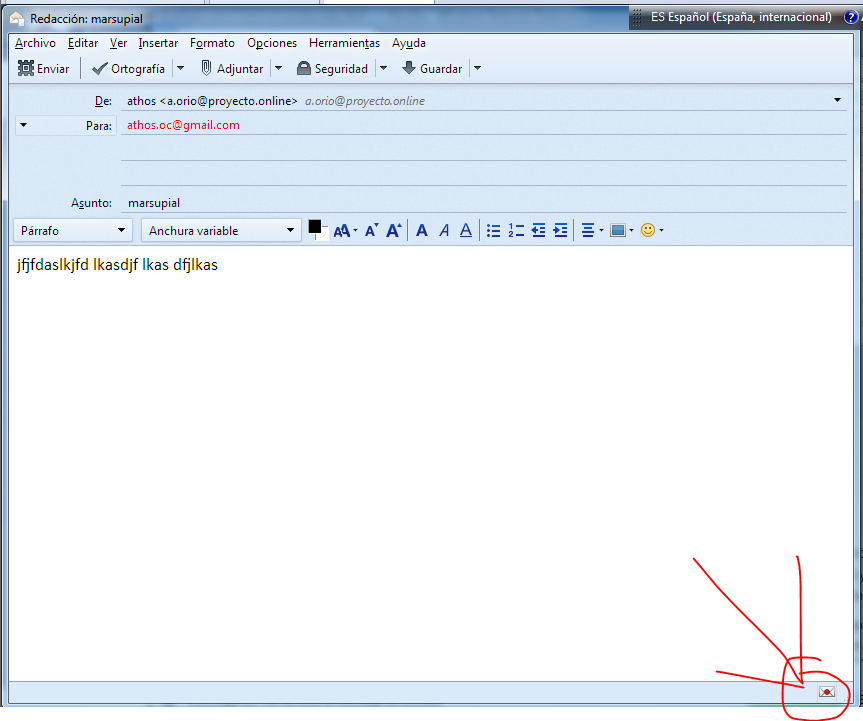
Una vez instalado nuestro certificado (el del cliente) e instalar el certificado de la ca, podremos seleccionar nuestro certificado desde el botón seleccionar.



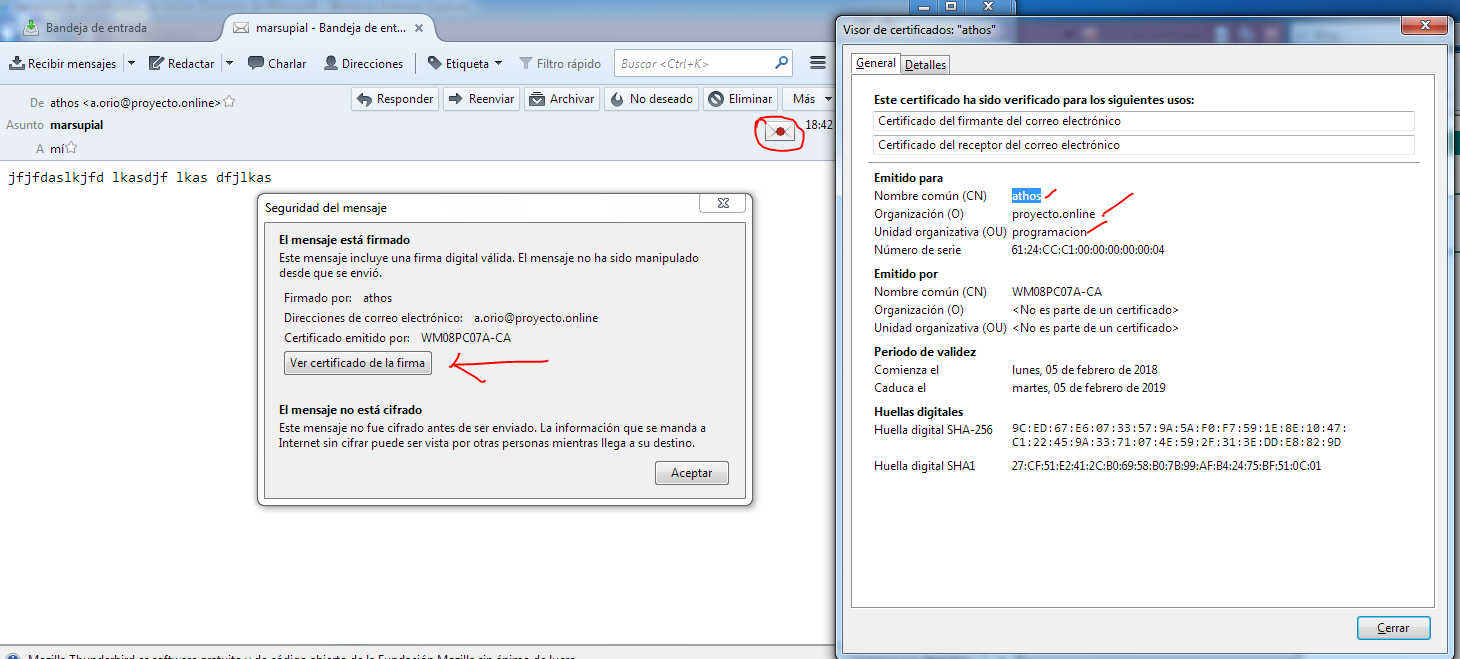
Ahora, si vamos a redactar un correo electrónico, veremos que podemos seleccionar en la pestaña seguridad, la opcion **firmar digitalmente este mensaje**. De momento, no podremos cifrarlo porque no tenemos la clave publica del destinatario.



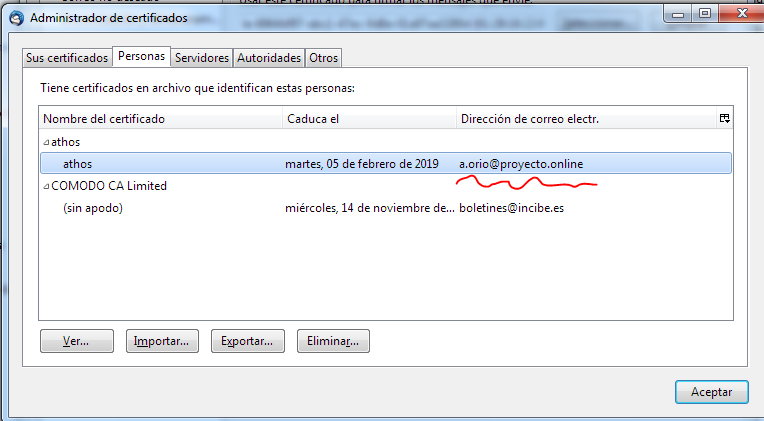
En la parte inferior del mensaje veremos un icono de un sobre que nos indica que el mensaje está firmado digitalmente



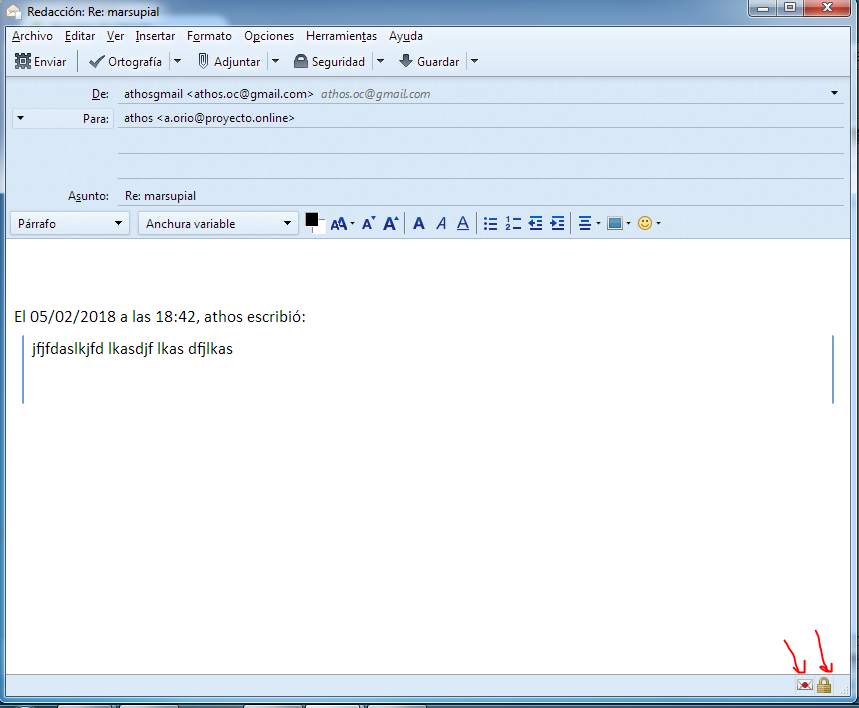
En el receptor del mensaje, cuando recibimos el correo veremos en la parte superior el icono del sobre indicando que ese mensaje viene firmado. Si pinchamos en el icono, podremos comprobar los datos de la firma del mensaje. Además, ahora tendremos también la clave pública del emisor, con lo cual podremos devolverle un mensaje cifrado como vemos más adelante.



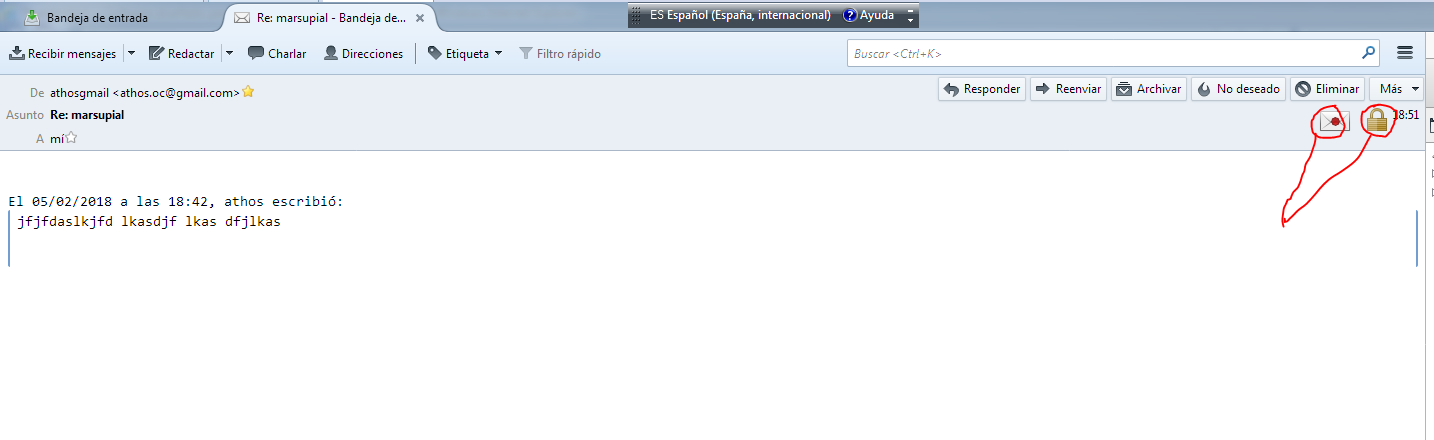
Si nos metemos en el administrador de certificados, vemos en la pestaña personas, tendremos el certificado del que nos envió el mensaje.



Así, que ahora podemos responder el mensaje, y desde la pestaña seguridad, podremos firmar el mensaje y también cifrarlo. Como se puede ver en la siguiente imagen, ahora nos sale un icono del sobre indicando que hemos firmado el correo, pero también nos sale un icono de un candado indicando que el mensaje está cifrado.



Al recibir el correo de respuesta, vemos en la cabecera los dos iconos indicando que es un mensaje cifrado y firmado.



Si pinchamos en los iconos, nos aparecerá una ventana dándonos información al respecto

