Guide
Installing Digital Certificates in Outlook 2000

Document SIGNE_PAPET. Ver. 1.0
Date of application 06/08/2012

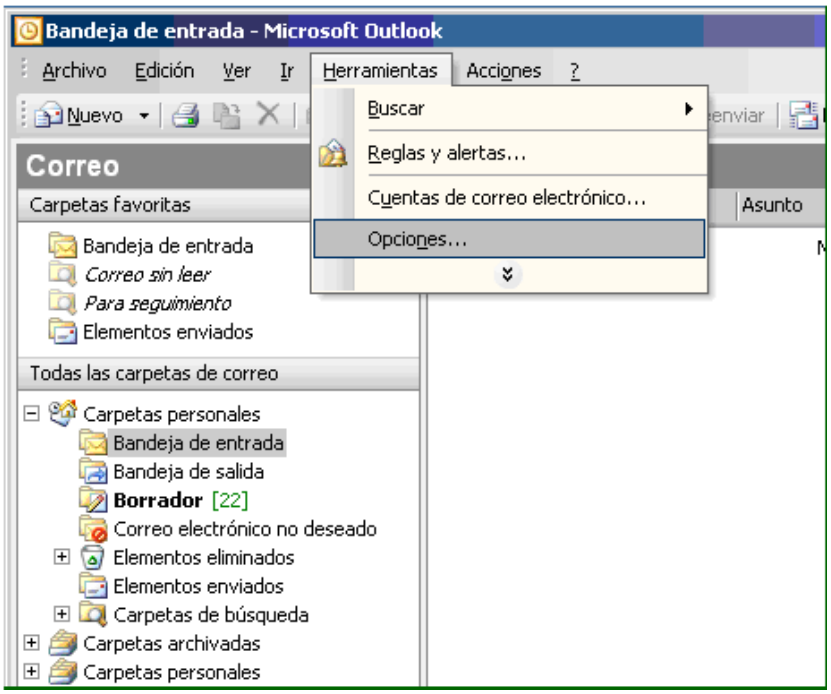
signe
Seguridad documental

Introduction

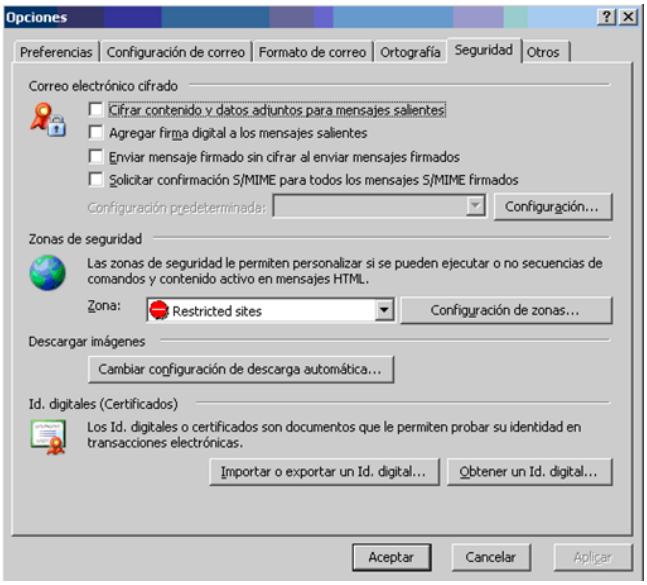
This document describes the steps for configuring and using certificates in the Microsoft Outlook email application. The digital certificate may be software-based or on a smart card. If your certificate is on a card, insert it into the card reader. If you have a software-based digital certificate with a high level of security, you will be asked to enter the password every time you use it. Likewise, if your certificate is on a card, you will be asked for

Procedure

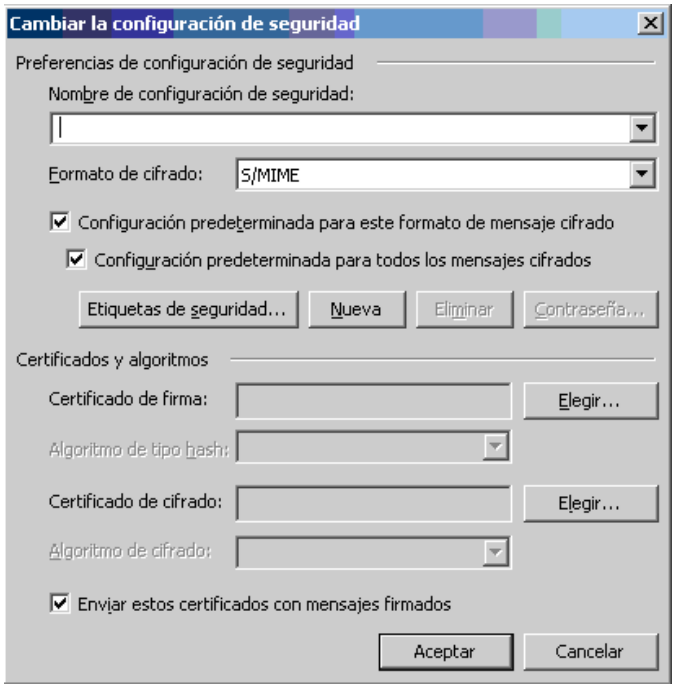
The steps to configure the sending of signed email in Microsoft Outlook, regardless of where your certificate is stored (software or card) are: Open the application and select “Options” in the “Tools” context menu.



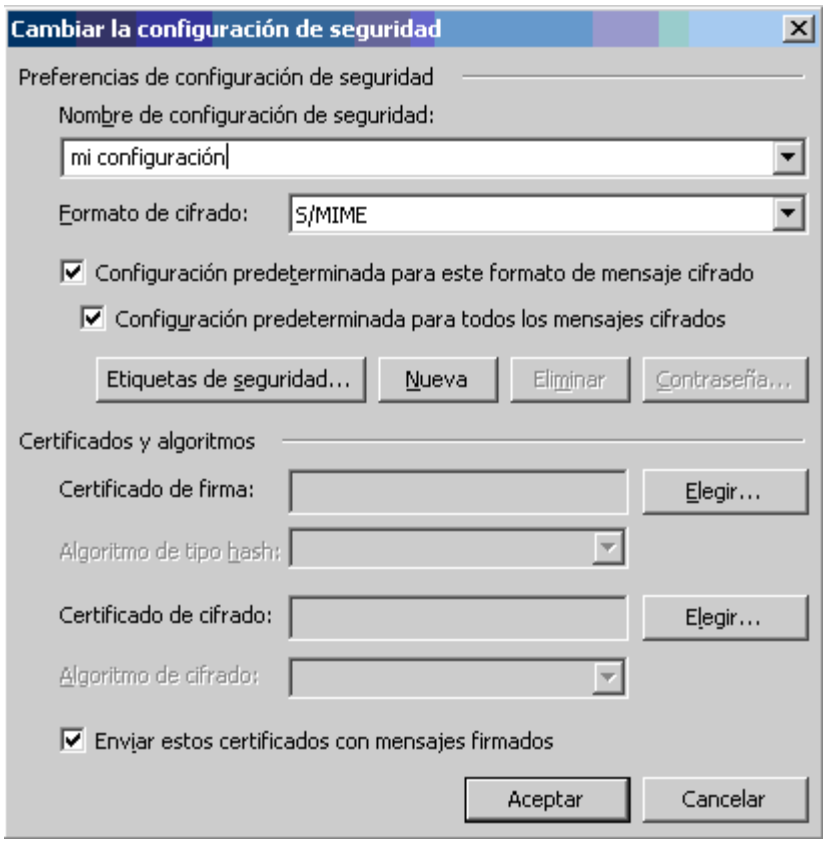
In the next window, select the “Security” tab.



In the section “Secure email”, click “Configuration”. The following window will open.

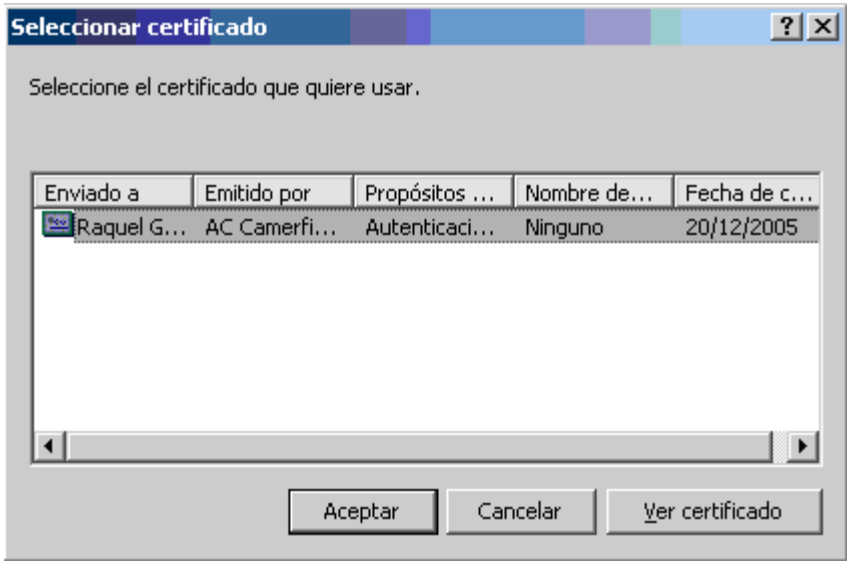


First give the security configuration that you are going to create a name.

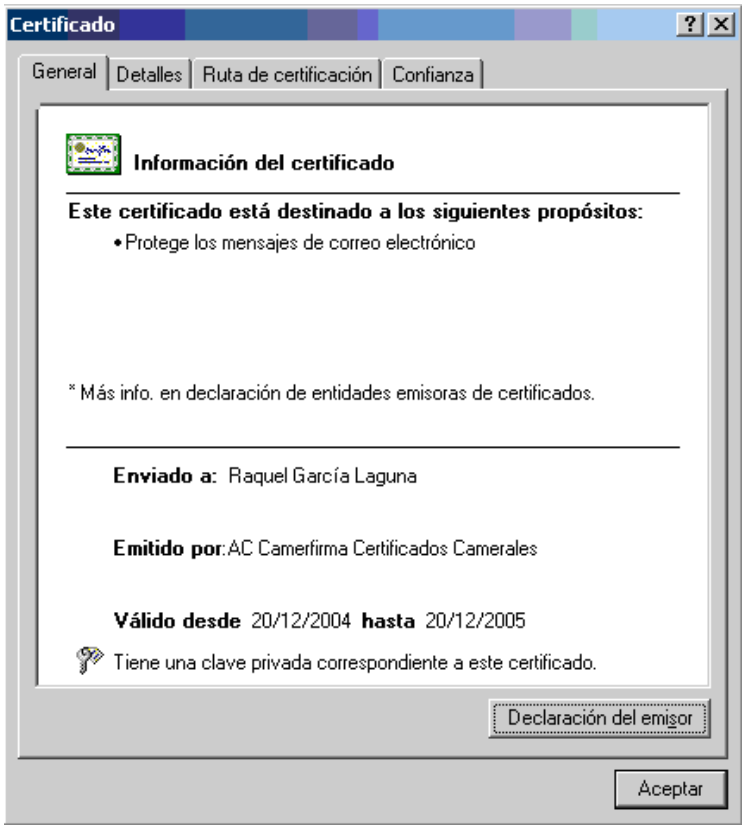


Then click “Choose” in “Signature certificate”. A window will open with the different certificates that are valid for your email account. Note: If the certificate is software-based, you will only be able to choose from the certificates that have already been installed in Internet Explorer. Certificates that are installed in Netscape, Mozilla, or other browsers will have to be installed in Internet Explorer in order to use them in Outlook. If the certificate is on a card, you will also be able to select from among the certificates on the card.

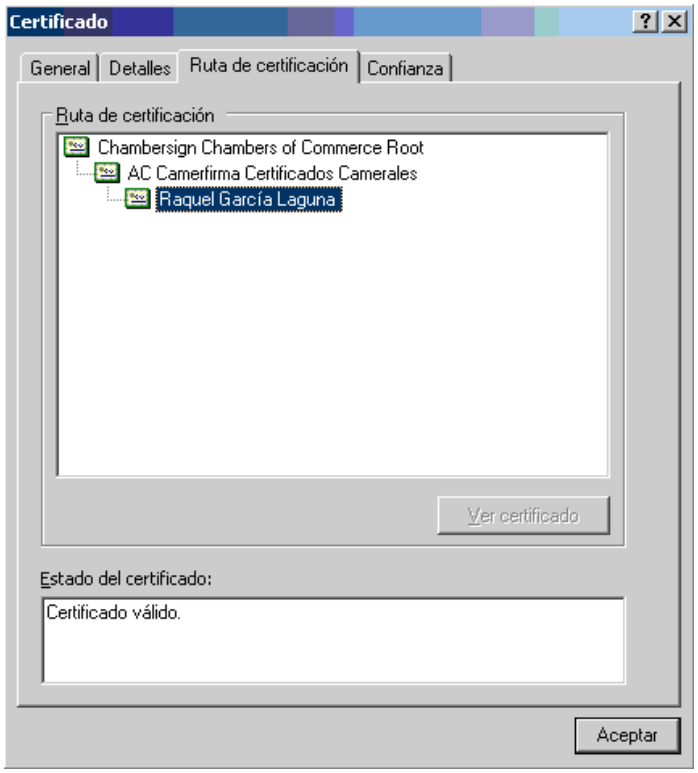
If the certificate email does not match the account email, the certificate will not be displayed. The certificate will also not be displayed if the public key of the Certification Authority that issued the certificate is not installed. Lastly, revoked or expired certificates will also not be displayed.



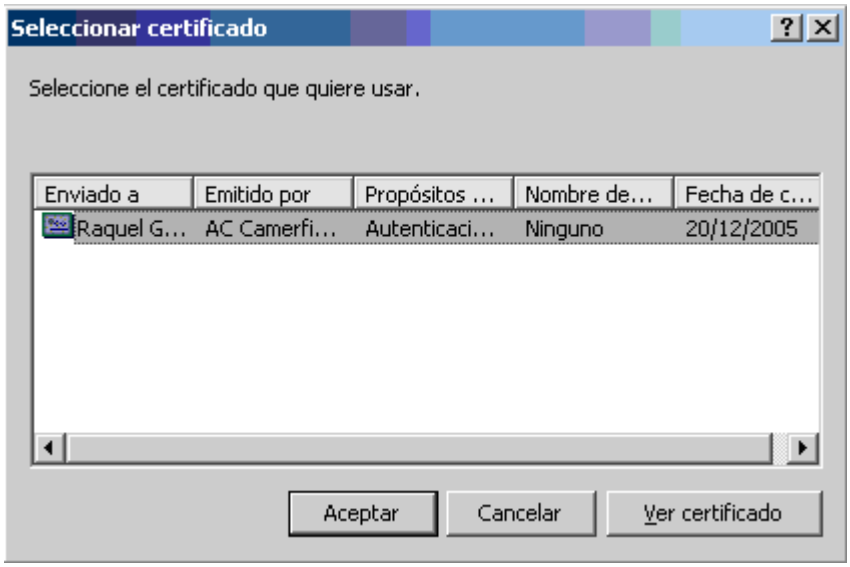
To verify that the information that will be displayed is correct, select a certificate and click “View certificate”. Confirm that the there are no exclamation points next to the icon representing the certificate, as shown in the image.



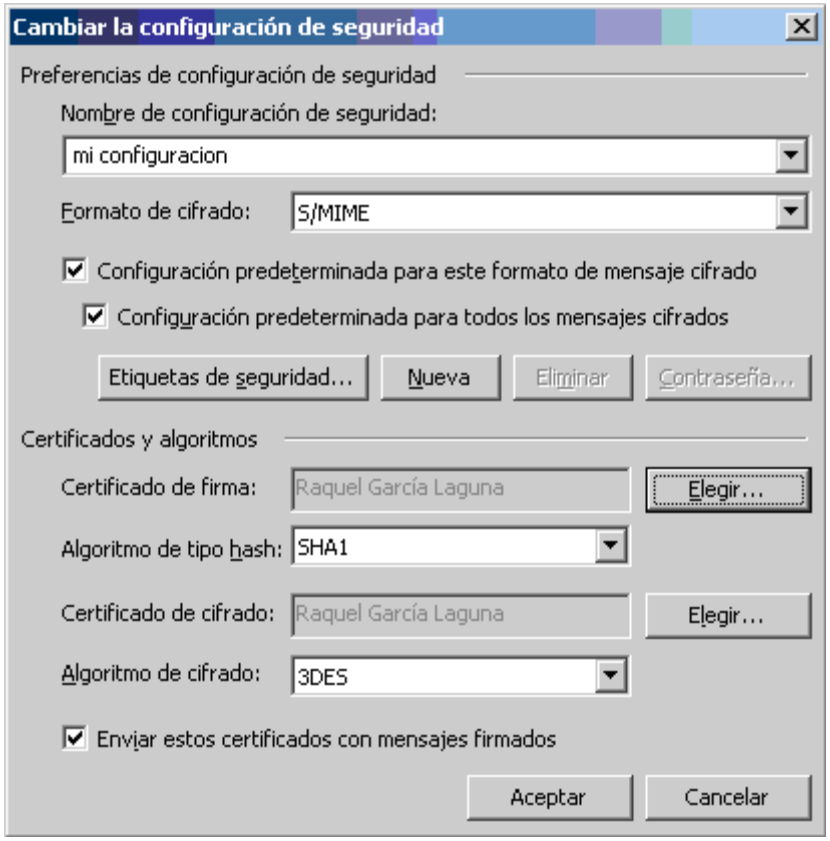
The name of the Certification Authority that signed the certificate and the name of your certificate should be displayed in the “Certification path” tab. The “Certificate status” section should read “Certificate valid”.



If the certificate is correct, click OK in the “Certificate” window. The certificate selection screen will be displayed again.

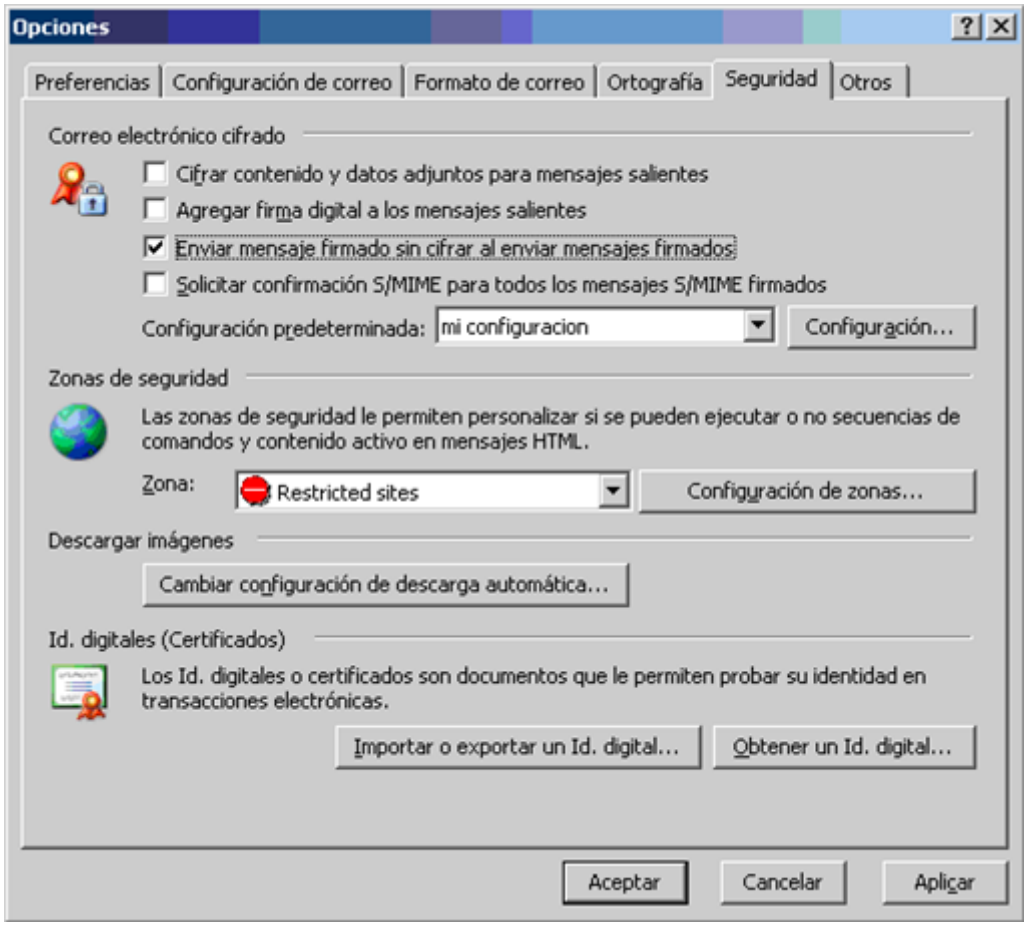


After the certificate has been selected, click OK. You will note that in the "Change security settings" window, the name of the certificate will be displayed in the "Certificates and algorithms" section in both "Signature certificate" and "Encryption certificate".



The encryption certificate is included in the digitally-signed email, so that other people can send you email encrypted with these options. In other words, when a user receives a signed message from you, the certificate that he will store for encrypting the email messages that he wants to send you will be this one. If you want to specify a certificate that is not the signature certificate, you can change it by clicking "Choose". The process is exactly the same as for the signature certificate. We recommend that the same certificate be used in both sections, and that the default algorithms be used for security reasons.

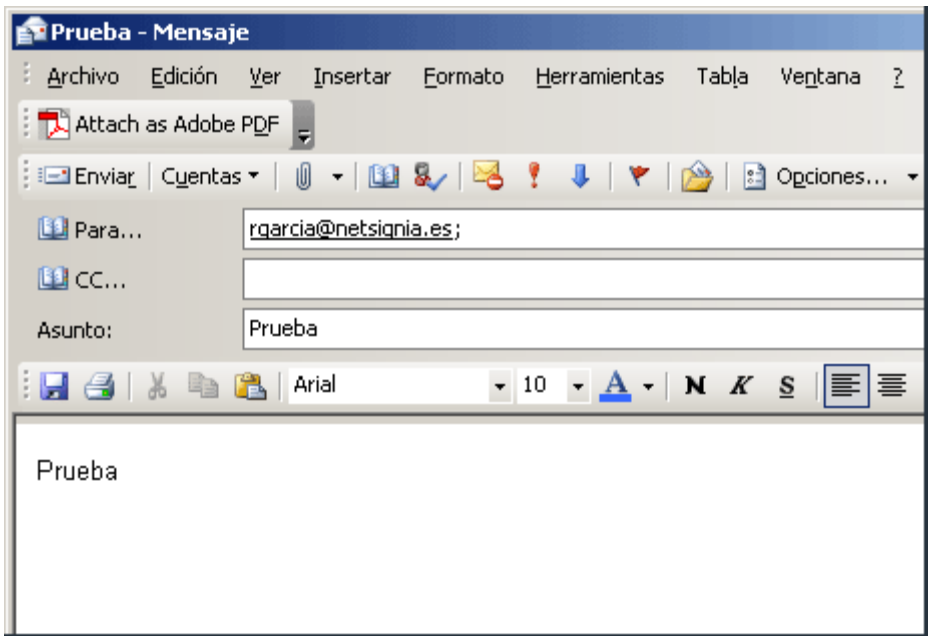
Click Accept. The "Options" window will be displayed again. Mark the "Send signed message unencrypted when sending signed messages" box.



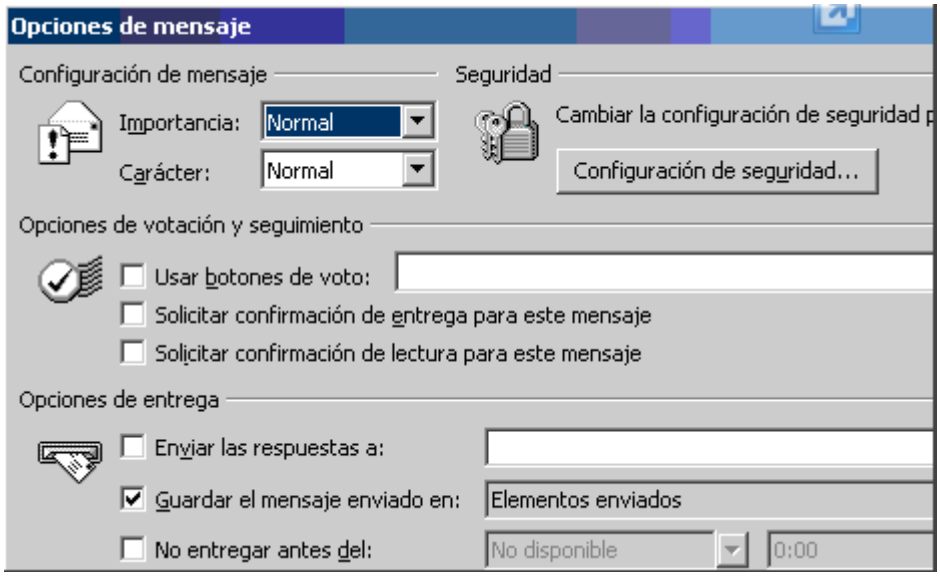
If you would like to send all messages signed by default, mark the box for "Add digital signature to outgoing messages". Leave this box unmarked if you would like to sign messages manually. Click OK and the settings for sending signed messages are configured. Once the certificate has been configured in Microsoft Outlook, it is ready to be used to sign emails.

IMPORTANT: Messages cannot be sent from an email address that does not match the one in the digital certificate. In other words, the digital certificate includes an email address provided by you. Only you will be able to sign messages sent from the address in your certificate.

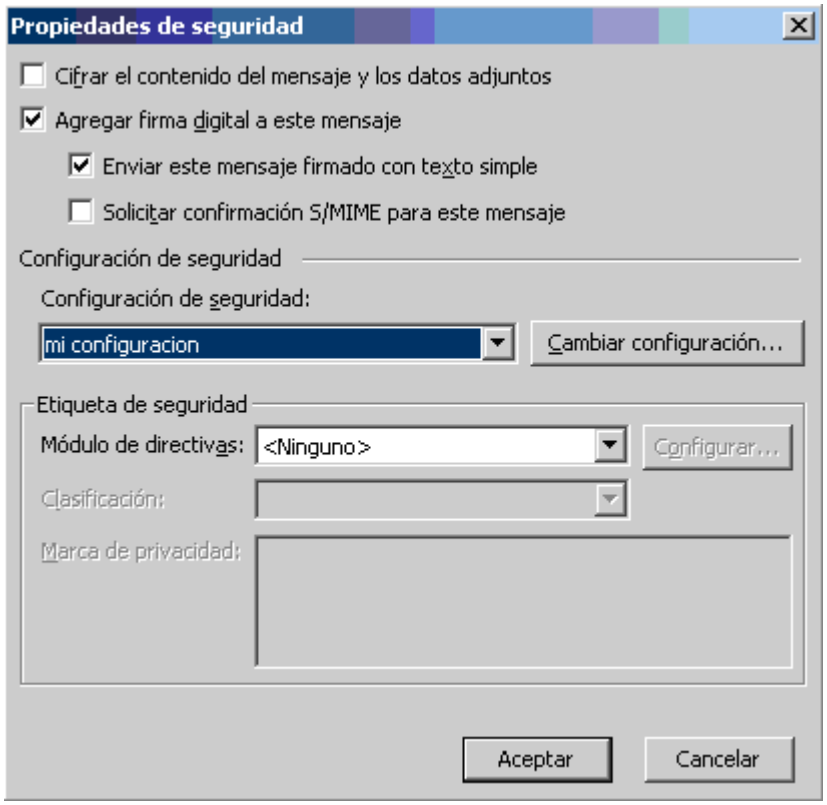
The first step is to create your message (write the text, attach files, enter the recipient/s, etc.).



After this information has been filled out, the message will be signed. This can be done is several different ways:
a) Click “Options". Then click the “Security settings” button.

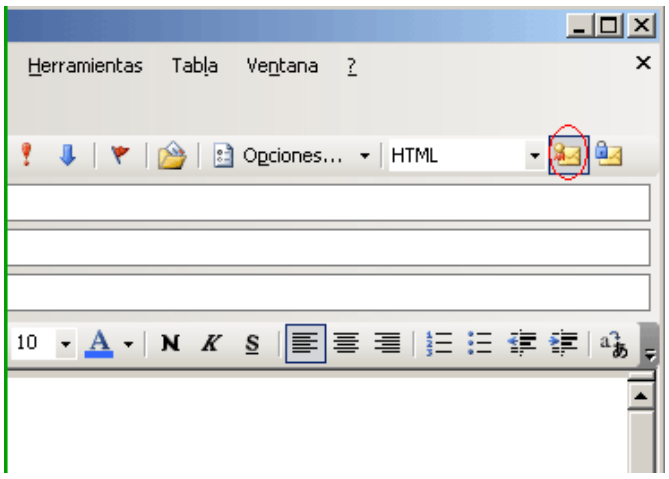


The following window will open. Mark the box for “Add digital signature to this message”. In the “Security settings” section, select the configuration that you created when you installed the certificate in Microsoft Outlook.



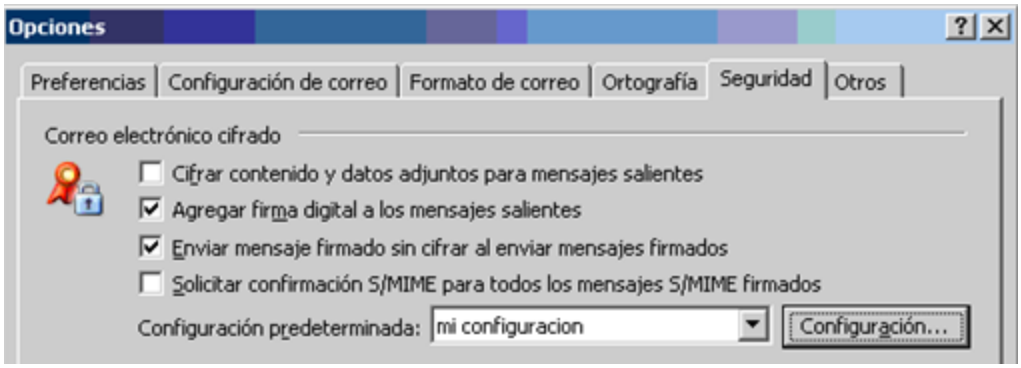
Click OK and then “Close” in the “Message options” window.

b) Another (faster) option to sign messages is to select the icon marked in red that is displayed in the window where the email message text is entered.

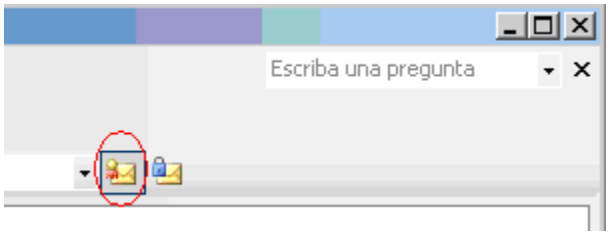


The result will be the same using any of the options explained earlier.

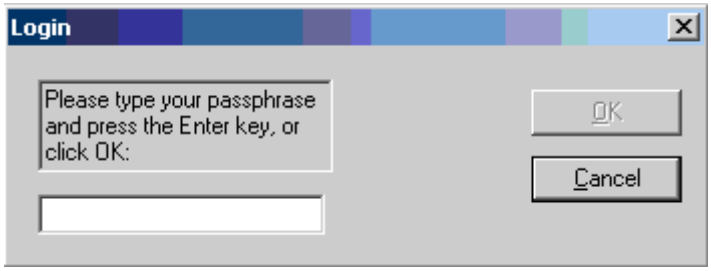
If you marked the box for “Add digital signature to outgoing messages” when you configured Microsoft Outlook...



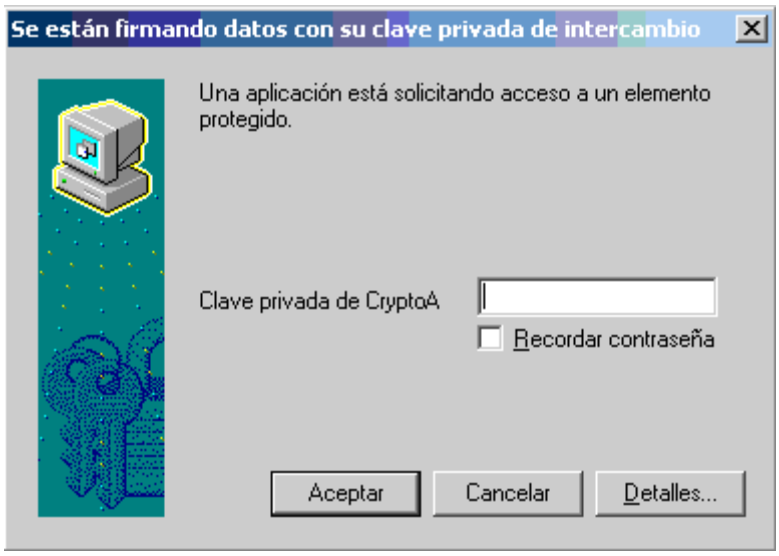
...when you click “New Message”, the signature icon will be marked automatically.



After you have written the email and marked the sign option, click “Send”. When you click the send button, the application will ask you to enter the PIN for the card, if the certificate is on it

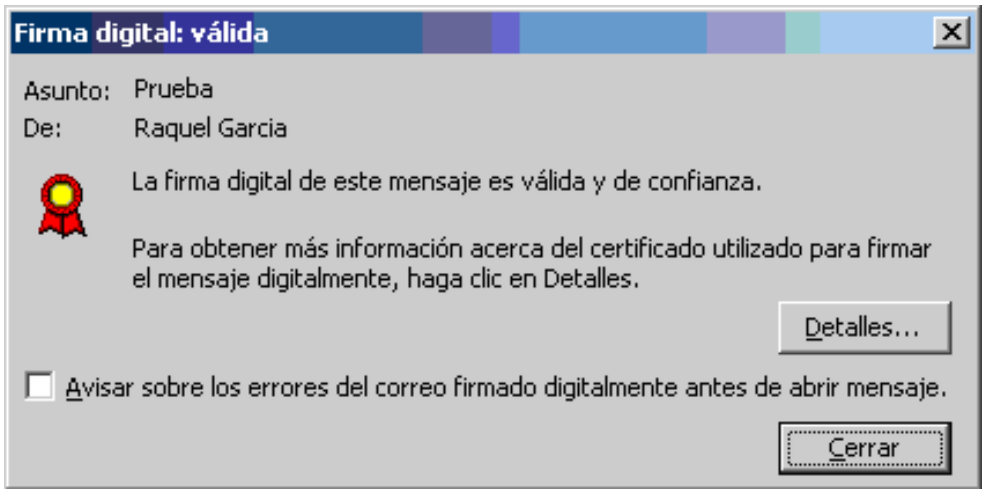


Or, the password for the software-based certificate, if a high security level has been applied to the certificate. In this case, the confirmation screen for using your private key will be displayed. Enter the password (PIN) that you gave to your certificate during the installation. Do NOT select Remember password. If you do, anyone will be able to use your private key. Click OK.



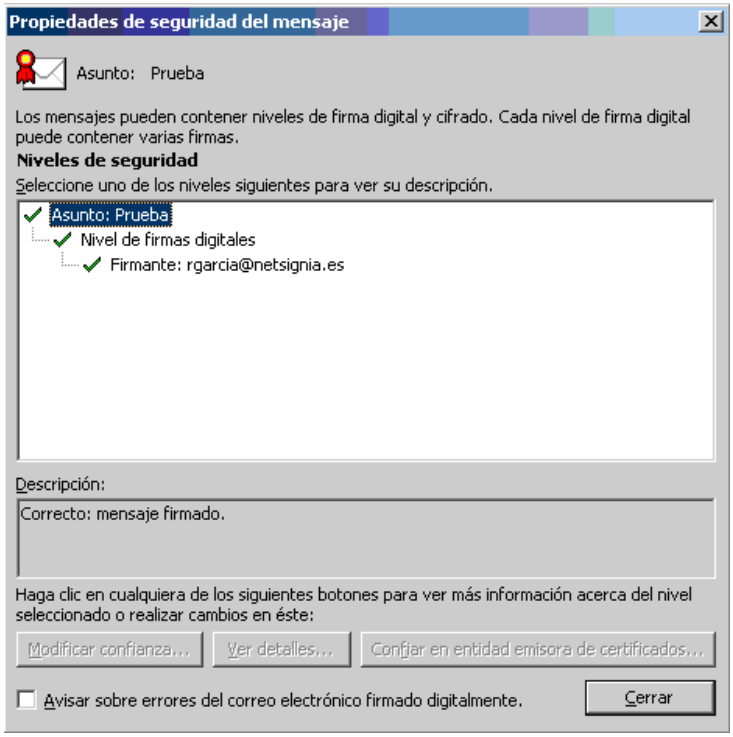
The message will be sent after the correct PIN is entered. To validate a signed email, you must have the Certification Authority certificates for the certificate used to sign the received message. Microsoft Outlook checks to see if these certificates are in the "Intermediate certification authorities" stores and in "Trusted root certification authorities". If they are not, they will be installed automatically, so the message signature will be valid. When you receive an email that is digitally signed by another user, the message will be associated with an icon with a seal icon, which will indicate that the message is signed.

If you click on the red icon, you can see who signed the message, whether the digital signature is valid, and trusted.

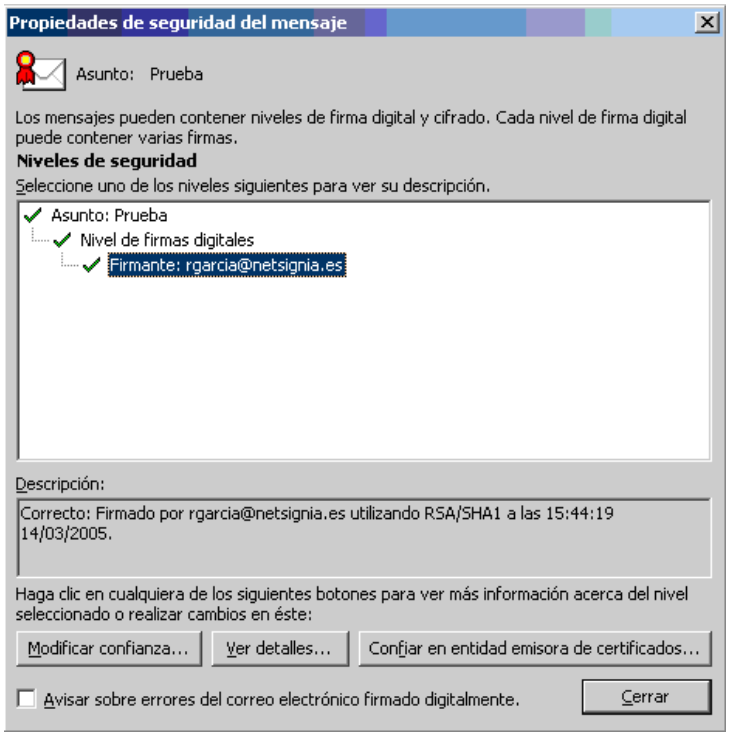


For more information, click “Details”.

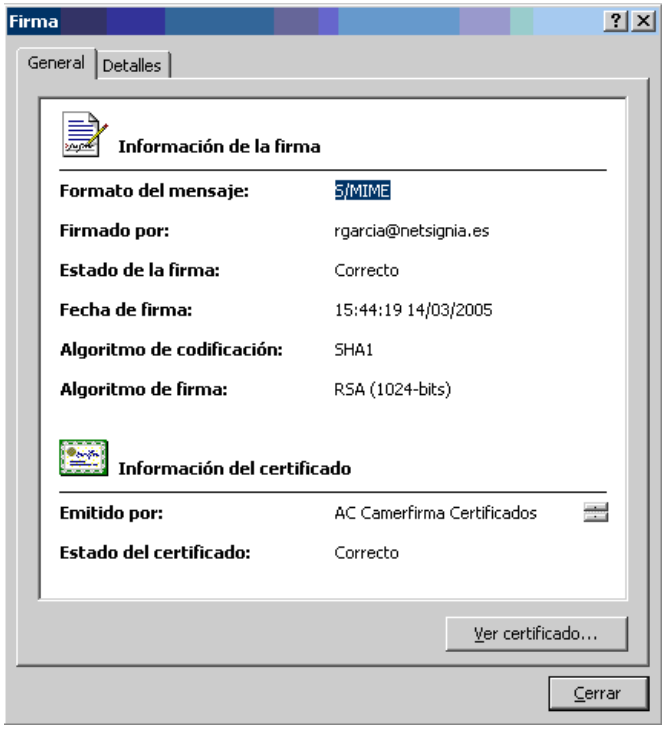
The following image shows that the message was signed correctly.



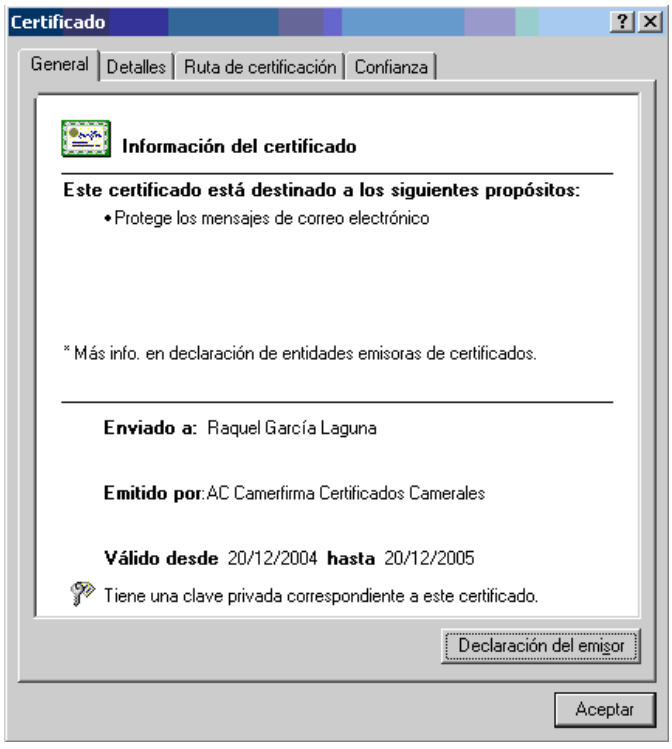
Click “Signer” to see who signed the email. Click “Show details”.



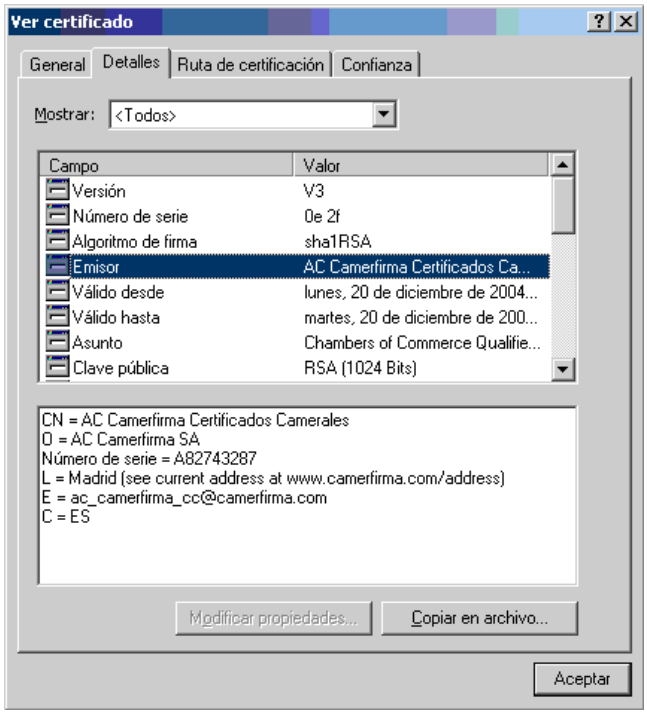
. Click “Show details”.



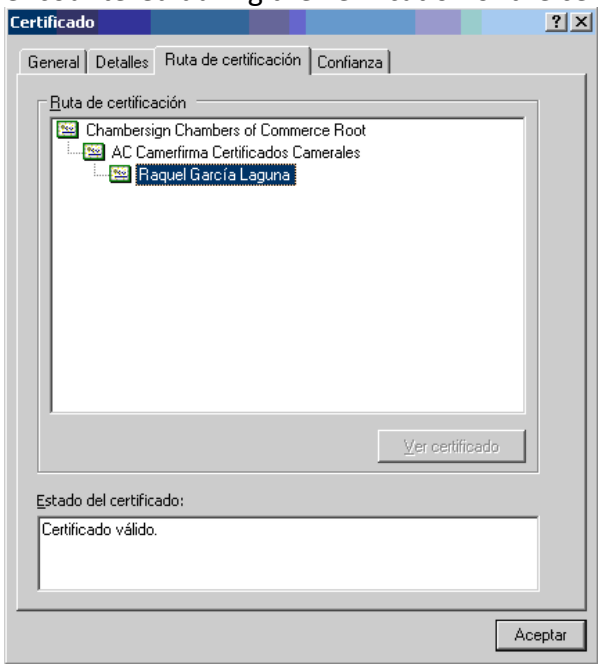
Then click “View certificate”. This will allow you to see all of the details for the certificate that signed the message.



The “Details” tab will provide information on the certification authority, the owner, the certificate expiration date, digital fingerprint, etc.



The “Certification path” will show the trust hierarchy to which the certificate belongs. The “Certificate status” section also shows any problems that were encountered during the verification of the certificate, if any.



Una compañía de GRUPO signe

www.signe.es

Avda. de la Industria, 18
28760 Tres Cantos (Madrid)
España

Tel.: + 34 918 06 00 99
comercial@signe.es