

# respuesta digital

Taller:

*La Firma Digital en el correo electrónico*



Gobierno  
de Navarra



La seguridad digital del futuro, hoy

respuesta  
digital



Gobierno  
de Navarra



La seguridad digital del futuro, hoy

Juan Carlos Rodríguez  
[jcrodriguez@s21sec.com](mailto:jcrodriguez@s21sec.com)

## En que consiste el correo electrónico

- Comunicación Offline, rápida, utilizada de forma masiva y sin coste aparente.
- Permite el envío de todo tipo de contenidos: (texto, imágenes, audio, programas, ...).
- Permite el envío de mensajes de 1 a n en una sola operación.
- Fácil de instalar y utilizar.



## Características del correo electrónico

Utiliza una plataforma cliente-servidor.

El servidor envía los mensajes (SMTP) y los recibe (POP, IMAP,...) almacenándolos en los buzones de usuario.

Los usuarios descargan a sus equipos el contenido de sus buzones (POP) o los leen directamente del servidor (IMAP, Webmail, ...)

Cada usuario dispone al menos de un buzón que lo identifica con su nombre y dirección de email.

El control de acceso se realiza por la utilización de un usuario/password.

## Características del correo electrónico

- Identificación básica de una cuenta de correo de usuario.

Dirección Servidor correo

Nombre del usuario

Dirección de correo (email)

¿Puede asegurarse la veracidad de esta información?

## Problemas de seguridad, identificación

- La información del usuario en la cuenta de correo no es verificada y podemos incluir cualquier dato en ella.

Datos ficticios

Dirección de correo verdadera

¿Podemos enviar un correo con esta identificación?

- Envío de un correo con la identificación “falseada”

The image shows two windows from Outlook Express. The left window is titled 'Campaña publicidad' and shows an email being composed. The 'Enviar' button in the toolbar is circled in red. The recipient is 'administrador@s21edu.com' and the subject is 'Campaña publicidad'. The body of the email contains the text: 'En breve recibirá noticias nuestros. Un saludo. -- Bill Gates --'. The right window is titled 'Bandeja de entrada - Outlook Express' and shows the inbox. A message from 'Juan Carlos Rodriguez' with the subject 'Correo confidencial' is highlighted in red. Below it, a message from 'Bill Gates' with the subject 'Campaña publicidad' is visible. The status bar at the bottom indicates '9 mensajes, 1 no leídos' and 'Con conexión'.

## Problemas de seguridad, envío credenciales

- La identificación del usuario para poder acceder a su buzón se realiza mediante la validación de un nombre de **usuario** y una **contraseña**.
- El envío de estas credenciales se realiza por defecto sin ningún cifrado, por lo que un sniffer puede capturar esta información.

```

C:\> Símbolo del sistema - mailsnarf
C:\tools\dsniff>dsniff
02/28/07 16:47:47 xp-pro.s21edu.com -> srv2k03.s21edu.com <pop>
USER jcrodriguez
PASS jcrr21!$
    
```

## Confidencialidad mensaje

- No solo el envío de credenciales se realiza sin cifrar, ¡todo el mensaje es transmitido en "texto claro", por lo que puede ser interceptado.

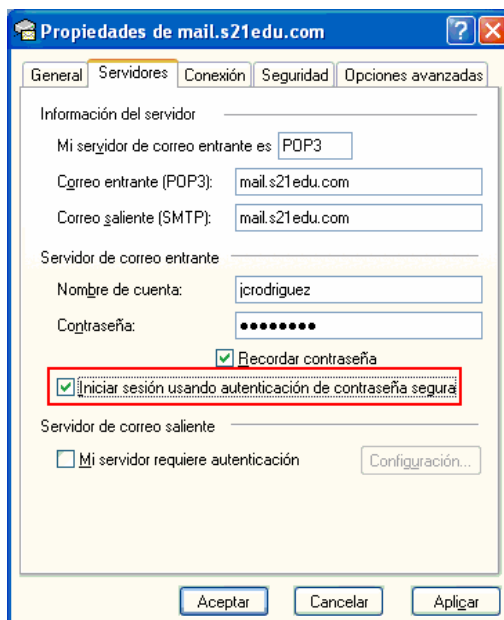
```

C:\> Símbolo del sistema - mailsnarf
C:\tools\dsniff>mailsnarf
From jcrodriguez@s21sec.com Wed Feb 28 16:48:50 2007
Message-ID: <000801c75b4f5f0b9a23050264a8c0@s21edu.com>
From: "Juan Carlos Rodriguez" <jcrodriguez@s21sec.com>
To: <administrador@s21edu.com>
Subject: Correo confidencial
Date: Wed, 28 Feb 2007 16:48:49 +0100
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="-----_NextPart_000_0005_01C75B58.523B0DC0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1106
X-MimeOLE: Produced By Microsoft MimeOLE 06.00.2800.1106

This is a multi-part message in MIME format.
-----_NextPart_000_0005_01C75B58.523B0DC0
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Este mensaje no debe ser leído por nadie m=E1s
-----_NextPart_000_0005_01C75B58.523B0DC0
Content-Type: text/html;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
    
```

## Proteger el envío de credenciales

Podemos proteger el envío de credenciales (usuario/password) utilizando las opciones incluidas en la mayoría de los programas cliente de correo electrónico.

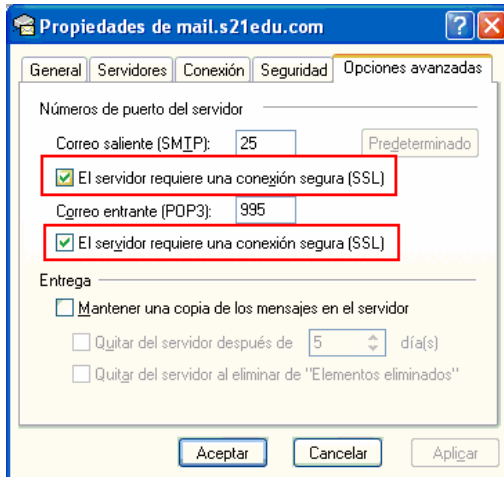


```

C:\> Símbolo del sistema -
C:\tools\dsniff>dsniff
    
```

## Asegurar la confidencialidad

- Para proteger la confidencialidad del mensaje, cuando se envía al servidor de correo o cuando es leído el buzón de entrada, es necesario utilizar las opciones de cifrado, basadas generalmente en el establecimiento de un canal seguro SSL (similar al utilizado en las conexiones Web, https://.....)

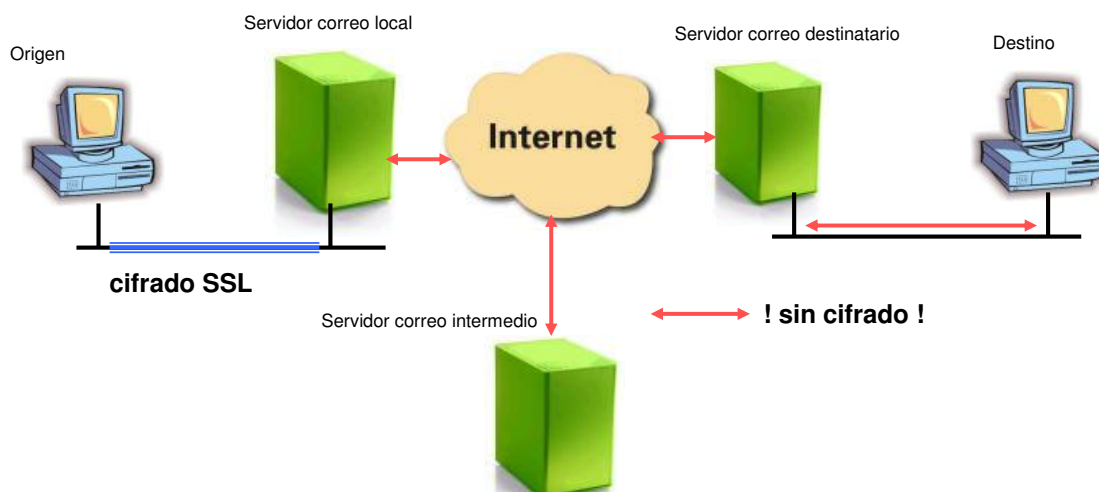


- Para utilizar esta opción es necesario además instalar un certificado de identificación de equipo en el servidor de correo.

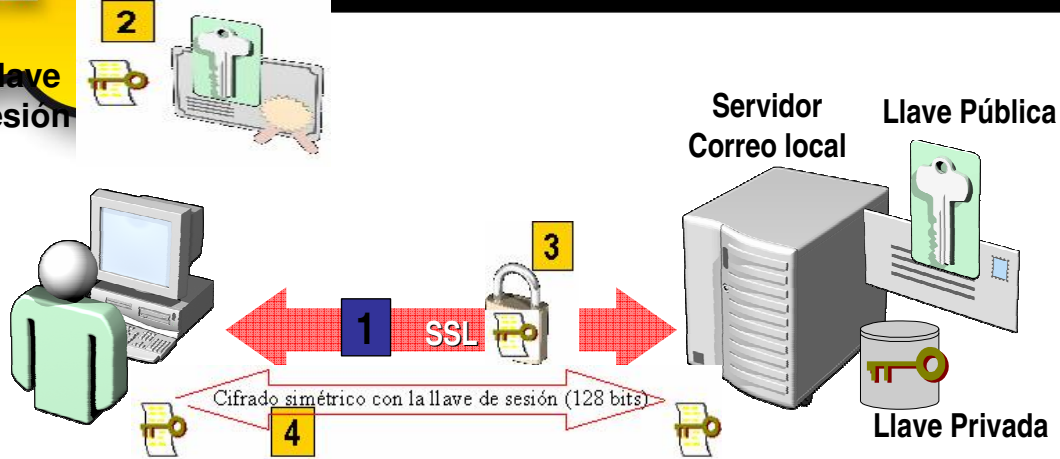
- Los equipos de los clientes de correo deben de tener instalada la confianza en la AC que emitió el certificado del servidor.

## Asegurar la confidencialidad

- La opción anterior asegura la confidencialidad del mensaje solo durante el trayecto del cliente al servidor de correo local, **!No mientras el mensaje viaja a través de Internet desde un servidor de correo a otro hasta alcanzar su destino final!**



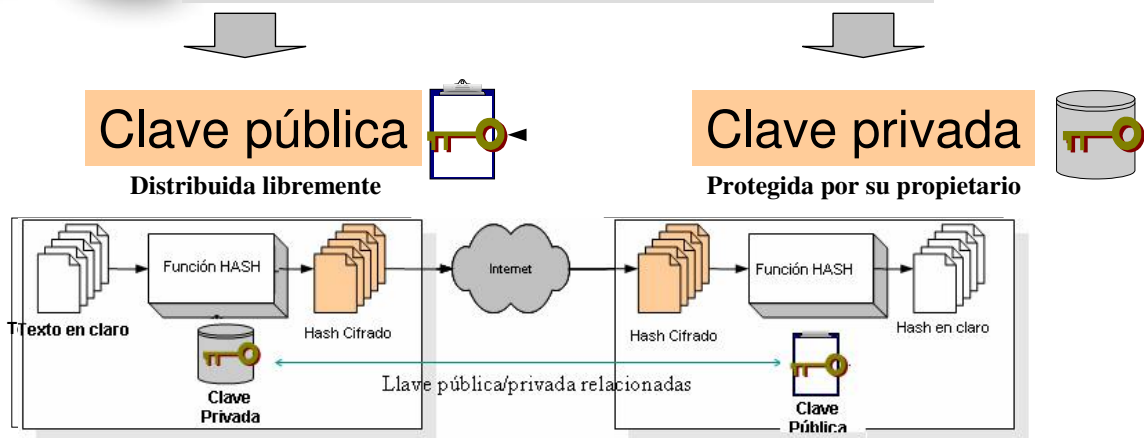
Llave sesión



- 1** El cliente accede al servidor de correo mediante SSL
- 2** crea una clave de sesión única y la codifica usando la clave pública del servidor obtenida a partir del certificado presentado
- 3** El servidor recibe la clave de la sesión y la decodifica mediante su clave privada
- 4** A partir de ese momento se realiza un cifrado simétrico con la llave de sesión en poder de ambos.

## Firma digital electrónica

Clave diferente para cifrar y descifrar



En la firma electrónica se invierte el sentido, clave privada para firmar clave pública para verificar la firma

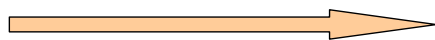
**Características:**

- **Autenticación.** Se puede comprobar la identidad del firmante
- **Integridad.** Comprueba que el texto no ha sido modificado.
- **No repudio.** El firmante no puede negar haber generado y entregado el documento.



**!No incluye Confidencialidad!,** ya que no se cifra el mensaje

Integridad



Hash

El emisor realiza el Hash (función resumen) del texto en claro y lo envía junto con el mensaje. El receptor realiza la misma función y comprueba el resultado. Si el texto no se ha modificado el resultado obtenido debe ser el mismo.

Autenticación y no repudio



Hash cifrado

Se cifra el Hash con la clave privada del emisor. Sólo el emisor posee esa clave, por lo tanto no puede negar la firma. Cualquiera tercera persona puede comprobar la firma si tiene acceso a la clave pública relacionada con la privada, la cual se distribuye libremente.

proceso de firma electrónica



### proceso de verificación



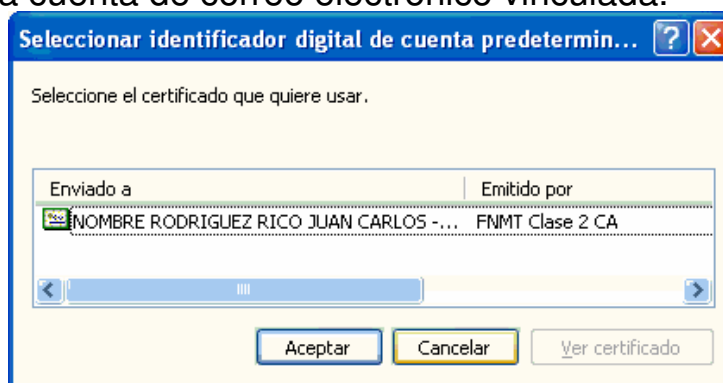
### Creando y verificando una firma digital



Si el código hash calculado no concuerda con el resultado de la firma digital desencriptada, o el documento fue modificado después de hacer la firma, o la firma no fue generada por la clave privada del emisor del documento

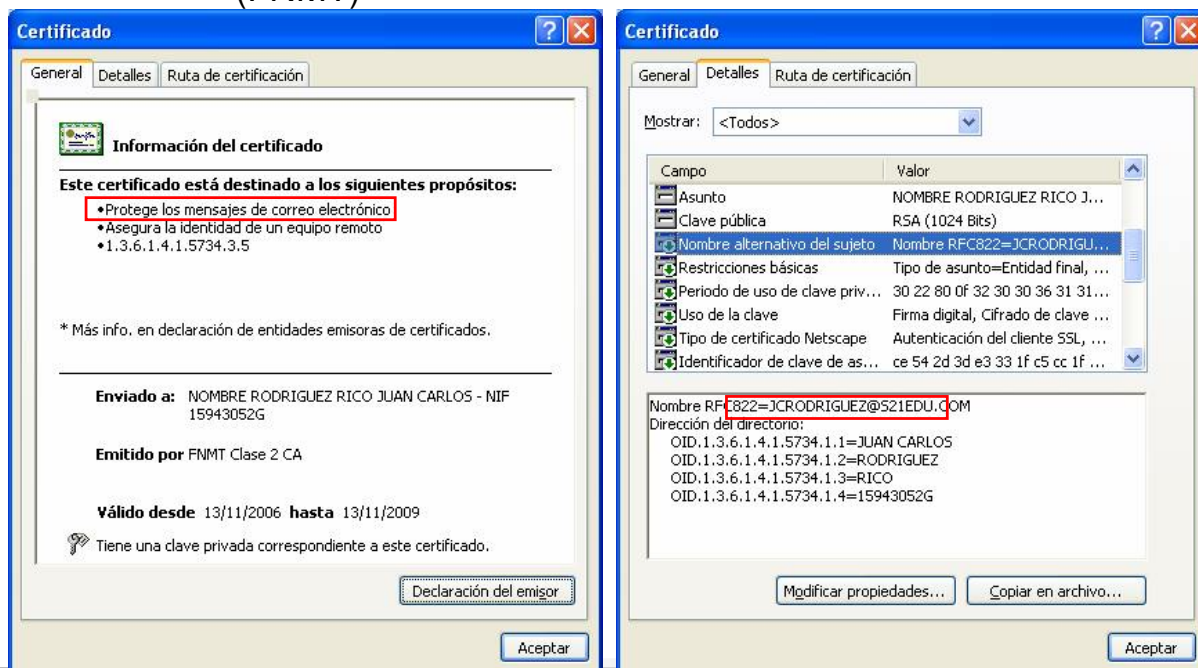
## Autenticidad e Integridad del mensaje

- Para poder asegurar la identidad y la integridad del mensaje se utiliza la criptografía de llave pública/privada para “firmar” digitalmente el mensaje.
- Para ello es necesario disponer de un certificado digital, emitido por una Autoridad Certificadora reconocida, en el que conste nuestro nombre así como la cuenta de correo electrónico vinculada.

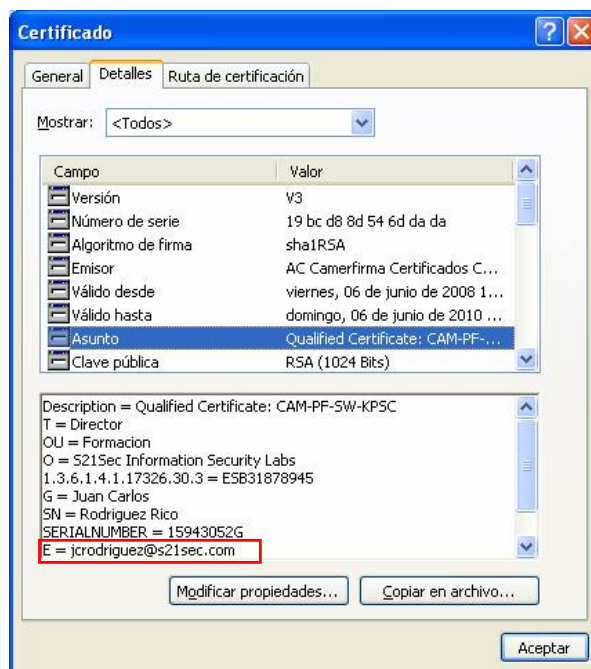
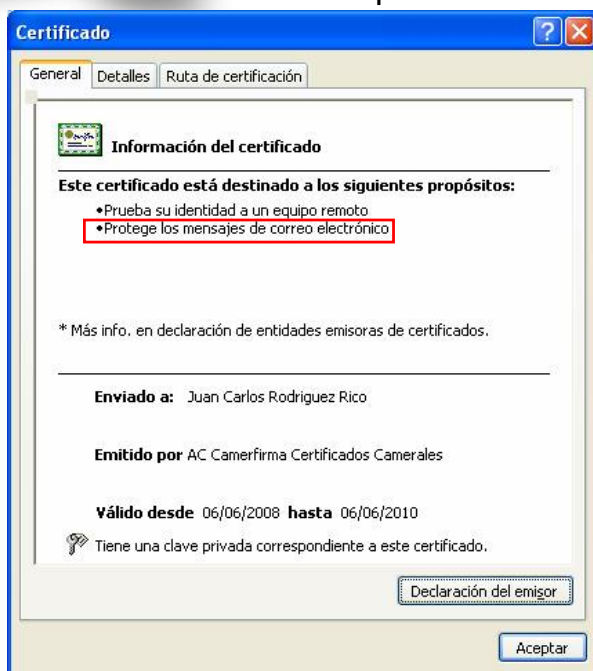


## Certificado de Usuario

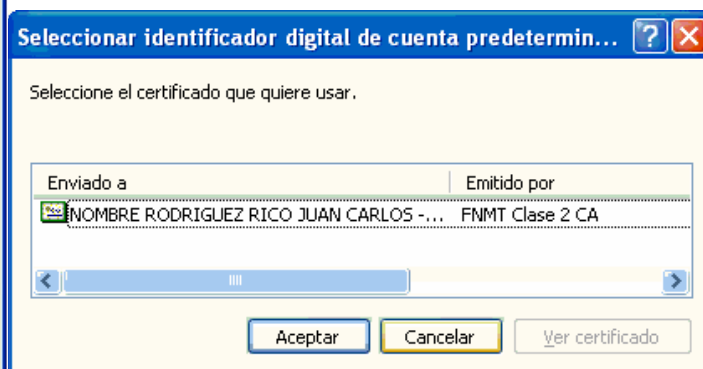
- Ejemplo de certificado de usuario para varios propósitos, emitido por la “Fábrica Nacional de Moneda y Timbre” (FNMT)



- Ejemplo de certificado de usuario para varios propósitos, emitido por CAMERFIRMA

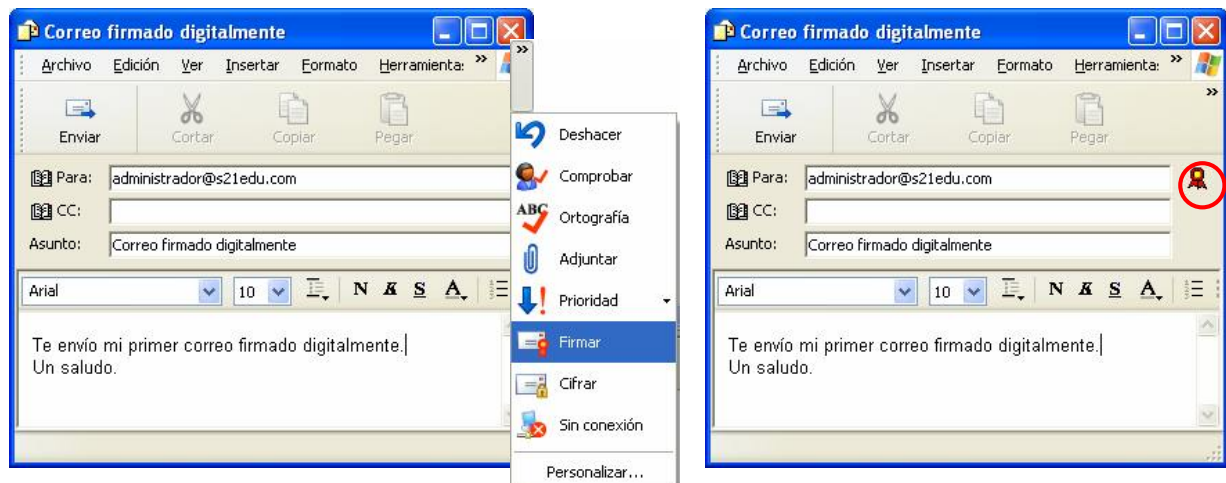


- Para poder utilizar la firma electrónica debe vincularse el certificado a la cuenta de correo correspondiente.



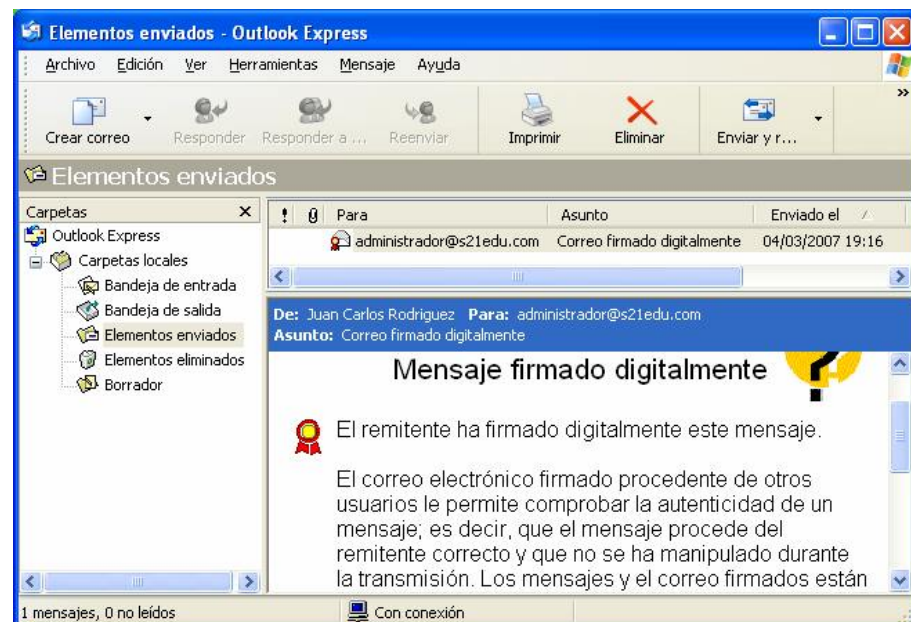
## Firma electrónica

- Para “firmar” un mensaje debemos seleccionar la opción correspondiente antes del envío del mensaje.



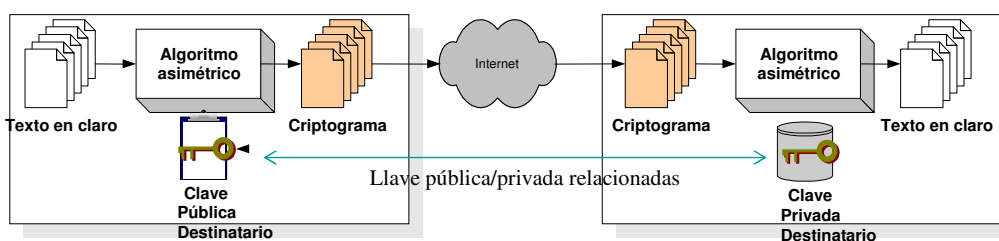
## Envío de mensaje con firma digital

- Mensaje enviado firmado digitalmente



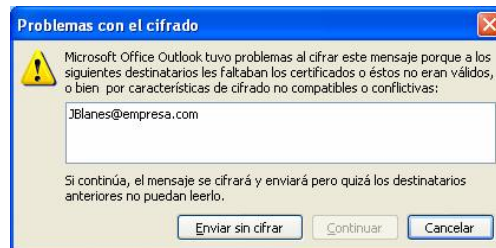
## Firma electrónica

- La firma electrónica proporciona la **autenticidad** (el mensaje proviene de quien dice ser) y la **integridad** (el mensaje no ha sido modificado desde que se envió)
- Para la confidencialidad del mensaje es necesario “cifrarlo” con la llave pública del destinatario de manera que solo pueda ser descifrado por éste con su llave privada relacionada.



## Cifrado del mensaje

- Si no se dispone de la llave pública del destinatario el mensaje no puede enviarse cifrado y recibimos una alerta al intentarlo.



Para disponer de la llave pública del destinatario tan solo es necesario recibir previamente un correo firmado de éste y responder al mismo, ya que en los mensajes con firma digital se envía la llave pública en formato de certificado digital.