



<b>PROJECTE:</b> Manuals d'ús de signatura electrònica	Versió: 1.5
<b>TÍTOL:</b> Signatura electrònica amb MS Windows Mail i MS Windows Vista	Codi Referència:
<b>RESUM:</b>	Data Publicació: 05/12/2008

## PROCEDIMENT

### Signatura electrònica amb MS Windows Mail i MS Windows Vista

<b>PREPARAT PER:</b>	<b>REVISAT PER:</b>	<b>APROVAT PER:</b>
Nom:	Nom:.	Nom:
Data: 05/12/2008	Data:	Data:



## ÍNDEX

<b>1</b>	<b>Objectiu i abast .....</b>	<b>4</b>
<b>2</b>	<b>Prerequisits .....</b>	<b>4</b>
<b>3</b>	<b>Configuració de signatura electrònica amb MS Windows Mail i Windows Vista.....</b>	<b>5</b>
<b>4</b>	<b>Enviament de missatges .....</b>	<b>14</b>
<b>4.1</b>	<b>Signats.....</b>	<b>14</b>
<b>4.2</b>	<b>Xifrats.....</b>	<b>18</b>
<b>5</b>	<b>Recepció de missatges .....</b>	<b>20</b>
<b>5.1</b>	<b>Signats.....</b>	<b>20</b>
<b>5.2</b>	<b>Xifrats.....</b>	<b>24</b>
<b>6</b>	<b>Referències.....</b>	<b>26</b>

## **1 Objectiu i abast**

El present document descriu el procés de configuració del client de correu electrònic Microsoft Windows Mail instal·lat al sistema operatiu Microsoft Windows Vista per poder realitzar la signatura electrònica de correus, i realitzar les accions de transmetre i rebre missatges signats o xifrats digitalment.

## **2 Prerequisits**

Per poder realitzar una correcta configuració del client de correu electrònic i realitzar les accions de transmetre i rebre missatges signats o xifrats, cal que es compleixin una sèrie de prerequisits. Els requisits previs indispensables per a realitzar les passes descrites en aquest manual son els següents:

- Cal tenir instal·lat el software per a la lectura del certificat digital UPC, aquest software es pot descarregar de la següent adreça web [https://www.upc.edu/identitatdigital/certificat\\_digital/programari-certificat-digital/descarrega-de-programari](https://www.upc.edu/identitatdigital/certificat_digital/programari-certificat-digital/descarrega-de-programari). Per obtenir els detalls d'instal·lació d'aquest software, es pot accedir a la següent adreça web [https://www.upc.edu/identitatdigital/certificat\\_digital/programari-certificat-digital/Guia\\_Basica\\_Instalacio.pdf/view](https://www.upc.edu/identitatdigital/certificat_digital/programari-certificat-digital/Guia_Basica_Instalacio.pdf/view).
- Cal que tingueu inserit el vostre carnet universitari de l'UPC al lector de targetes del vostre equip i el llum del lector en color verd fixa. Això indica que el lector esta preparat per a treballar.
- Cal que tingueu instal·lades les claus públiques de CATCert a Internet Explorer. Per obtenir els detalls d'instal·lació de les claus públiques, es pot accedir a la següent adreça web [https://www.upc.edu/identitatdigital/certificat\\_digital/programari-certificat-digital/Guia\\_Basica\\_Instalacio.pdf/view](https://www.upc.edu/identitatdigital/certificat_digital/programari-certificat-digital/Guia_Basica_Instalacio.pdf/view).

### 3 Configuració de signatura electrònica amb MS Windows Mail i Windows Vista

- 3.1 Per configurar la signatura electrònica per utilitzar-la amb l'eina Microsoft Windows Mail, s'ha d'obrir l'aplicació, accedir al menú "Eines" (pas 1) i fer clic a "Comptes..." (pas 2). A continuació s'obrirà el quadre "Comptes d'Internet" (pas 3) tal i com es pot veure a la figura 1.

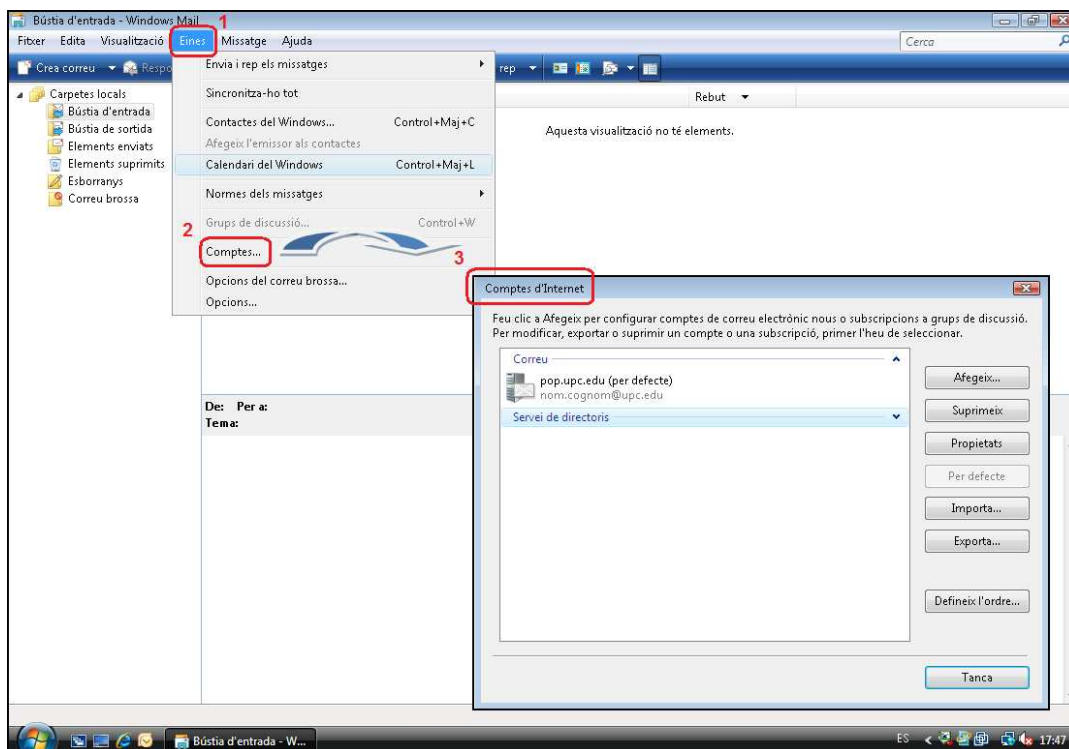


Figura 1. Finestra de l'eina MS Windows Mail

- 3.2 Un cop obert el quadre “Comptes d’Internet”, s’ha de seleccionar el compte de correu configurat i fer clic al botó “Propietats” (pas 1). A continuació, s’obre la finestra “Propietats de <compte de correu>” (pas 2), on cal accedir a la fitxa “Seguretat” (pas 3) per afegir el certificat digital emmagatzemat al carnet universitari a l’apartat “Certificat de signatura” i “Preferències de xifratge” (figura 2).

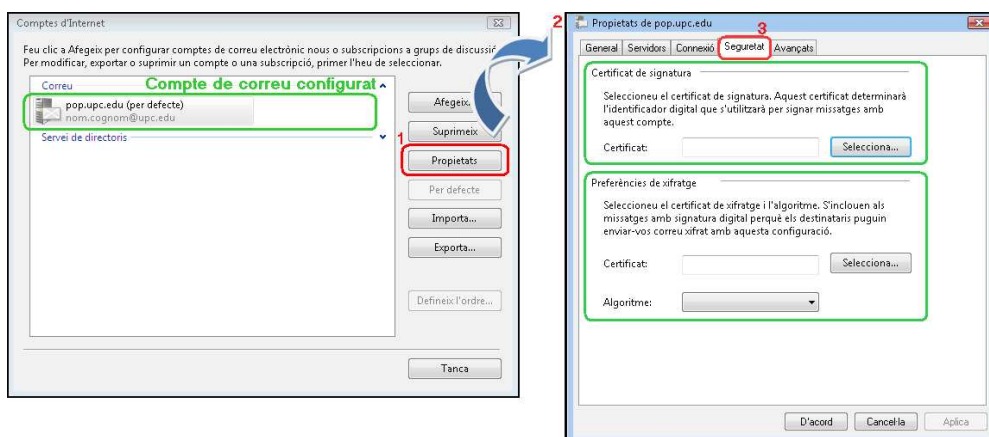


Figura 2. Opcions de seguretat

- 3.3 A la fitxa “Seguretat”, s’ha de fer clic al botó “Selecció de l’identificador digital del compte per defecte” (pas 1). A continuació, s’obre el quadre “Selecció de l’identificador digital del compte per defecte” (pas 2). Aquí s’ha de seleccionar el certificat digital emmagatzemat al carnet universitari i acceptar (pas 3) per confirmar el procés de selecció (figura 3).

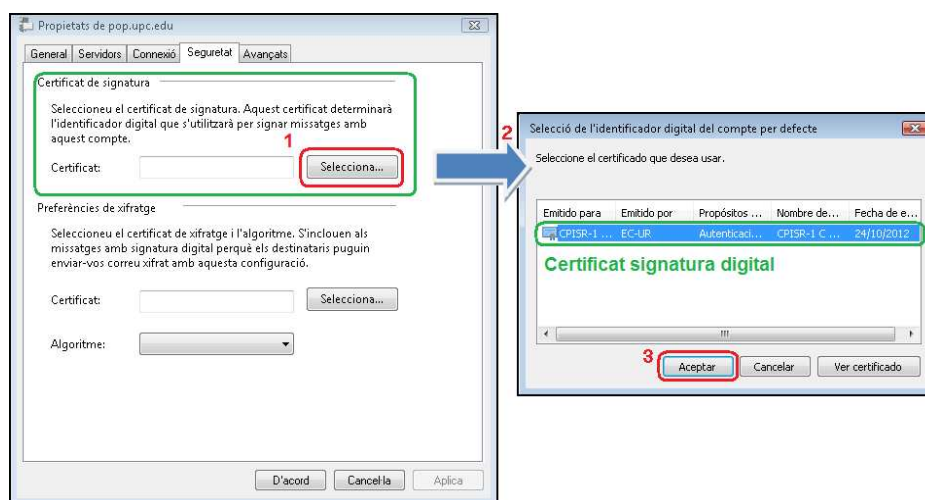


Figura 3. Configuració de signatura

- 3.4 Després de configurar el certificat de signatura, s'ha de fer clic al botó "Selecciona..." de l'apartat "Preferències de xifratge" (pas 1). A continuació, s'obre el quadre "Selecció de l'identificador digital del compte per defecte" (pas 2). Aquí s'ha de seleccionar el certificat digital emmagatzemat al carnet universitari i acceptar (pas 3) per confirmar el procés de selecció (figura 4).

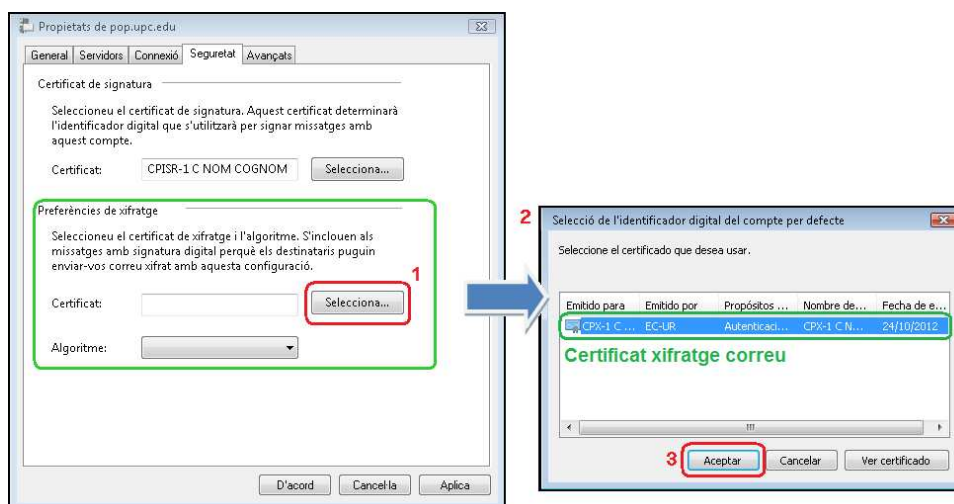


Figura 4. Configuració de xifratge

**NOTA:** Es possible que per un error d'instal·lació no es pugui accedir al certificat emmagatzemat al carnet universitari, en aquest cas cal consultar l'apartat de suport o la guia bàsica d'instal·lació a la nostra web. [https://www.upc.edu/identitatdigital/nou\\_certificat\\_digital\\_esborrany/programari-certificat-digital/Guia\\_Basica\\_Instalacio.pdf/view](https://www.upc.edu/identitatdigital/nou_certificat_digital_esborrany/programari-certificat-digital/Guia_Basica_Instalacio.pdf/view)

- 3.5 Un cop definit l'ús dels certificats emmagatzemats al carnet universitari, cal fer clic al botó "D'acord" per confirmar la configuració del compte de correu, tal i com es pot veure a la figura 5.

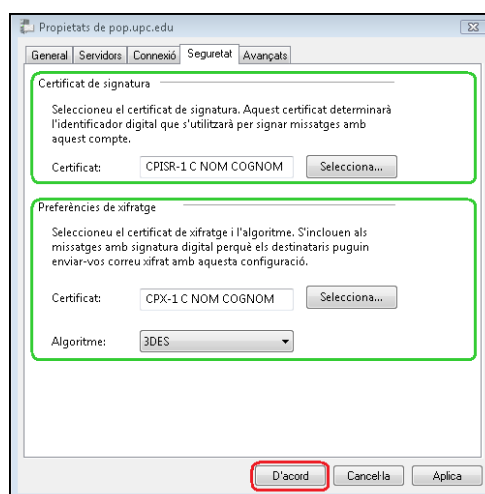


Figura 5. Fitxa seguretat amb l'ús de certificats definit

3.6 Finalment, s'ha de fer clic al botó “Tanca” de la finestra “Comptes d’Internet” per acceptar la configuració del compte de correu amb els certificats del carnet universitari. Tal i com es pot veure a la figura 6.

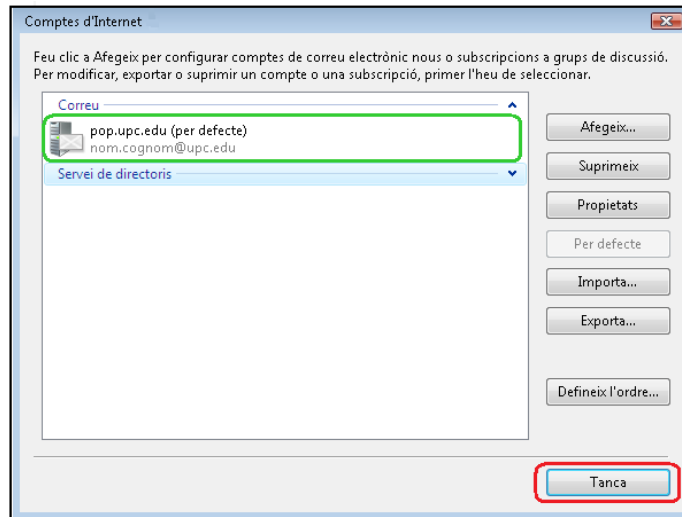


Figura 6. Finestra “Comptes d’Internet”

3.7 A continuació, s’ha de definir l’ús de la signatura de correu per l’enviament de TOTS els missatges de sortida. Cal accedir al menú “Eines” del client de correu MS Mail (pas 1) i fer clic a “Opcions...” (pas 2) per tal d’obrir la finestra “Opcions” (pas 3), tal i com es pot apreciar a la figura 7.

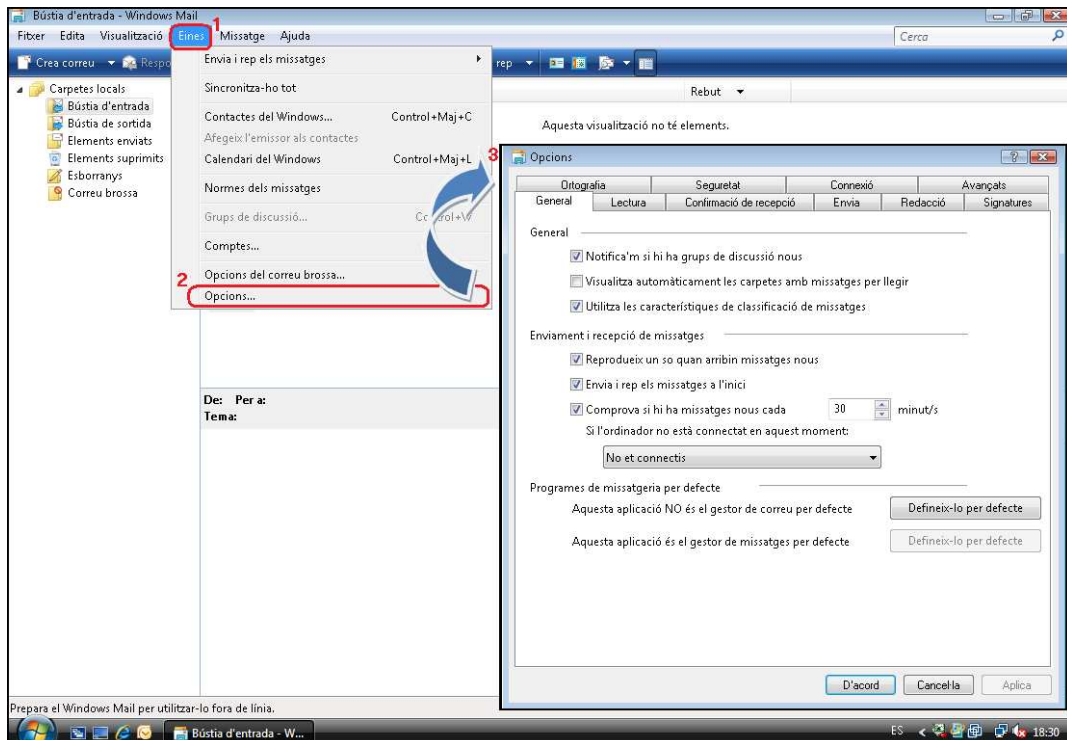


Figura 7. Accés a la finestra “Opcions” de MS Mail



- 3.8 A la finestra “Opcions”, cal fer clic a la fitxa “Seguretat” (pas 1) i marcar l’opció “Signa digitalment tots els missatges sortints” (pas 2) de l’apartat “Correu segur”. A continuació, cal fer clic al botó “D’acord” (pas 3) per validar els canvis i tancar la finestra (figura 8).

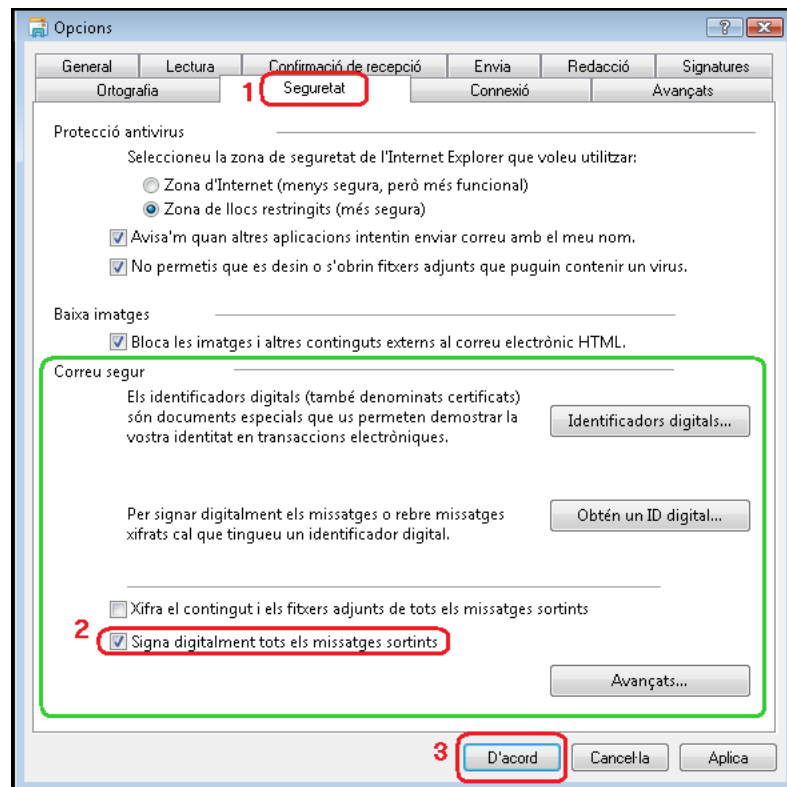


Figura 8. Quadre canvi de la configuració de seguretat omplert

- 3.9 Tots els certificats de CATCert tenen informades les propietats que permeten al sistema validar de forma automàtica l'estat del certificat i els certificats revocat (no vàlids). Aquestes propietats son visibles fent doble clic sobre l'icona de la targeta gemalto (pas 1) de la barra de tasques de Windows, seleccionant l'apartat "Contenido tarjeta" (pas 2) i fent clic a l'icona "Certificados" (pas 3), tal i com es pot apreciar a la figura 9.

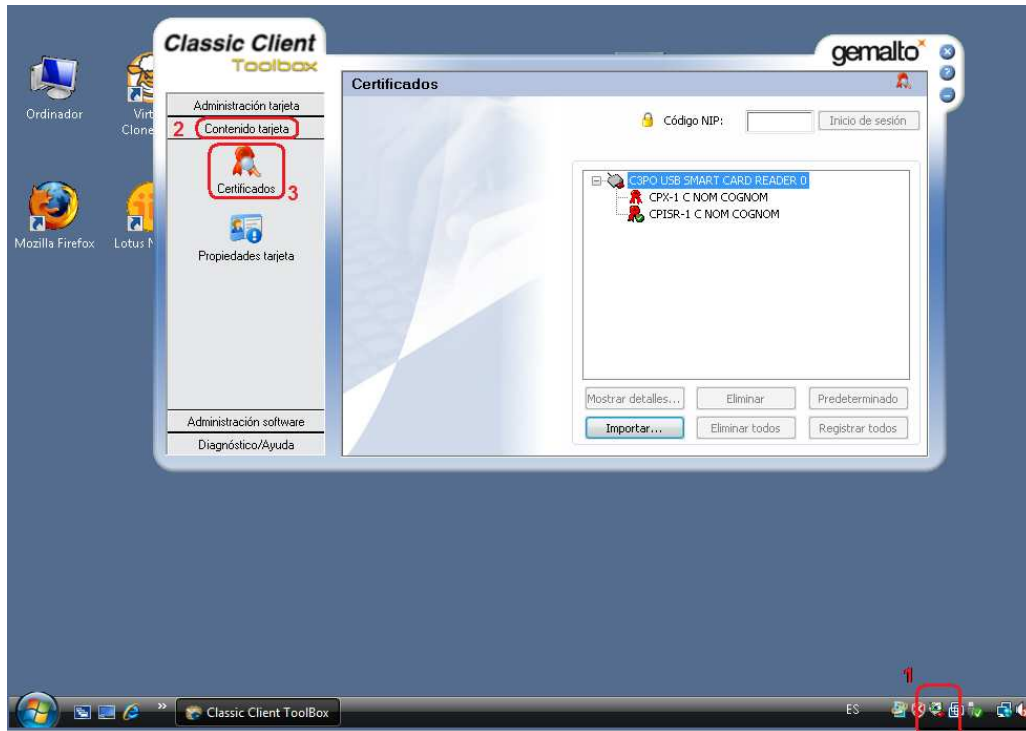


Figura 9. Propietats del certificat gemalto

3.10 Un cop dintre de l'apartat "Certificados" figura 9, cal seleccionar un dels certificats (pas 1) i seleccionar l'opció "Mostrar detalles" (pas 2) del certificat "CPISR-1 C NOM COGNOM" per obrir les propietats del certificat (pas 3), tal i com es por apreciar a la figura 10.

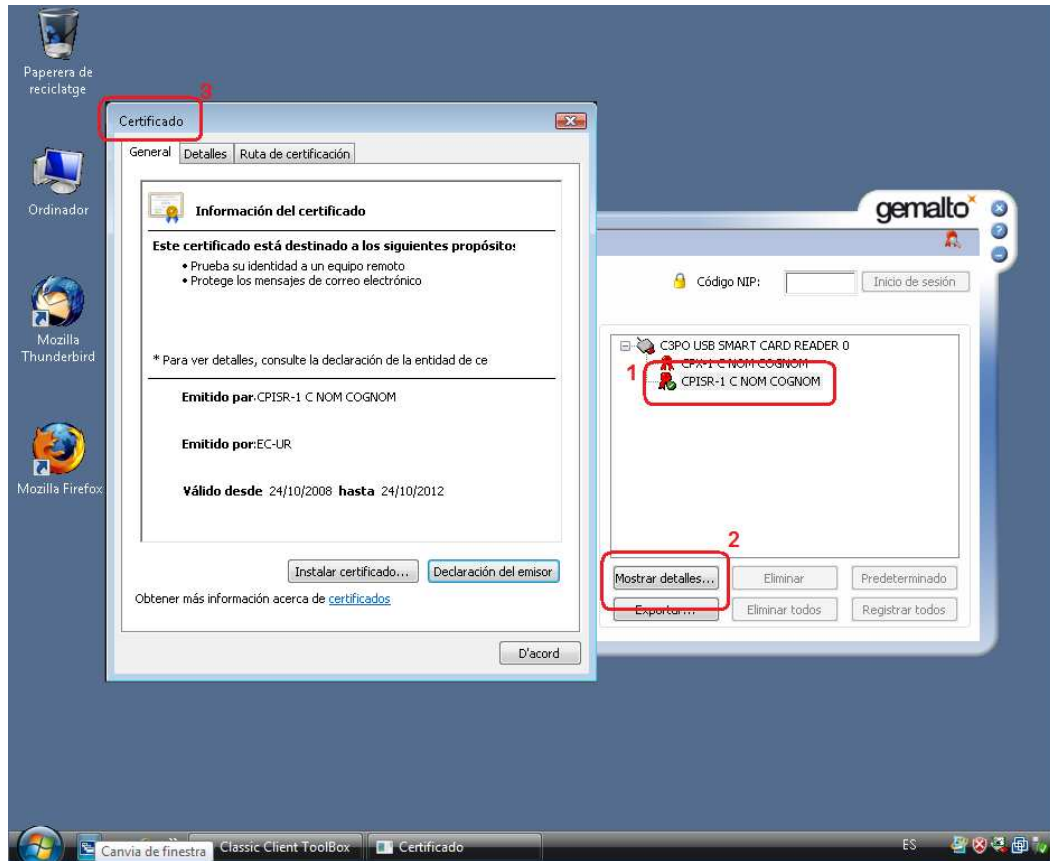


Figura 10. Propietats del certificat

3.11 Un cop a les propietats de la signatura, cal seleccionar la fitxa “Detalles”, on es pot veure les propietats de:

- “Acceso a la información de entidad emisora” (pas 1) que utilitza l’url <http://ocsp.catcert.net> (pas 2) per realitzar la verificació de l’estat del certificat, tal i com es pot apreciar a la figura 11.

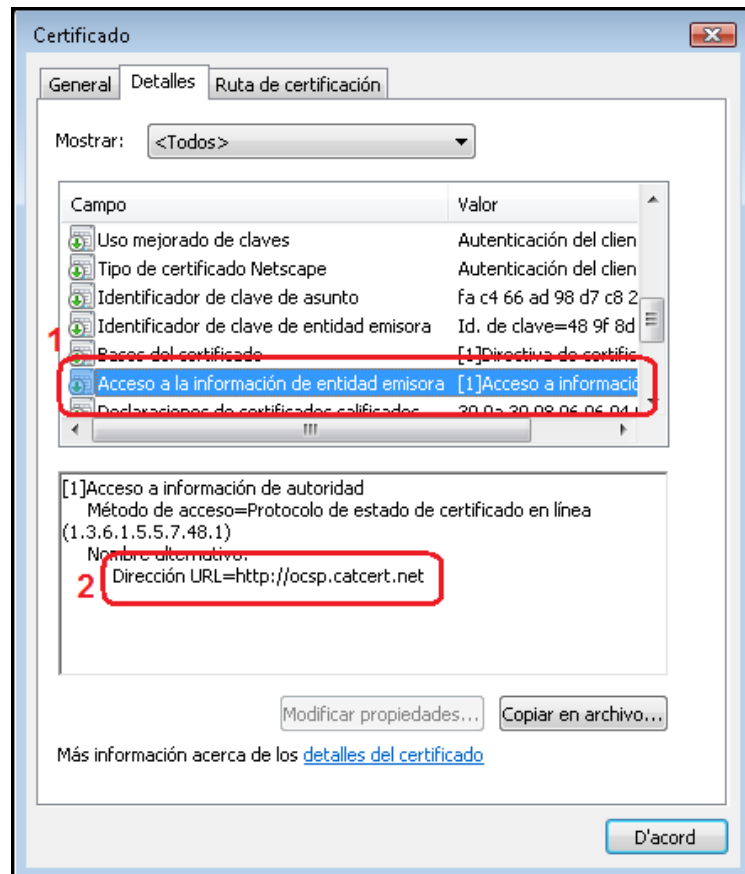


Figura 11. Propietats del certificat.

- “Puntos de distribución CRL” (pas 1) on ens indica les direccions url <http://epsdc.catcert.net/crl/ec-ur.crl> i <http://epsdc2.catcert.net/crl/ec-ur.crl> (pas 2) utilitzades com a punt de descàrrega de la llista de certificats revocats, tal i com es pot apreciar a la figura 12.

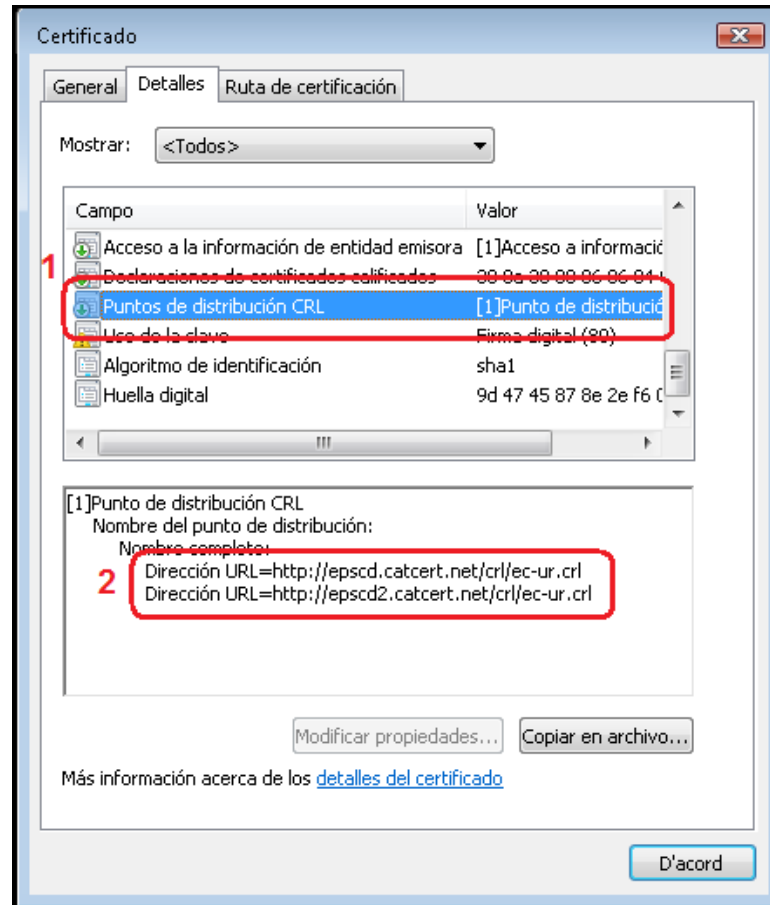


Figura 12. Propietats del certificat.

**NOTA:** Cal tenir en compte, que per que el procés de validació de l'estat del certificat es realitzi de forma correcta i poder descarregar la llista de certificats revocats, es imprescindible disposar d'accés a Internet per l'equip.


## 4 Enviament de missatges

### 4.1 Signats

La signatura electrònica dels correus garanteix l'identitat de l'emissor, que ha rebut la validació de la seva adreça de correu electrònic mitjançant la signatura electrònica de CATCert, i, alhora, garanteix tècnicament que el contingut del missatge no ha estat alterat en trànsit per tercers.

En el cas de no haver configurat la signatura electrònica de TOTS els missatges de correu de sortida com a opció per defecte (veure punts 3.7 i 3.8 de l'apartat anterior) i voler fer ús d'aquesta opció en un moment puntual, s'hauran de seguir les següents passes.

4.1.1 Un cop s'està editant un missatge nou i abans d'enviar-lo, fer clic al botó

“Signatura electrònica”  tal i com es pot apreciar a la figura 13.

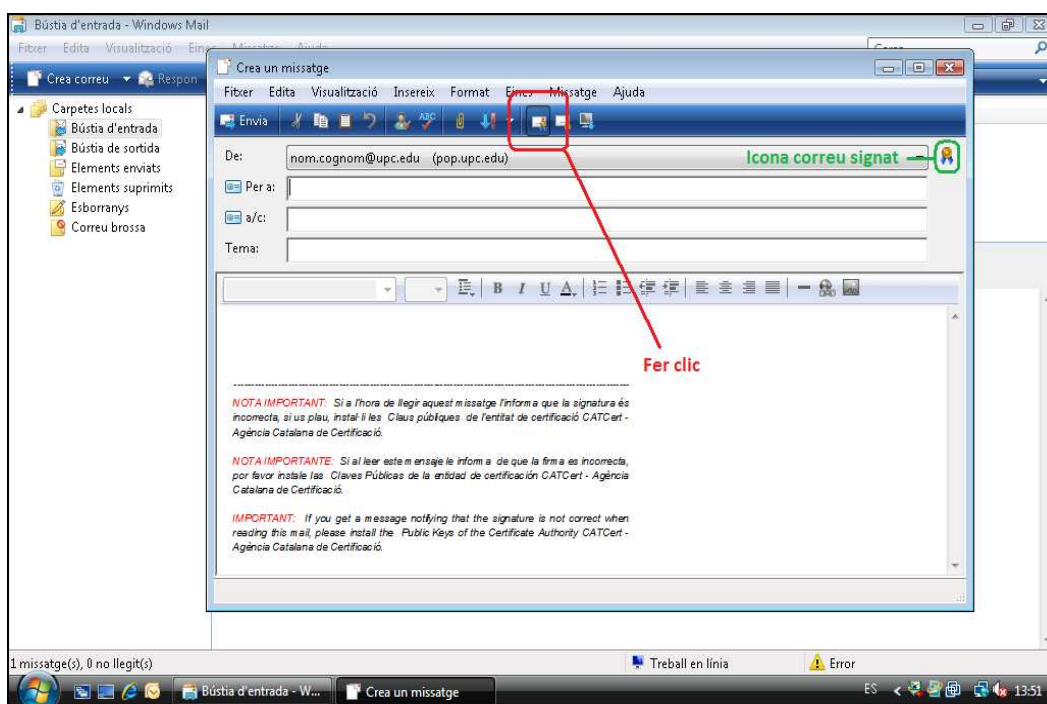


Figura 13. Activar l'enviament de correus signats

4.1.2 En el moment d'enviar el correu electrònic signat, es demanarà el número d'identificació personal del carnet universitari (NIP o PIN) en un quadre emergent (figura 14).

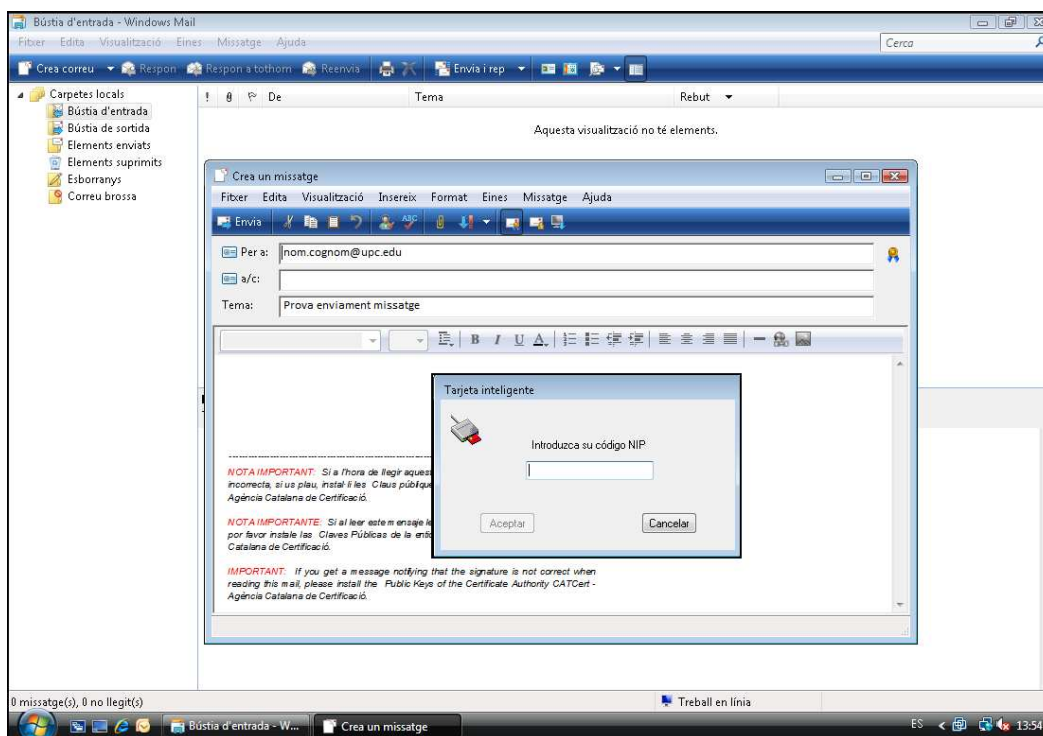


Figura 14. Quadre de diàleg d'introducció del PIN

Si no el poseu o bé introduïu un codi incorrecte, el programa us oferirà l'opció d'enviar el missatge sense signar.

## EL NOMBRE D'INTENTS ABANS DE QUE ES BLOQUEGI LA TARGETA ÉS DE 5

**NOTA:** En cas de bloqueig de la targeta, podeu consultar l'apartat de Gestió de PIN i PUK [https://www.upc.edu/identitatdigital/certificat\\_digital/gestio-pin-i-puk/desbloqueig\\_targeta.pdf/view](https://www.upc.edu/identitatdigital/certificat_digital/gestio-pin-i-puk/desbloqueig_targeta.pdf/view)

**NOTA:** En cas de no tenir instal·lades les claus públiques de CATCert o que l'adreça de correu no correspongui a la definida al certificat, apareixerà un missatge indicant que no es vàlid. Per solucionar-ho, podeu consultar l'apartat de suport a la nostra web o seguint els passos de la nostra guia bàsica [https://www.upc.edu/identitatdigital/nou\\_certificat\\_digital\\_esborrany/programari-certificat-digital/Guia\\_Basica\\_Instalacio.pdf/view](https://www.upc.edu/identitatdigital/nou_certificat_digital_esborrany/programari-certificat-digital/Guia_Basica_Instalacio.pdf/view)

- 4.1.3 A l'acceptar el quadre de diàleg d'introducció del NIP o PIN, s'enviarà el correu signat.
- 4.1.4 RECOMANACIÓ: Incorporació com a mínim un dels textos següents per facilitar la lectura al receptor del missatge, en cas de no tenir les claus públiques del CATCert instal·lades.

**NOTA IMPORTANT:** Si a l'hora de llegir aquest missatge l'informa que la signatura és incorrecta, si us plau, instal·li les Claus públiques de l'entitat de certificació CATCert - Agència Catalana de Certificació que podrà trobar a la web [http://www.catcert.cat/web/cat/descarrega\\_claus/totes\\_01.jsp](http://www.catcert.cat/web/cat/descarrega_claus/totes_01.jsp).

**NOTA IMPORTANTE:** Si al leer este mensaje le informa de que la firma es incorrecta, por favor instale las Claves Públicas de la entidad de certificación CATCert - Agència Catalana de Certificació que podrà encontrar en la direcció web [http://www.catcert.cat/web/cat/descarrega\\_claus/totes\\_01.jsp](http://www.catcert.cat/web/cat/descarrega_claus/totes_01.jsp).

**IMPORTANT:** If you get a message notifying that the signature is not correct when reading this mail, please install the Public Keys of the Certificate Authority CATCert - Agència Catalana de Certificació available at the web address [http://www.catcert.cat/web/cat/descarrega\\_claus/totes\\_01.jsp](http://www.catcert.cat/web/cat/descarrega_claus/totes_01.jsp).

- 4.1.4.1 Per inserir les notes a la signatura de correu, serà necessari realitzar les següents passes.

- 4.1.4.1.1 Per configurar la signatura de correu per utilitzar-la amb l'eina Microsoft Windows Mail, s'ha d'obrir l'aplicació, accedir al menú "Eines" (pas 1) i fer clic a "Opcions..." (pas 2). A continuació s'obrirà el quadre "Opcions" (pas 3) tal i com es pot veure a la figura 15.

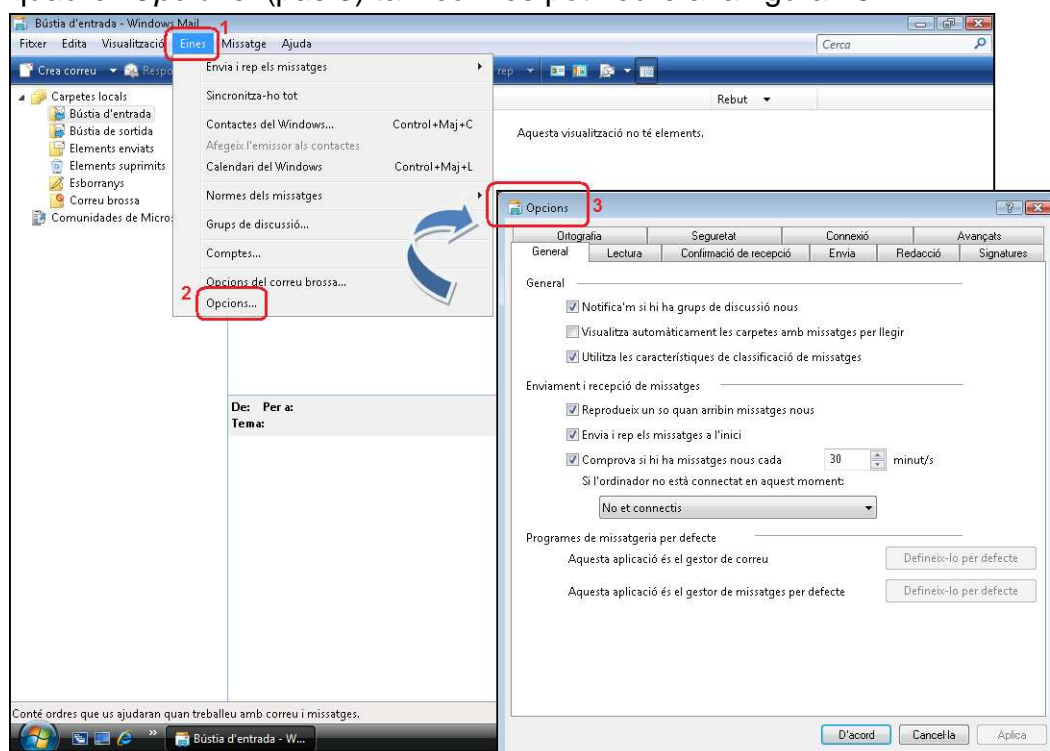


Figura 15. Opcions de correu



4.1.4.1.2 Un cop a les “Opcions” de correu. Cal fer clic a la fitxa “Signatures...” (pas 1 de la figura 16) on podrem configurar una signatura per l’enviament de correu.

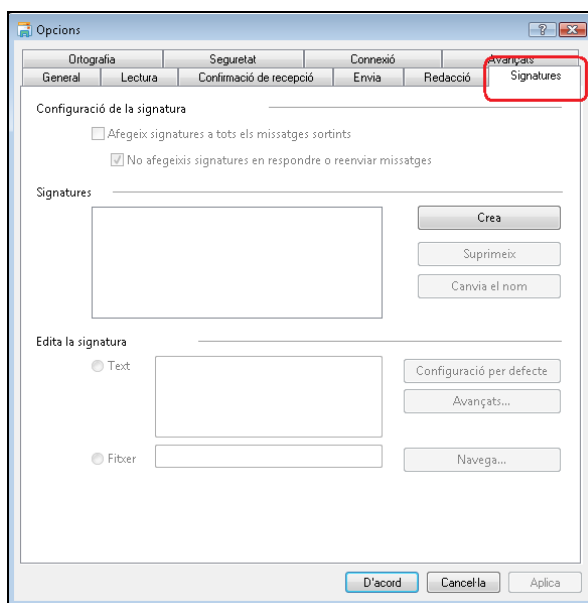


Figura 16. Opcions de format de correu

4.1.4.1.3 Un cop a la fitxa “Signatures”, cal fer clic al botó “Crea” (pas 1 de la figura 27) per generar una nova signatura (Signatura#1). Això habilita l’apartat “Edita la signatura” remarcat a la figura 17, permetent incorporar la signatura recomanada a l’apartat 4.1.4. A continuació cal fer clic a la opció “Afegeix signatures a tots els missatges sortints” (pas 2 de la figura 17) perquè sigui utilitzada en l’enviament de correus.

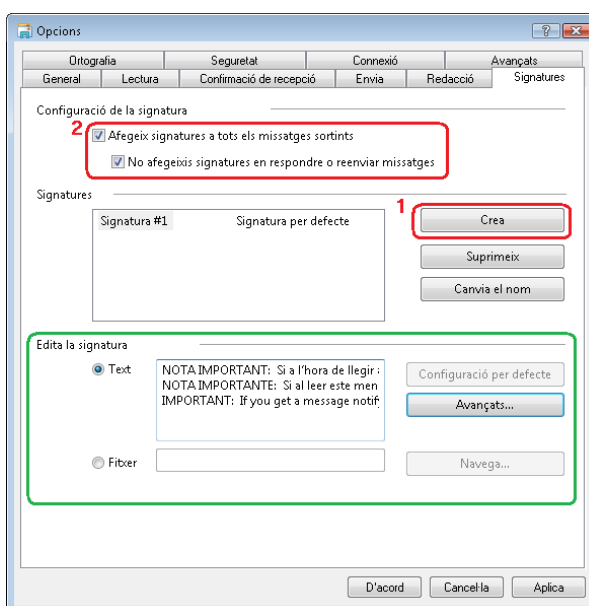


Figura 17. Opcions de format de correu

## 4.2 Xifrats

Un missatge xifrat amb la clau pública d'un receptor no pot ser desxifrat per ningú tret del receptor que posseeix la clau privada corresponent. Això s'utilitza per assegurar la confidencialitat.

La opció per defecte es l'enviament de tots el missatges de correu sense xifrar. Si es vol fer ús de l'enviament de correu xifrat s'han de seguir les següent passes.

4.2.1 Un cop s'està editant un missatge nou i abans d'enviar-lo fer clic al botó

“Xifra el missatge”  tal i com es pot veure a la figura 18.

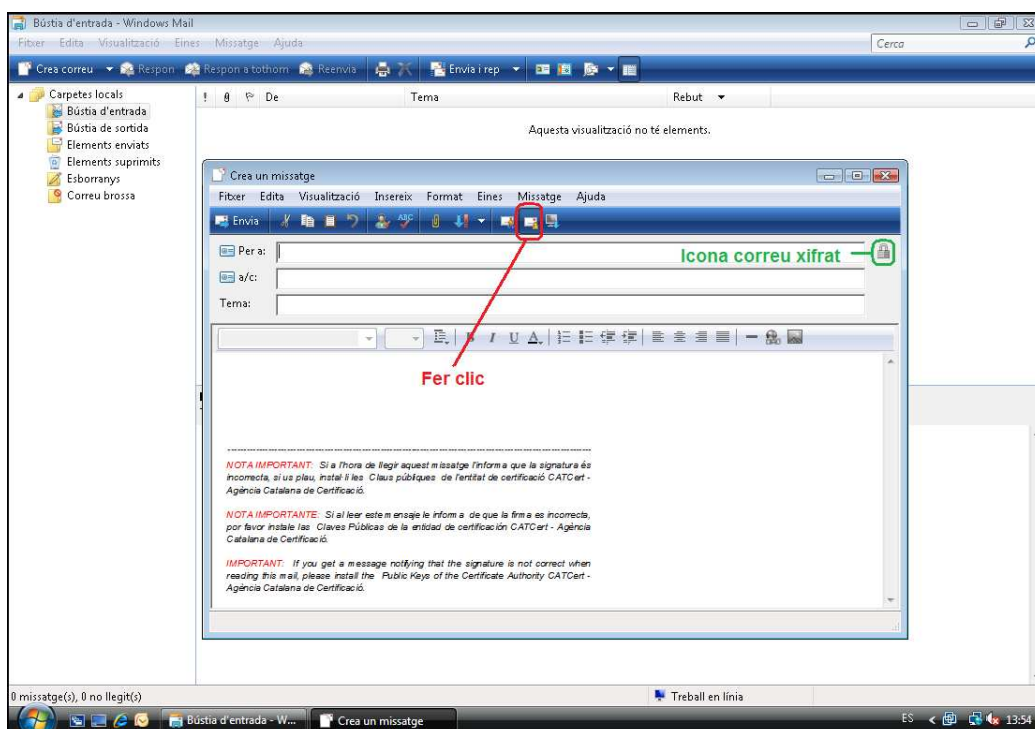


Figura 18. Enviament de correus xifrats

4.2.2 Prémer “*Envia*” i s’enviarà el correu xifrat. En cas de no disposar de la clau pública del destinatari per xifrar el missatge apareixerà el quadre de diàleg de la figura 19.

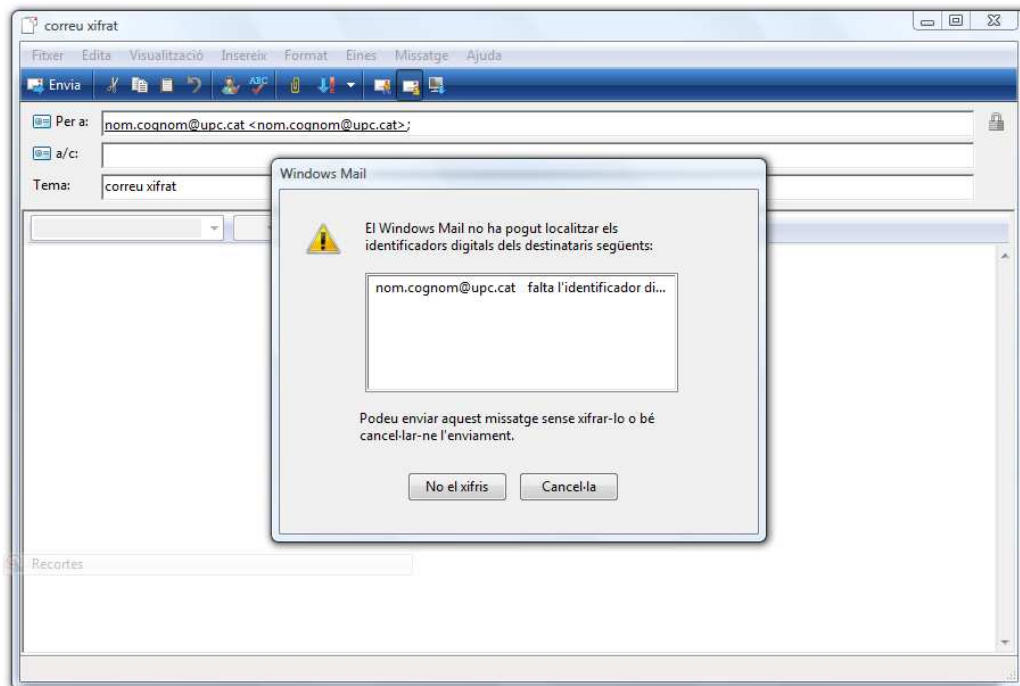



Figura 19. Problemes de xifratge.

Per solucionar aquesta situació s’ha d’obtenir la clau pública del certificat que utilitza el destinatari en el seu correu.

Per fer-ho, serà necessari que rebem un correu signat del destinatari al que volem enviar el correu xifrat. Un cop rebem aquest correu signat, el client de correu Microsoft Windows Mail tindrà disponible de forma automàtica la clau pública del certificat per utilitzar-la en l’enviament de correu xifrat a aquest destinatari.

## 5 Recepció de missatges

### 5.1 Signats

En el cas de rebre missatges signats digitalment, es poden reconèixer per la icona  que surt a l'esquerra del correu electrònic rebut i el missatge “Ajuda de seguretat Missatge signat digitalment” que apareix al panell de lectura (figura 20).

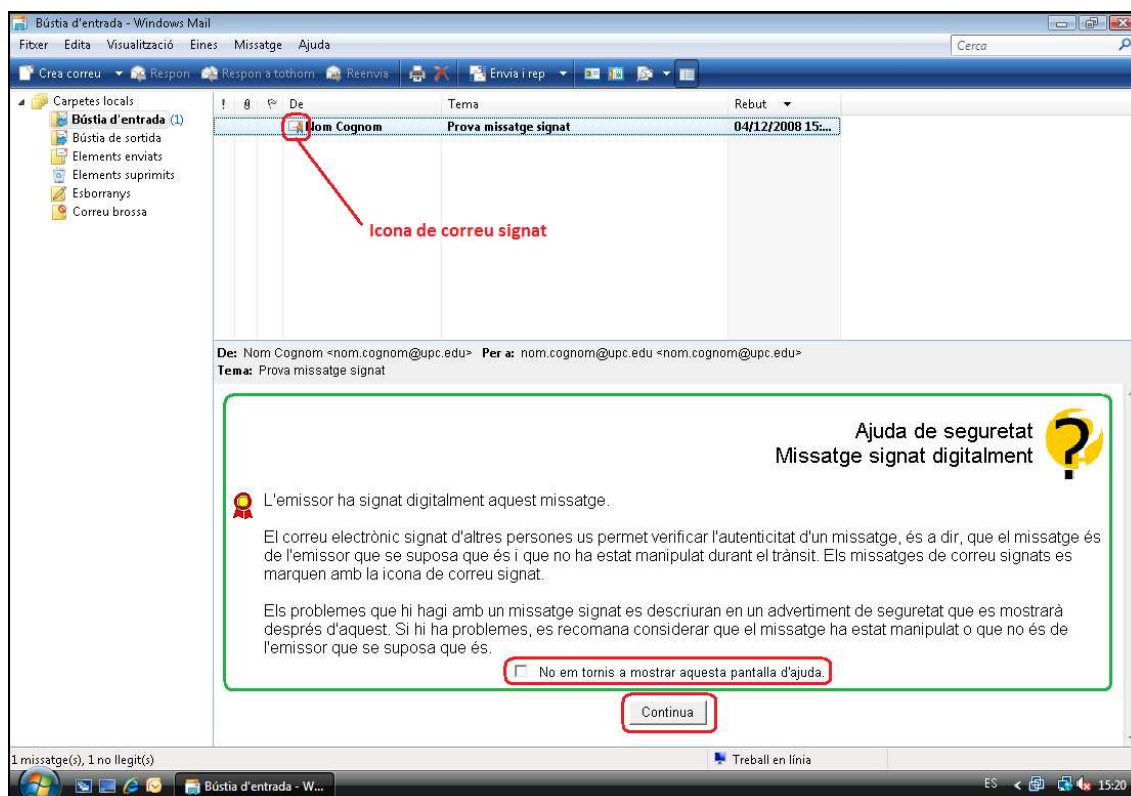



Figura 20. Recepció de correu electrònic signat

Fent clic al botó “Continua” (figura 20) o fent doble clic sobre el nou missatge rebut, podem trobar-nos dos situacions.

### 5.1.1 Recepció de missatges signats amb les claus públiques de l'emissor instal·lades.

Al seleccionar el missatge, es pot veure a la dreta de la pantalla la icona  que indica que el correu està signat correctament (figura 21).

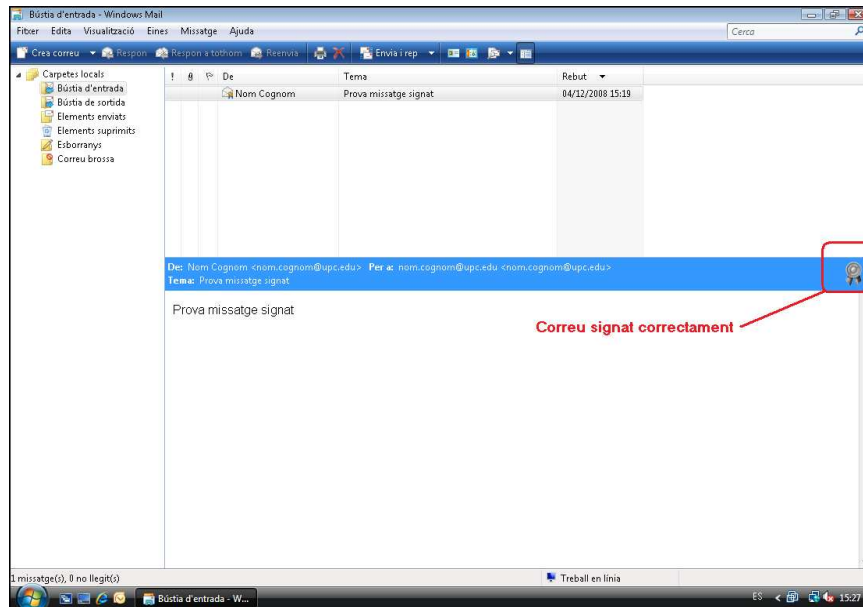


Figura 21. Correu electrònic signat correctament

Per veure les propietats de la signatura del missatge electrònic rebut, s'ha de fer clic sobre la icona remarcada a la figura 21.

A continuació, s'obre la finestra de propietats del missatge on s'ha de fer clic a fitxa "Seguretat" (pas 1 de la figura 22) i fer clic al botó "Visualitza els certificats..." (pas 2 de la figura 22) on s'obrirà el quadre de diàleg "Visualitza els certificats" (pas 3 de la figura 22). Aquí podrem veure el certificat de signatura fent clic al botó "Certificat de signatura..." (pas 4 de la figura 22).

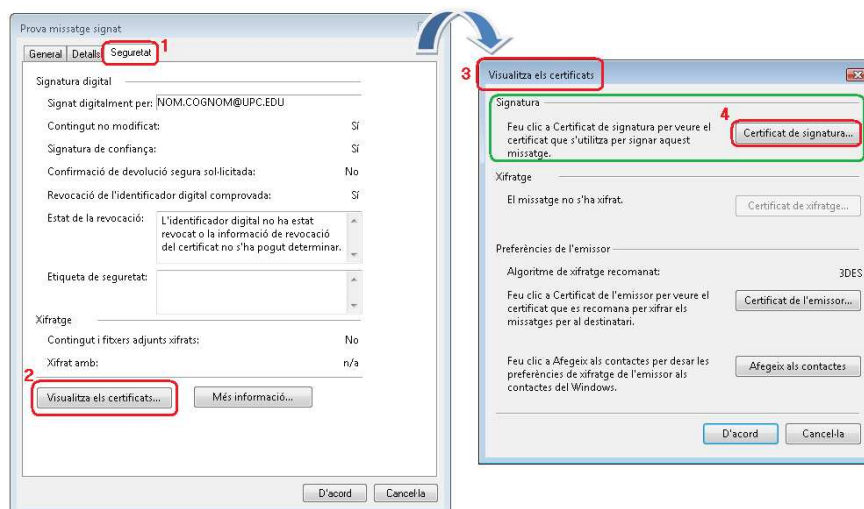


Figura 22. Visualitzar les propietats de la signatura digital

Al fer clic al botó “Certificat de signatura...” s’obre la finestra “Propietats de l’identificador digital de la signatura” (figura 23). Aquí es pot veure les dades del certificat de signatura.

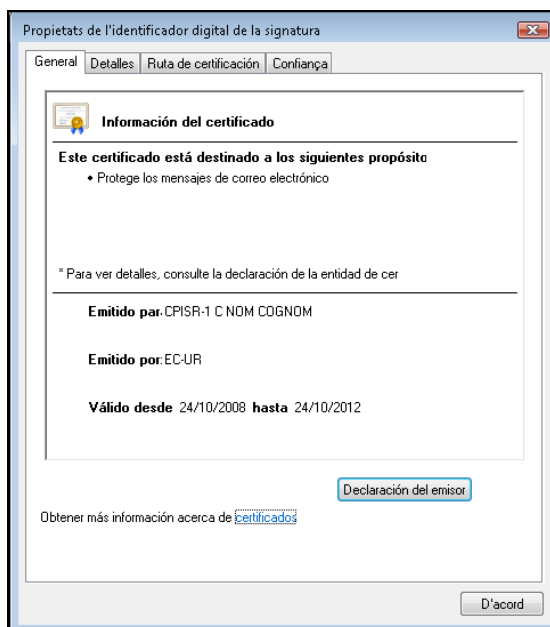


Figura 23. Propietats de la signatura digital

### 5.1.2 Recepció de missatges signats amb les claus públiques de l'emissor NO instal·lades.

Quan intentem llegir un missatge electrònic signat digitalment i no tenim instal·lades les claus públiques de l'entitat de certificació del certificat utilitzat per la persona que ens envia el missatge signat, apareix el l'advertiment de seguretat de la figura 26.

El missatge es pot llegir igualment fent clic al botó “*Obre el missatge*” (opció remarcada a la figura 24).

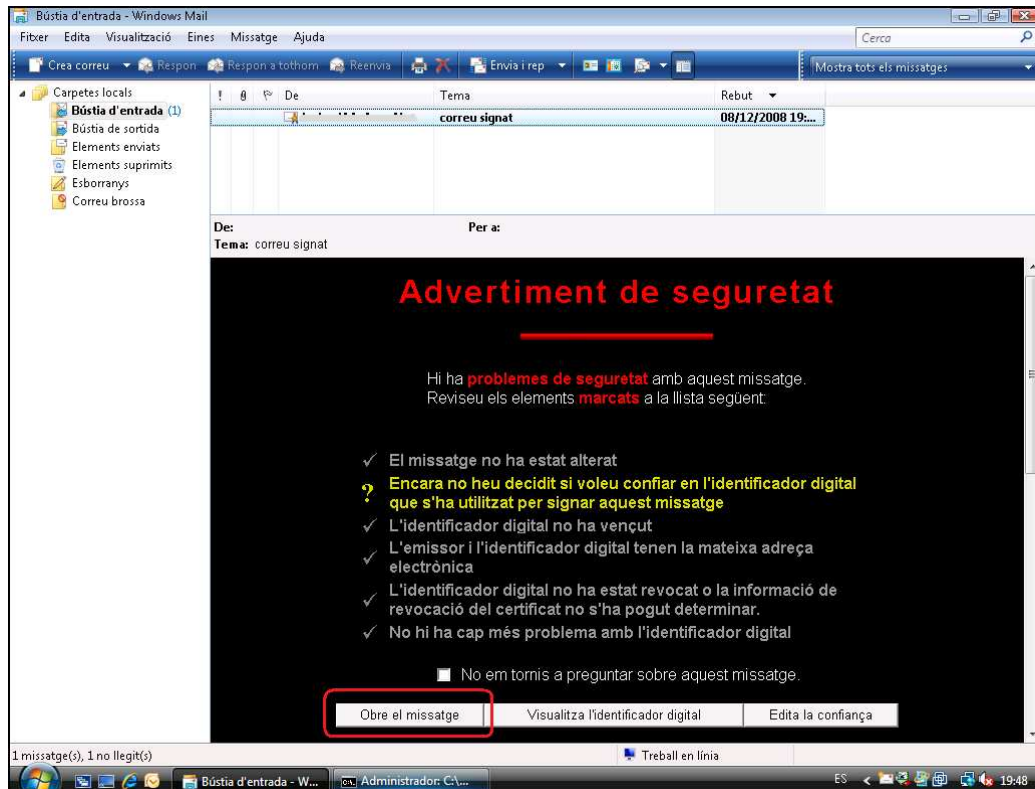



Figura 24. Recepció de missatges amb signatura no vàlida

## 5.2 Xifrats

En el cas de rebre missatges xifrats, es poden reconèixer per la icona  que surt a l'esquerra del correu electrònic rebut i el missatge “Ajuda de seguretat Missatge xifrat” que apareix al panell de lectura (figura 25).

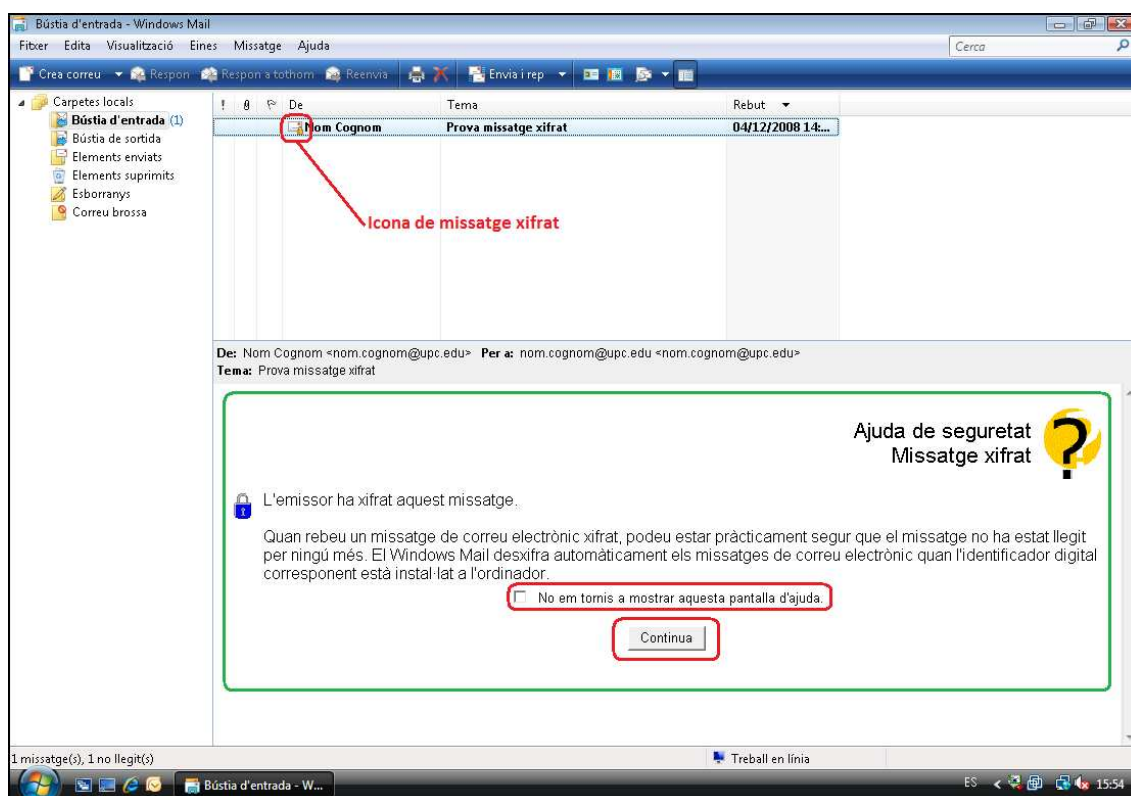



Figura 25. Recepció de missatge xifrat

Si nosaltres som la persona a la que anava destinat aquest correu, en fer clic a botó “Continua”, es podrà obrir i llegir sense cap problema.

A la part dreta del correu es podrà veure la icona d'un cadenet  que ens indica que el correu està xifrat. Fent clic sobre aquesta icona (pas 1 de la figura 26), s'obre la fitxa “Seguretat” de la finestra Propietats del missatge (pas 2 de la figura 26). A continuació, fent clic al botó “Visualitza els certificats...” (pas 3 de la figura 26) s'obrirà el quadre de diàleg “Visualitza els certificats” (pas 4 de la figura 26) on podrem veure el certificat de xifratge fent clic al botó “Certificat de xifratge...” (pas 5 de la figura 26).



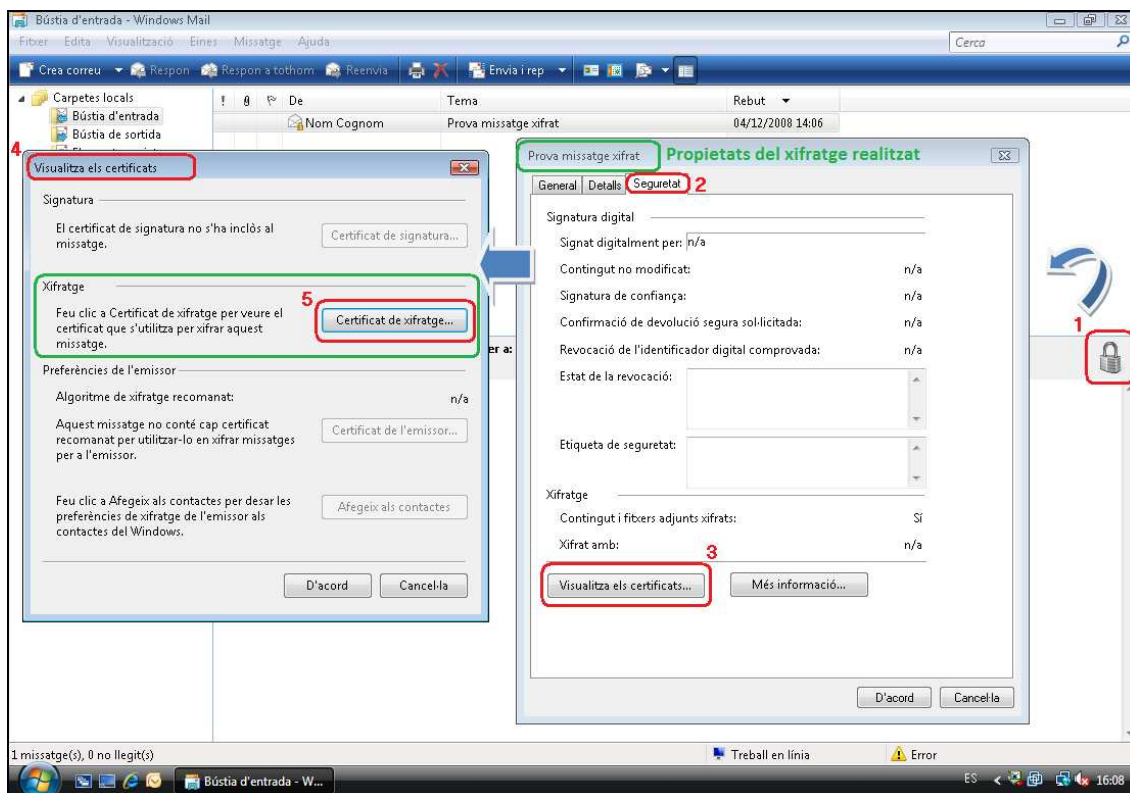


Figura 26. Recepció de missatge xifrat

Al fer clic al botó “Certificat de xifratge...” s’obre la finestra “Propietats de l’identificador digital de la signatura” (figura 27). Aquí es pot veure les dades del certificat de xifratge.

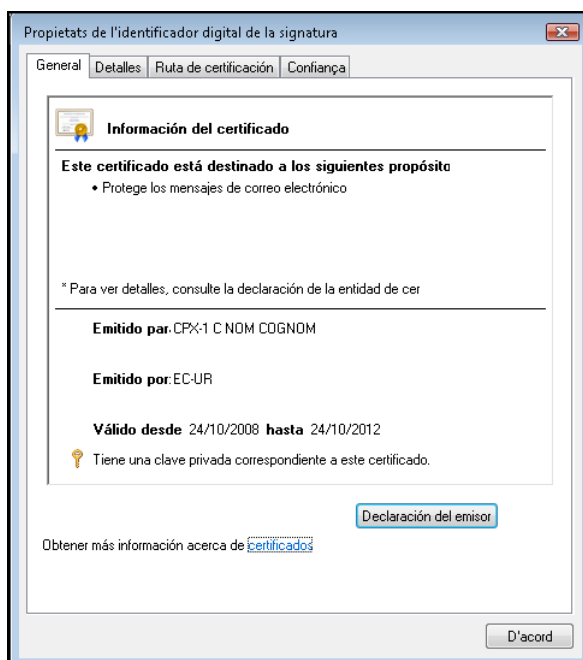


Figura 27. Recepció de missatge xifrat

## 6 **Referències**

- Informació sobre què és un certificat

[http://www.catcert.cat/web/cat/0\\_0\\_0\\_0\\_quees.jsp](http://www.catcert.cat/web/cat/0_0_0_0_quees.jsp)

- Preguntes freqüents sobre el funcionament dels certificats

[http://www.catcert.cat/web/cat/0\\_0\\_1\\_preguntes.jsp](http://www.catcert.cat/web/cat/0_0_1_preguntes.jsp)

- Web de l' Identitat digital UPC

<https://www.upc.edu/identitatdigital/>

- Espai de preguntes i respostes més freqüents de l' Identitat digital UPC

<https://www.upc.edu/identitatdigital/altres>