UNIVERSITAT POLITÈCNICA DE CATALUNYA	**INFORMACIÓ GENERAL**
PROJECTE: Manuals d'ús de signatura electrònica	Versió: 2.0
TÍTOL: Signatura electrònica amb MS Outlook 2003 i MS Windows XP	Codi Referència:
RESUM:	Data Publicació: 10/10/2008

PROCEDIMENT

Signatura electrònica amb MS Outlook 2003 i MS Windows XP

PREPARAT PER:	REVISAT PER:	APROVAT PER:
Nom:	Nom:	Nom:
Data: 18/09/2008	Data:	Data:

UNIVERSITAT POLITÈCNICA DE CATALUNYA	**INFORMACIÓ GENERAL**
PROJECTE: Manuals d'ús de signatura electrònica	Versió: 2.0
TÍTOL: Signatura electrònica amb MS Outlook 2003 i MS Windows XP	Codi Referència:
RESUM:	Data Publicació: 10/10/2008

Versió	Parts que canvien	Descripció del canvi	Data del canvi
1.0	Tot	Creació del document	18/09/08
1.1	Tot	Divisió de procediment i incorporació d'imatges	30/09/08
1.2	Enviament i recepció de missatges	Incorporació de xifrat	17/10/08
1.3	Tot	Incorporació d'imatges i referències	12/11/08
1.4	Enviament i recepció de missatges	Modificacions per revisió	21/11/08
1.5	Prerequisits	Incorporació dels prerequisits	22/12/08
1.6	Configuració signatura correu	Configuració signatura correu	30/12/08
1.7	Certificats CRL i OCSP	Certificats CRL i OCSP	16/01/08
1.8	Recuperar clau pública xifratge correu	Recuperar clau pública xifratge correu	16/01/08
1.9	Tot	Revisió	19/01/09
2.0	Apartat 3.7	Justificat de l'apartat 3.7	23/01/09

ÍNDEX

1 Objectiu i abast

El present document descriu el procés de configuració del client de correu electrònic Microsoft Outlook 2003 instal·lat al sistema operatiu Microsoft Windows XP 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. 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

- 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

3 Configuració de signatura electrònica amb MS Outlook 2003 i Windows XP

3.1 Per configurar la signatura electrònica per utilitzar-la amb l'eina Microsoft Outlook 2003, 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 1.

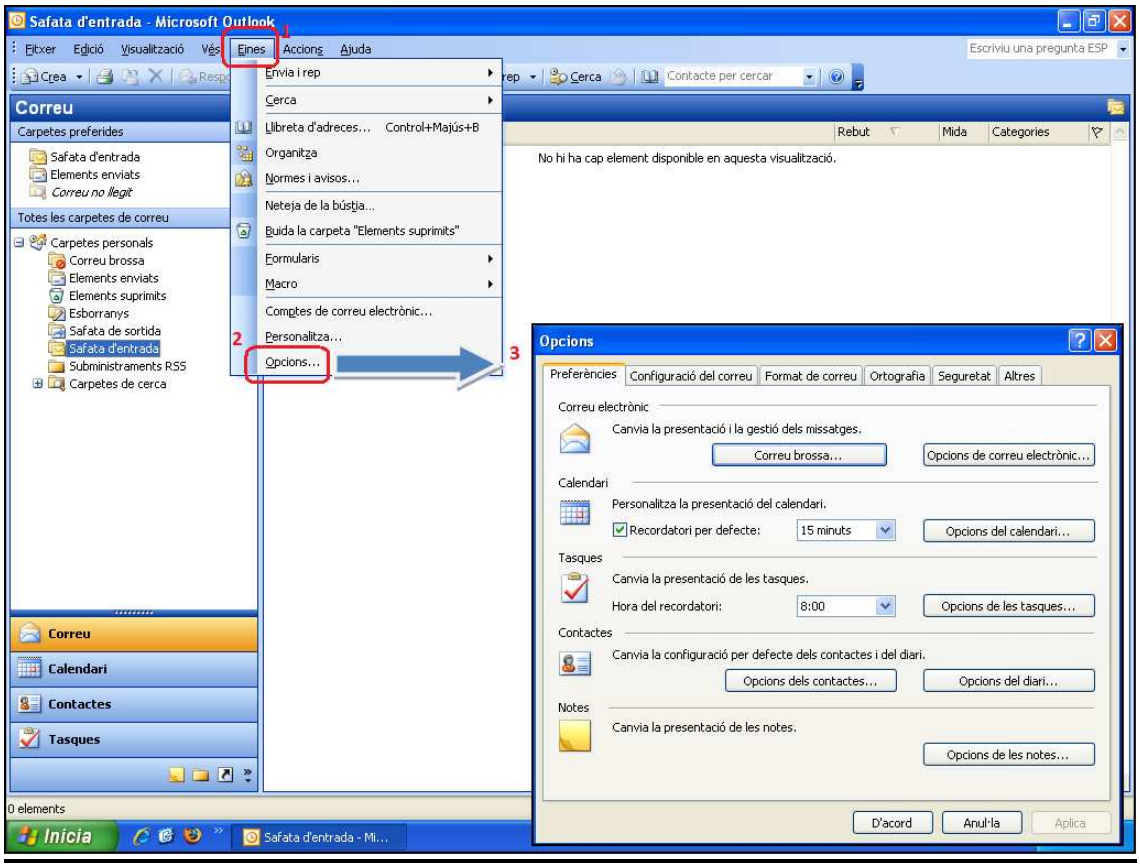

Figura 1. Finestra de l'eina MS Outlook 2003

3.2 Un cop obert el quadre *"Opcions"* s'ha de fer clic a la pestanya *"Seguretat"* (pas 1) i a continuació al botó "*Configuració...*" (pas 2) dins l'apartat "*Correu electrònic xifrat*" (figura 2) per tal de configurar el vostre correu electrònic i poder signar els correus mitjançant el certificat digital emmagatzemat al carnet universitari.

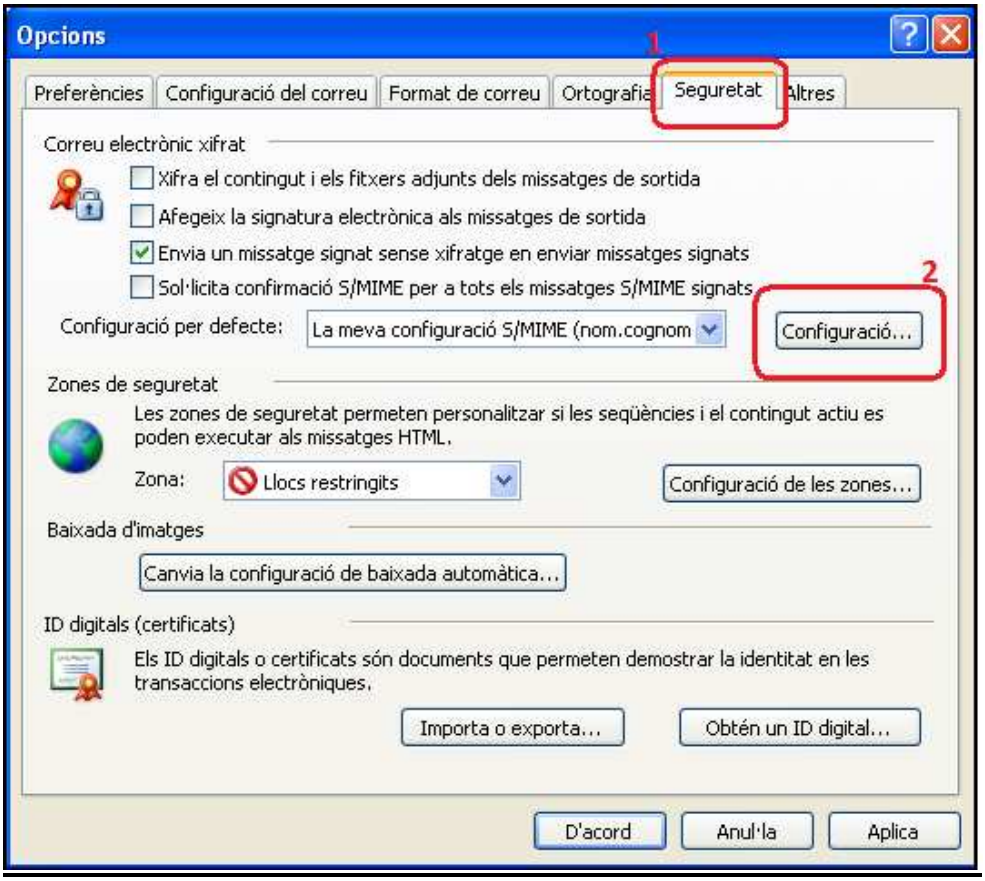

Figura 2. Opcions de seguretat

3.3 Al fer clic al botó "*Configuració…*" s'obre el quadre "*Canvi de la configuració de seguretat*" (figura 3) on es podrà veure si ja existeix alguna configuració de seguretat. Si apareixen buides les dades del quadre de la figura 3, significa que no s'ha definit cap configuració de seguretat i s'haurà de continuar en el punt 3.3.1.

Si aquestes dades no apareixen buides, com per exemple a la figura 4, vol dir que ja existeix una configuració de seguretat i que s'haurà d'afegir una nova, continuarem llavors en el punt 3.3.2.

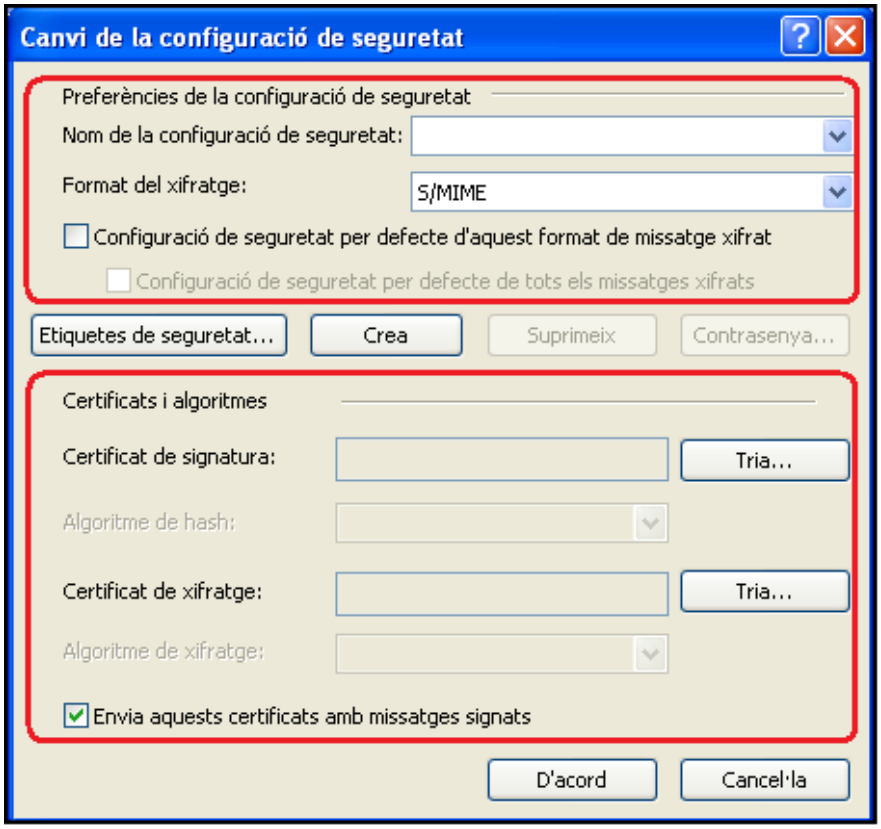

Figura 3. Configuració de seguretat no definida

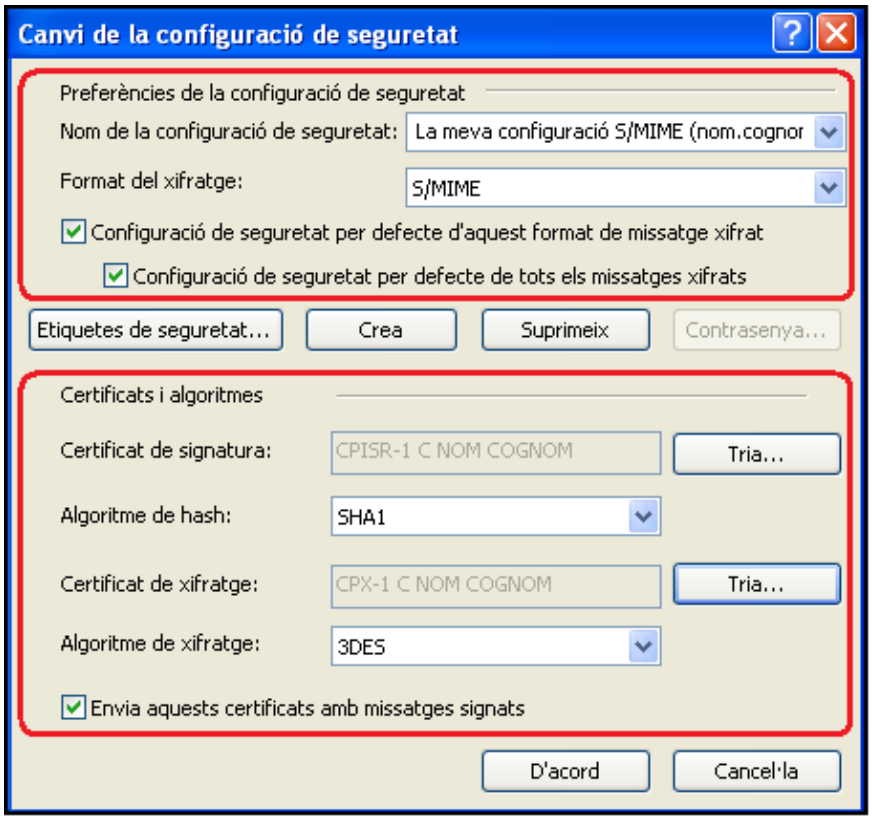

Figura 4. Configuració de seguretat definida

3.3.1 S'ha de definir una nova configuració de seguretat.

3.3.1.1 En aquest cas, s'ha de fer la configuració de seguretat afegint al camp "*Nom de la configuració de seguretat*" una descripció que la permeti reconèixer fàcilment, com per exemple "*Configuració UPC*" (pas 1 de la figura 5).

3.3.1.2 El pas següent es fer clic al botó "*Tria*" de la casella "*Certificat de signatura*" (pas 2 de la figura 5).

3.3.1.3 Un cop s'ha fet clic al botó "*Tria*", s'obra el quadre de selecció de certificat (pas 3 de la figura 5). En aquest moment s'ha de seleccionar el certificat propi i acceptar per confirmar la selecció (pas 4 de la figura 5).

3.3.1.4 El pas següent es fer clic al botó "*Tria*" de la casella "*Certificat de xifratge*" (pas 5 de la figura 5).

3.3.1.5 Un cop s'ha fet clic al botó "*Tria*", s'obra el quadre de selecció de certificat (pas 6 de la figura 5). En aquest moment s'ha de seleccionar el certificat propi i acceptar per confirmar la selecció (pas 7 de la figura 5).

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 a la nostra web.

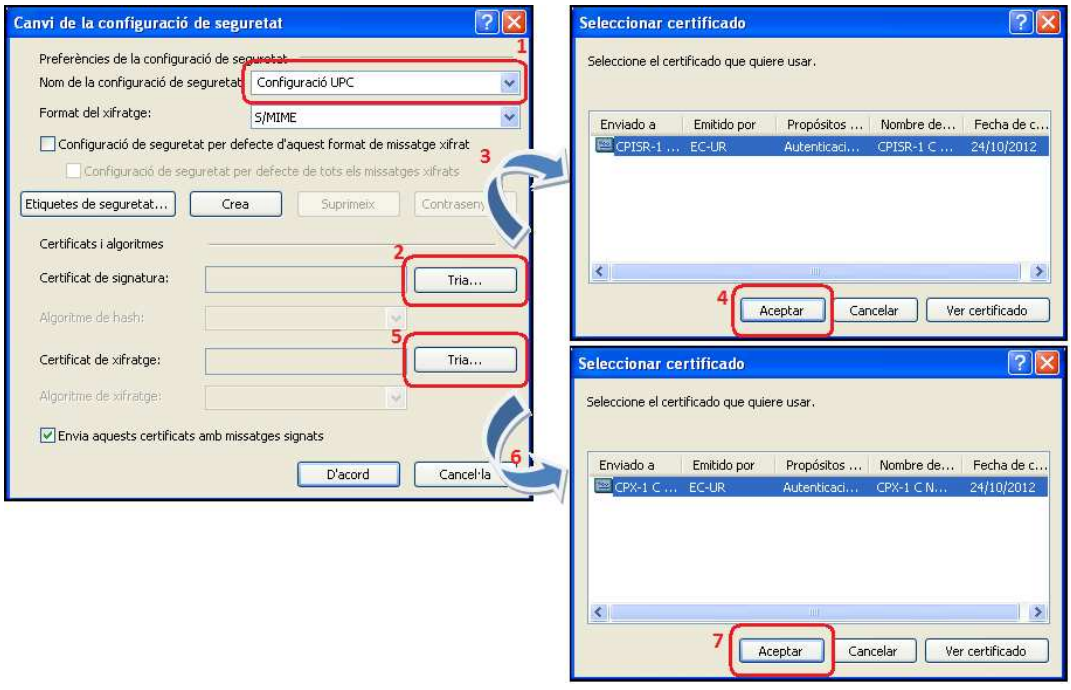

Figura 5. Nova configuració de seguretat

3.3.1.6 Un cop feta la selecció anterior a d'aparèixer el quadre "*Canvi de la configuració de seguretat*" (figura 6) omplert automàticament amb les dades del certificat als camps *"Certificat de signatura"* i *"Certificat de xifrat",* tal com es pot veure a la figura 6. Fent clic al botó "*D'acord*" s'acceptaran els canvis tornant a la pestanya de seguretat de la finestra de configuració. Un cop aquí es podrà continuar la configuració al punt 3.4 d'aquest document.

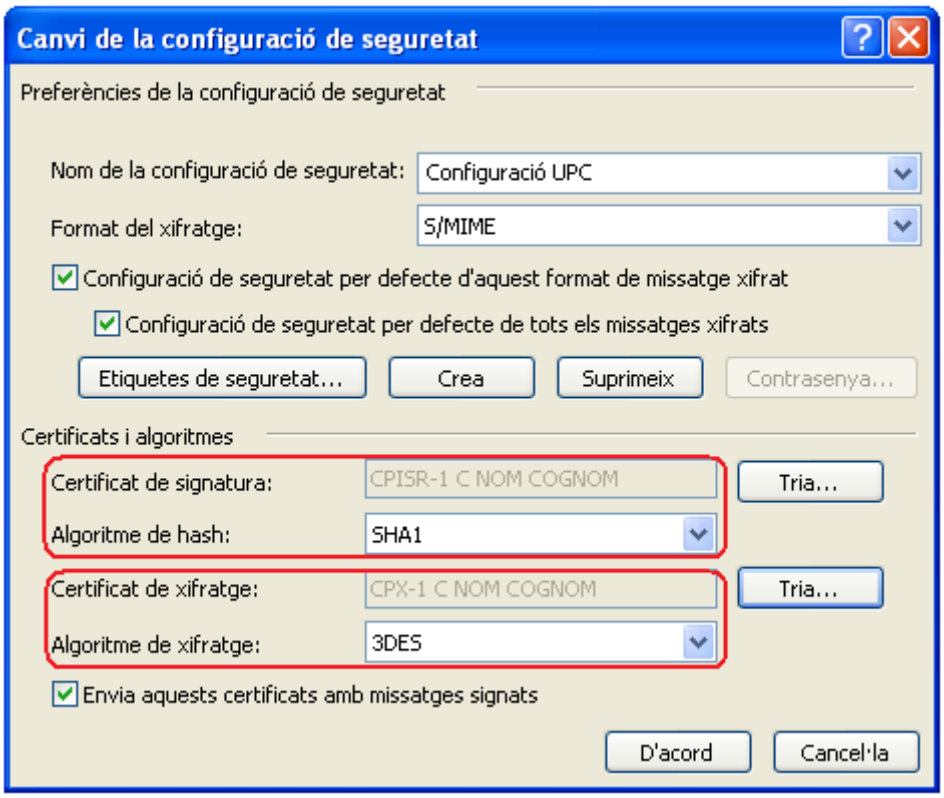

Figura 6. Quadre canvi de la configuració de seguretat omplert

3.3.2 Ja existeix una configuració de seguretat.

3.3.2.1 S'ha de fer clic al botó "*Crea*" (pas 1 de la figura 7) fent que aparegui la possibilitat d'afegir una nova configuració de seguretat (pas 2 de la figura 7). A partir d'aquí es el mateix cas de no tenir cap configuració de seguretat feta i voler crear una nova *(revisar del punt 3.3.1.1 al punt 3.3.1.6)*.

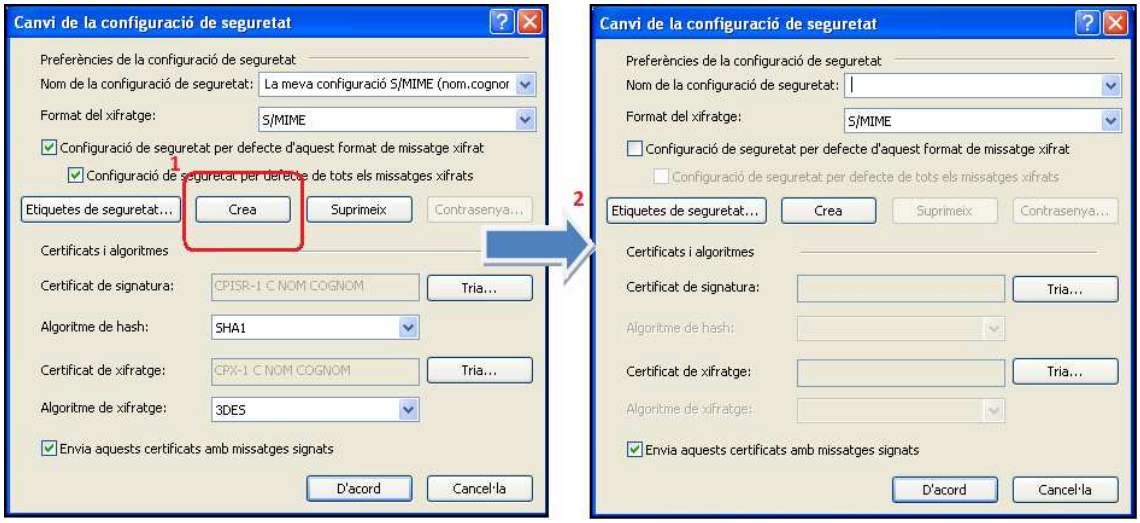

Figura 7. Nova configuració de seguretat

3.4 Un cop creada la configuració de seguretat per utilitzar el certificat emmagatzemat al carnet universitari, tornarem a la pestanya de seguretat de la finestra de configuració (figura 8). Seleccionant l'opció *"Afegeix la signatura electrònica als missatges de sortida"*, activarem la signatura digital per defecte en TOTS els missatges de correu electrònic que envieu mitjançant MS Outlook 2003 (pas 1 de la figura 8).

3.5 Fent clic al botó "*D'acord*" (pas 2 de la figura 8) l'aplicació MS Office 2003 restarà configurada per signar digitalment els missatges de correu electrònic.

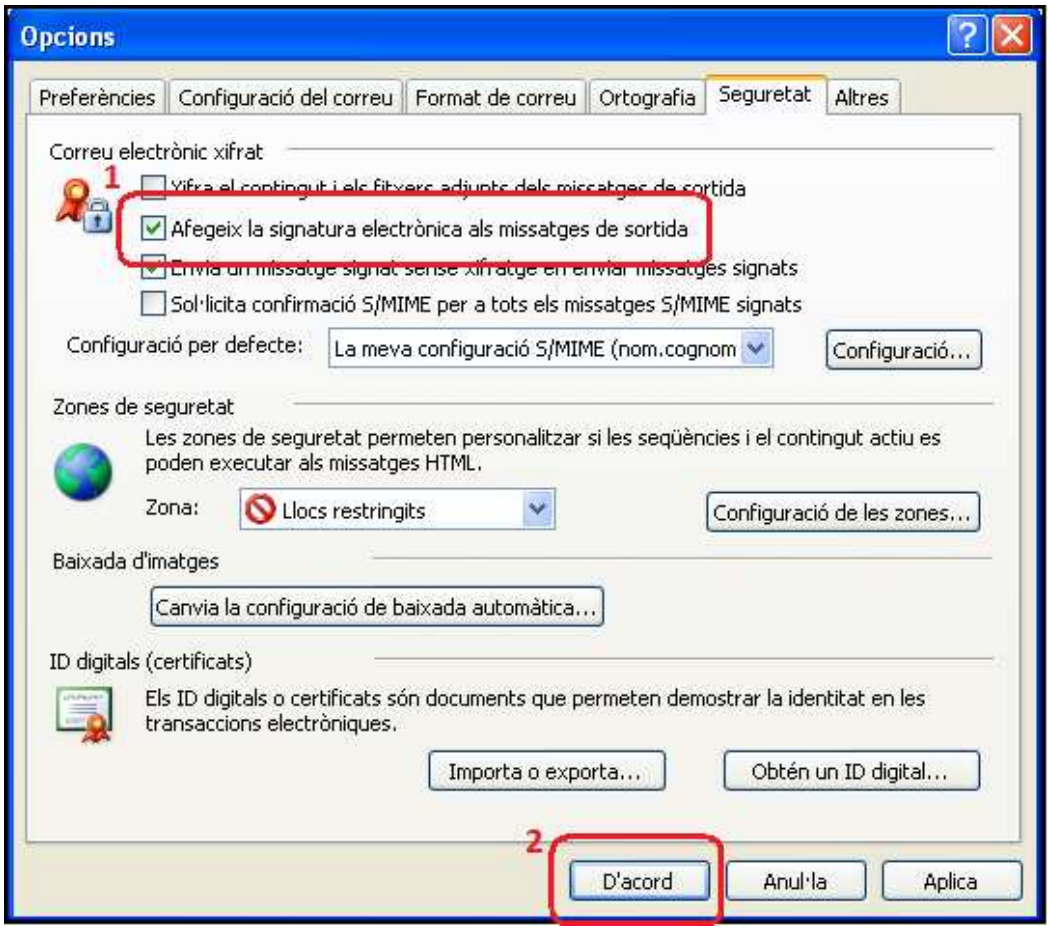

Figura 8. Ús de la signatura digital pels missatges de sortida

3.6 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.

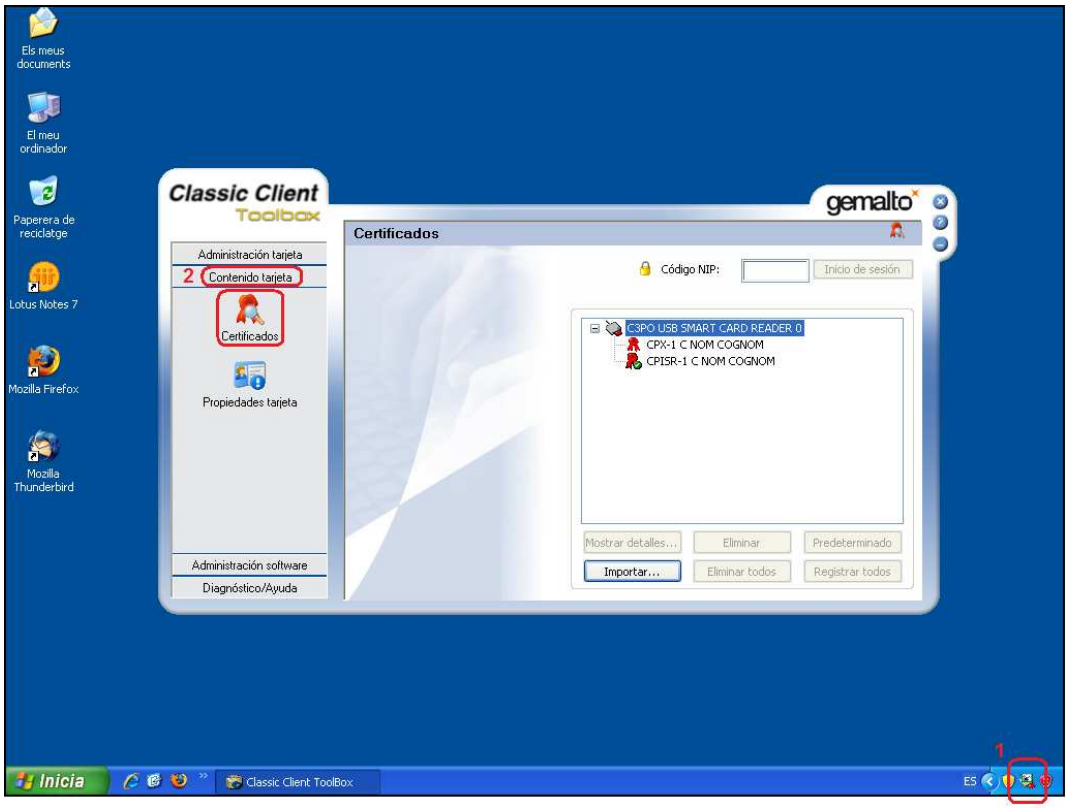

Figura 9. Propietats del certificat gemalto

3.7 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.

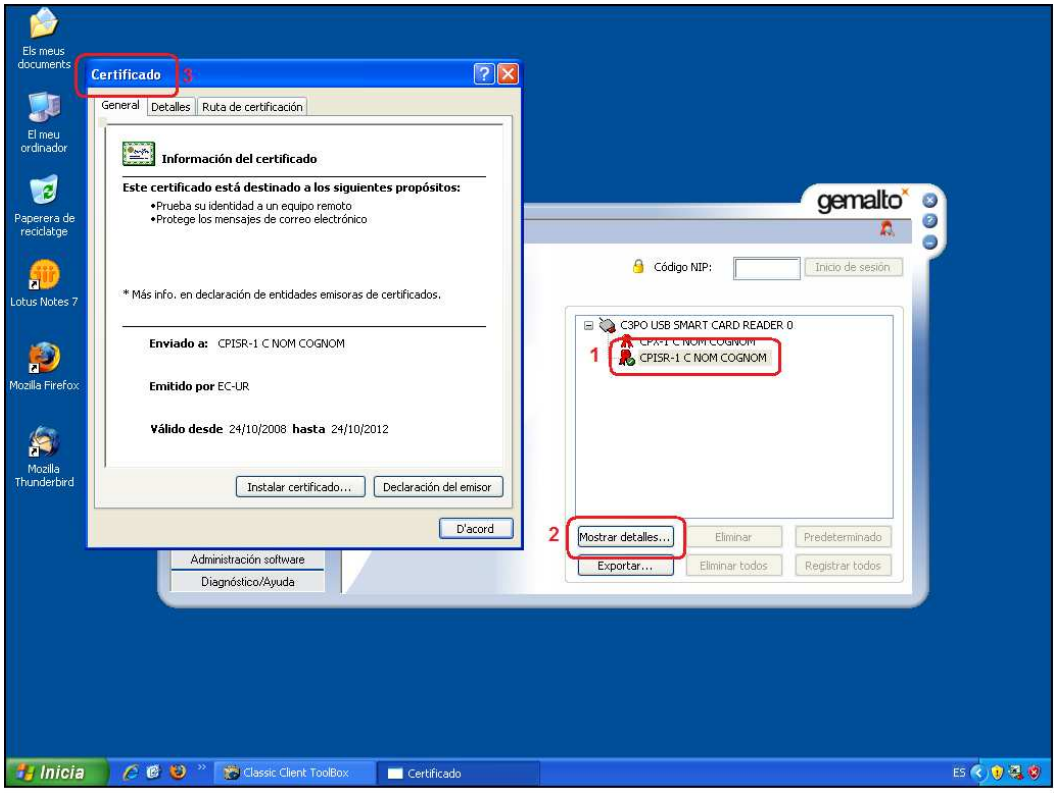

Figura 10. Propietats del certificat

3.8 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.

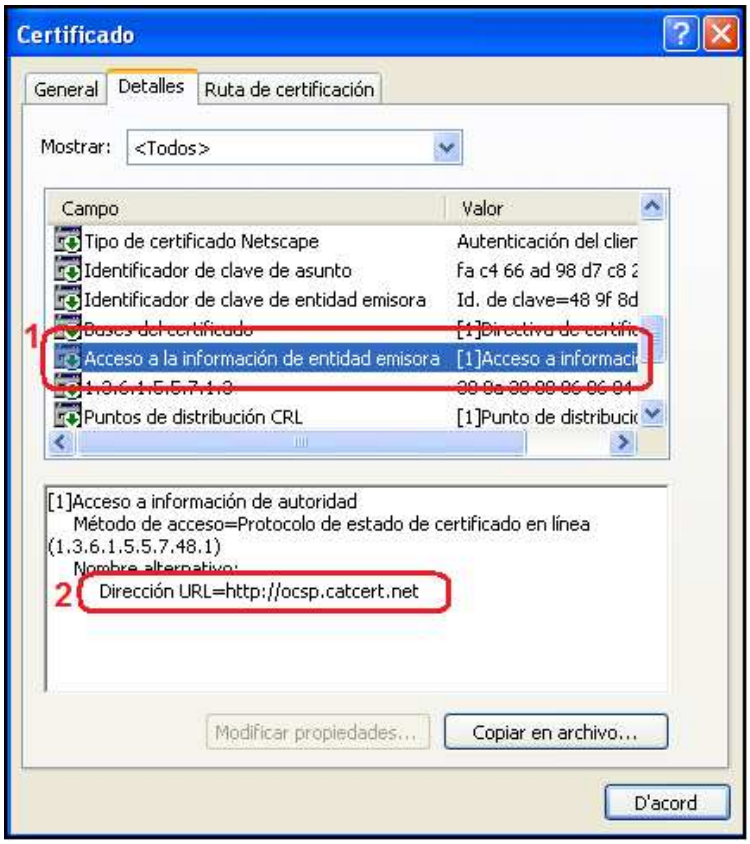

Figura 11. Propietats del certificat.

- *"Puntos de distribución CRL"* (pas 1) on ens indica les direccions url http://epscd.catcert.net/crl/ec-ur.crl i http://epscd2.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.

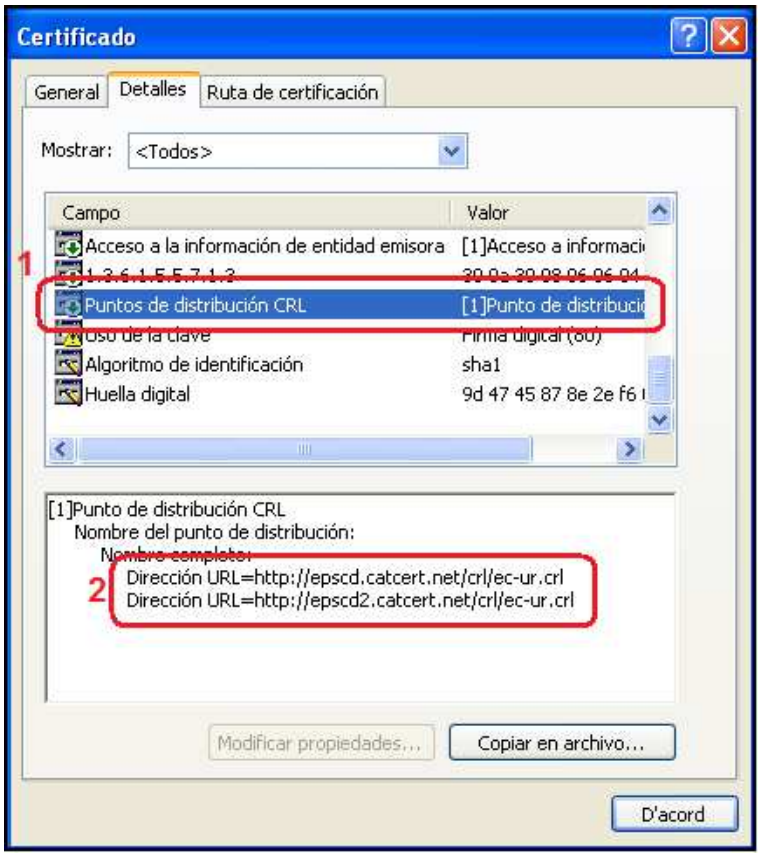

Figura 12. Propietats del certificat.

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 la 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 el missatges de correu de sortida com a opció per defecte (veure punts 3.4 i 3.5 de l'apartat anterior) i voler fer us 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.

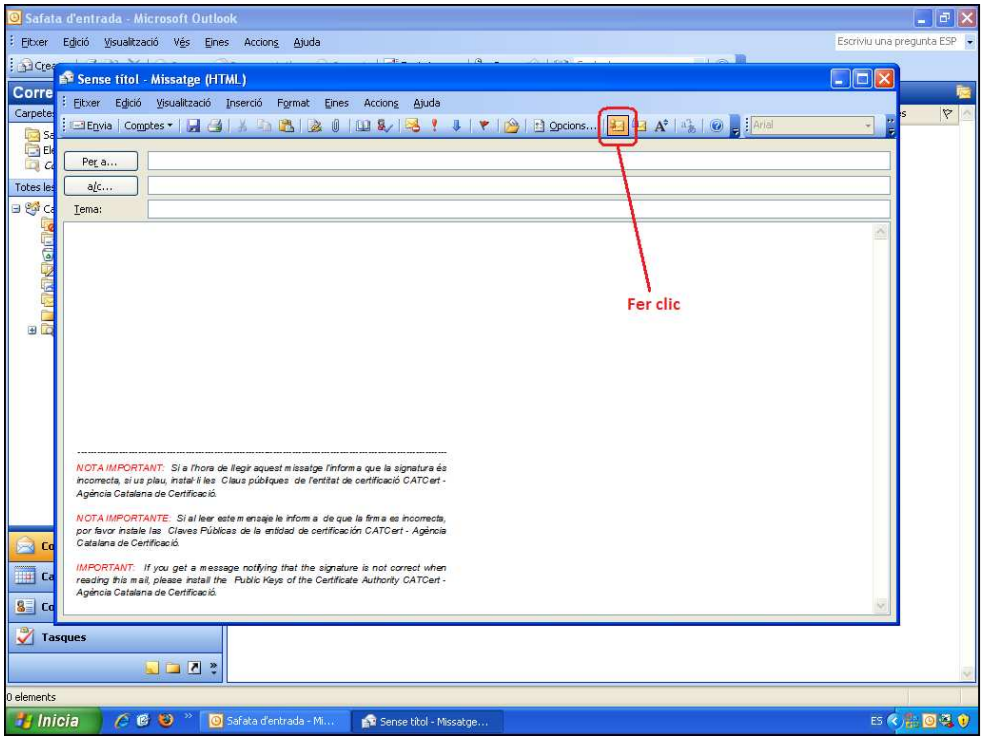

Figura 13. Activar l'enviament de correus signats

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).

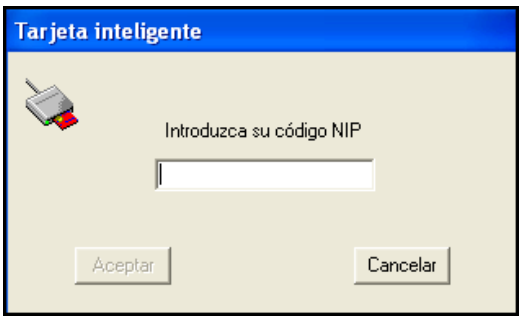

Figura 14. Quadre de diàleg d'introducció del PIN

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

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 indican que el certificat no es vàlid. Per solucionar-ho, podeu consultar l'apartat de suport a la nostra web o seguint els pasos de la nostra guia básica 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.
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 podrá encontrar en la dirección web 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.

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 Outlook 2003, 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.

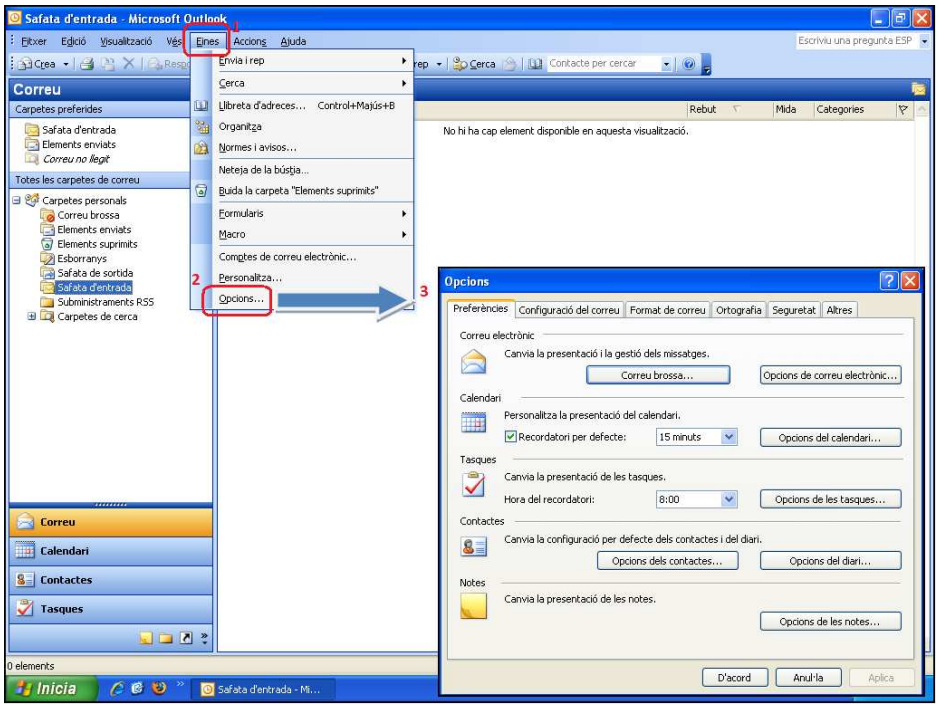

Figura 15. Opcions de correu

4.1.4.1.2 Un cop a les *"Opcions"* de correu. Cal seleccionar la fitxa *"Format de correu"* (pas 1) i seleccionar l'opció *"Signatures..."* (pas 2) tal i com es pot apreciar a la figura 16.

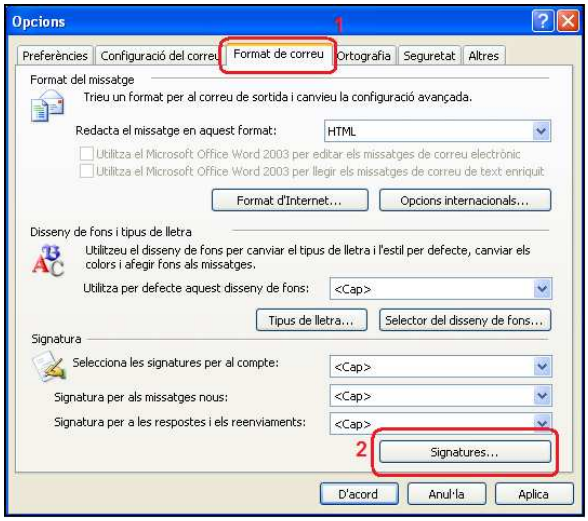

Figura 16. Opcions de format de correu

4.1.4.1.3 Un cop a l'apartat *"Creació de la signatura"* de correu. Cal fer clic al botó *"Crea"* (pas 1) que executarà l'assistent de creació d'una signatura nova (pas 2 de la figura 17).

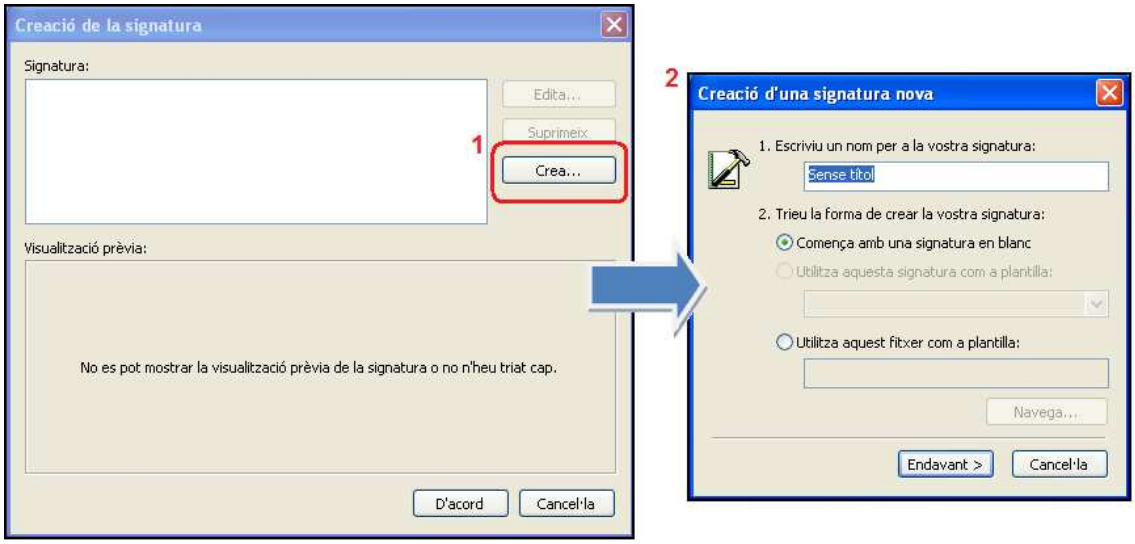

Figura 17. Opcions de format de correu

4.1.4.1.4 Un cop a l'assistent de creació de signatura nova, cal especificar un nom per a la signatura (pas 1 figura 18) i seleccionar *"Endavant >"* (pas 2 figura 18) per poder crear una signatura de correu nova.

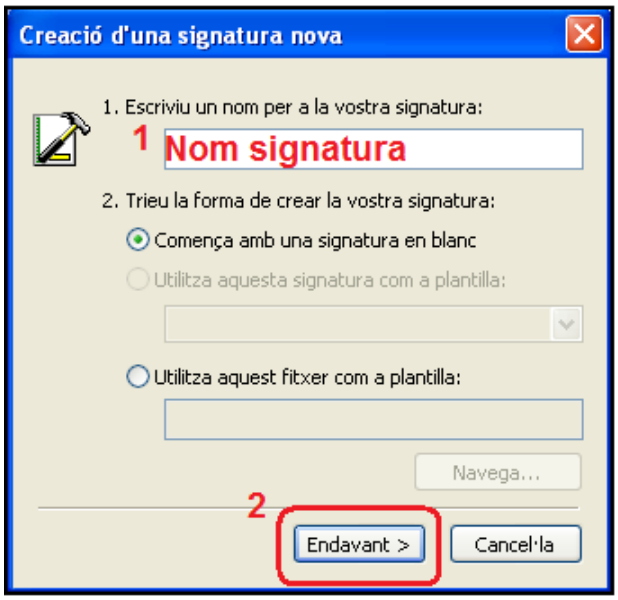

Figura 18. Creació d'una signatura nova

4.1.4.1.5 Cal inserir la signatura recomanada a l'apartat 4.1.5 (pas 1) i fer clic al botó *"D'acord"* (pas 2) per que els canvis es dugin a terme tal i com es pot apreciar a la figura 19.

Figura 19. Edició de la signatura

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 apreciar a la figura 20.

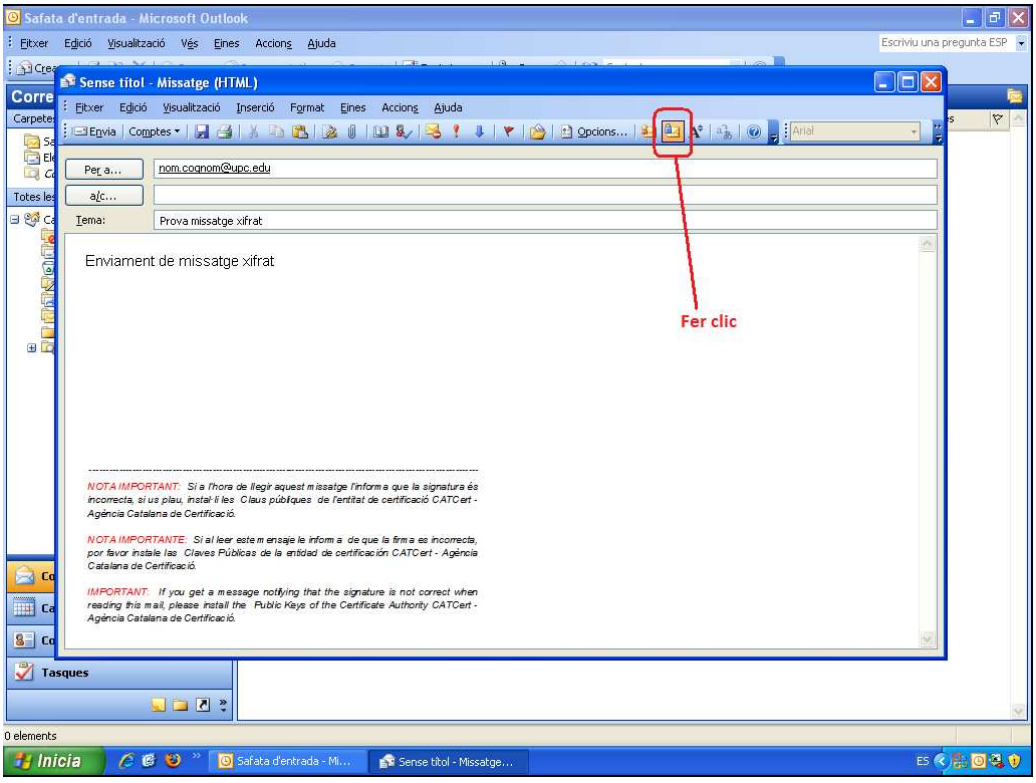

Figura 20. Activar l'enviament de correus xifrats

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 21.

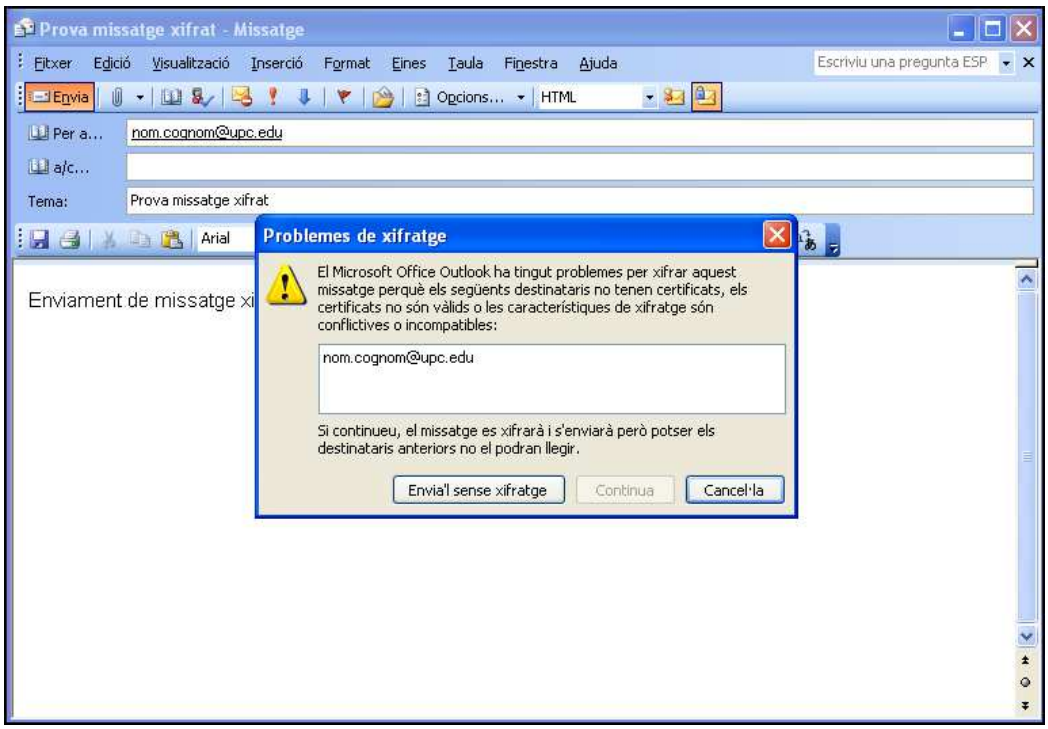

Figura 21. Problemes de xifratge.

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, caldrà obrir-lo i agregar el remitent com a contacte d'Outlook. D'aquesta manera, el client de correu Microsoft Outlook 2003 tindrà disponible de forma automàtica la clau pública del certificat per utilitzar-la en el enviament de correu xifrat a aquest destinatari.

Per agregar el destinatari a la nostra llibreta de contactes, s'ha de seleccionar el nom del destinatari al correu rebut amb el botó dret del ratolí (pas 1 de la figura 22) i fer clic a l´opció *"Afegeix als contactes de l'Outlook"* (pas 2 de la figura 22).

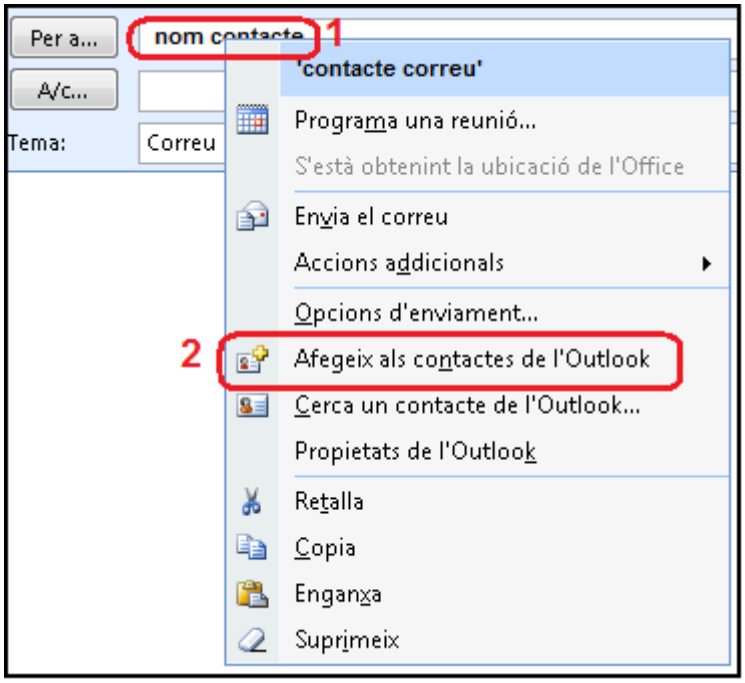

Figura 22. Afegir contacte

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 (figura 23).

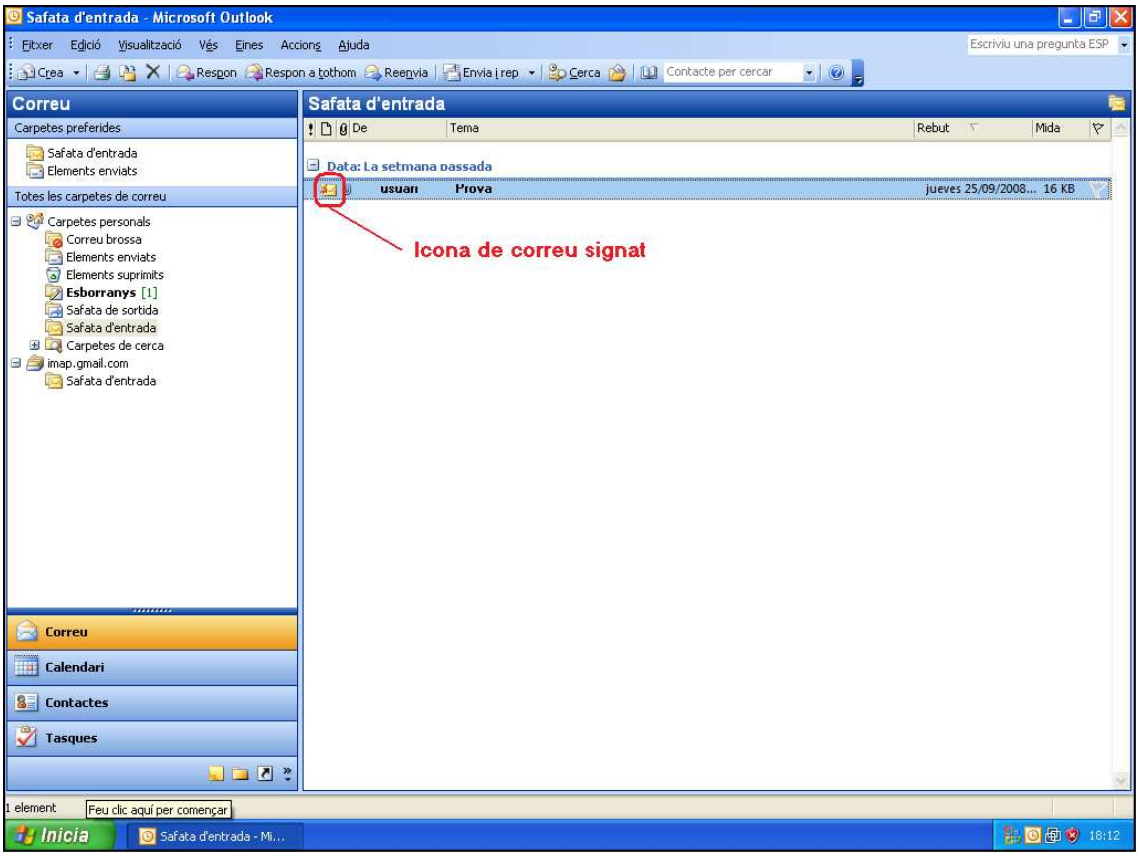

Figura 23. Recepció de correu electrònic signat

En fer doble clic sobre el nou missatge rebut, podem trobar-nos en dos situacions.

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

Obrint el missatge es pot veure a la dreta de la pantalla una icona vermella  que indica que el correu està signat (figura 24).

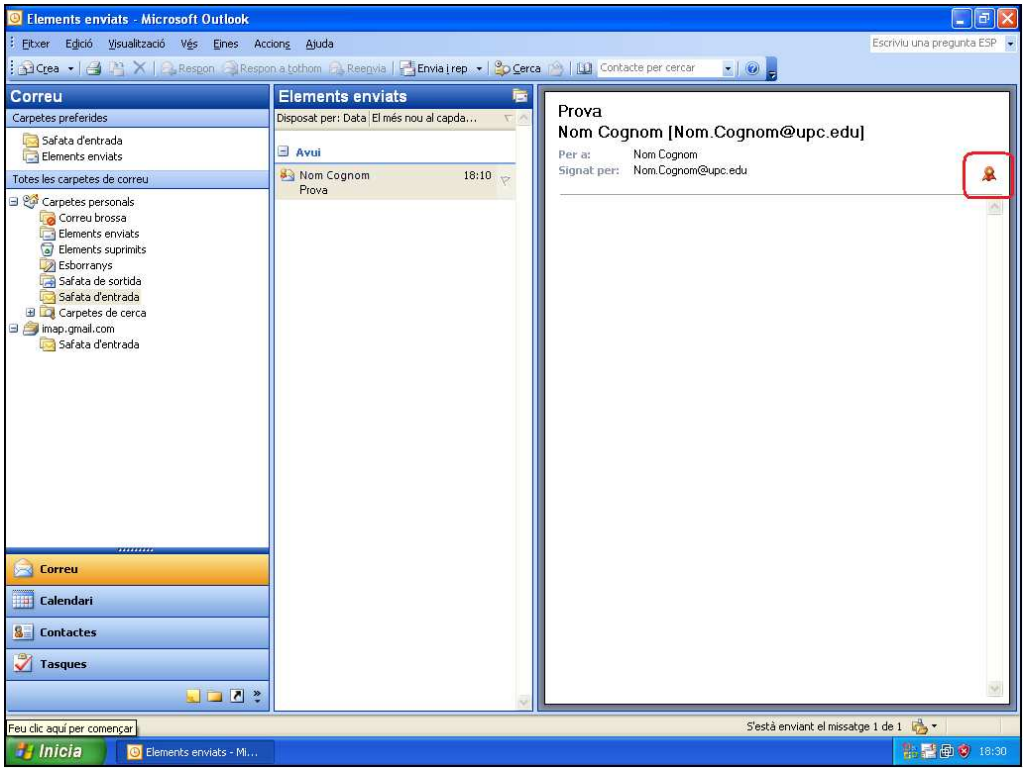

Figura 24. Correu electrònic signat i confiable

En cas de que vulguem veure les propietats de la signatura del missatge electrònic rebut, s'ha de fer clic sobre la icona remarcada a la figura 24. Al fer clic, s'obrirà el quadre de diàleg *"Signatura electrònica: vàlida"* com el de la figura 25. Fent clic al botó *"Detalls..."* (pas 1 de la figura 25) ens permet visualitzar les propietats de la signatura digital (pas 2 de la figura 25).

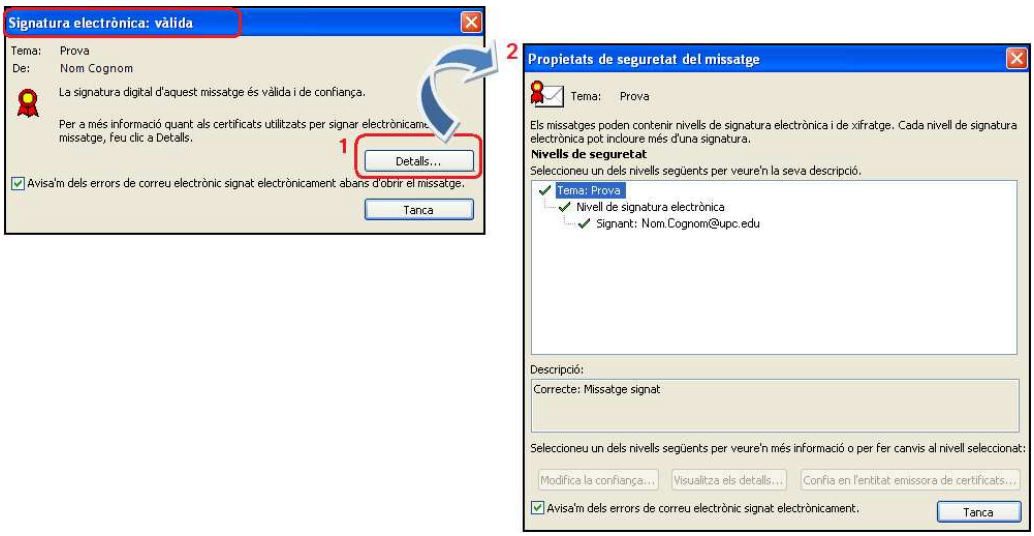

Figura 25. Visualitzar les propietats de la signatura digital.

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 emissora de certificats del certificat utilitzat pel remitent del correu signat, apareix el quadre *"Signatura electrònica: no vàlida"* de la figura 26.

El missatge es pot llegir igualment fent clic al botó "*Visualitza el missatge*" (opció remarcada a la figura 26).

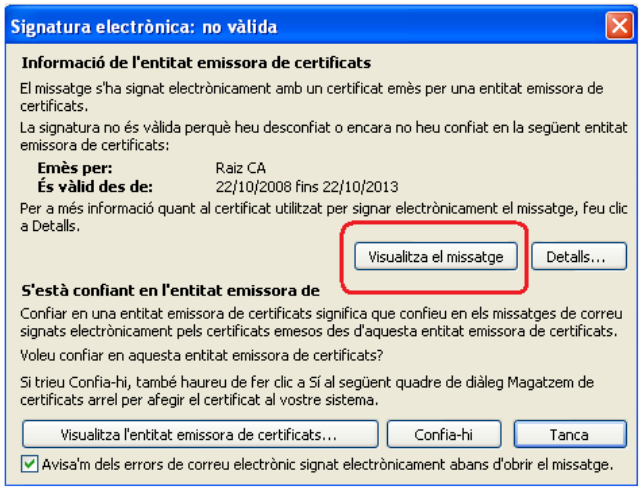

Figura 26. Recepció de missatges amb signatura no vàlida.

En aquest cas no es comprova la signatura i s'haurien d'instal·lar les claus públiques de l'entitat emissora del certificat utilitzat pel remitent del correu signat. Per fer-ho cal fer clic al botó *"Confia-hi"* de la figura 27 i fer clic a *"Sí"* al quadre de diàleg *"Magatzem de certificats arrel"* per afegir el certificat al vostre sistema.

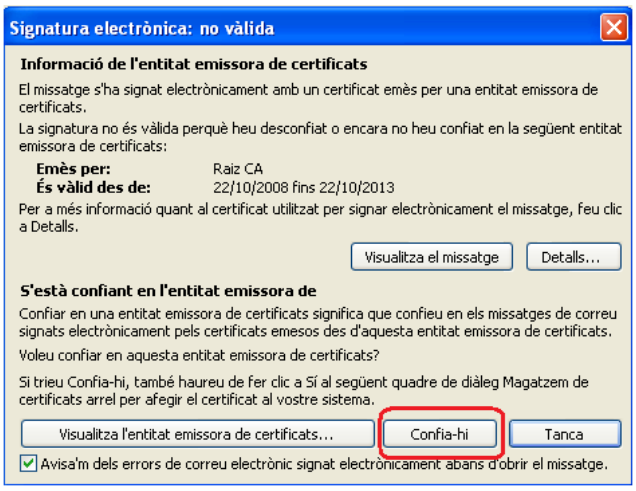

Figura 27. Confiar claus públiques externes

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 (figura 28).

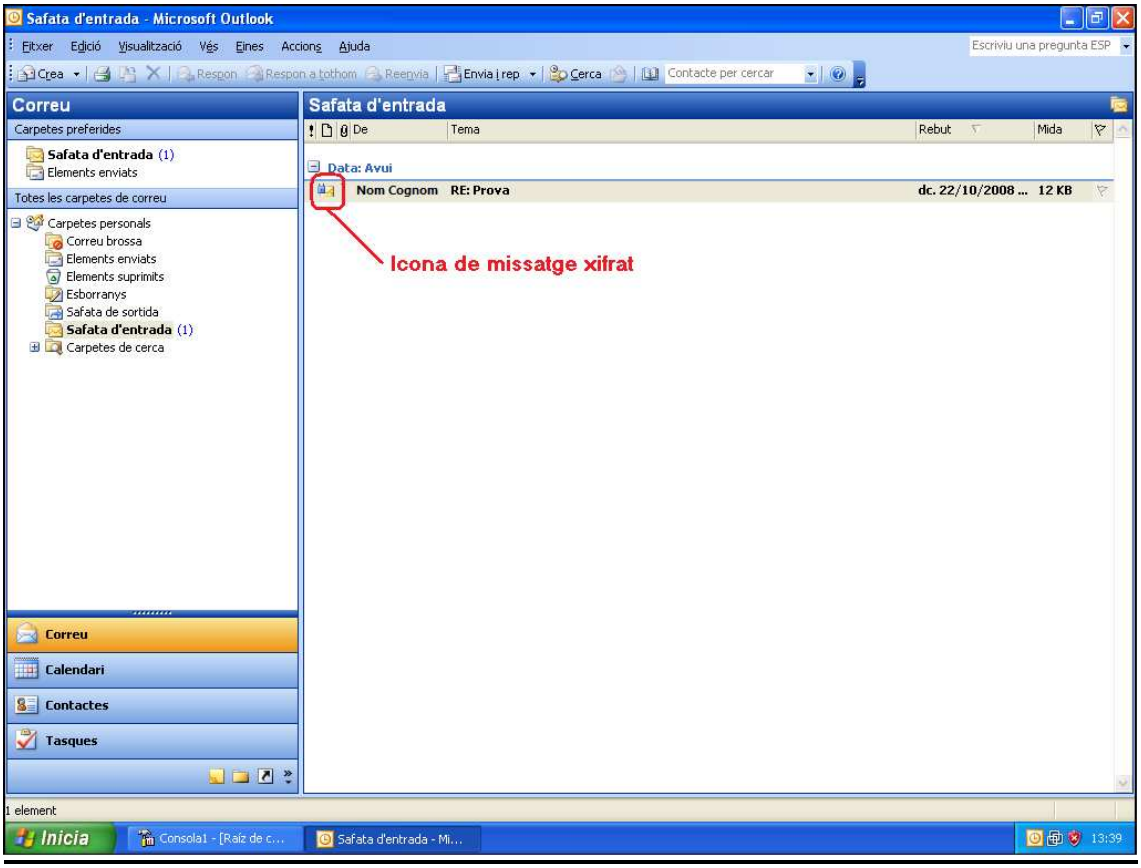

Figura 28. Recepció de missatge xifrat.

Si nosaltres som la persona a la que anava destinat aquest correu, en fer doble clic, es podrà obrir i llegir sense cap problema (figura 29).

A la part dreta del correu es podrà veure la icona d'un cadenat que ens indica que el correu està xifrat. Fent clic sobre aquesta icona (pas 1 de la figura 29), podrem accedir a les propietats del xifratge realitzat (pas 2 de la figura 29).

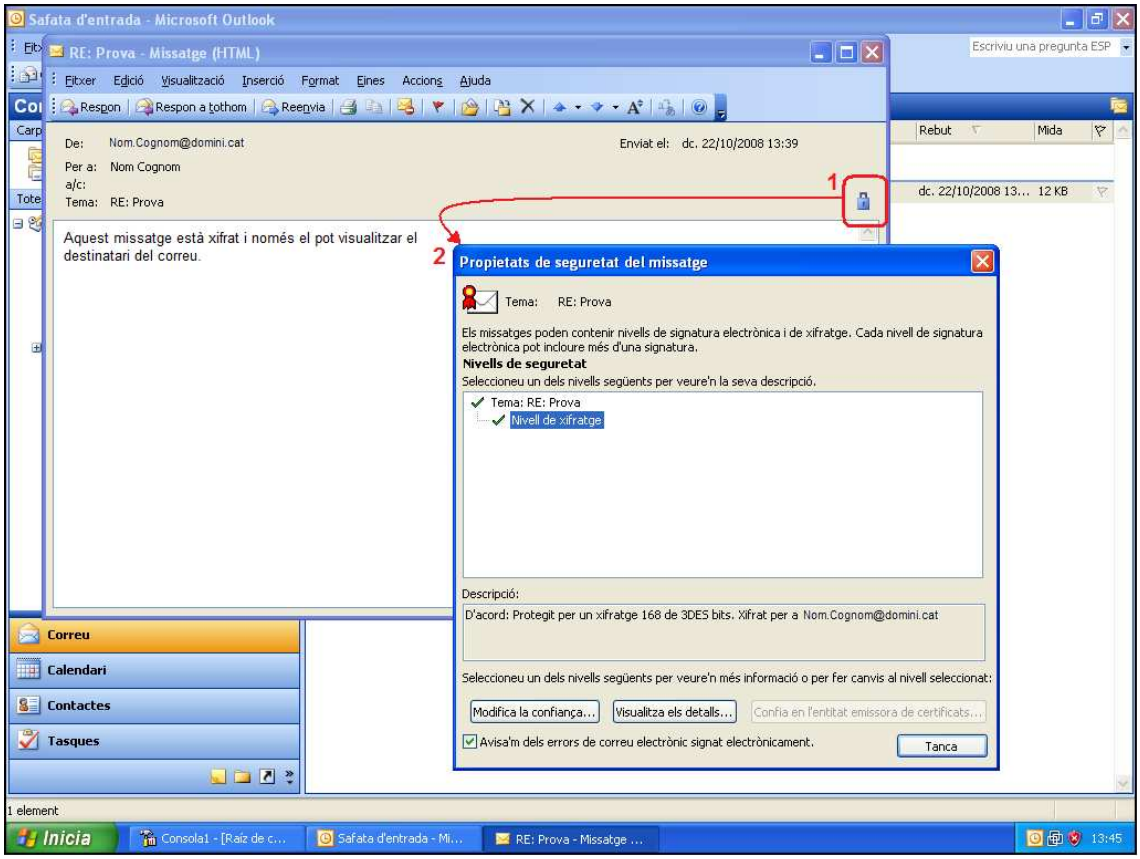

Figura 29. Recepció de missatge xifrat.

6 Referències

- Informació sobre què és un certificat

  http://www.catcert.cat/web/cat/0_0_quees.jsp

- Preguntes freqüents sobre el funcionament dels certificats

  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