UNIVERSITAT POLITÈCNICA DE CATALUNYA	**INFORMACIÓ GENERAL**
PROJECTE: Manuals d'ús de signatura electrònica	Versió: 1.5
TÍTOL: Signatura electrònica amb Mozilla Thunderbird 2 i MS Windows XP	Codi Referència:
RESUM:	Data Publicació: 18/11/2008

PROCEDIMENT

Signatura electrònica amb Mozilla Thunderbird 2 i Windows XP

PREPARAT PER:	**REVISAT PER:**	**APROVAT PER:**
Nom:	Nom:	Nom:
Data: 25/11/2008	Data:	Data:

UNIVERSITAT POLITÈCNICA DE CATALUNYA	**INFORMACIÓ GENERAL**
PROJECTE: Manuals d'ús de signatura electrònica	Versió: 1.5
TÍTOL: Signatura electrònica amb Mozilla Thunderbird 2 i MS Windows XP	Codi Referència:
RESUM:	Data Publicació: 18/11/2008

Versió	Parts que canvien	Descripció del canvi	Data del canvi
1.0	Tot	Creació del document	25/11/08
1.1	Tot	Modificació document inicial	22/12/08
1.2	Introducció configuració signatura	Introducció configuració signatura correu	05/12/08
1.3	Certificats CRL i OCSP	Certificats CRL i OCSP	16/01/08
1.4	Recuperar clau pública xifratge correu	Recuperar clau pública xifratge correu	16/01/08
1.5	Tot	Revisio	26/01/09

ÍNDEX

1 Objectiu i abast

El present document descriu el procés de configuració del client de correu electrònic Mozilla Thunderbird 2 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 Mozilla Firefox. 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 Mozilla Thunderbird 2 i Windows XP

3.1 Per poder configurar la signatura electrònica per utilitzar-la amb l'eina Mozilla Thunderbird 2, s'ha de definir l'ús del lector de targetes amb el client de correu. Per fer-ho cal 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.

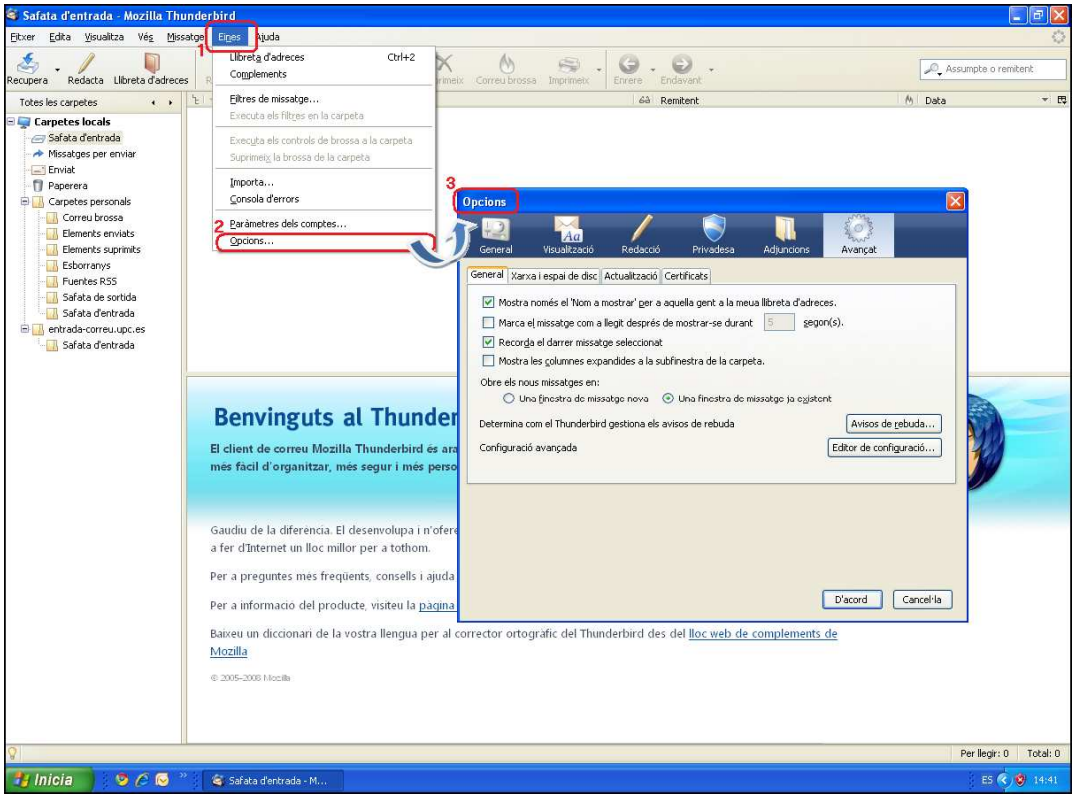

Figura 1. Finestra de l'eina Mozilla Thunderbird 2

3.2 Dintre de la finestra *"Opcions"* de Mozilla Thunderbird 2, caldrà accedir a l'apartat *"Avançat"* (pas 1) i fer clic a la fitxa *"Certificats"* (pas 2) tal i com es veu a la figura 2.

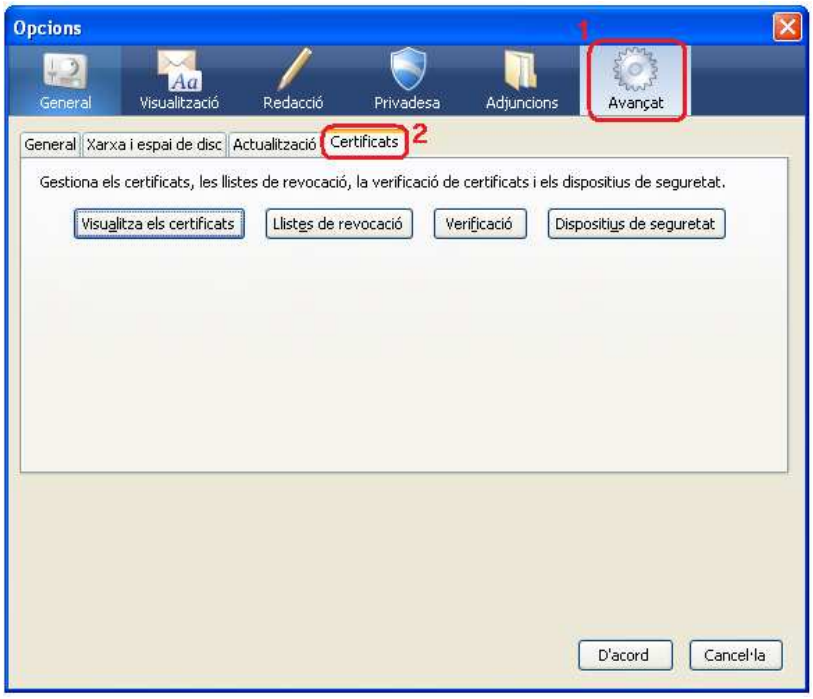

Figura 2. Finestra Opcions de Mozilla Thunderbird 2

3.3 Un cop a la fitxa *"Certificats"* s'ha de configurar el lector de targetes per que el pugui utilitzar el client de correu. Fer fer-ho, s'ha de fer clic al botó *"Dispositius de seguretat"* (pas 1) per tal d'obrir la finestra *"Gestor de dispositius"* (pas 2) tal i com es veu a la figura 3.

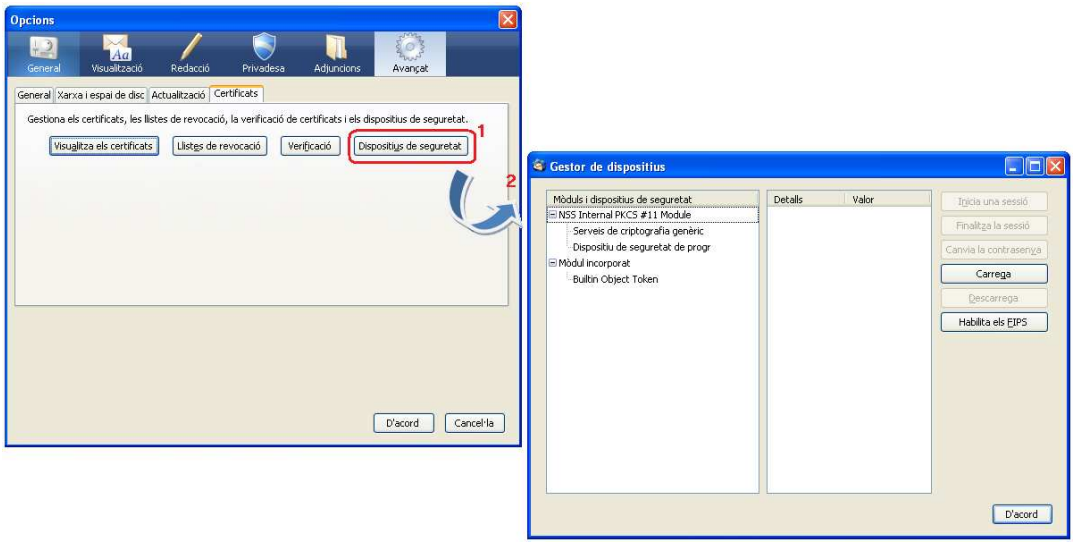

Figura 3. Finestra de l'eina Mozilla Thunderbird

3.4 Un cop oberta la finestra del "*Gestor de dispositius*", cal fer clic al botó *"Carrega"* (pas 1) per accedir a la finestra *"Carrega el dispositiu PKCS#11"* (pas 2) tal i com podem veure a la figura 4.

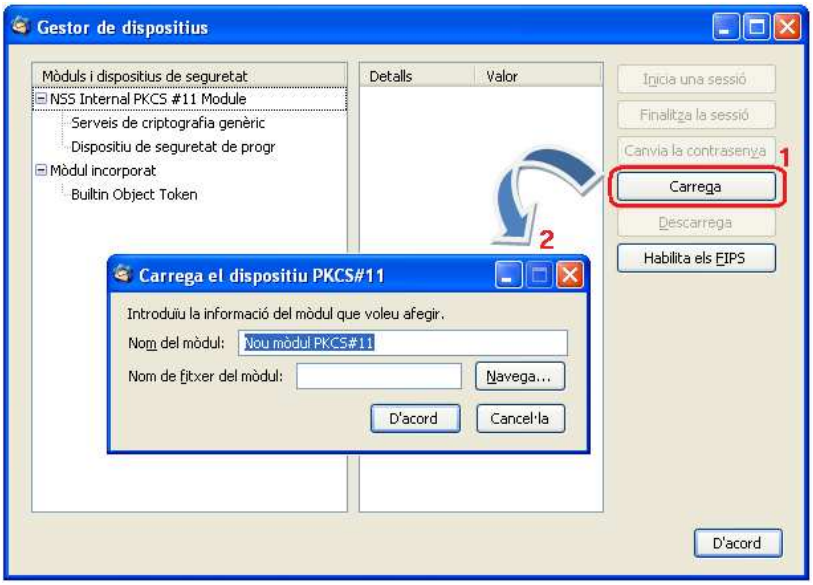

Figura 4. Gestor de dispositius

3.5 A la finestra *"Carrega el dispositiu PKCS#11"*, s'ha d'incorporar un nom descriptiu pel lector de targetes al quadre *"Nom del mòdul"* (pas 1), com per exemple "*Lector de targetes Gemalto"*, i al quadre *"Nom de fitxer del mòdul"* s'ha de fer clic al botó *"Navega"* (pas 2) per seleccionar l'arxiu *"C:\Archivos de programa\Gemalto\Classic Client\BIN\gclib.dll"* (pas 3) i fer clic al botó *"Obre"* (pas 4), tal i com podem veure a la figura 5.

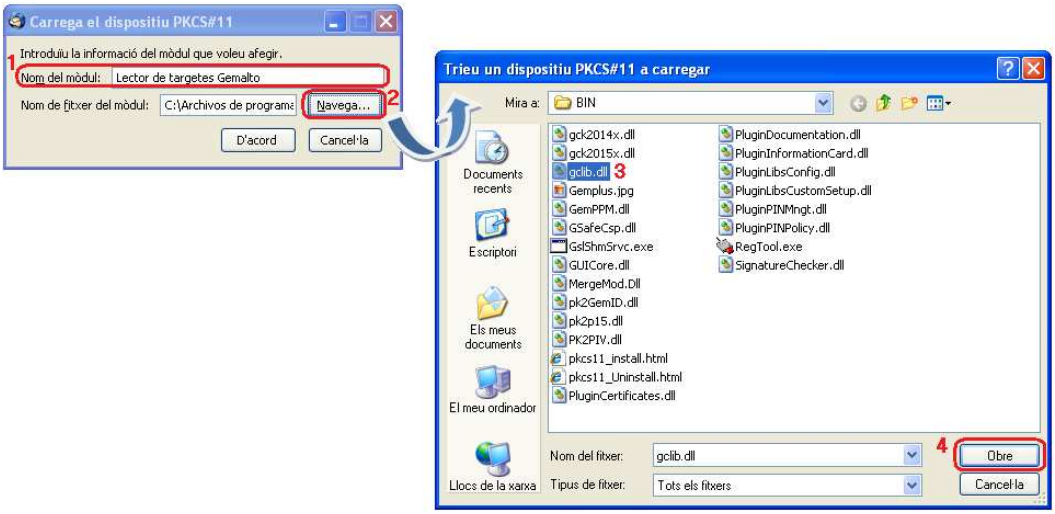

Figura 5. Selecció de fitxer del mòdul lector de targetes

3.6 Un cop seleccionat l'arxiu de mòdul del lector de targetes, s'ha de fer clic al botó *"D'acord"* per confirmar la càrrega del lector de targetes a la finestra *"Carrega el dispositiu PKCS#11"* (figura 6).

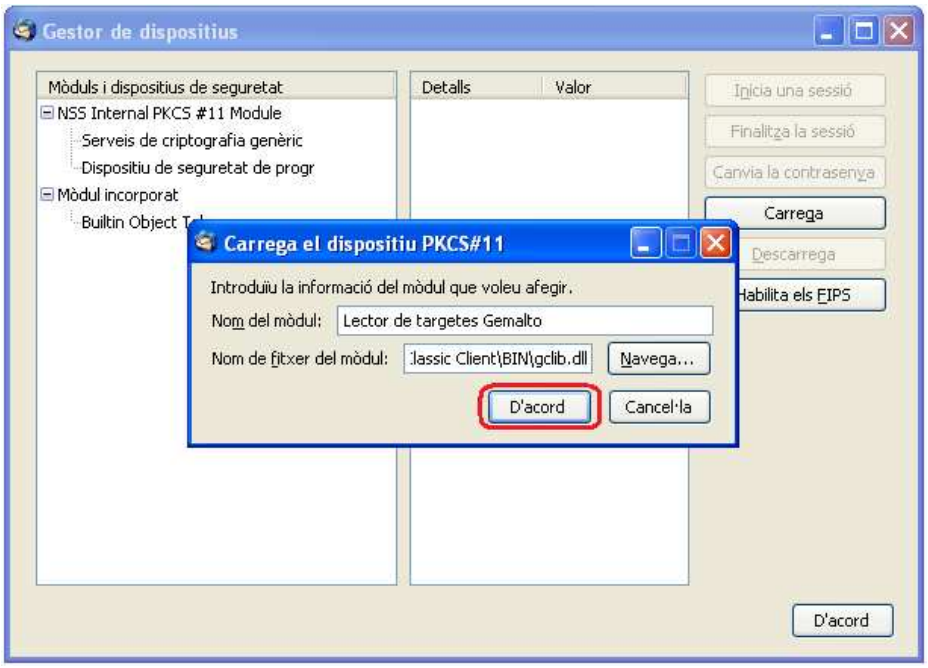

Figura 6. Selecció de mòdul de dispositiu

3.7 Al fer clic al botó "*D'acord"* apareix el quadre de confirmació de la figura 7 on s'ha d'acceptar l'instal·lació del mòdul seleccionat anteriorment.

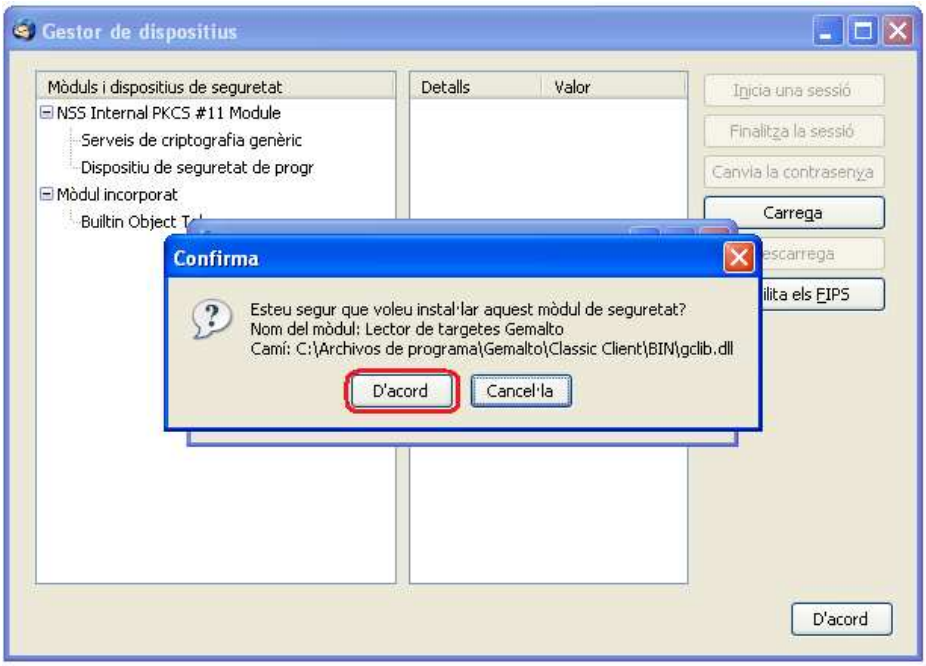

Figura 7. Confirmació d'instal·lació de mòdul

3.8 A continuació apareix el quadre d'avís de la figura 8 on s'ha de fer clic al botó *"D'acord"* (pas 1) per acceptar l' instal·lació.

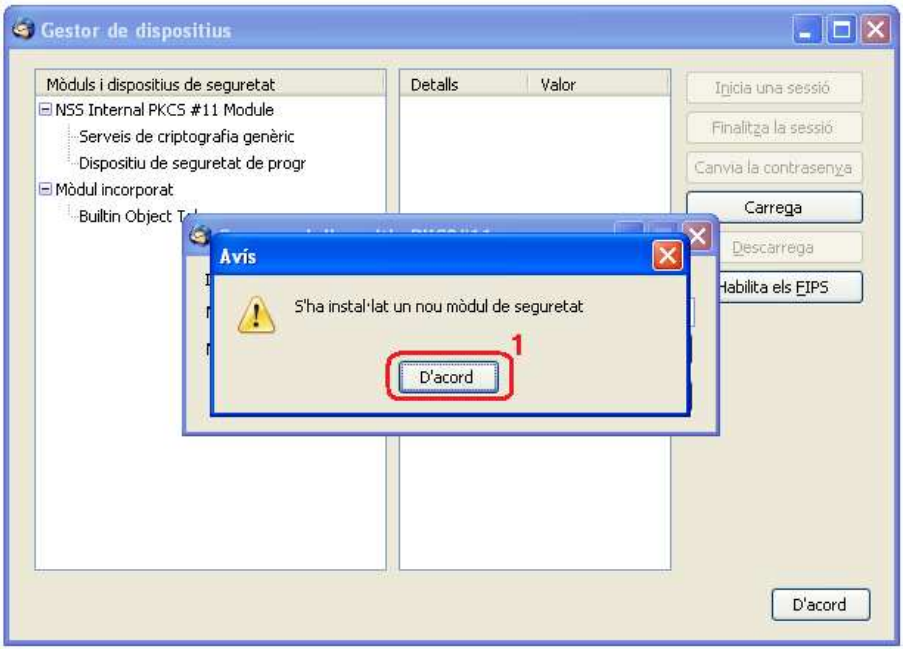

Figura 8. Avís d'instal·lació de mòdul.

3.9 Després de la confirmació de l'instal·lació apareixen les dades del mòdul instal·lat a la finestra *"Gestor de dispositius".* Seleccionant el nou mòdul a la part esquerra, es poden veure els seus detalls a la part dreta d'aquesta finestra, tal i com es pot veure a la figura 9

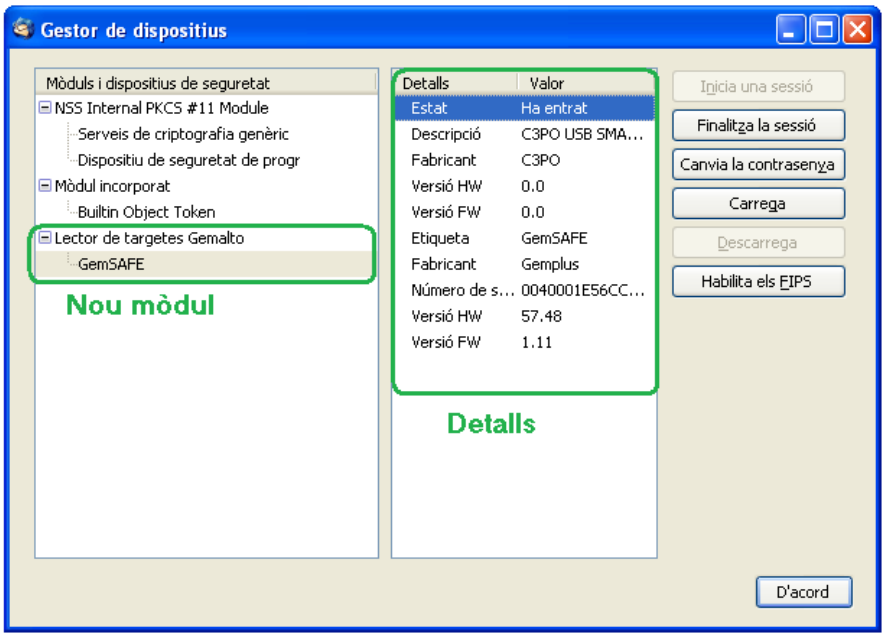

Figura 9. Mòdul instal·lat

3.10 A continuació s'ha de fer clic al botó *"D'acord"* per confirmar tot el procés perquè el client de correu tingui accés al certificat del carnet universitari (figura 10).

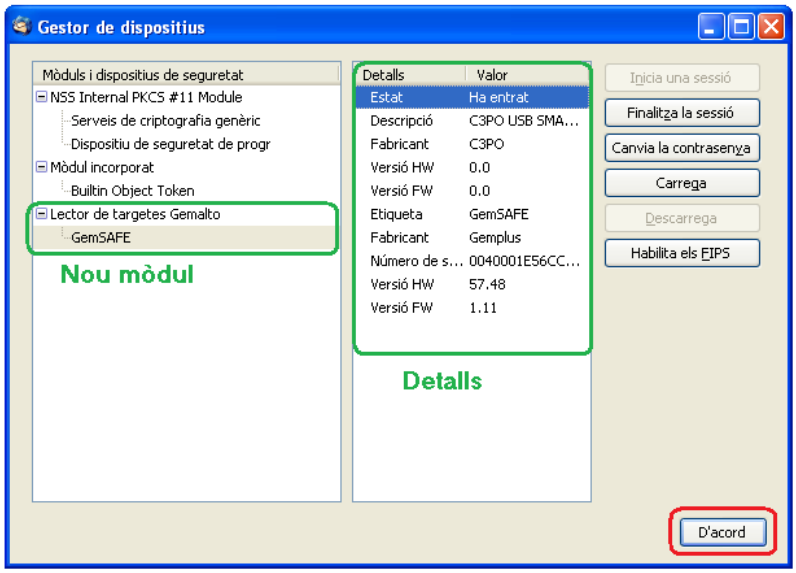

Figura 10. Confirmació de tot el procés d'instal·lació del lector de targetes.

3.11 Un cop configurat el client de correu Mozilla Thunderbird per utilitzar el lector de targetes, cal configurar el compte de correu perquè utilitzi el certificat del carnet universitari. Per fer-ho, cal accedir al menú *"Eines"* de l'aplicació (pas 1) i seleccionar *"Paràmetres dels comptes..."* (pas 2) perquè s'obri la finestra *"Paràmetres de compte"* tal i com es pot veure a la figura 11.

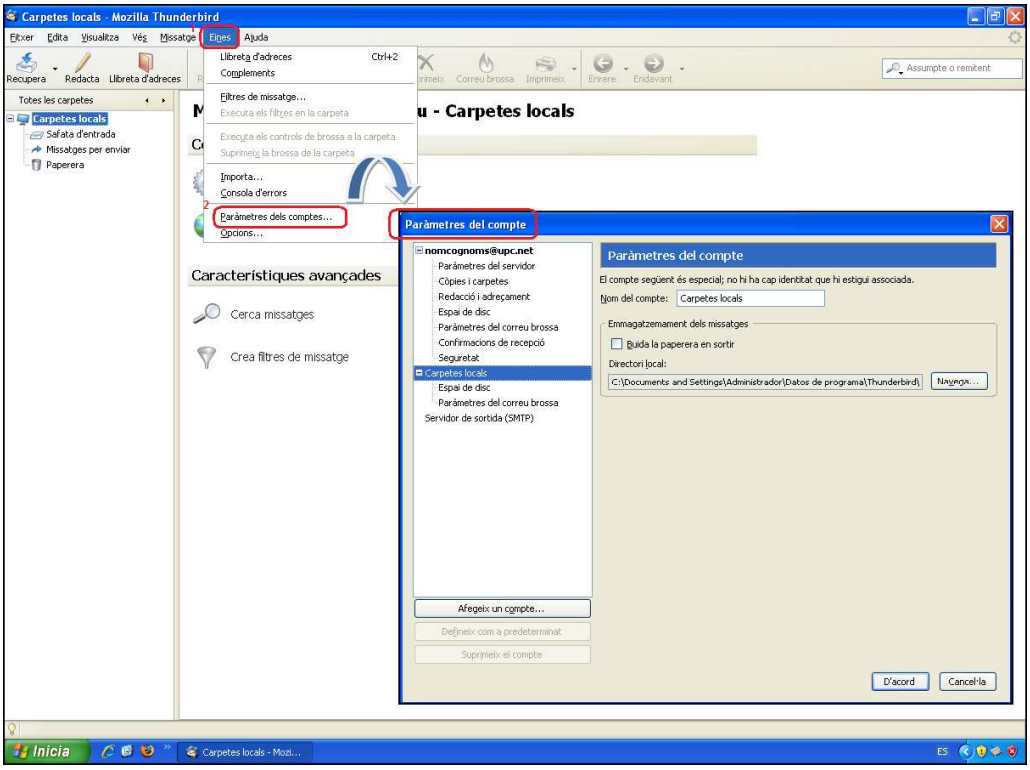

Figura 11. Configuració de seguretat no definida

3.12 Un cop a la finestra *"Paràmetres del compte"* s'ha de definir una nova configuració de seguretat. Per fer-ho, cal que accedim a l'apartat *"Seguretat"* (pas 1) del compte de correu que tenim configurat i a continuació fer clic al botó *"Seleccioneu.."* (pas 2) dintre de l'apartat *"Signatura digital"*, com podem apreciar a la figura 12.

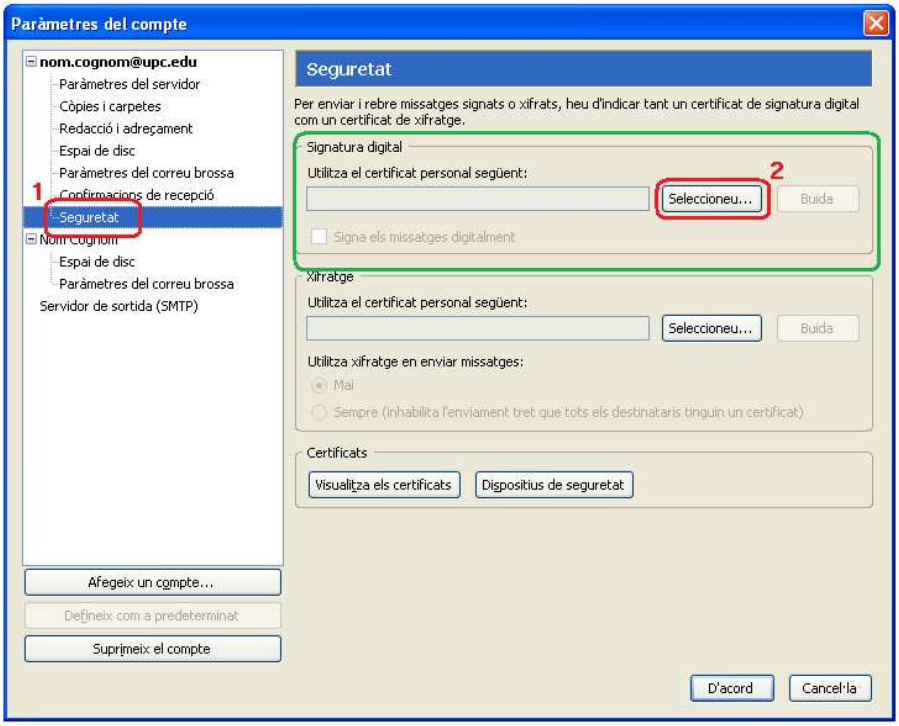

Figura 12. Configuració de seguretat no definida

3.13 En fer clic al botó *"Seleccioneu..."* demanarà el número d'identificació personal del carnet universitari (NIP o PIN) en un quadre emergent, tal i com es pot veure a la figura 13. On caldrà introdiur-lo i fer clic al botó *"D'acord"* per poder accedir als certificats del carnet universitari.

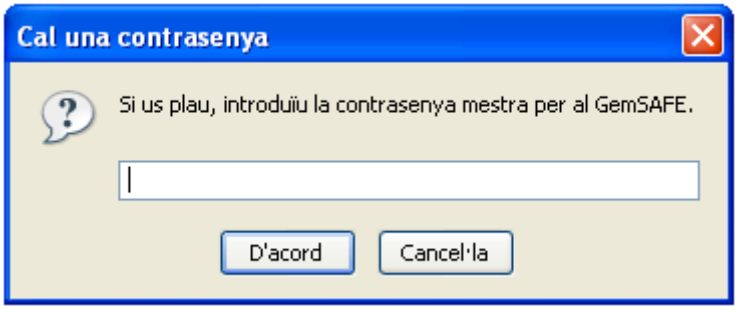

Figura 13. Quadre emergent per introduir el NIP

3.14 A continuació, s'obre el quadre *"Selecciona un certificat"* on es pot veure el certificat del carnet universitari i les seves dades. Cal seleccionar-lo i fer clic al botó *"D´acord"*, tal i com es pot veure a la figura 14.

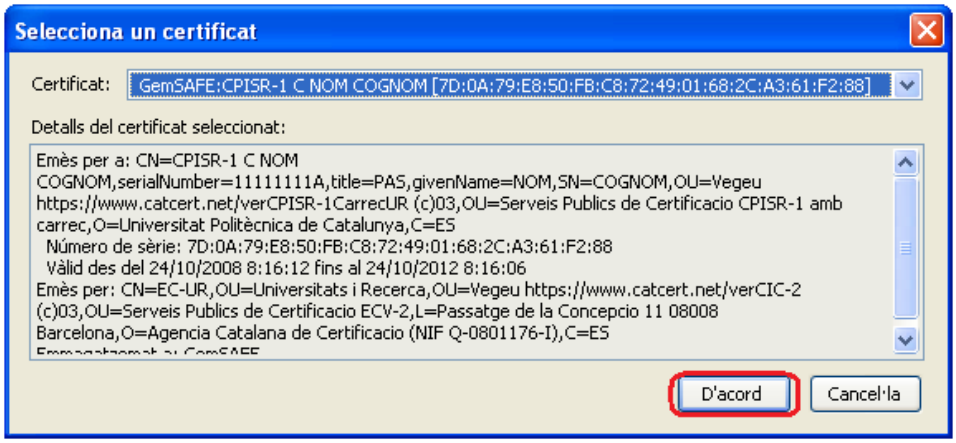

Figura 14. Configuració de seguretat no definida

3.15 Un cop s'ha fet clic al botó *"D´acord"*, apareix el missatge de Mozilla Thunderbird que permet configurar el certificat de xifratge. Això es pot apreciar a la figura 15. S'ha de fer clic a botó *"D'acord"* (pas 1) per continuar amb la configuració.

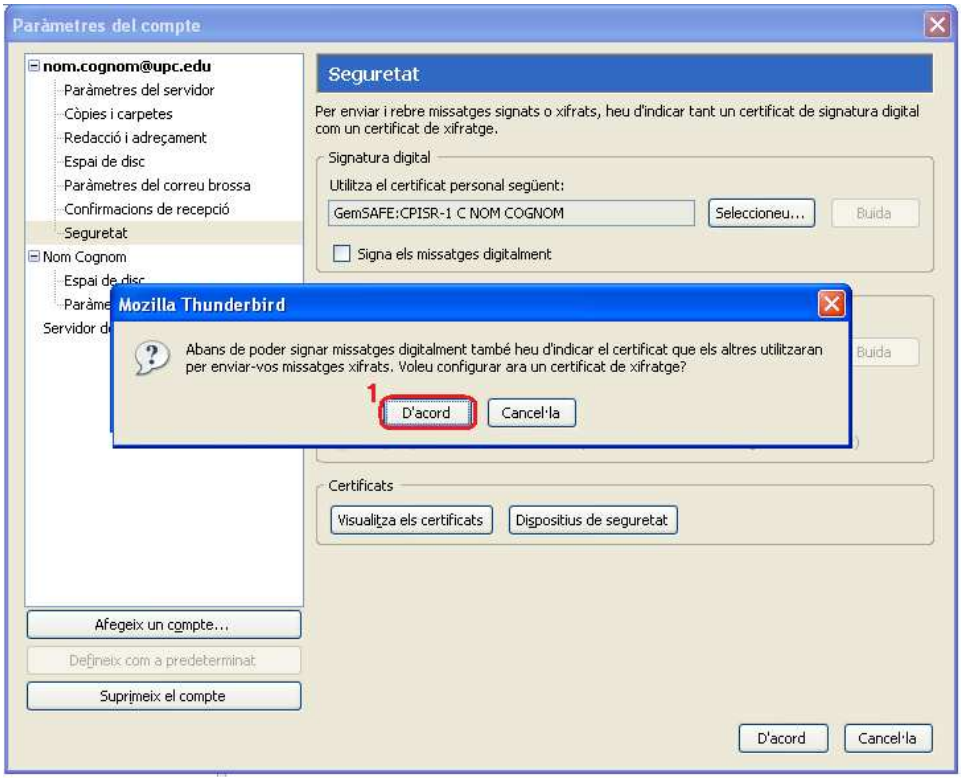

Figura 15. Missatge de configuració de certificat de xifratge.

3.16 En fer clic al botó *"D'acord"*, s'obra el quadre *"Selecciona un certificat"* on es pot veure el certificat del carnet universitari per xifratge i les seves dades. En fer clic al botó *"D'acord"* (pas 1 de la figura 16) quedarà configurat també el certificat de xifratge, tal i com es pot veure a la figura 17.

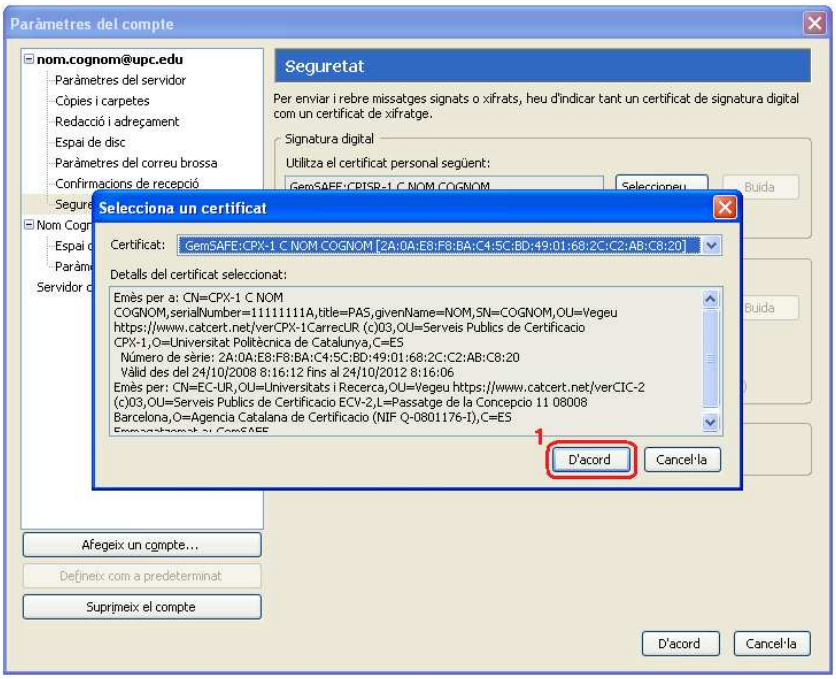

Figura 16. Selecció del certificat per xifratge

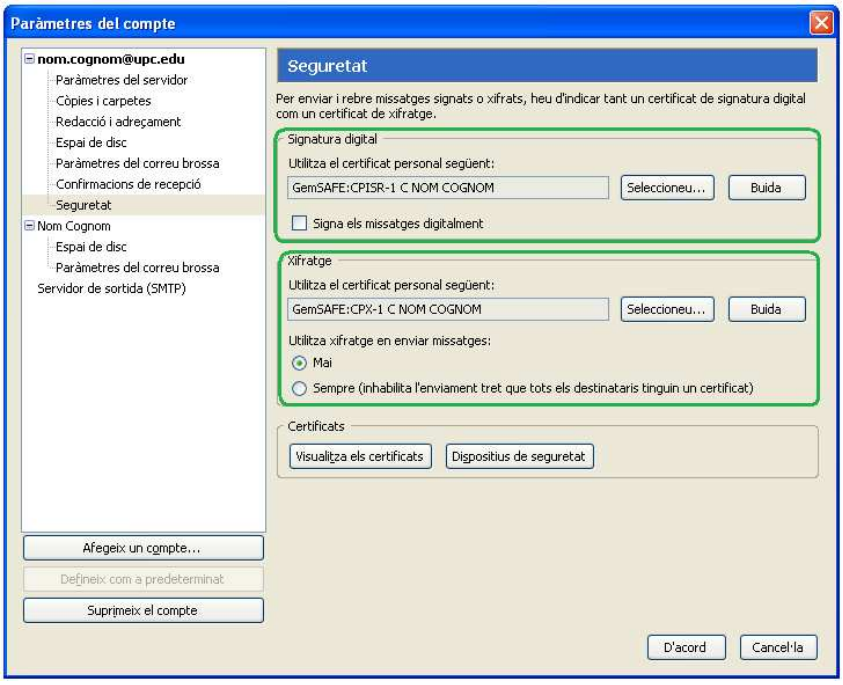

Figura 17. Configuració de Seguretat amb els certificats de signatura i xifratge

3.17 Amb la configuració de *"Signatura Digital"* i *"Xifratge"* ja definida (figura 18), només caldrà habilitar l´opció *"Signa els missatges digitalment"* dindre de l´apartat *"Signatura digital"* (pas 1) per fer que TOTS el missatges siguin enviats per defecte signats digitalment. Cal fer clic al botó *"D'acord"* (pas 2), per confirmar tota la configuració realitzada, tal i com es pot veure a la figura 18.

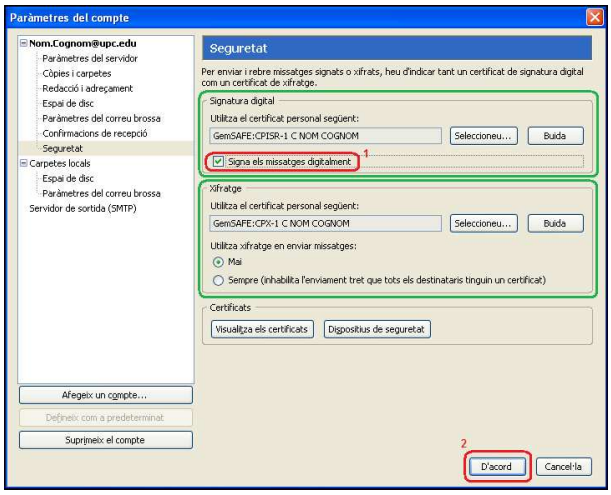

Figura 18. Apartat *"Seguretat"* omplert

3.18 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 19.

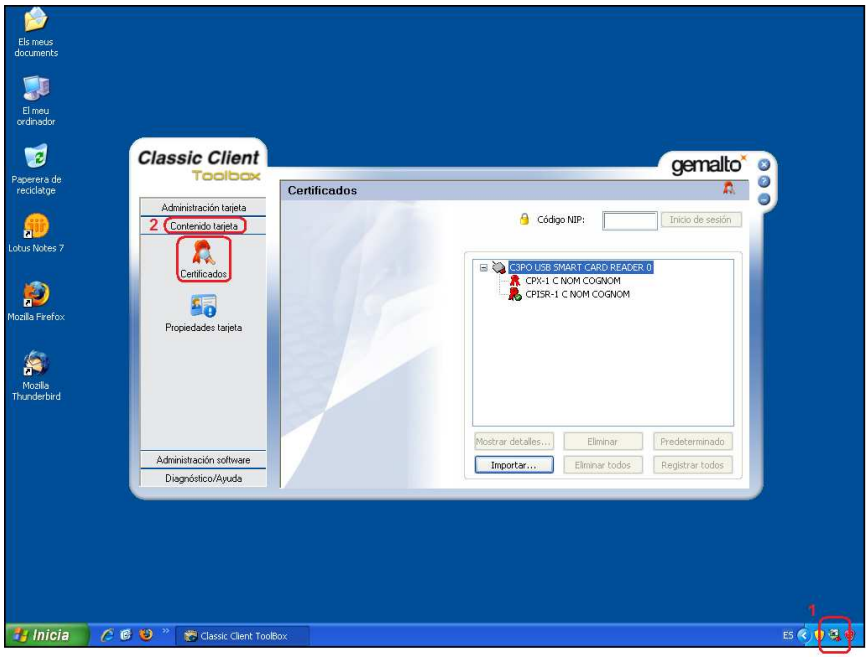

Figura 19. Propietats del certificat gemalto

3.19 Un cop dintre de l'apartat *"Certificados"* figura 19, 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 20.

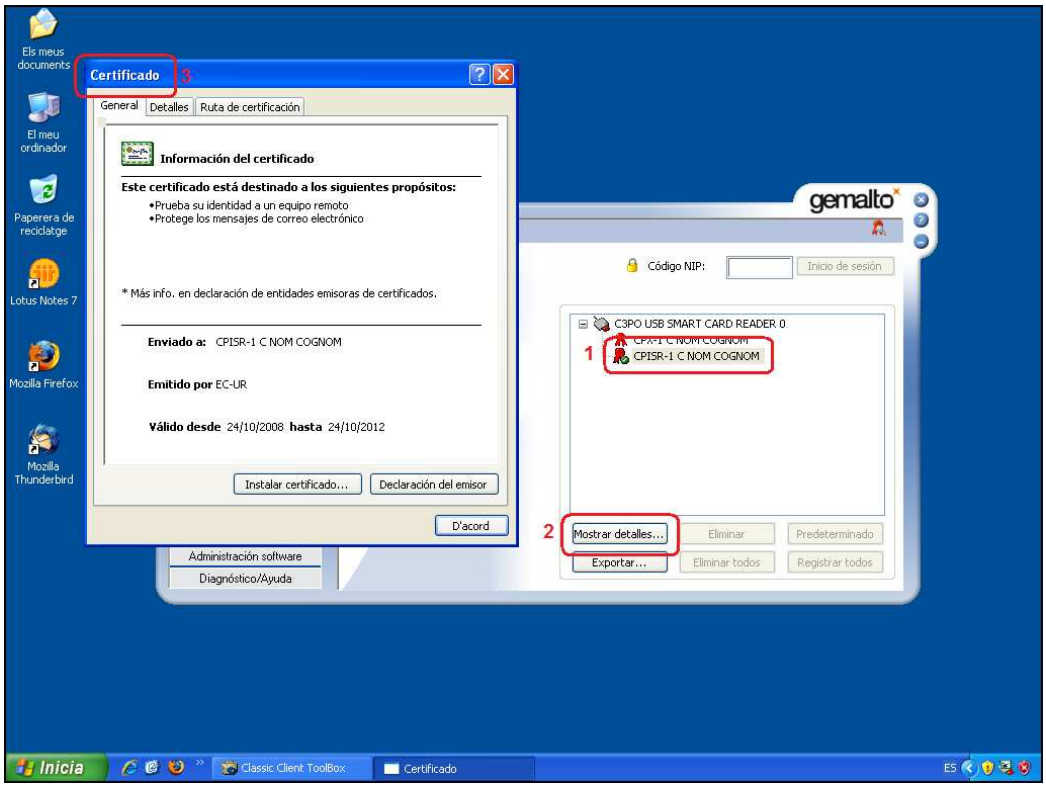

Figura 20. Propietats del certificat

3.20 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 21.

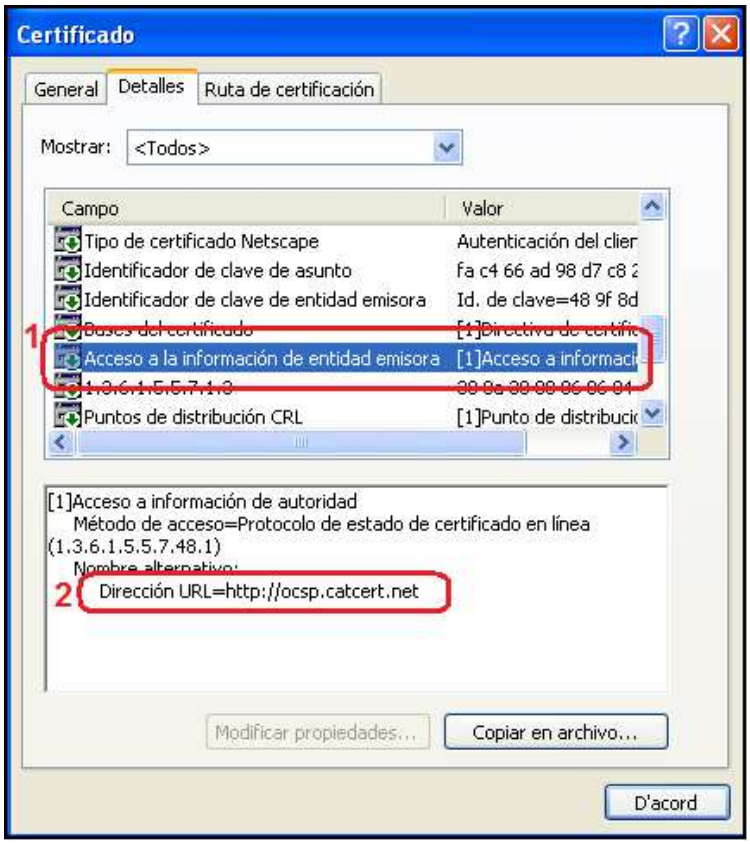

Figura 21. Propietats del certificat.

- *"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 22.

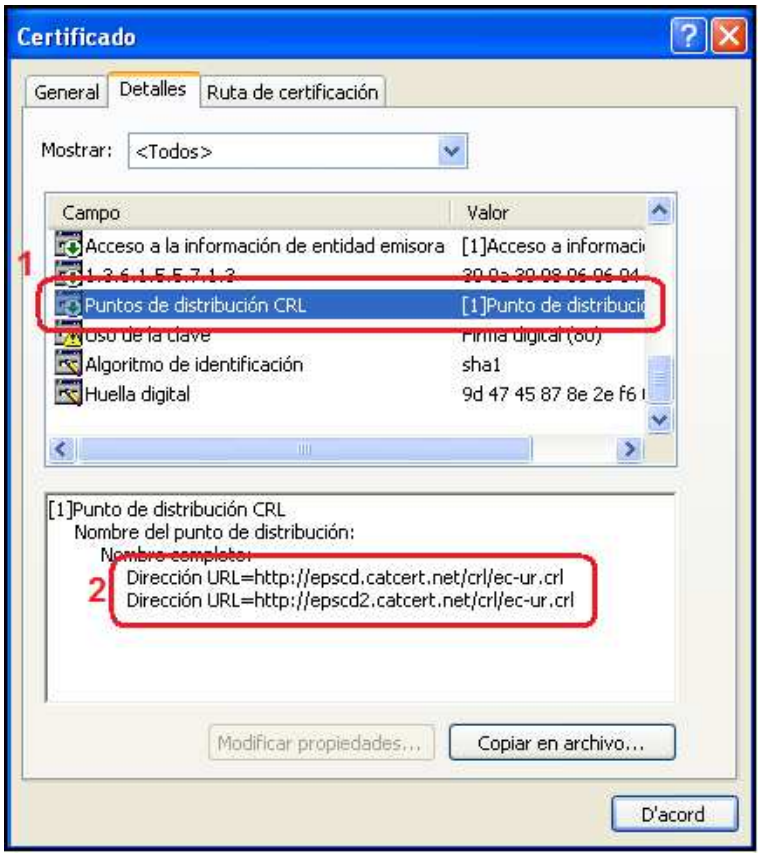

Figura 22. Propietats del certificat.

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 punt 3.17 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, es necesari fer clic al botó *"Seguretat"* (pas 1) i marcar l´opció *"Signa digitalment"* (pas 2) tal i com es pot apreciar a la figura 23.

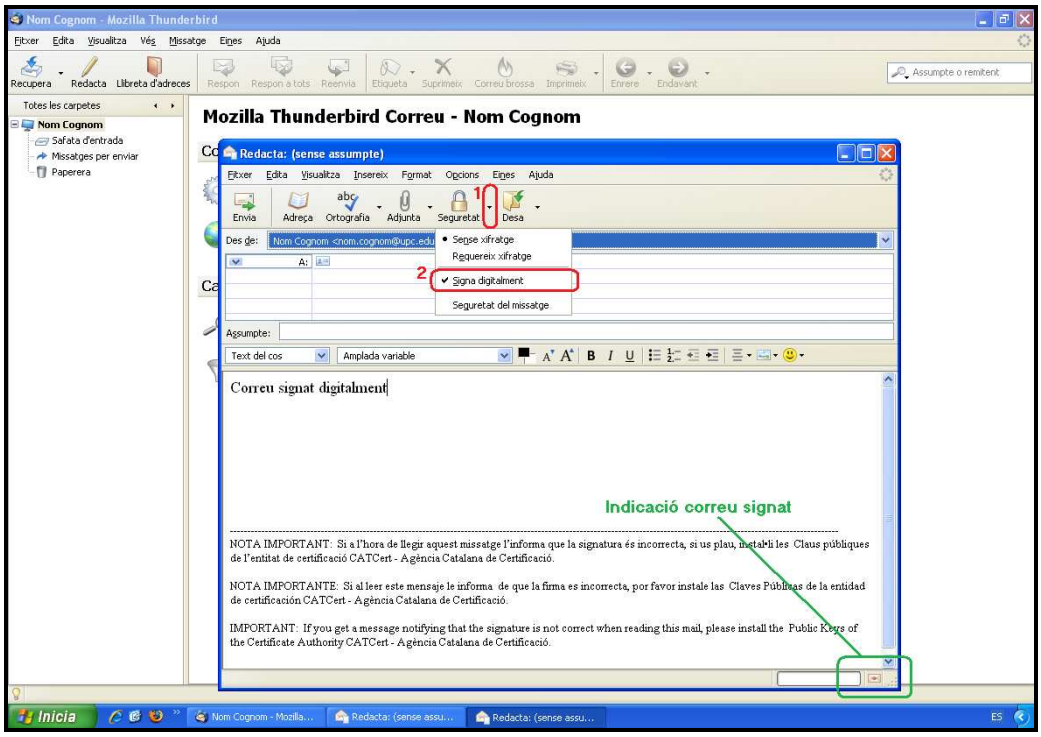

Figura 23. Activar l'enviament de correus signats

4.1.2 En el moment d'enviar el correu electrónic signat, es demanarà el número d'identificació personal del carnet universitari (NIP o PIN) en un quadre emergent (figura 24).

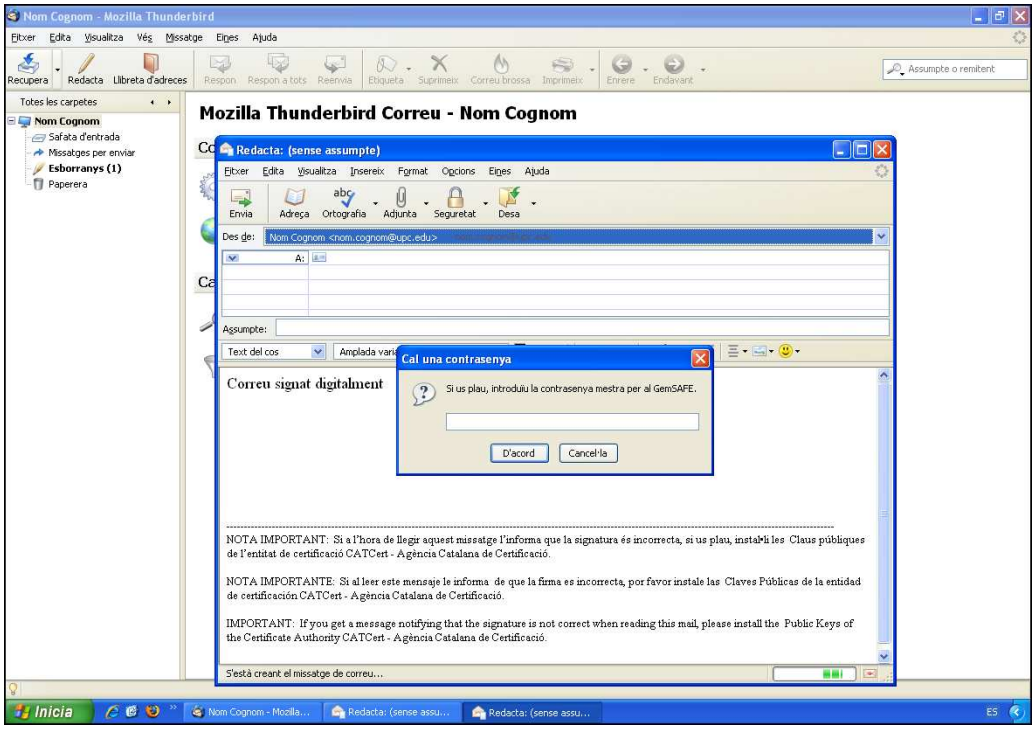

Figura 24. Quadre de diàleg d'introducció del NIP o PIN del canet universitari

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 fer clic al botó *"D'acord"* al 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 a la signatura per a missatges, 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 Mozilla Thunderbird, s'ha d'obrir l'aplicació, accedir al menú *"Eines"* (pas 1) i fer clic a *"Paràmetres dels comptes..."* (pas 2). A continuació s'obrirà el quadre *"Paràmetres dels compte"* (pas 3) tal i com es pot veure a la figura 25.

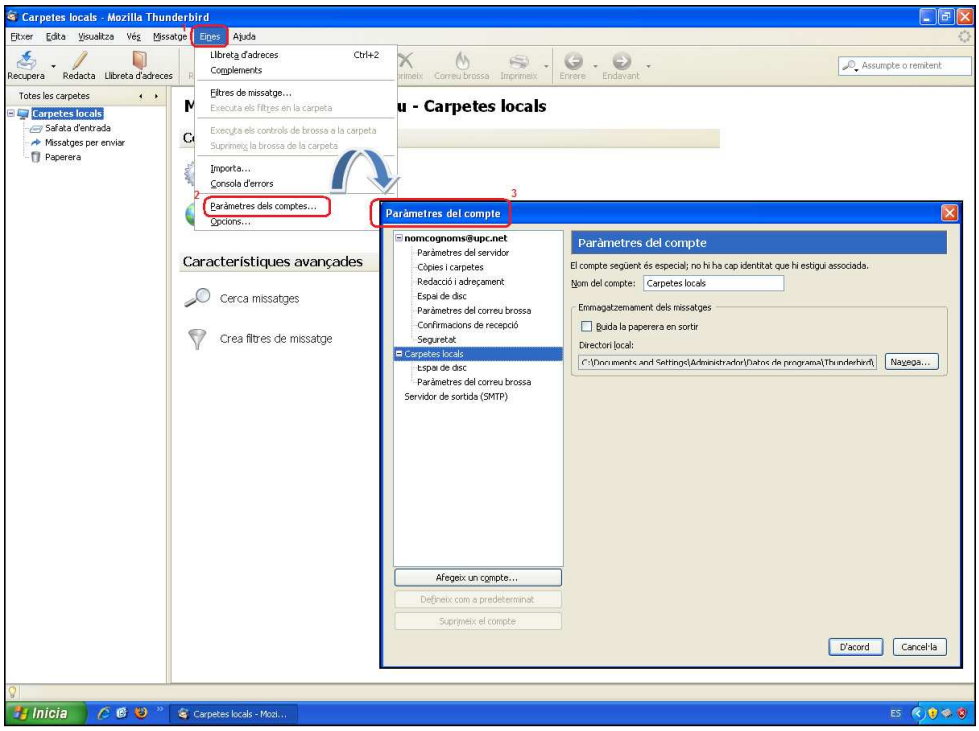

Figura 25. Opcions de correu

4.1.4.1.2 Un cop al quadre *"Paràmetres dels compte"*. Cal seleccionar el nostre compte de la UPC i marcar la casella de validació *"Adjunta aquesta signatura"* (pas 1) i a continuació fer clic al botó *"Trieu..."* (pas 2), tal i com es pot veure a la figura 26.

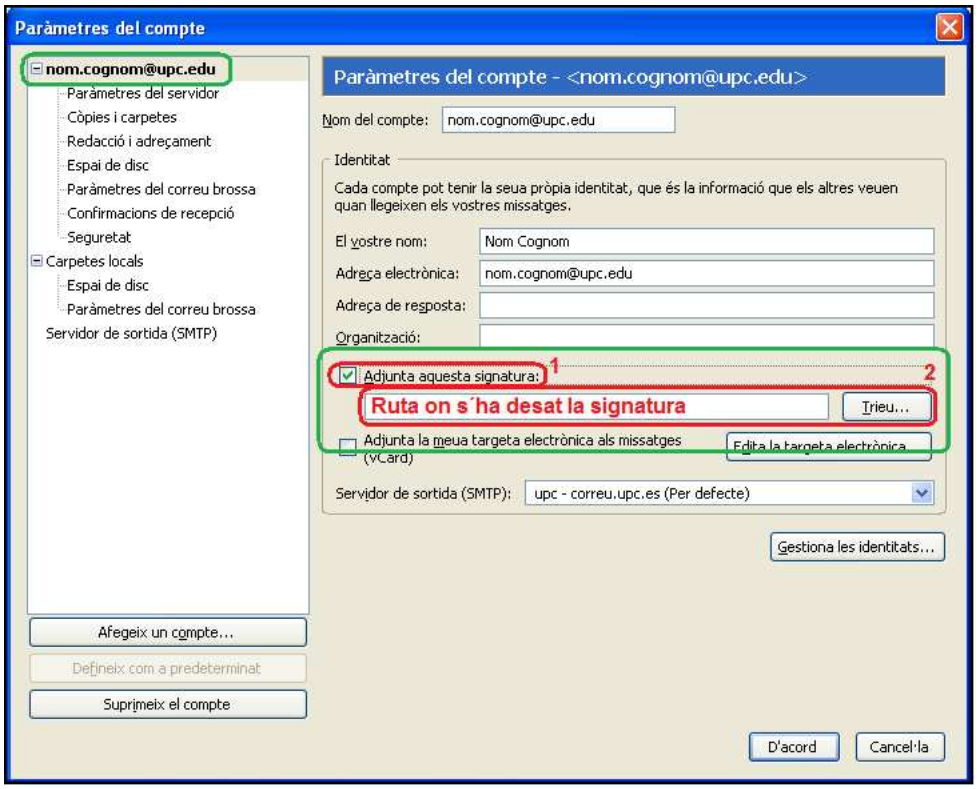

Figura 26. Opcions de format de correu

NOTA: Abans de poder adjuntar la signatura tal i com indica l'apartat anterior, es necessari copiar el text recomanat de signatura en un arxiu i desar-ho al vostre equip. Aquest arxiu, s'ha de seleccionar mitjançant l'explorador d'arxius emergent al fer clic al botó "Trieu".

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, cal fer clic al botó *"Seguretat"* (pas 1) i marcar l´opció *"Requereix xifratge"* (pas 2) tal i com es pot apreciar a la figura 27.

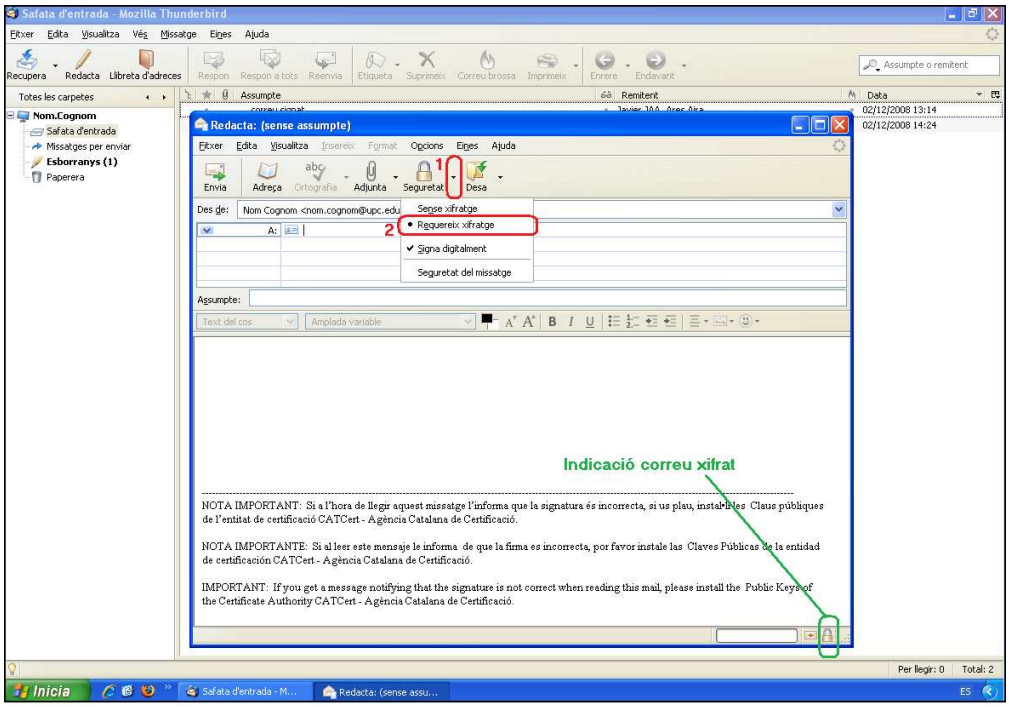

Figura 27.Activar l'enviament de correus xifrats

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 28.

Figura 28. 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 a la *"llibreta d'adreces"* del Thunderbird. D'aquesta manera, el client de correu Mozilla Thunderbird 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 d'adreces, s'ha de seleccionar el nom del destinatari al correu rebut amb el botó dret del ratolí (pas 1 de la figura 29) i fer clic a l´opció "Afegeix a la llibreta d'adreces..." (pas 2 de la figura 29).

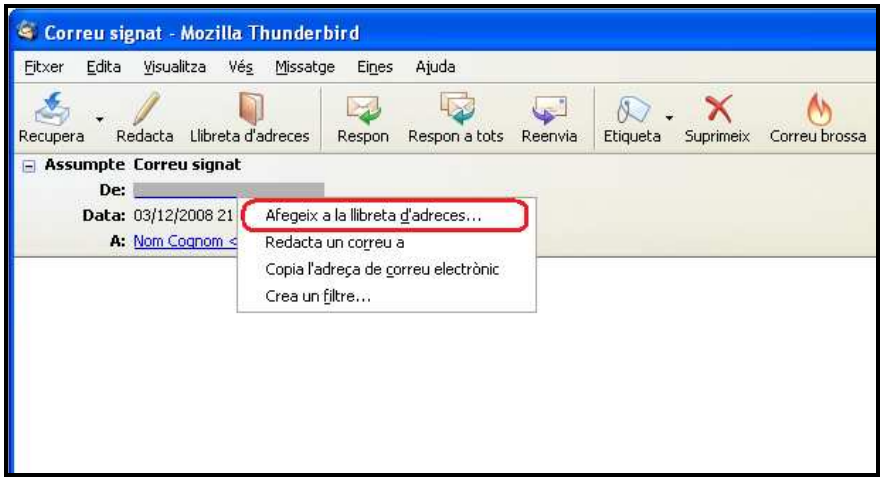

Figura 29. Afegeix a la llibreta d'adreces

5 Recepció de missatges

5.1 Signats

En el cas de rebre missatges signats digitalment, es poden reconèixer per la icona  que apareix a la dreta del correu un cop obert (figura 30).

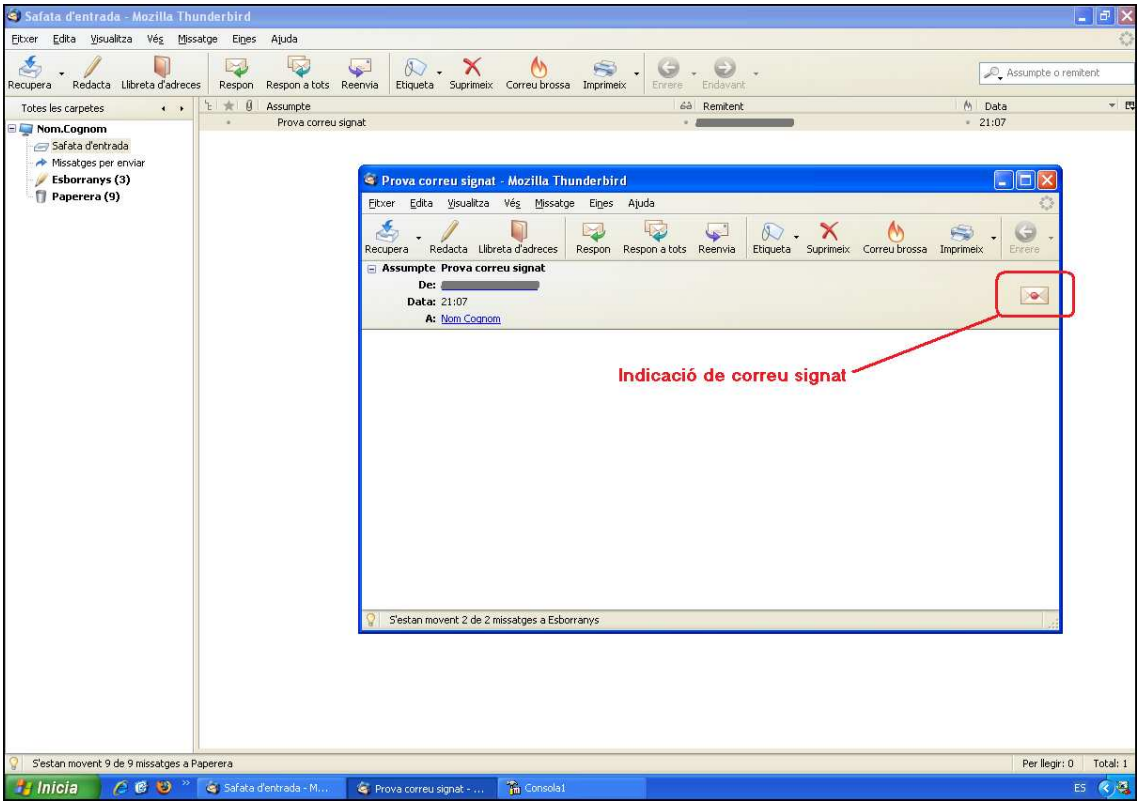

Figura 30.Recepció de correu electrònic signat

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. En obrir el missatge es pot veure la icona  que indica que el correu està signat correctament (figura 31).

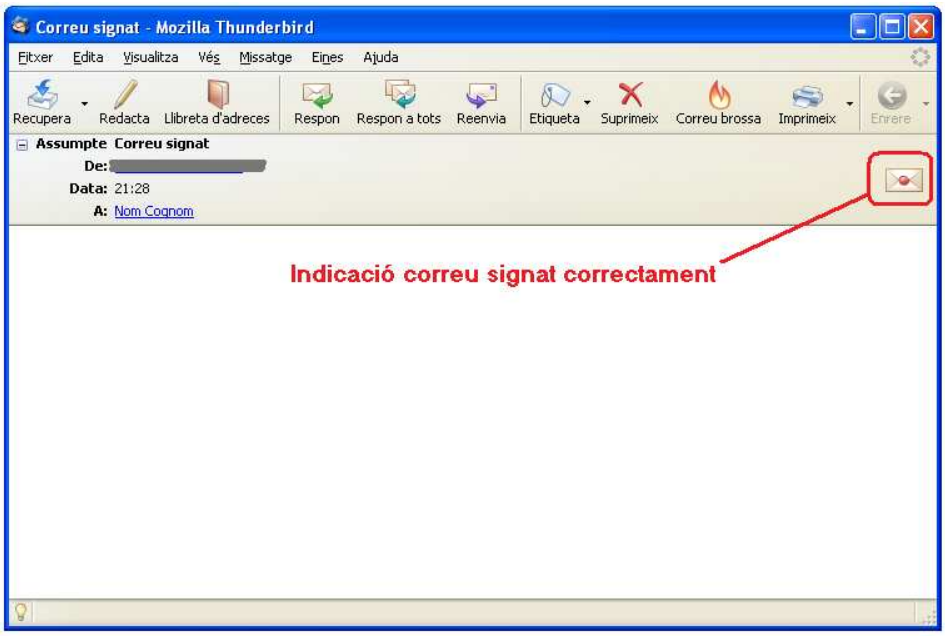

Figura 31. Correu electrònic signat i confiable

En fer doble clic sobre la icona s'obre el quadre *"Seguretat del missatge"* que ens aporta detalls sobre la seguretat del missatge, tal i com es pot veure a la figura 32.

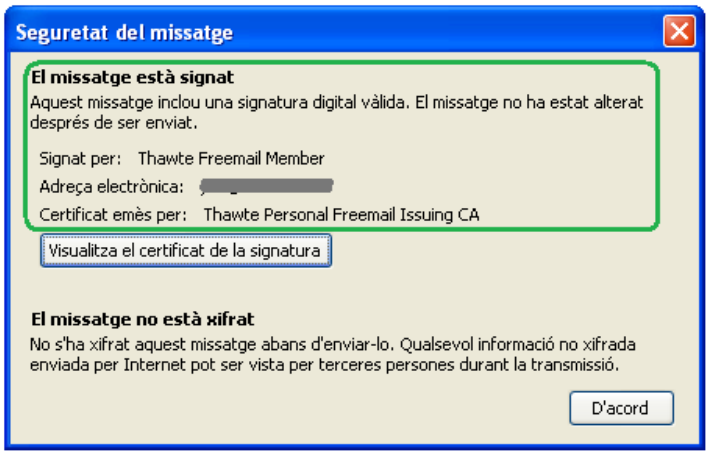

Figura 32. Quadre *"Seguretat del missatge"*

En cas de que vulguem visualitzar més dades sobre el certificat de la signatura, s'ha de fer clic sobre el botó "*Visualitza el certificat de la signatura*" (pas 1) fent que s'obri el quadre *"Visualitzador de certificats:"*. Aquí podrem visualitzar totes les dades del certificat (pas 2), tal i com es pot veure a la figura 33.

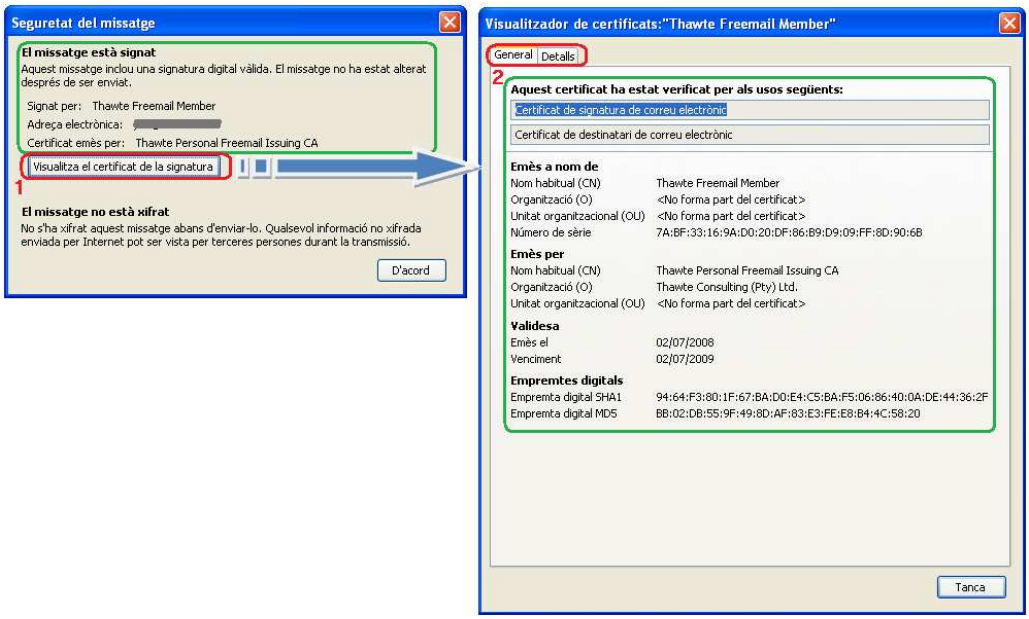

Figura 33. Visualitzar les propietats del certificat.

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 o a sigut considerat no vàlid, apareix a la part dreta del missatge la icona  (figura 34).

Figura 34. Recepció de missatges amb signatura no vàlida.

En fer doble clic sobre la icona s'obre el quadre *"Seguretat del missatge"* que ens aporta detalls sobre la seguretat del missatge, tal i com es pot veure a la figura 35.

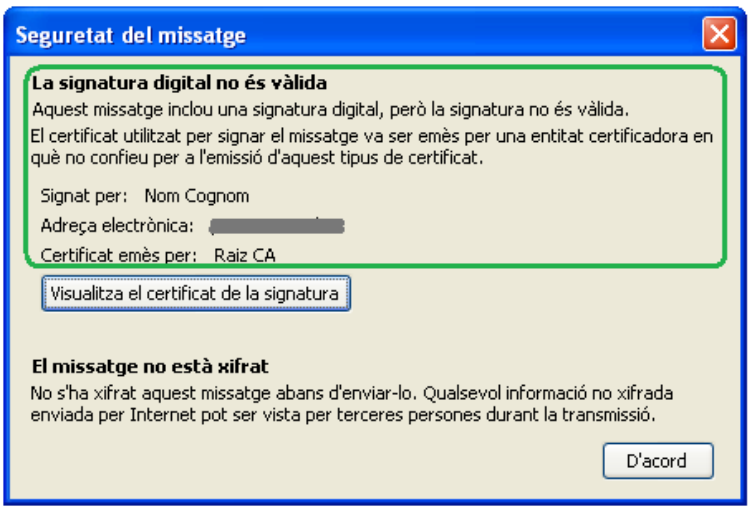

Figura 35. Quadre *"Seguretat del missatge"*

En cas de que vulguem visualitzar més dades sobre el certificat de la signatura, s'ha de fer clic sobre el botó "*Visualitza el certificat de la signatura*" (pas 1) fent que s'obri el quadre *"Visualitzador de certificats:"*. Aquí podrem visualitzar totes les dades del certificat (pas 2), tal i com es pot veure a la figura 36.

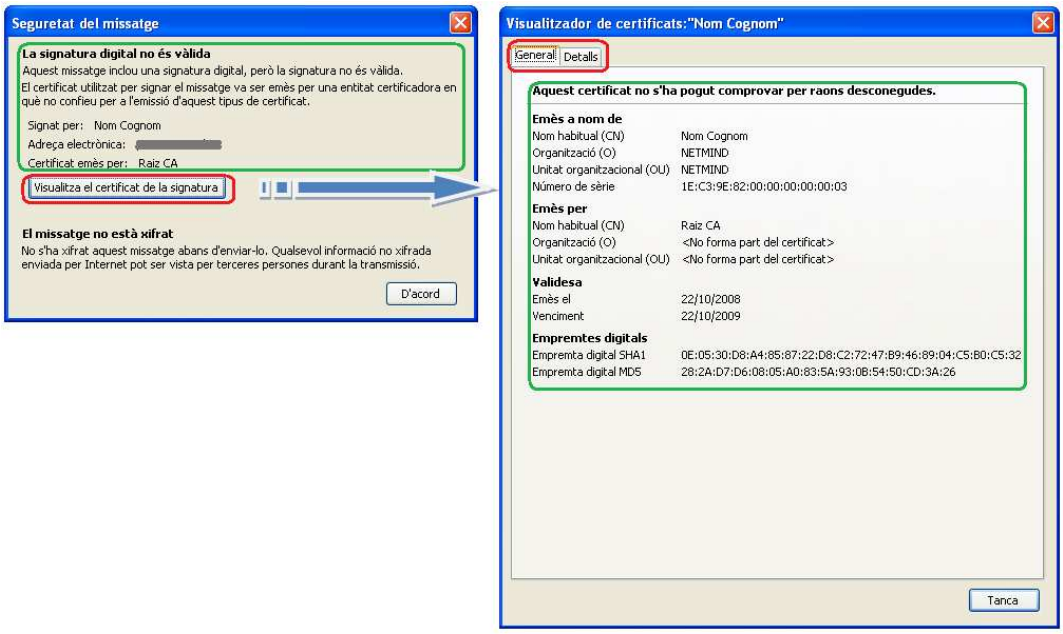

Figura 36 Visualitzar les propietats del certificat.

5.2 Xifrats

Per poder llegir un missatge xifrat, el gestor de correu ha de tenir accés a la nostra clau privada de xifratge emmagatzemada al carnet universitari. Això implica que quan arriba un correu xifrat, es demana el codi NIP o PIN del carnet universitari.

Si el carnet universitari no està inserit al lector, o no s'indica el pin correcte, no es podrà llegir el missatge i es mostrarà un missatge d'error, tal i com es pot veure a la figura 37.

També es pot reconèixer per la icona  que surt a la dreta del correu electrònic rebut (figura 37).

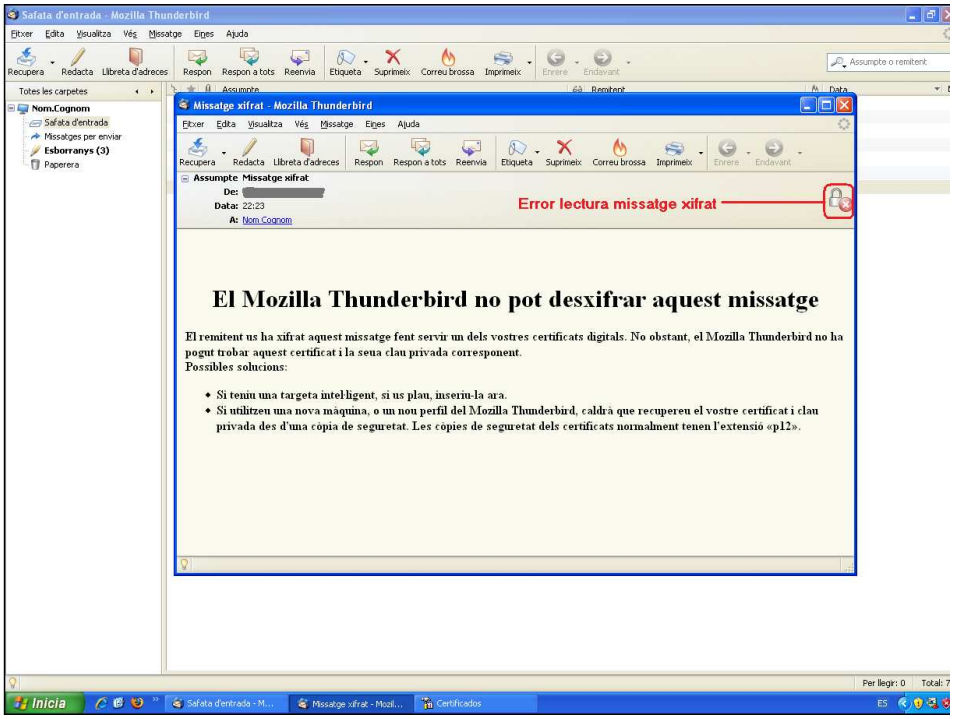

Figura 37. Error lectura missatge xifrat

Si es fa doble clic a l'icona de la clau, apareix la informació de seguretat del missatge de la figura 37.

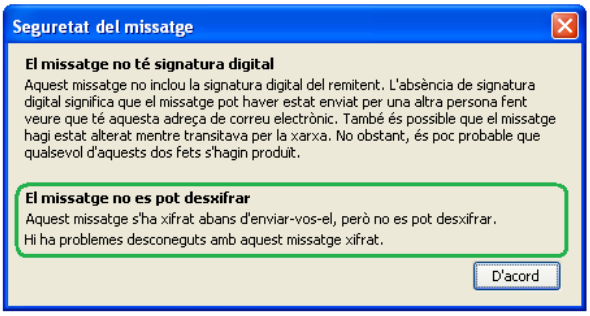

Figura 38. Quadre *"Seguretat del missatge"*

Si nosaltres som la persona a la que va destinat aquest correu i tenim accés a la nostra clau privada de xifratge emmagatzemada al carnet universitari, en fer doble clic, es podrà obrir i llegir sense cap problema. Aquest correu es pot identificar que està xifrat per que apareix l'icona de la clau a la part dreta del missatge, tal i com es pot veure a la figura (figura 39).

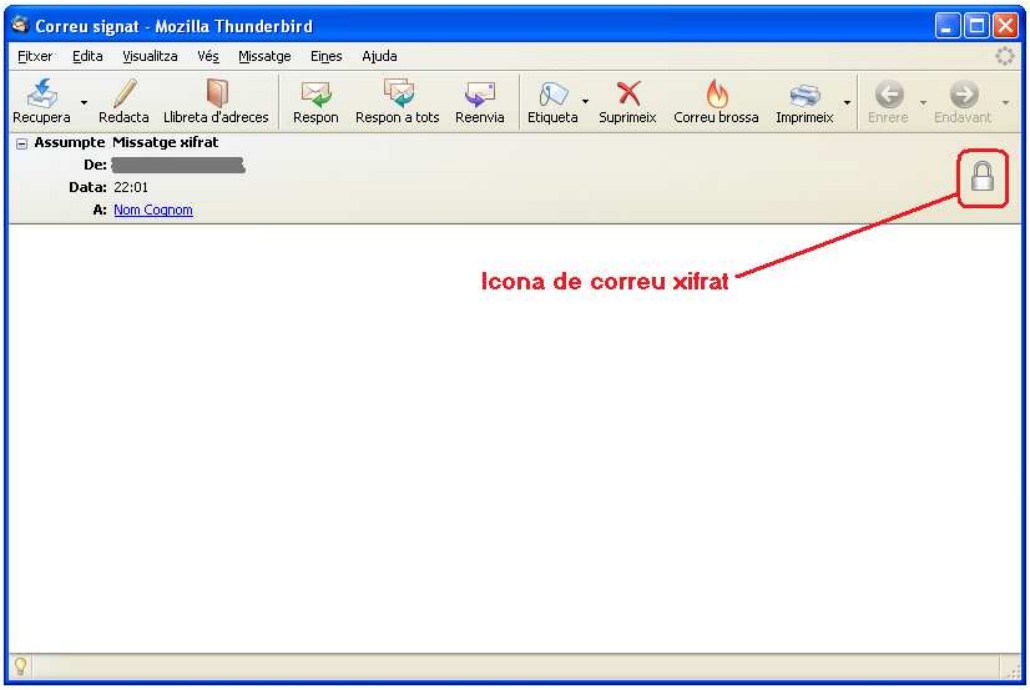

Figura 39. Quadre *"Seguretat del missatge"*

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