



PROJECTE: Manuals d'ús de signatura electrònica	Versió: 1.5
TÍTOL: Signatura electrònica amb IBM Lotus Notes 7 i MS Windows Vista	Codi Referència:
RESUM:	Data Publicació: 19/11/2008

PROCEDIMENT

Signatura electrònica amb IBM Lotus Notes 7 i MS Windows Vista

PREPARAT PER:	REVISAT PER:	APROVAT PER:
Nom:	Nom:	Nom:
Data: 19/11/2008	Data:	Data:

PROJECTE: Manuals d'ús de signatura electrònica	Versió: 1.5
TÍTOL: Signatura electrònica amb IBM Lotus Notes 7 i MS Windows Vista	Codi Referència:
RESUM:	Data Publicació: 19/11/2008

[illegible]

ÍNDIX

1	Objectiu i abast	4
2	Prerequisits	4
3	Configuració de signatura electrònica amb IBM Lotus Notes 7 i Windows Vista.....	5
4	Enviament de missatges	13
4.1	Signats.....	13
4.2	Xifrats.....	18
5	Recepció de missatges	20
5.1	Signats.....	20
5.2	Xifrats.....	23
6	Referències.....	24

1 Objectiu i abast

El present document té per objectiu descriure el procés de configuració del client de correu electrònic Lotus Notes 7 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 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 IBM Lotus Notes 7 i Windows Vista

- 3.1 Per configurar la signatura electrònica per utilitzar-la amb l'eina IBM Lotus Notes 7, s'ha d'obrir l'aplicació, accedir al menú "Fitxer" (pas 1), fer clic a "Seguretat" (pas 2) i finalment fer clic a l'opció "Seguretat de l'usuari..." del menú emergent (pas 3) tal i com es pot veure a la figura 1.

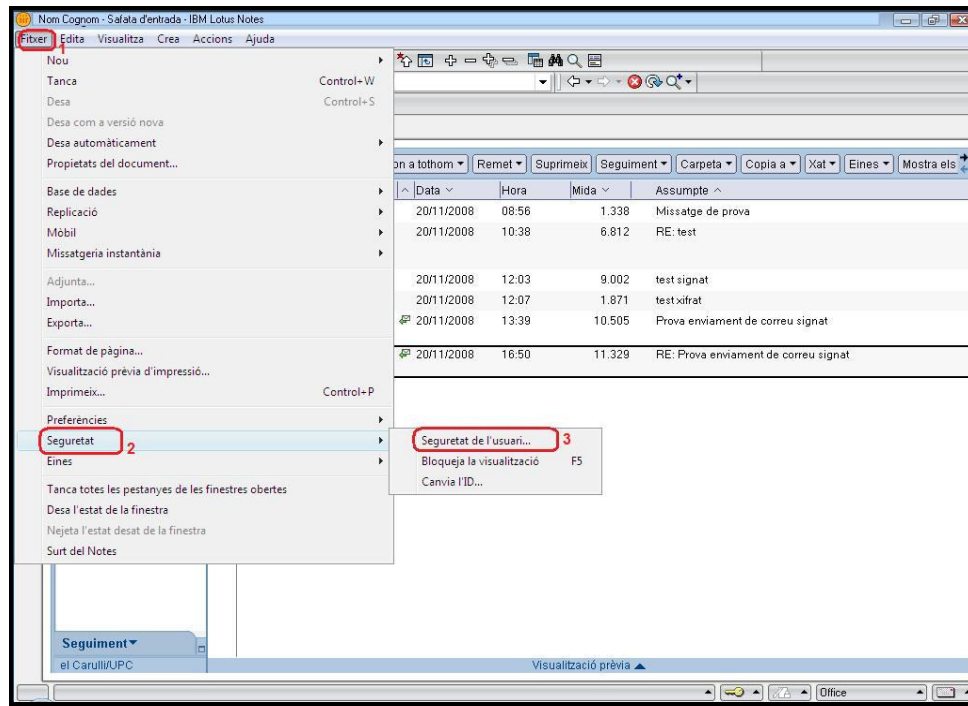


Figura 1. Finestra de l'eina IBM Lotus Notes 7

- 3.2 Un cop obert el quadre "Seguretat de l'usuari..." (figura 2) s'ha de fer clic a la pestanya "La vostra identitat" (pas 1) i a continuació a l'opció "La vostra targeta intel·ligent..." (pas 2) aquí heu de configurar el vostre lector de targeta xip per poder signar els correus mitjançant el certificat digital emmagatzemat al carnet universitari.

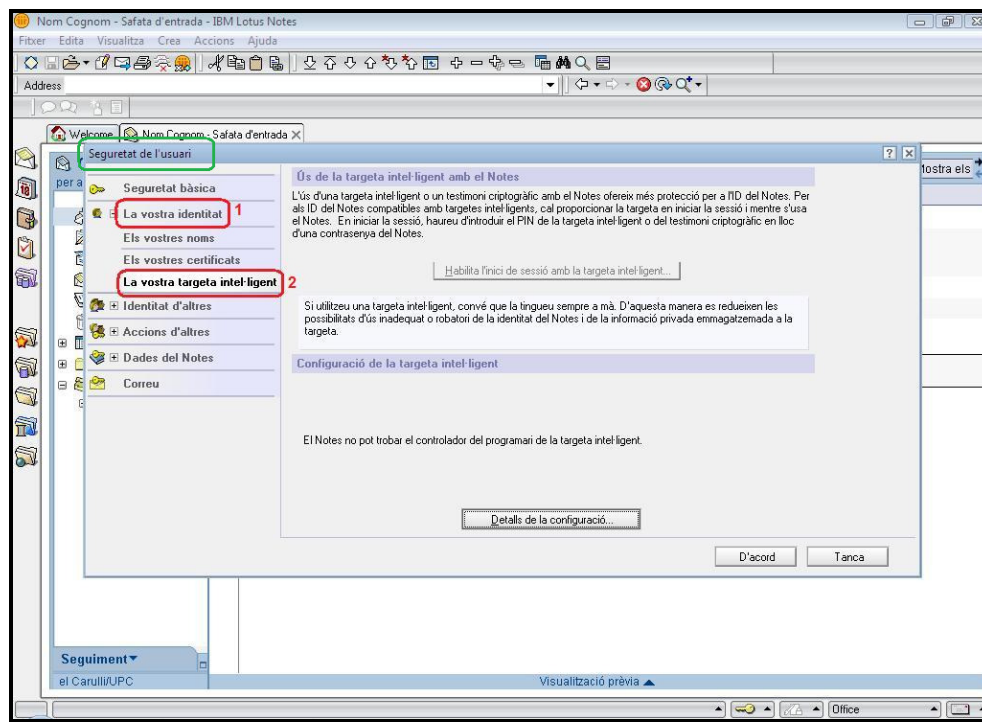


Figura 2. Opcions de seguretat

- 3.3 Si no existeix cap targeta intel·ligent configurada, demanarà que indiqueu l'emplaçament del fitxer per utilitzar-la. Al quadre de text "Fitxer controlador de la targeta intel·ligent" s'ha d'introduir la següent ruta d'arxius (pas 1) "C:\Archivos de programa\Gemalto\Classic Client\BIN\gclib.dll" (figura 3). I a continuació escollir "Continua..." (pas 2)

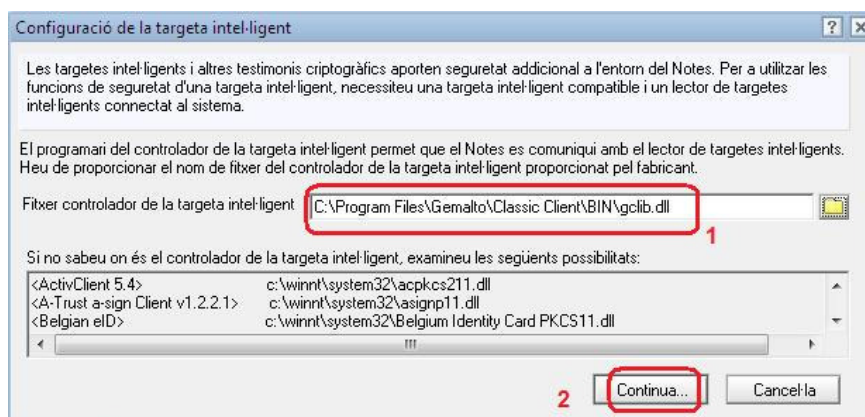


Figura 3. Configuració Targeta Intel·ligent

- 3.4 Una vegada detectada, veurem la identificació de la targeta a la pantalla “Seguretat de l’usuari” (pas 1 de la figura 4). A continuació acceptarem les dades prement el botó “D’acord” (pas 2 de la figura 4).

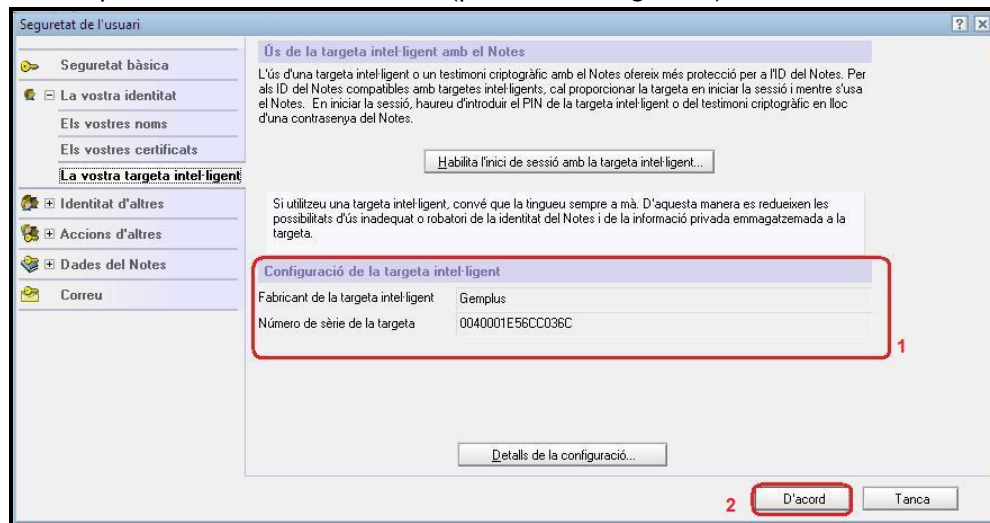


Figura 4. Configuració de targeta intel·ligent finalitzada

NOTA: No s’ha d’activar la opció “Habilita l’inici de sessió amb la targeta intel·ligent”, sense contacta abans amb els administradors del sistema, perquè podria causar el bloqueig permanent de l’accés al IBM Lotus Notes.

- 3.5 Un cop creada la configuració de seguretat per utilitzar la targeta xip, tornarem al menú “Fitxer” (pas 1 de la figura 5), i en la opció “Preferències” (pas 2 de la figura 5), hem d’escollir “Preferències de l’usuari” (pas 3 de la figura 5).

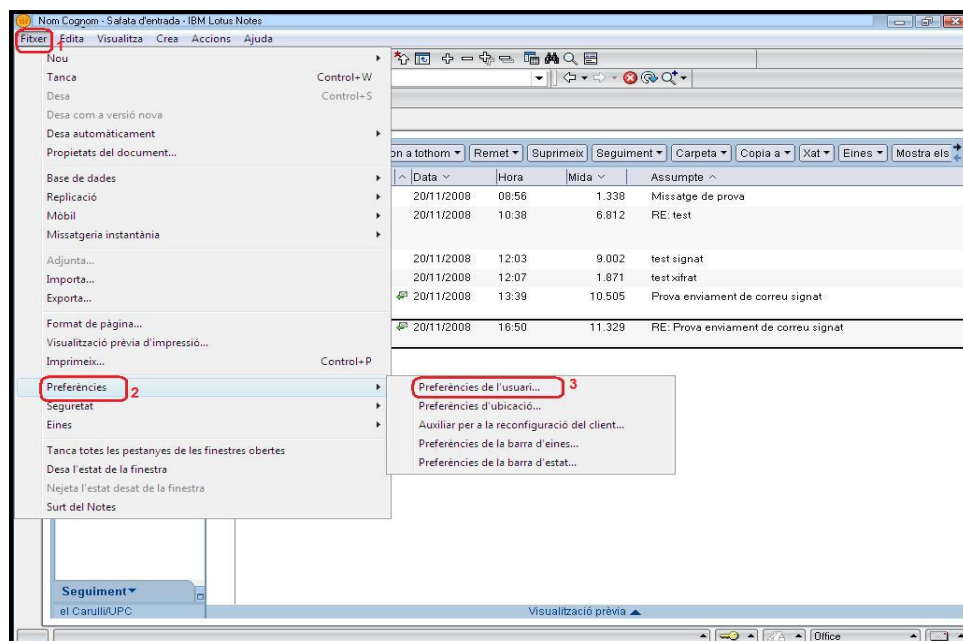


Figura 5. Ús de la signatura digital pels missatges de sortida

- 3.6 Un cop a la finestra de “*Preferències de l'usuari*”, s’ha de seleccionar l’opció “*General*” (pas 1 de la figura 6) dintre de la secció “*Correu*” i finalment marcar la casella de verificació “*Signa el correu que s’envii*” (pas 2 de la figura 6). D’aquesta forma activarem la signatura digital per defecte en TOTS els missatges de correu electrònic que envieu mitjançant IBM Lotus Notes 7. Fent clic al botó “*D’acord*” (pas 3 de la figura 6) l’aplicació IBM Lotus Notes 7 restarà configurada per signar digitalment els missatges de correu electrònic.

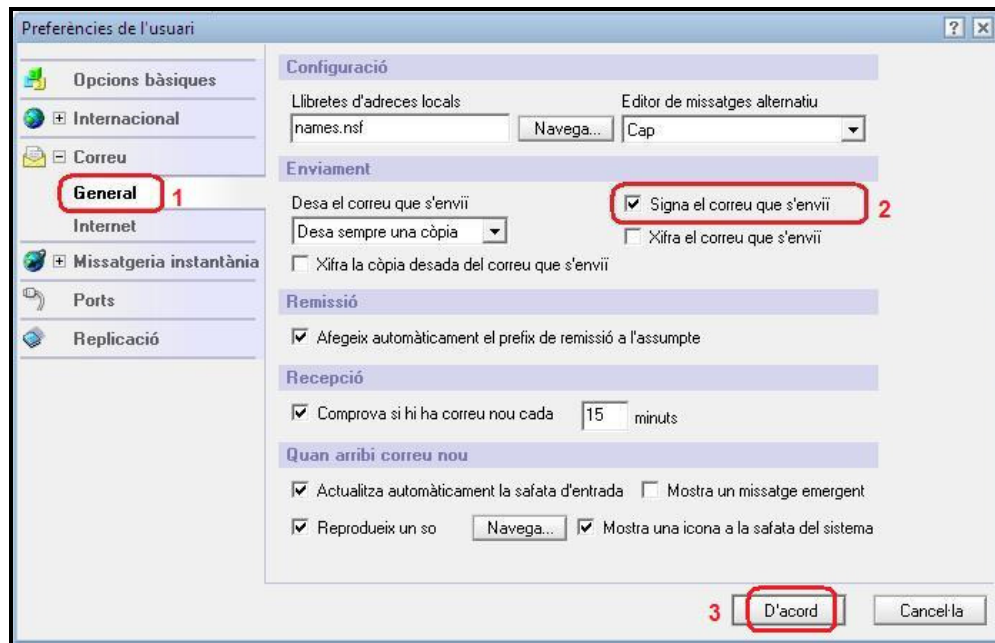


Figura 6. Ús de la signatura digital pels missatges de sortida

- 3.7 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 7.

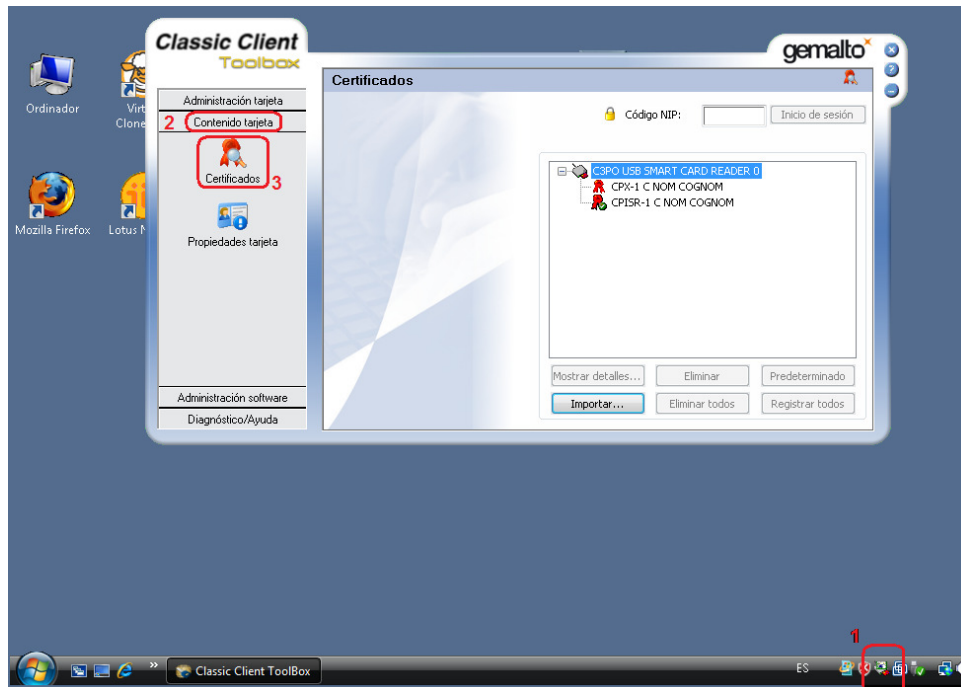


Figura 7. Propietats del certificat gemalto

- 3.8 Un cop dintre de l'apartat "*Certificados*" figura 7, 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 8.

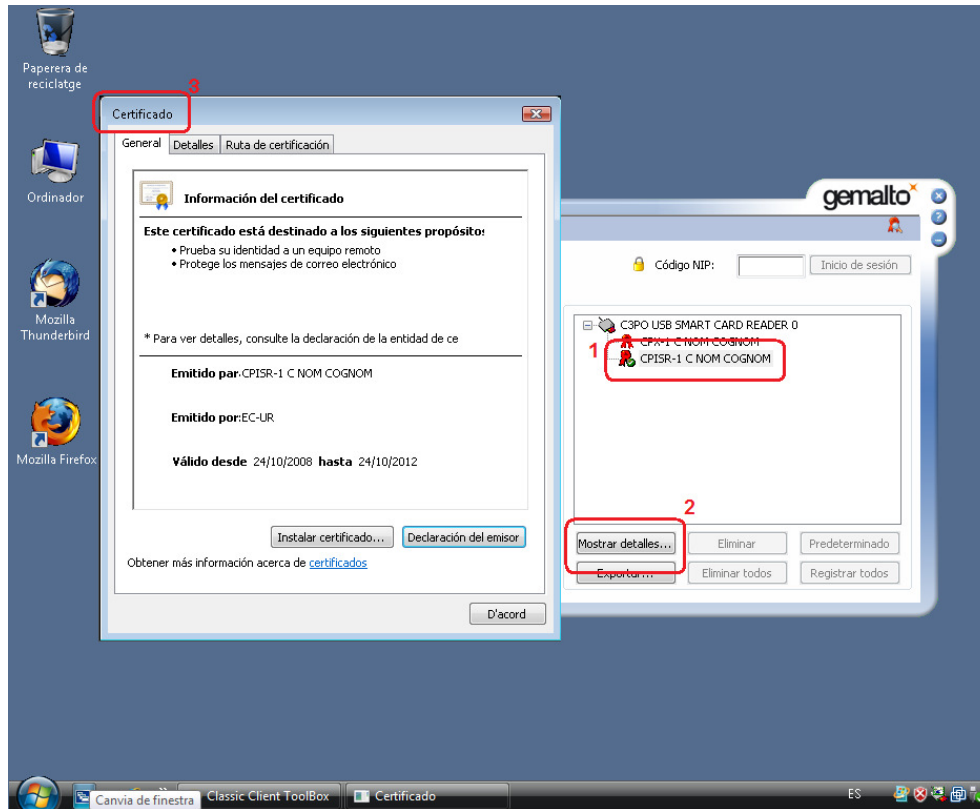


Figura 8. Propietats del certificat

3.9 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 9.

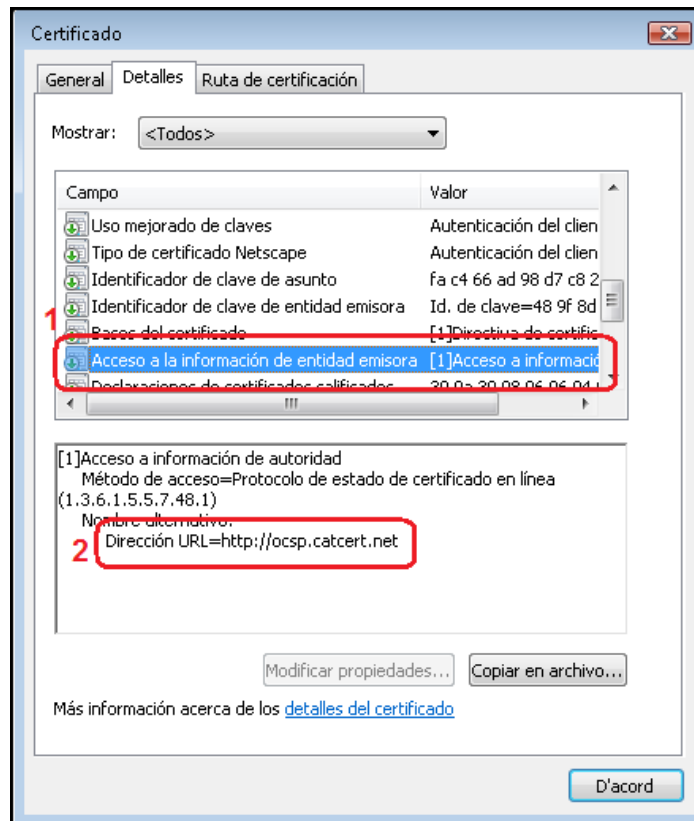


Figura 9. Propietats del certificat.

- “Puntos de distribución CRL” (pas 1) on ens indica les direccions url <http://epsd.catcert.net/crl/ec-ur.crl> i <http://epsd2.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 10.

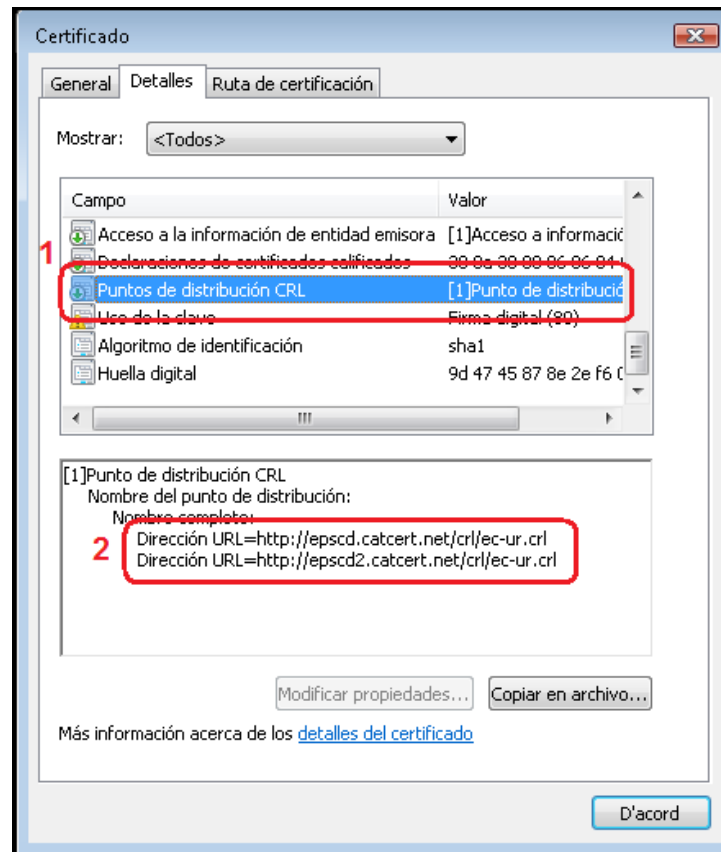


Figura 10. Propietats del certificat.

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 els missatges de correu de sortida com a opció per defecte (veure punt 3.6 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 a la casella de verificació "Signa" tal i com es pot apreciar a la figura 11.

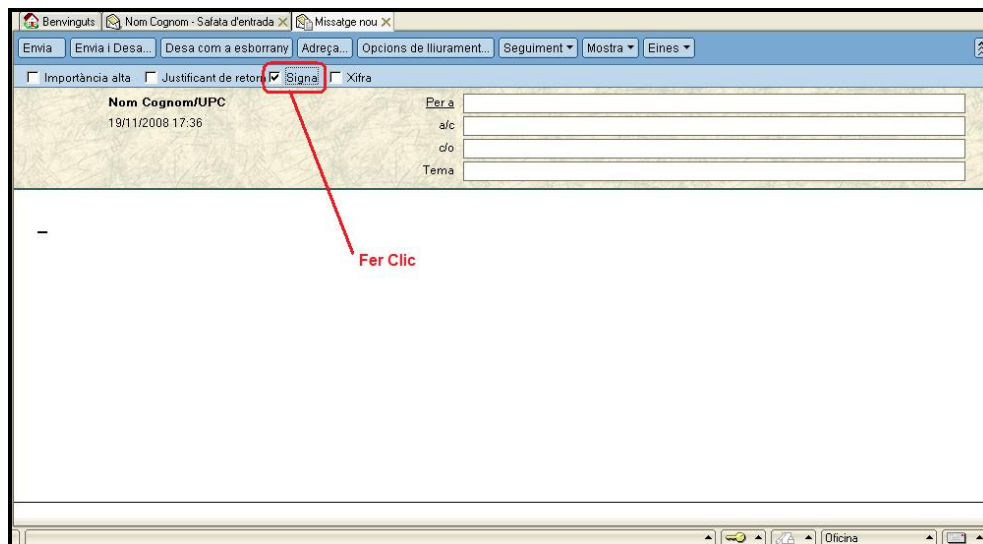


Figura 11. Activar l'enviament de correus signats

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 12). S'ha d'introduir el numero (pas 1) i fer clic al botó "D'acord" (pas 2).

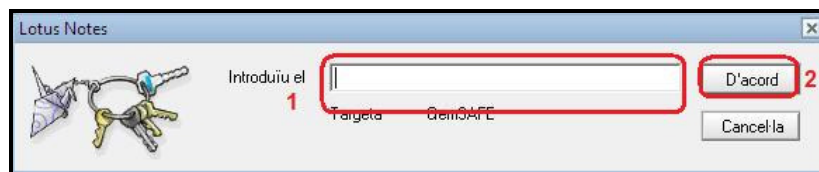


Figura 12. Introducció de número d'identificació personal del carnet universitari (NIP o PIN)

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

- 4.1.3 Un cop introduït el número d'identificació personal del carnet universitari (NIP o PIN) explicat a l'apartat anterior, es sol·licitarà escollir el certificat a utilitzar per signar aquest missatge (pas 1 de la figura 13), enviant després el correu signat una vegada fem clic al botó "D'acord" (pas 2 de la figura 13).

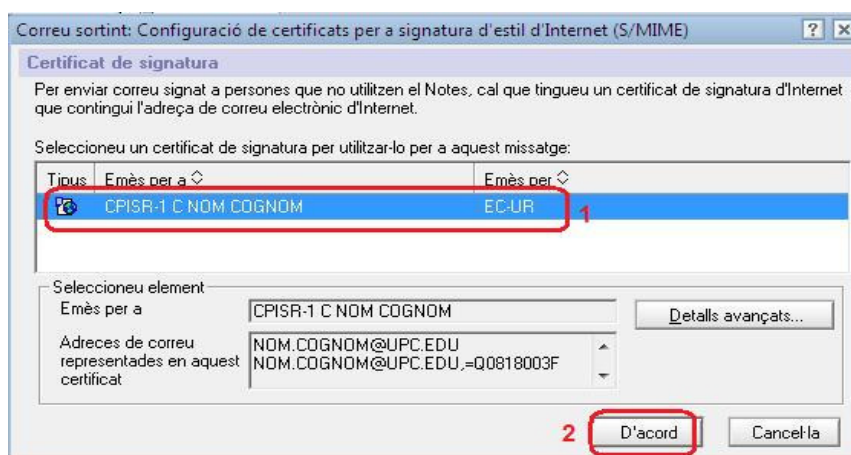


Figura 13. Selecció de certificats per enviament de correu signat

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 el certificat no és 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_esberrany/programari-certificat-digital/Guia_Basica_Instalacio.pdf/view

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 podrà encontrar en la direcció 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 Lotus Notes 7, s'ha d'obrir l'aplicació, accedir al menú "Eines" (pas 1) i fer clic a "Preferències..." (pas 2). A continuació s'obrirà el quadre "Preferències..." (pas 3) tal i com es pot veure a la figura 14.

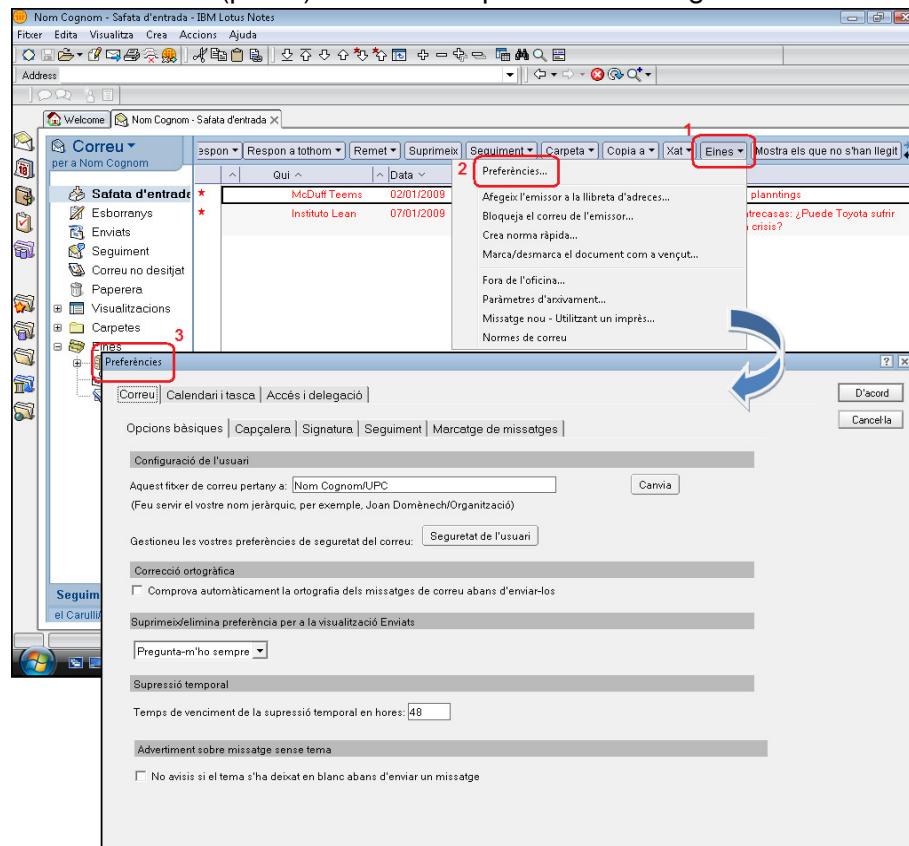


Figura 14. Preferències de correu

4.1.4.1.2 Un cop al quadre “*Preferències...*”, cal fer clic a la fitxa “*Signatura*” (pas 1). Per poder adjuntar la signatura al correu, caldrà fer clic a la casella de verificació “*Afegeix automàticament una signatura a la part final dels meus missatges de correu de sortida*” (pas 2) i a continuació afegir la signatura utilitzant l’opció “*Text*” o “*Fitxer HTML o d’imatges*” tal i com es pot veure a la figura 15.

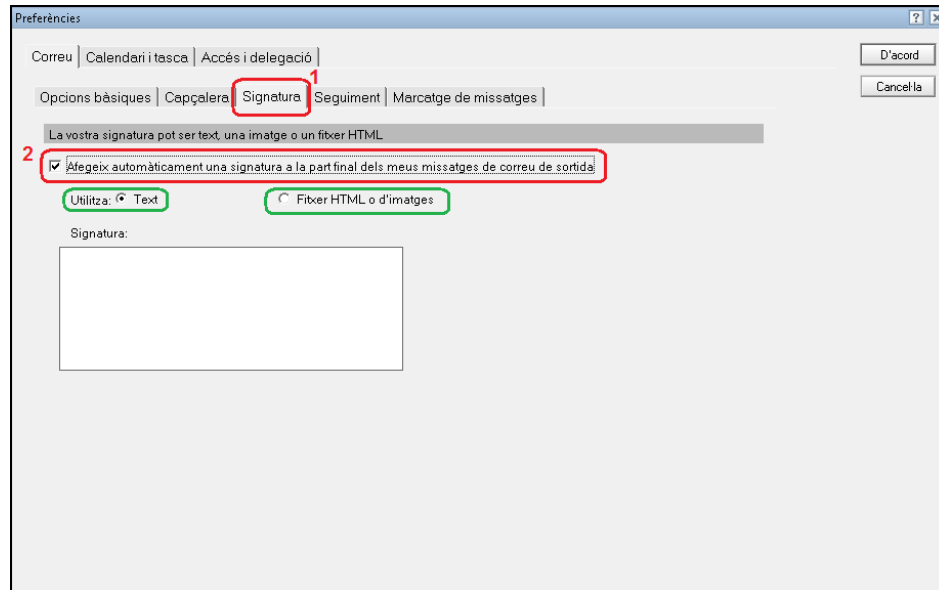


Figura 15. Opcions de format de correu

4.1.4.1.3 Per finalitzar aquest procés, cal inserir la signatura recomanada a l’apartat 4.1.4 al quadre “*Signatura:*” (pas 1) utilitzant l’opció “*Text*” i seleccionar “*D’acord*” (pas 2) per que els canvis es dugin a terme tal i com es pot apreciar a la figura 16.

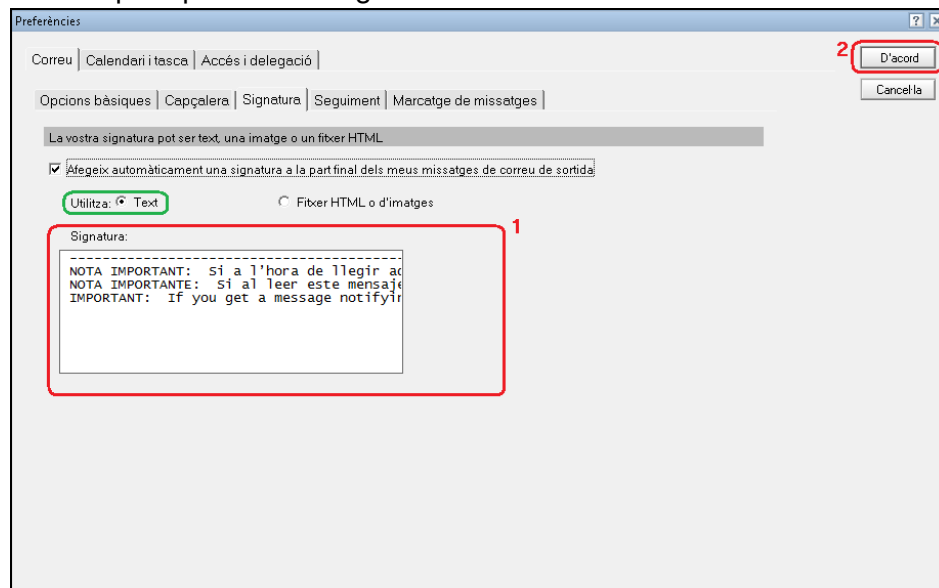


Figura 16. Inserir signatura

4.1.4.1.4 Per poder definir la signatura de correu utilitzant l'opció “Fitxer HTML o d’imatges”, cal seleccionar l’opció “Fitxer HTML o d’imatge” (pas 1 de la figura 17) i fer clic al botó “Navega...” (pas 2 de la figura 17) on es podrà seleccionar el fitxer HTML o l’imatge que té com a contingut la signatura recomanada a l’apartat 4.1.4.

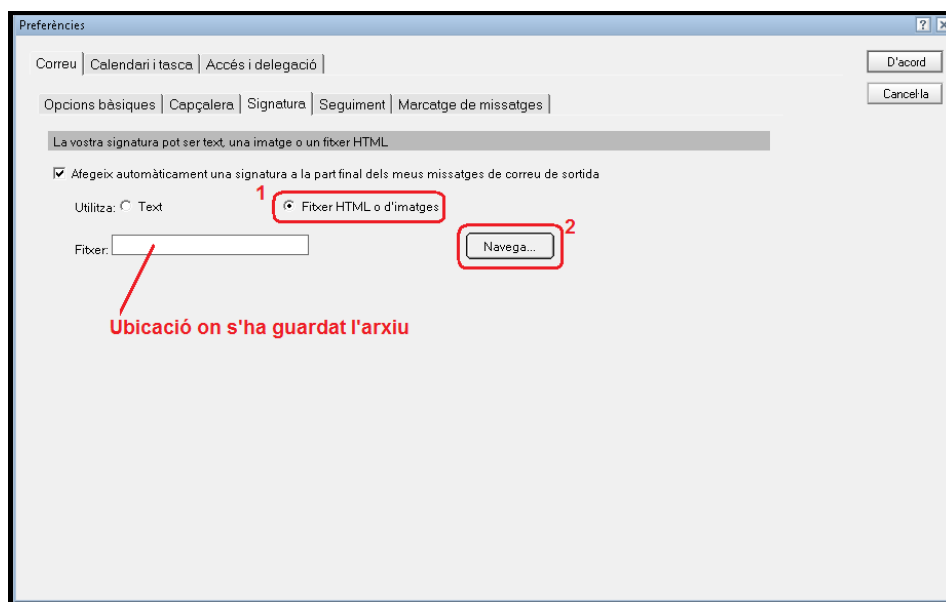


Figura 17. Inserir signatura en el mode fitxer HTML o d’imatges

NOTA: Abans de poder inserir la signatura tal i com s’especifica a l’apartat anterior, es necessari copiar el text recomanat a l’apartat 4.1.4 en format HTML o copiar-lo com una imatge i desar-ho en el vostre equip.

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 us 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 a la casella de verificació “Xifra” tal i com es pot apreciar a la figura 18.

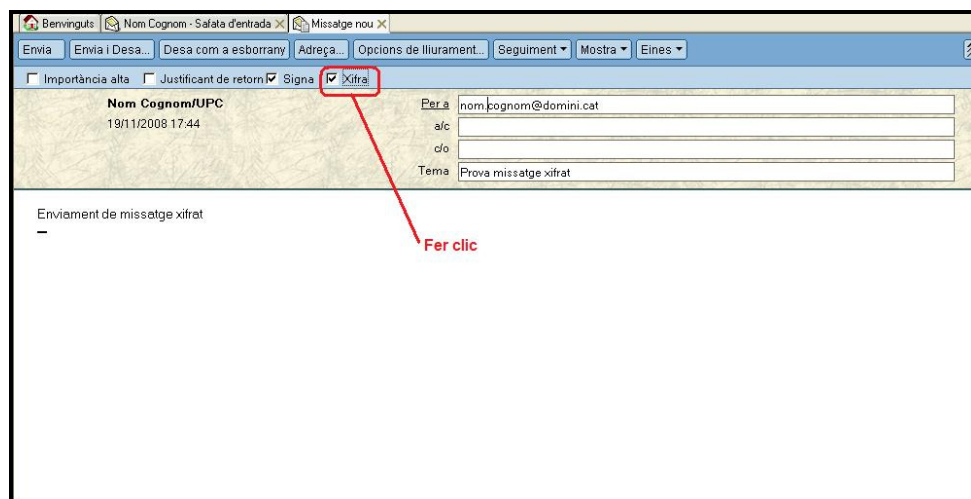


Figura 18. Activar l'enviament de correus xifrats

4.2.2 Al prémer el botó “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.

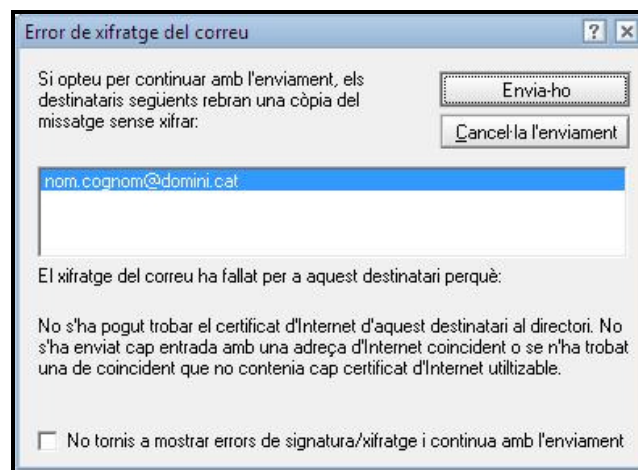


Figura 19. Problemes de xifratge

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

NOTA: Si l'usuari pertany a la mateixa organització la clau pública estarà emmagatzemada al servidor i no caldrà realitzar aquest procés.

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 seleccionar-lo i fer clic dret sobre el missatge. A continuació seleccionar la opció *"Afegeix l'emissor a la llibreta d'adreces..."* del menú contextual. D'aquesta manera, el client de correu Lotus Notes 7 tindrà disponible de forma automàtica la clau pública del certificat per utilitzar-la en el enviament de correu xifrat a aquest destinatari.

5 Recepció de missatges

5.1 Signats

En el cas de rebre correus signats digitalment, es poden reconèixer per la icona



que surt a sota a la dreta del correu electrònic rebut (figura 20).

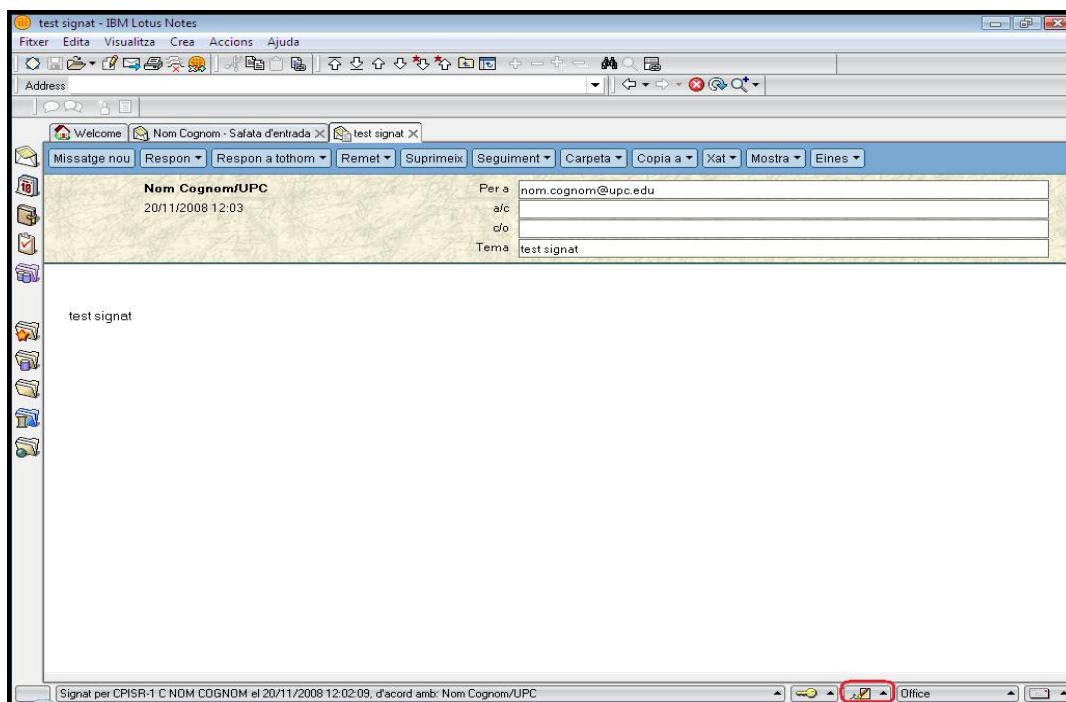


Figura 20. Recepció de correu electrònic signat

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

Si no hi ha cap tipus de conflicte amb les claus públiques de l'emissor o el certificat utilitzat per signar el correu rebut, es podrà obrir el missatge rebut sense cap missatge per part del client de correu Notes.

5.1.2 Recepció de missatges signats amb les claus públiques de NO l'emissor 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 21.

En obrir el nou missatge rebut, ens dona la opció de generar un certificat encreuat que validi l'usuari que ens a enviat el correu signat. D'aquest forma restarà emmagatzemat a la llibreta d'adreces i es podrà utilitzar mes endavant per envia correus xifrats (pas 1 de la figura 21).

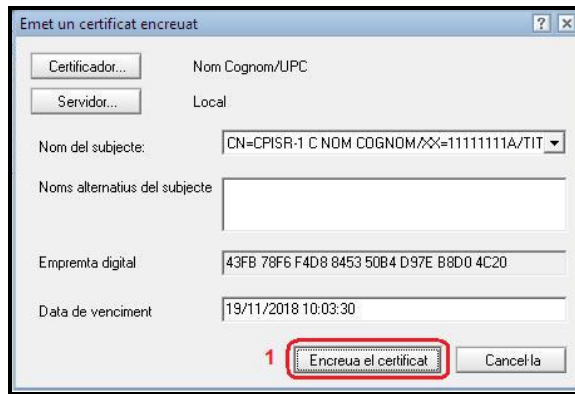


Figura 21. Emetre certificat encreuat

En cas de que vulguem veure les propietats de la signatura del correu electrònic rebut, s'ha d'accedir al menú "Fitxer" (pas 1), fer clic a "Seguretat" (pas 2) i seleccionar del menú contextual l'opció "Seguretat de l'usuari..." (pas 3) tal i com es pot veure a la figura 22.

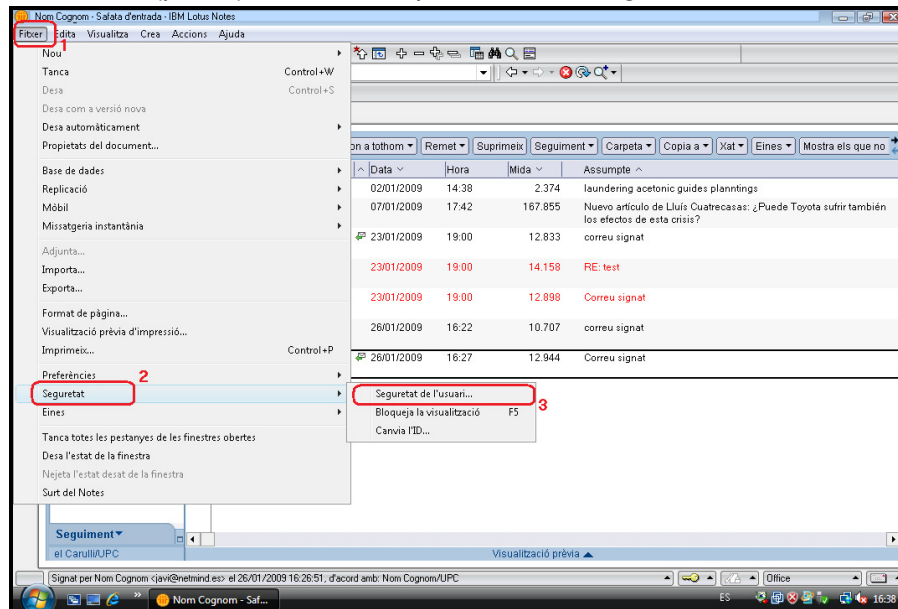


Figura 22. Visualitzar les propietats de la signatura digital

Al fer clic, s'obrirà el quadre de diàleg “Seguretat de l'usuari”. S'ha de seleccionar l'opció del panell esquerre “Identitat d'altres” (pas 1) i a continuació “Persones, Serveis” (pas 2). Seleccionant la opció “Mostrar tots els que hi hagi a la llibreta d'adreces” (pas 3), fent clic a un certificat (pas 4) i a continuació al botó “Detalls sobre la confiança” (pas 5) podrem visualitzar les propietats de la signatura digital. Tal i com es pot veure a la figura 23.

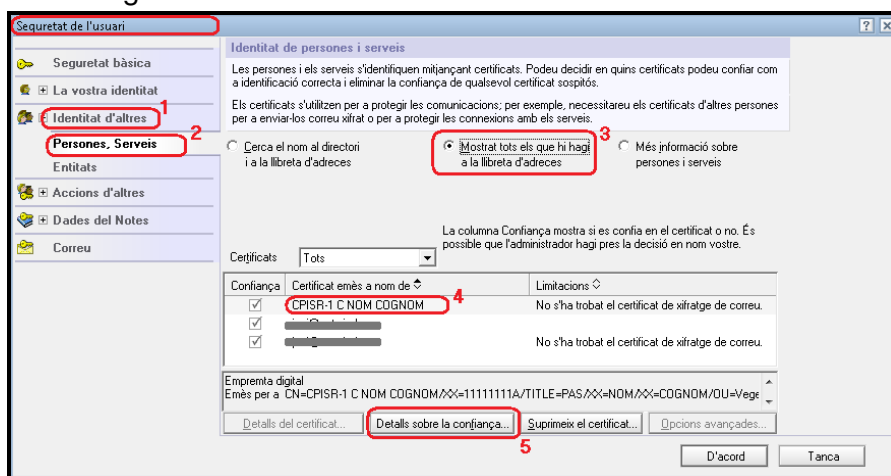


Figura 23. Visualitzar les propietats de la signatura digital

5.2 Xifrats

En el cas de rebre correus xifrats, es poden reconèixer per la icona  que surt a sota a la dreta del correu electrònic rebut (figura 24).

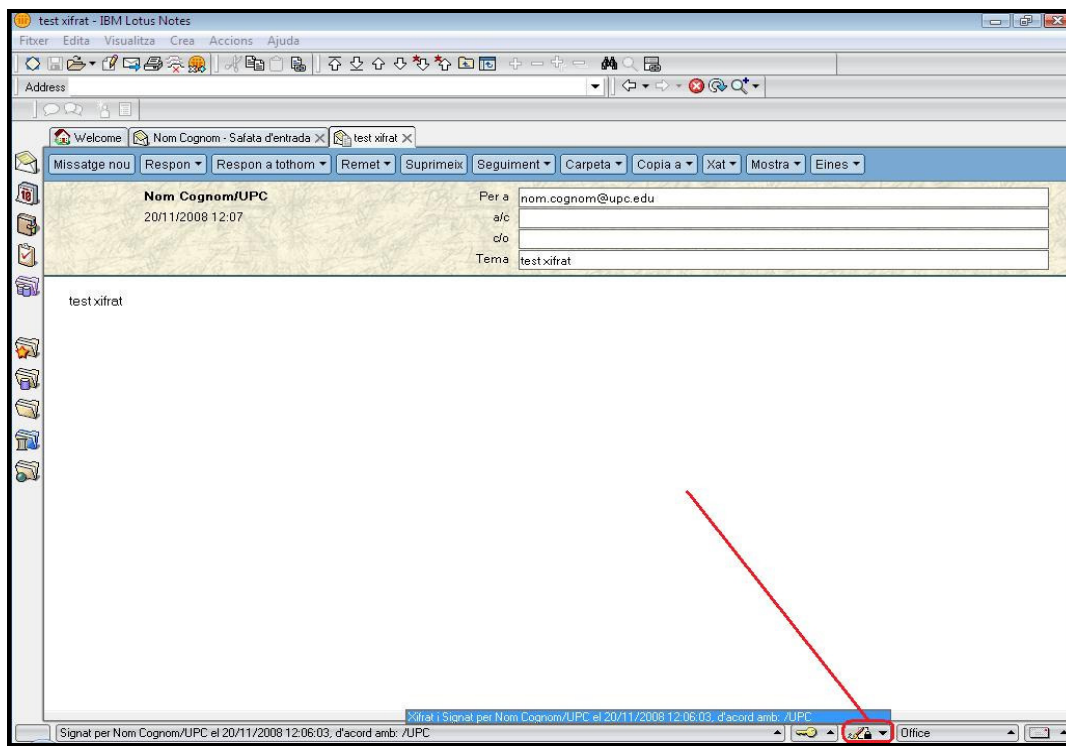


Figura 24. Recepció de missatge xifrat

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 24).

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>