UNIVERSITAT ROVIRA I VIRGILI

Ús de la signatura electrònica amb Mozilla Thunderbird 2.0

Servei de Recursos Informàtics i TIC

UNIVERSITAT ROVIRA I VIRGILI

Sumari

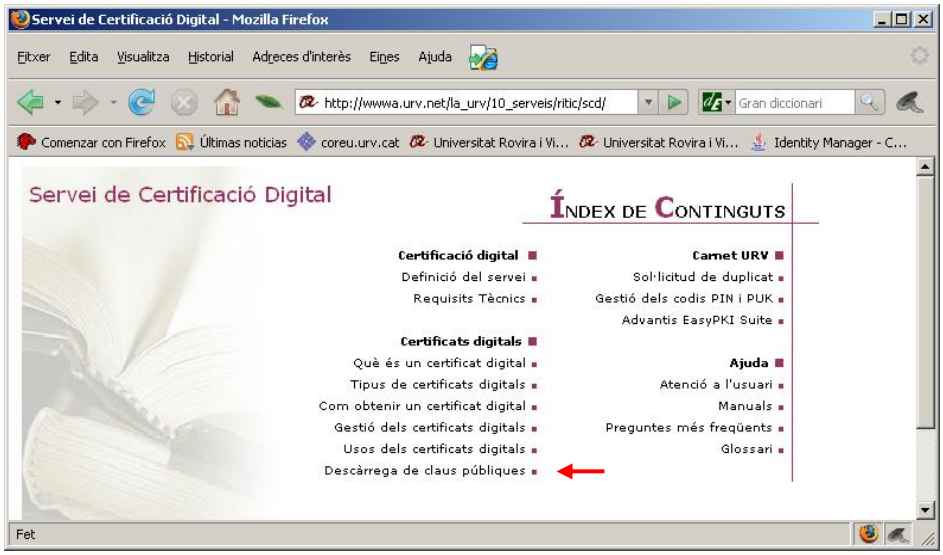
Objectius del document

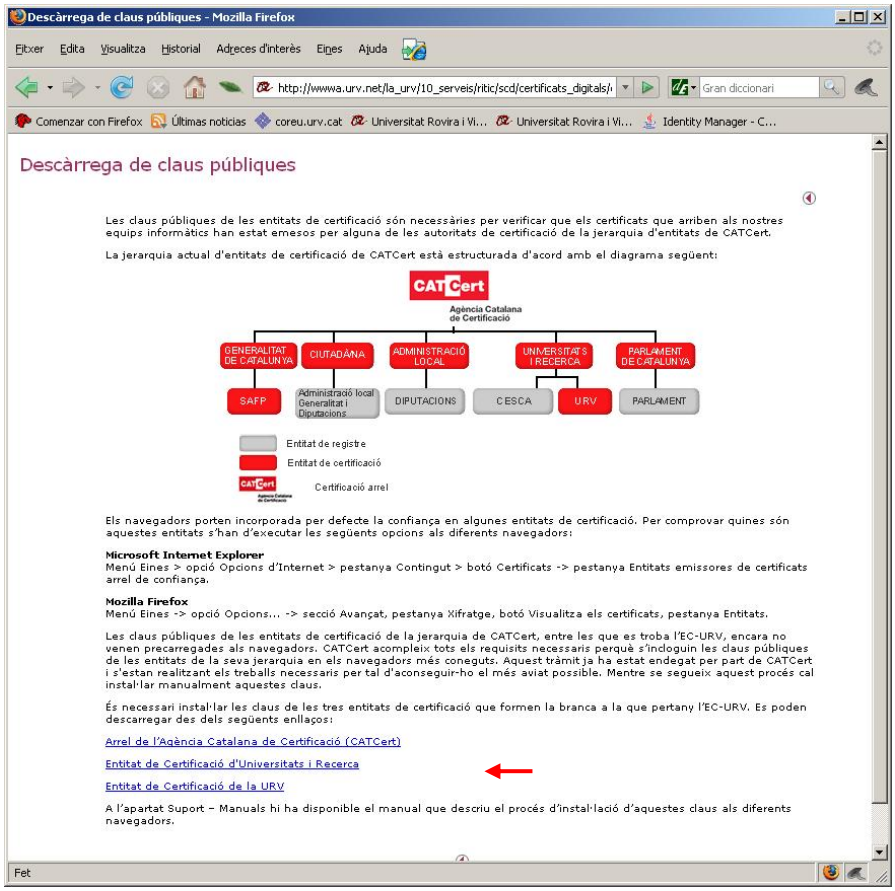
El present document descriu el procés de configuració del gestor de correu Mozilla Thunderbird 2.0 per poder enviar correus signats i/o xifrats digitalment mitjançant els certificats digitals que emet l'entitat de certificació de la Universitat Rovira i Virgili; així com el procés d'enviament i recepció de missatges signats i/o xifrats digitalment.

Instal·lació de les claus públiques en el Thunderbird

És necessari instal·lar les claus públiques de les entitats de certificació en el Thunderbird.

Les claus públiques es poden descarregar des de la pàgina web del Servei de Certificació Digital.





Per descarregar les claus públiques en local, cal prémer el botó dret sobre cada enllaç i escollir ***Desa l'enllaç al disc...*** del menú emergent.

Per instal·lar les claus, cal seleccionar el menú ***Eines*** -> opció ***Opcions*** -> secció ***Avançat*** -> pestanya ***Certificats*** -> botó ***Visualitza els certificats***. [Figura 1]

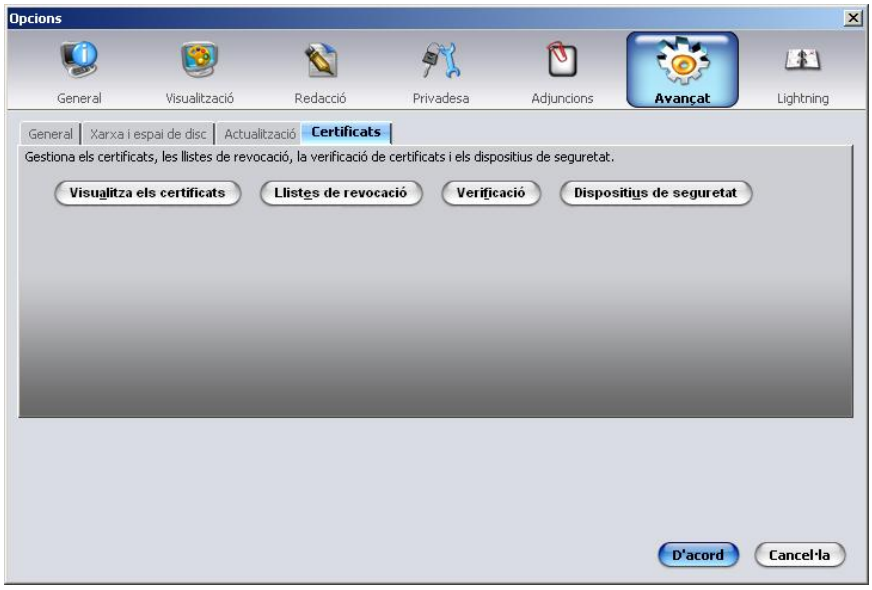


Figura 1

En la finestra ***Gestor de certificats***, seleccionar la pestanya ***Entitats*** i fer clic en el botó ***Importa***. [Figura 2]

Figura 2

Seleccionar del directori on es troben els certificats els que es vol instal·lar [Figura 3]

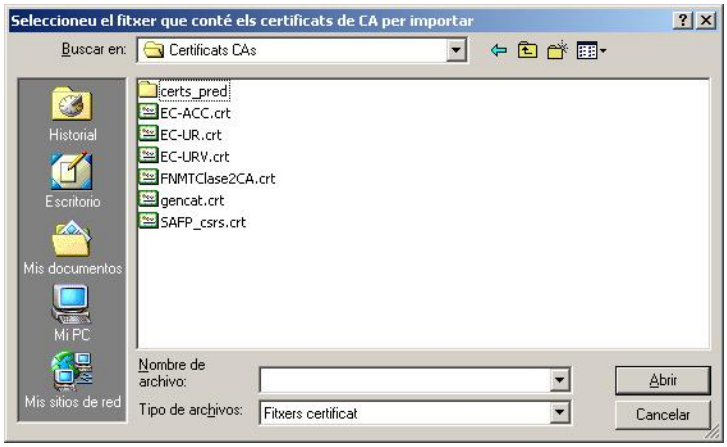


Figura 3

Per a cada certificat a importar, cal marcar totes les opcions de confiança [Figura 4]

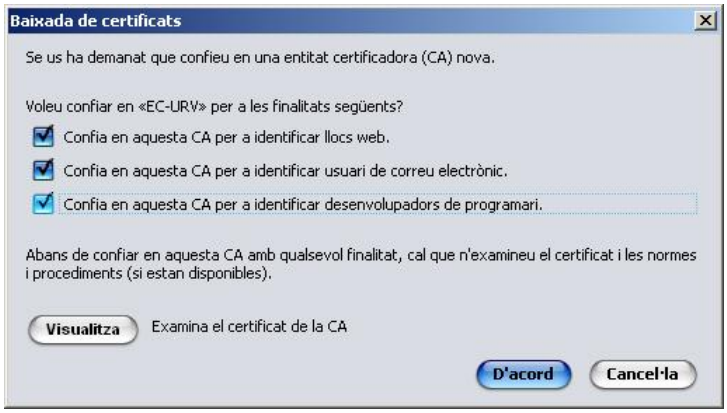


Figura 4

En acabar el procés, el gestor de certificats del Thunderbird ha de contenir tots els certificats de les entitats que s'han importat [Figura 5]

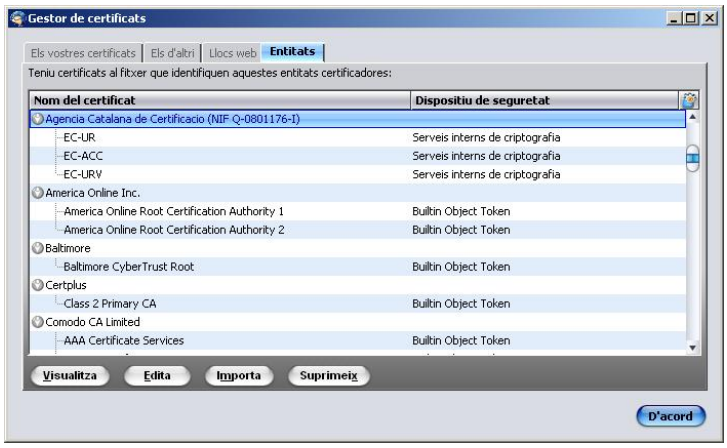


Figura 5

Configuració del client per a l'ús de certificats digitals

Configuració del "dispositiu de seguretat"

Per tal que l'Administrador de certificats del Mozilla Thunderbird pugui accedir als certificats de la targeta, cal configurar el lector de targetes criptogràfiques com a dispositiu criptogràfic de seguretat.

Per fer-ho, cal seleccionar el menú ***Eines*** -> opció ***Opcions*** -> secció ***Avançat*** -> pestanya ***Certificats*** -> botó ***Dispositius de seguretat***. [Figura 6]

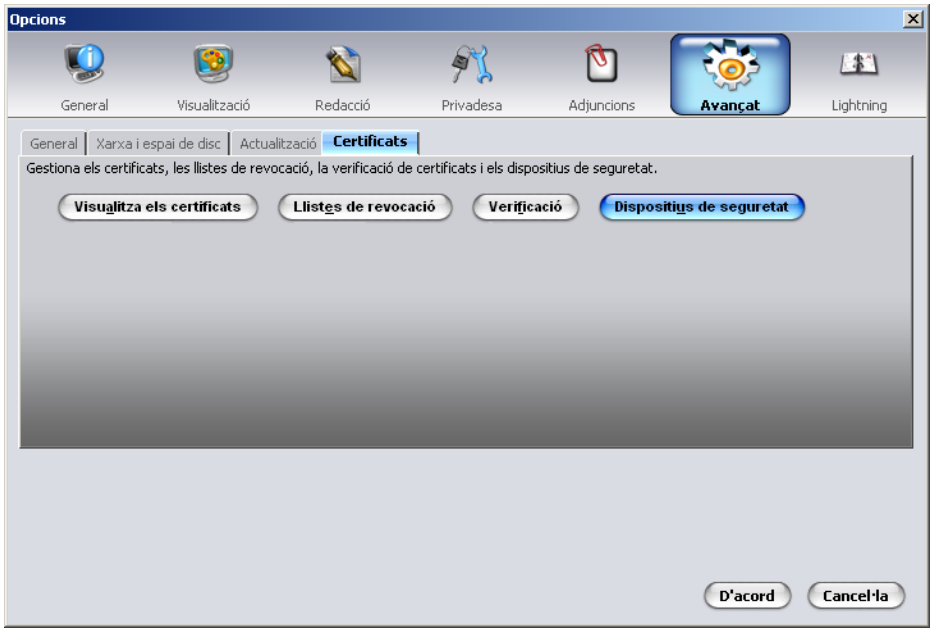


Figura 6

En la finestra ***Gestor de dispositius***, fer clic en el botó ***Carrega***. [Figura 7]

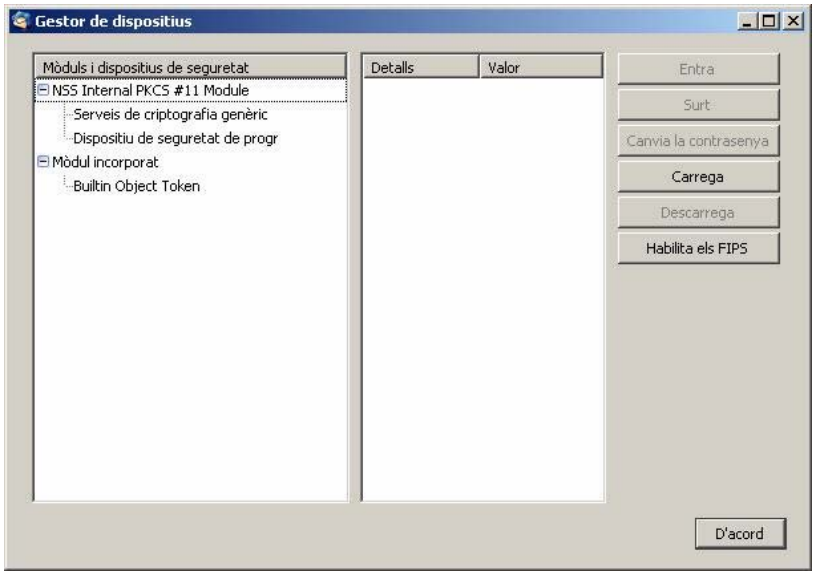


Figura 7

Introduir ***Lector URV*** com a nom del dispositiu i seleccionar el fitxer corresponent al dispositiu PKCS#11 que es troba al directori d'instal·lació de Windows (***\system32\AdvantisPKCS11.dll***). [Figura 8]

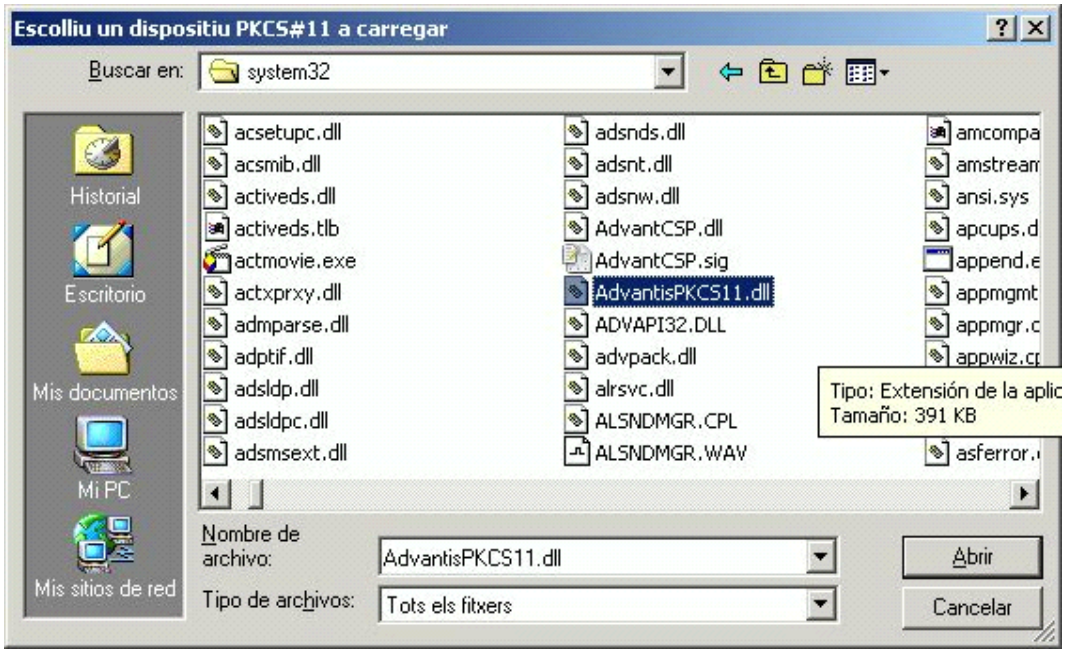


Figura 8

En la finestra ***Gestor de dispositius***, apareixerà el mòdul Advantis carregat. [Figura 9]

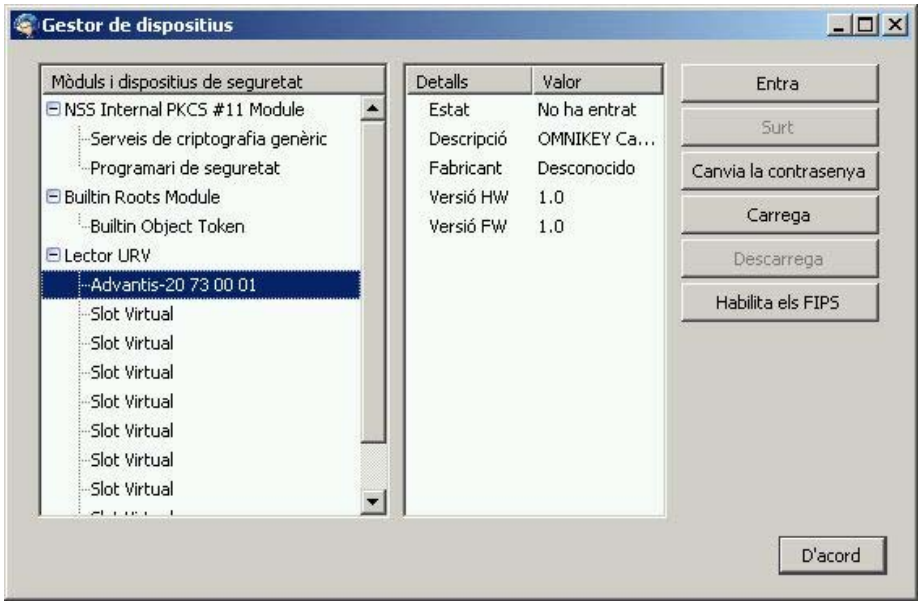


Figura 9

Configuració del compte de correu

En aquest apartat s'explica con associar els certificats digitals al compte de correu per poder signar i xifrar digitalment.

Per fer-ho, cal seleccionar el menú ***Eines***, opció ***Paràmetres del compte de correu***, secció ***Seguretat*** del compte de correu que es correspon amb l'adreça de correu que conté el certificat. [Figura 10]. Cal tenir inserit el carnet URV al lector de targetes.

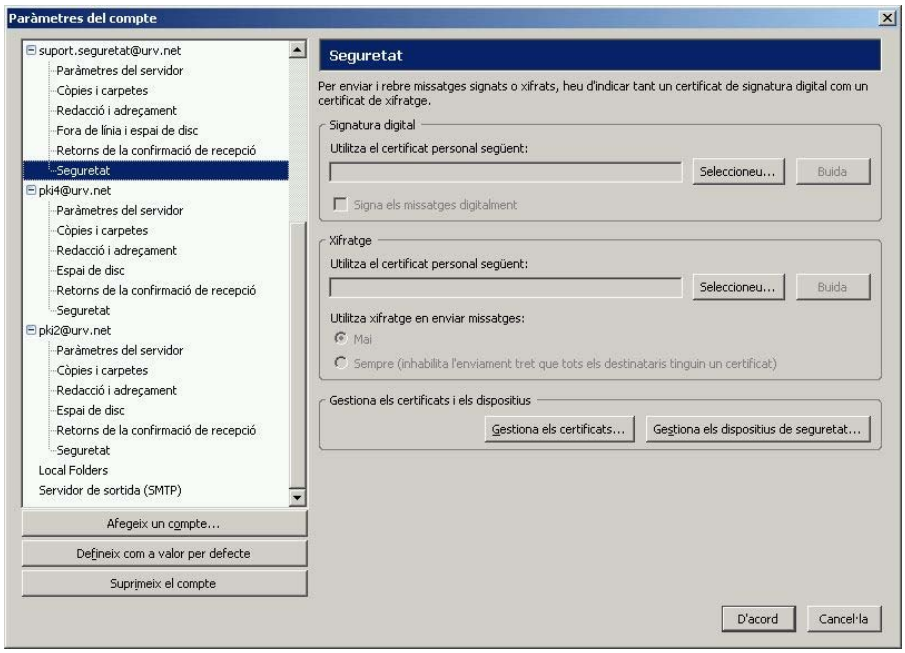


Figura 10

Mitjançant el botó ***Seleccioneu*** es seleccionen els certificats del carnet URV a utilitzar per signar (CPISR-1 C) i per xifrar (CPX-1 C). [Figures 11 i 12]

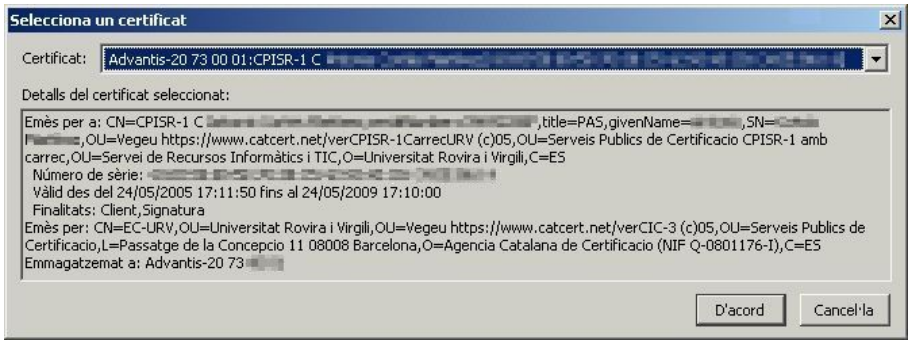


Figura 11

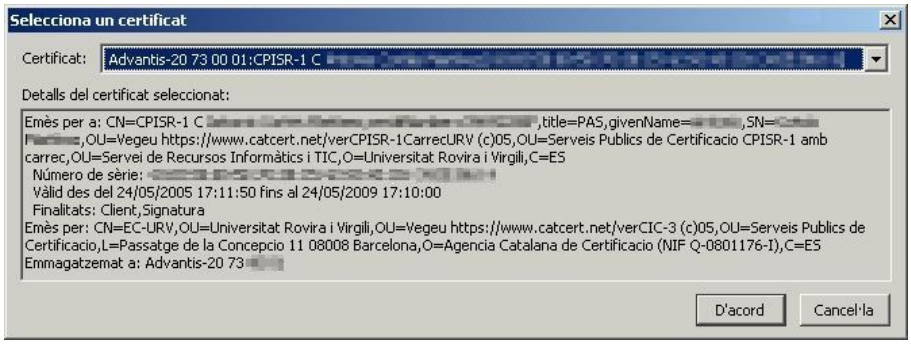


Figura 12

L'opció ***Signa els missatges digitalment*** permet signar automàticament tots els missatges que s'envien.
L'opció ***Utilitza xifratge en enviar missatges*** permet xifrar tots els missatges que s'envien.

Si es configuren aquestes opcions per defecte, es poden desactivar per a un missatge en concret de la finestra de redacció del missatge.

Signatura i xifrat de missatges

Si no s'han configurat les opcions per defecte, quan es necessiti signar o xifrar un correu electrònic, des de la finestra d'edició de missatges, caldrà seleccionar de la barra de botons, el botó ***Seguretat.*** [Figura 13]

Figura 13

- Sense xifratge. El correu no es xifra.
- Requereix encriptació. El correu s'enviarà xifrat al destinatari si es disposa de la seva clau pública de xifratge.
- Signa digitalment. El correu es signarà amb la nostra clau privada de signatura, continguda a la targeta criptogràfica.
- Seguretat del missatge. Opcions de seguretat que s'han aplicat al missatge.

Per enviar un correu xifrat es necessari disposar de la clau de xifratge del destinatari. En el cas de la URV, aquesta es troba en qualsevol dels correus signats que ens ha enviat el destinatari. El Mozilla Thunderbird la incorpora automàticament.

Per visualitzar les claus de xifratge dels usuaris que disposem, seleccionar el menú ***Eines*** -> opció ***Opcions...->*** secció ***Avançat***, pestanya ***Certificats***, botó ***Visualitza els certificats*** [Figura 14]

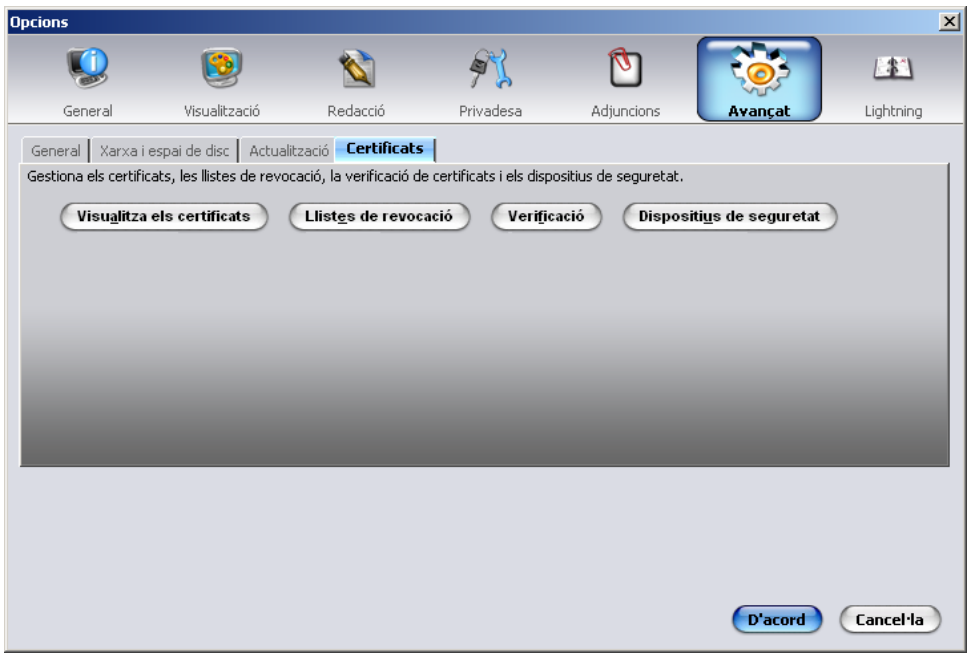


Figura 14

A la finestra ***Gestor de certificats,*** seleccionar la pestanya ***Els d'altri*** [Figura 15]

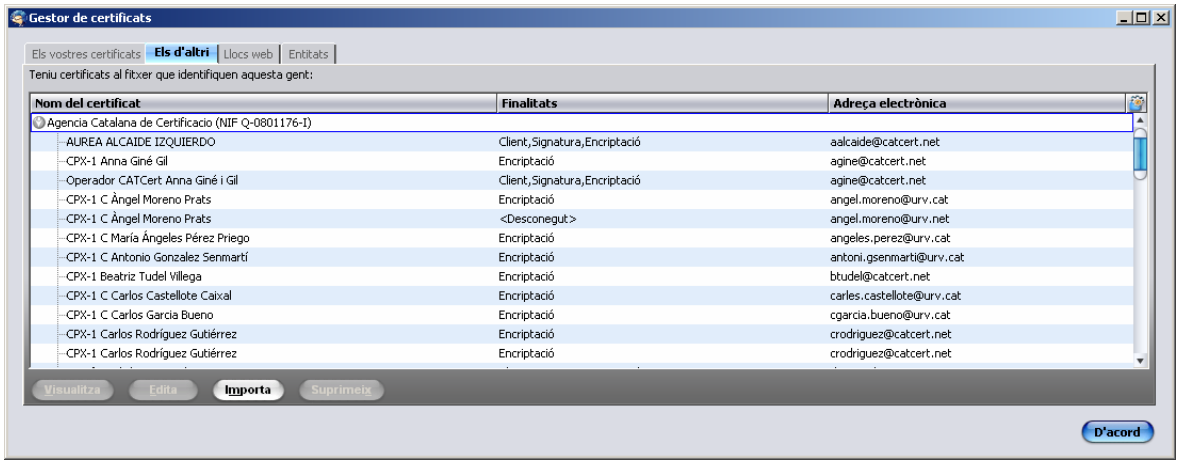


Figura 15

En activar les opcions de signatura i xifratge, en la finestra de redacció del correu, es poden veure les icones corresponents a signatura (en forma d'un bolígraf) i xifratge (en forma d'una clau). [Figura 16]

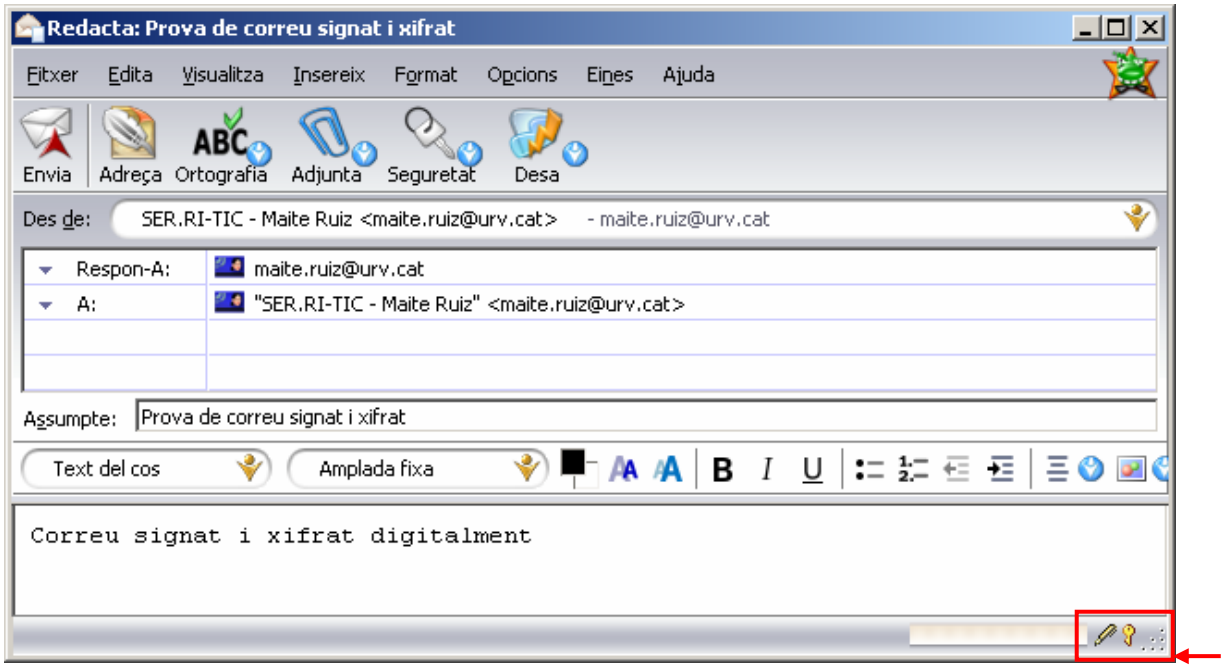


Figura 16

Quan s'envia el correu, es sol·licita la introducció del codi PIN de la targeta criptogràfica (carnet URV). [Figura 17]

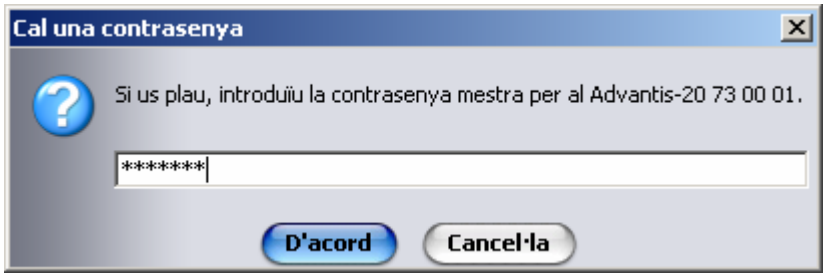


Figura 17

Si no s'introdueix o es fa de forma incorrecta, el programa oferirà l'opció d'enviar el missatge sense xifrar.

Cal tenir en compte que el nombre màxim d'intents incorrectes abans de que es bloquegi la targeta és de 3. En cas de bloqueig, es pot utilitzar el codi PUK per desbloquejar.

Lectura de correus signats

Per poder llegir un missatge signat digitalment no és necessari tenir accés a la clau privada de signatura emmagatzemada a la targeta criptogràfica. [Figura 18]

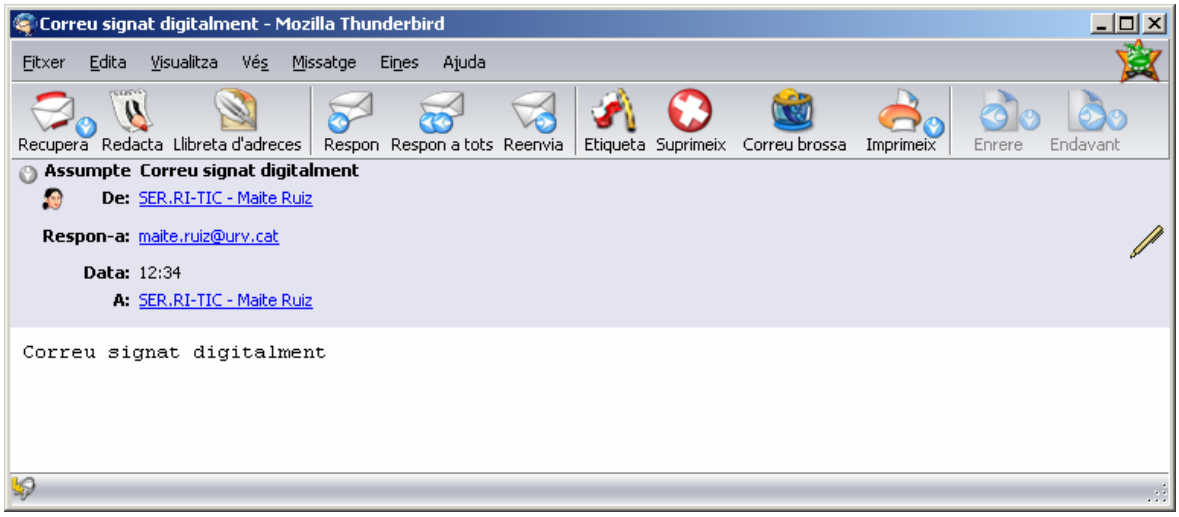


Figura 18

Si es fa doble clic en l'icona del llapis, apareix la informació de seguretat del missatge. [Figura 19]

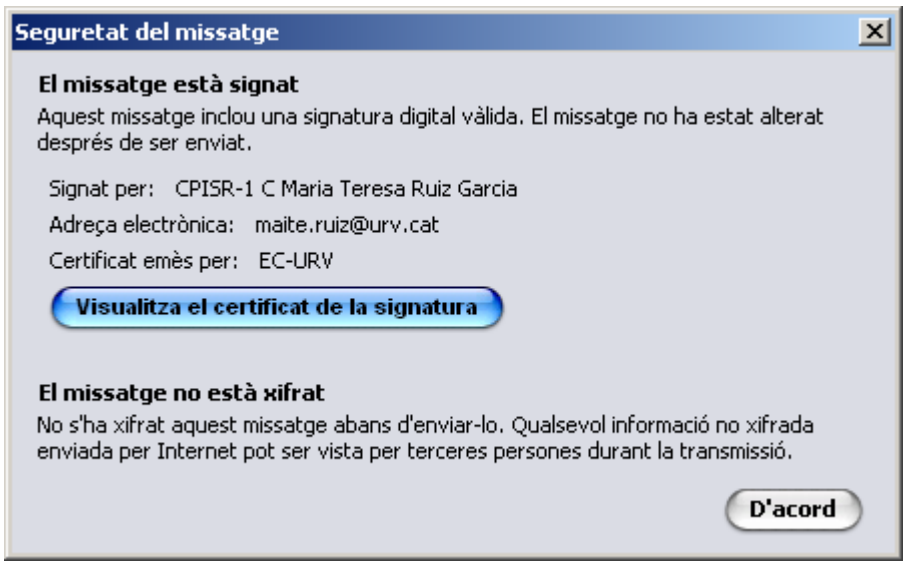


Figura 19

Es pot veure la informació del certificat digital del remitent seleccionant el botó ***Visualitza el certificat de la signatura.*** [Figura 20]

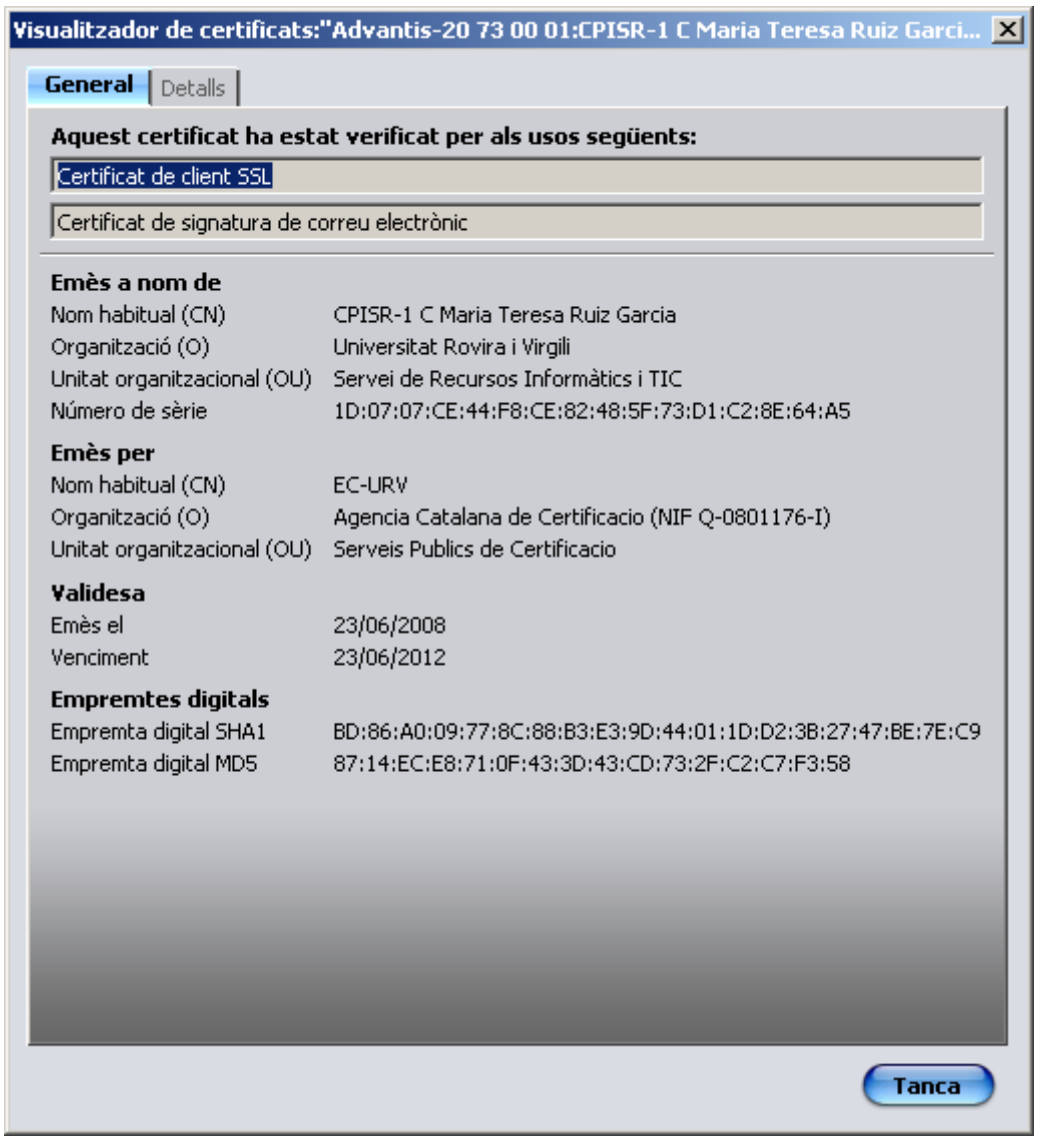


Figura 20

Lectura de correus xifrats

Per poder llegir un missatge xifrat, el gestor de correu ha de tenir accés a la nostra clau privada de xifratge emmagatzemada a la targeta criptogràfica.

Si la targeta criptogràfica no està inserida al lector, o no s'indica el pin correcte, no es podrà llegir el missatge i es mostrarà un missatge d'error. [Figura 21]

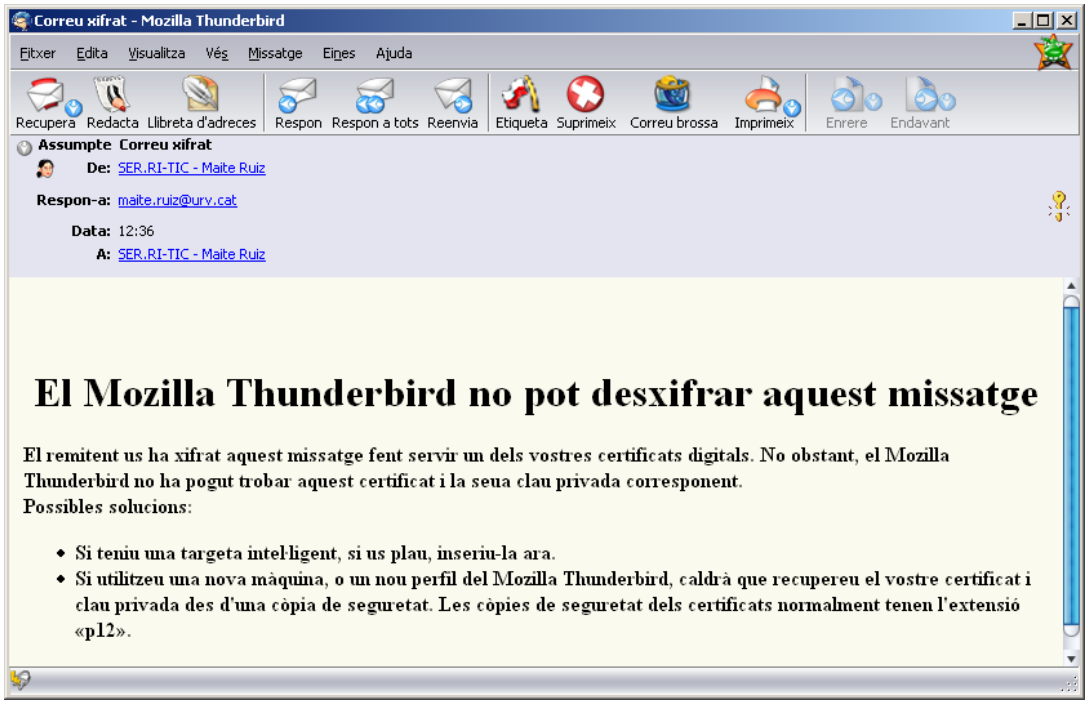


Figura 21

Si es fa doble clic en l'icona de la clau, apareix la informació de seguretat del missatge. [Figura 22]

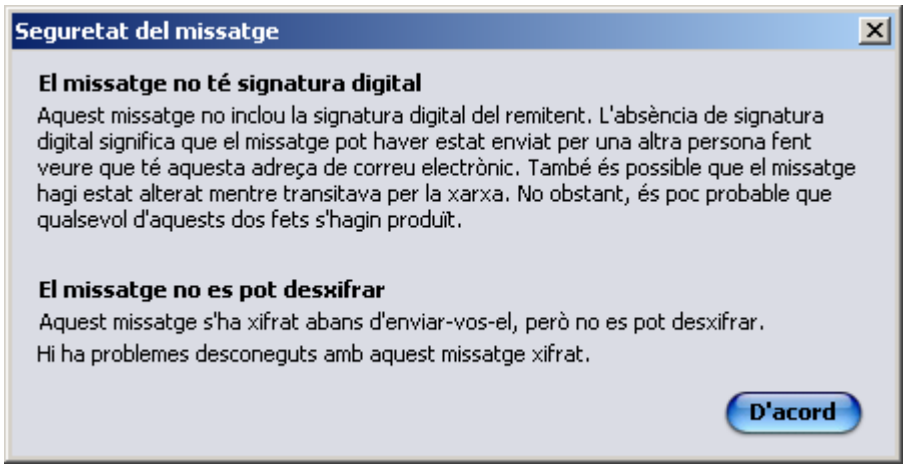


Figura 22