

Universitat Rovira i Virgili

Ús de la signatura electrònica amb Mozilla Thunderbird 2.0

Servei de Recursos Informàtics i TIC



Sumari

OBJECTIUS DEL DOCUMENT	
INSTAL·LACIÓ DE LES CLAUS PÚBLIQUES EN EL THUNDERBIRD	2
CONFIGURACIÓ DEL CLIENT PER A L'ÚS DE CERTIFICATS DIGITALS	5
Configuració del "dispositiu de seguretat"	5
Configuració del compte de correu	7
SIGNATURA I XIFRAT DE MISSATGES	9
LECTURA DE CORREUS SIGNATS	12
LECTURA DE CORREUS XIFRATS	14



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]

Opcions						×
I	I	1	FL.	1		1
General	Visualització	Redacció	Privadesa	Adjuncions	Avançat	Lightning
General Xarxa i e	espai de disc 📔 Actualit	zació Certificats	-			
Gestiona els certific	ats, les llistes de revoc	ació, la verificació de	e certificats i els dispo	ositius de seguretat.		1
Visualitza	els certificats) (Llistes de revoc	ació) (Verific	ació) (Disposit	ius de seguretat	
					-	
					D'acord	Cancel·la

Figura 1

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

Iom del certificat	Dispositiu de seguretat	
-Autoridad de Certificacion Firmaprofesional CIF A62634068	Builtin Object Token	
) (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.		
-TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	Builtin Object Token	
ABA.ECOM, INC.		
-ABA.ECOM Root CA	Builtin Object Token	
AC Camerfirma SA CIF A82743287		
-Chambers of Commerce Root	Builtin Object Token	
-Global Chambersign Root	Builtin Object Token	
AOL Time Warner Inc.		
-AOL Time Warner Root Certification Authority 1	Builtin Object Token	
-AOL Time Warner Root Certification Authority 2	Builtin Object Token	
AddTrust AB		



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]

Nom del certificat	Dispositiu de seguretat	<u></u>
Agencia Catalana de Certificacio (NIF Q-0801176-I)	4	4
-EC-UR	Serveis interns de criptografia	
-EC-ACC	Serveis interns de criptografia	6
EC-URV	Serveis interns de criptografia	
🖉 America Online Inc.		
-America Online Root Certification Authority 1	Builtin Object Token	
America Online Root Certification Authority 2	Builtin Object Token	
Baltimore		
Baltimore CyberTrust Root	Builtin Object Token	
Certplus		
Class 2 Primary CA	Builtin Object Token	
Comodo CA Limited		
-AAA Certificate Services	Builtin Object Token	



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]

Opcions						×
V	(29)	1	₽Y,	1		
General	Visualització	Redacció	Privadesa	Adjuncions	Avançat	Lightning
General Xarxa i	i espai de disc 🛛 Actuali	tzació Certificats	l			
Gestiona els certifi	icats, les llistes de revoi	ació, la verificació de	certificats i els dispo	sitius de seguretat.		
Visualitza	els certificats) (Llistes de revoca	nció (Verific	nció) (Disposi	tius de seguretat	
					D'acord	Cancel·la

Figura 6

En la finestra *Gestor de dispositius*, fer clic en el botó *Carrega*. [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.d11*). [Figura 8]

Escolliu un dispos	itiu PKCS#11 a c	arregar			? ×
<u>B</u> uscar en:	🔄 system32		-	🗈 💣 🎫	
Historial Escritorio Mis documentos	 acsetupc.dll acsmib.dll activeds.dll activeds.tlb activeds.tlb actmovie.exe actxprxy.dll admparse.dll adsldp.dll adsldpc.dll 	4	adsnds.dll adsnt.dll adsnt.dll adsnw.dll AdvantCSP.dll AdvantCSP.sig AdvantisPKCS11.d AdvantisPKCS11.d advpack.dll advpack.dll ALSNDMGR.CPL	Tipo: Ext Tamaño:	 amcompa amstream ansi.sys apcups.d append.e appmgmt appmgr.c appwiz.ct
MiPC	adsmsext.dll	L	ALSNDMGR.WAV		sterror.
	<u>N</u> ombre de archivo:	AdvantisPKCS11.dll		. [Abrir
Mis sitios de red	Tipo de arc <u>h</u> ivos:	Tots els fitxers			Cancelar

Figura 8

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

Mòduls i dispositius de seguretat	Detalls	Valor	Entra
NSS Internal PKCS #11 Module Serveis de criptografia genèric	Estat Descripció	No ha entrat OMNIKEY Ca	Surt
-Programari de seguretat	Fabricant	Desconocido	Canvia la contrasenya
🖻 Builtin Roots Module	Versió HW	1.0	Carrage
Builtin Object Token	Versió FW	1.0	Carrega
E Lector URV			Descarrega
Advantis-20 73 00 01			Habilita els ETDS
Slot Virtual			
Slot Virtual	-1		
i eta ora d			



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.

∃suport.seguretat@urv.net	Seguretat
-Paràmetres del servidor -Còpies i carpetes -Redacció i adreçament -Fora de línia i espai de disc	Per enviar i rebre missatges signats o xifrats, heu d'indicar tant un certificat de signatura digital com un certificat de xifratge. Signatura digital
-Retorns de la confirmació de recepció	Utilitza el certificat personal següent:
-Populetat Pki4@urv.net -Paràmetres del servidor -Còpies i carpetes	Signa els missatges digitalment
-Redacció i adreçament -Espai de disc -Retorns de la confirmació de recenció	Xitratge Utilitza el certificat personal següent: Seleccioneu Buida
-Seguretat ∃pki2@urv.net -Paràmetres del servidor -Còpies i carpetes	Utilitza xifratge en enviar missatges:
-Redacció i adreçament -Espai de disc -Retorns de la confirmació de recepció -Seguretat	Gestiona els certificats i els dispositius
Local Folders Servidor de sortida (SMTP)	
Afegeix un compte	
Defineix com a valor per defecte	

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]







5elecciona) un certificat	×
Certificat:	Advantis-20 73 00 01:CPISR-1 C	
Detalls del	certificat seleccionat:	
Emès per 4 carrec, OU Número 6 Vàlid des Finalitats Emès per: Certificaci Emmagatz	a: CN=CPISR-1 C , title DU=Vegeu https://www.catcert.net/verCPISR-1CarrecURV (c)05,OU=Ser I=Servei de Recursos Informàtics i TIC,O=Universitat Rovira i Virgili,C=ES de sèrie: : del 24/05/2005 17:11:50 fins al 24/05/2009 17:10:00 :: Client,Signatura : CN=EC-URV,OU=Universitat Rovira i Virgili,OU=Vegeu https://www.catc io,L=Passatge de la Concepcio 11 08008 Barcelona,O=Agencia Catalana c zemat a: Advantis-20 73	=PAS, givenName=,SN= veis Publics de Certificacio CPISR-1 amb ert.net/verCIC-3 (c)05,OU=Serveis Publics de le Certificacio (NIF Q-0801176-I),C=ES
		D'acord Cancel·la

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]





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

m del certificat	Finalitats	Adreça electrònica	
gencia Catalana de Certificacio (NIF Q-0801176-I)			
-AUREA ALCAIDE IZQUIERDO	Client, Signatura, Encriptació	aalcaide@catcert.net	
CPX-1 Anna Giné Gil	Encriptació	agine@catcert.net	
Operador CATCert Anna Giné i Gil	Client, Signatura, Encriptació	agine@catcert.net	
CPX-1 C Àngel Moreno Prats	Encriptació	angel.moreno@urv.cat	
CPX-1 C Àngel Moreno Prats	<desconegut></desconegut>	angel.moreno@urv.net	
CPX-1 C María Ángeles Pérez Priego	Encriptació	angeles.perez@urv.cat	
CPX-1 C Antonio Gonzalez Senmartí	Encriptació	antoni.gsenmarti@urv.cat	
CPX-1 Beatriz Tudel Villega	Encriptació	btudel@catcert.net	
CPX-1 C Carlos Castellote Caixal	Encriptació	carles.castellote@urv.cat	
CPX-1 C Carlos Garcia Bueno	Encriptació	cgarcia.bueno@urv.cat	
CPX-1 Carlos Rodríguez Gutiérrez	Encriptació	crodriguez@catcert.net	
	Encriptació	crodriguez@catcert.net	

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]

🚔 Redacta: Prova de correu signat i xifrat	
Ejtxer Edita Visualitza Insereix Format Opcions Eines Ajuda	2
Envia Adreça Ortografia Adjunta Seguretat	
Des <u>d</u> e: SER.RI-TIC - Maite Ruiz <maite.ruiz@urv.cat> - maite.ruiz@urv.cat</maite.ruiz@urv.cat>	*
Respon-A: Imaile.ruiz@urv.cat A: Imaile.ruiz@urv.cat>	
A <u>s</u> sumpte: Prova de correu signat i xifrat	
Text del cos 🔌 🗛 Anplada fixa 🛛 🔌 🖛 🗛 🗛 🛛 B 🛛 💆 🗮 🗄 🖽 🗮	🎱 💌 🎸
Correu signat i xifrat digitalment	
	18.



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

Cal una	contrasenya 🔀
?	Si us plau, introduïu la contrasenya mestra per al Advantis-20 73 00 01.

	D'acord Cancel·la

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]

🧟 Correu signat digitalment - Mozilla Thunderbird	
Eitxer Edita Visualitza Vé <u>s M</u> issatge Eines Ajuda	Ŕ
Recupera Redacta Llibreta d'adreces Respon a tots Reenvia Etiqueta Suprimeix Correu brossa Imprimeix Enrere En	davant
🕥 Assumpte Correu signat digitalment	
De: SER.RI-TIC - Maite Ruiz	
Respon-a: maite.ruiz@urv.cat	
Data: 12:34	, i
A: SER.RI-TIC - Maite Ruiz	
Correu signat digitalment	
	:

Figura 18

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





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

ualitzador de certificats: General Detalls	"Advantis-20 73 00 01:CPISR-1 C Maria Teresa Ruiz Garci
Aquest certificat ha esta	at verificat per als usos següents:
Certificat de client SSL	
Certificat de signatura de co	orreu electrònic
Emès a nom de Nom habitual (CN) Organització (O) Unitat organitzacional (OU) Número de sèrie	CPISR-1 C Maria Teresa Ruiz Garcia Universitat Rovira i Virgili Servei de Recursos Informàtics i TIC 1D:07:07:CE:44:F8:CE:82:48:5F:73:D1:C2:8E:64:A5
Emès per Nom habitual (CN) Organització (O) Unitat organitzacional (OU)	EC-URV Agencia Catalana de Certificacio (NIF Q-0801176-I) Serveis Publics de Certificacio
Validesa Emès el Venciment	23/06/2008 23/06/2012
Empremtes digitals Empremta digital SHA1 Empremta digital MD5	BD:86:A0:09:77:8C:88:B3:E3:9D:44:01:1D:D2:3B:27:47:BE:7E:C9 87:14:EC:E8:71:0F:43:3D:43:CD:73:2F:C2:C7:F3:58
	Tanca



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]

Ekker Edita Ysualitza Vég Missatge Eiges Ajuda Recupera Redacta Libereta d'adreces Respon Respon a tots Reenvia Etiqueta Suprimeix Correu brossa Imprimeix Envero Enventin Envero	🗣 Correu xifrat - Mozilla Thunderbird	
Recuperà Redacta Ulbreta d'adreces Respon Respon a tots Reenvia Assumpte Correu Mirat Messonnete Correu Mirat Messonn	Eitxer Edita Visualitza Vé <u>s M</u> issatge Ei <u>n</u> es Ajuda	<u> </u>
 Assumpte Correu xifrat De: SER.RL-TIC - Maite Ruiz Respon-a: maite.ruiz@urv.cat Data: 12:36 A: SER.RL-TIC - Maite Ruiz El Mozilla Thunderbird no pot desxifrar aquest missatge El remitent us ha xifrat aquest missatge fent servir un dels vostres certificats digitals. No obstant, el Mozilla Thunderbird no ha pogut trobar aquest certificat i la seua clau privada corresponent. Possibles solucions: Si teniu una targeta intel·ligent, si us plau, inseriu-la ara. Si teniu una targeta intel·ligent, si us plau, inseriu-la ara. Si teniu una targeta intel·ligent, si us plau, inseriu-la ara. Si tutilitzeu una nova màquina, o un nou perfil del Mozilla Thunderbird, caldrà que recupereu el vostre certificat i clau privada des d'una còpia de seguretat. Les còpies de seguretat dels certificats normalment tenen l'extensió «pl2».	Recupera Redacta Llibreta d'adreces Respon Respon a tots Reenvia Respon Respon a tots Reenvia	
 De: SER.RITIC - Mate Ruiz Respon-a: mate.ruiz@urv.cat Data: 12:36 A: SER.RITIC - Mate Ruiz El Mozilla Thunderbird no pot desxifrar aquest missatge El remitent us ha xifrat aquest missatge fent servir un dels vostres certificats digitals. No obstant, el Mozilla Thunderbird no ha pogut trobar aquest certificat i la seua clau privada corresponent. Possibles solucions: Si teniu una targeta intel·ligent, si us plau, inseriu-la ara. Si utilitzeu una nova màquina, o un nou perfil del Mozilla Thunderbird, caldrà que recupereu el vostre certificat i clau privada des d'una còpia de seguretat. Les còpies de seguretat dels certificats normalment tenen l'extensió «pl2».	🕜 Assumpte Correu xifrat	
Respon-a: make.ruiz@urv.cat Data: 12:36 A: SER.RI-TIC - Make Ruiz	De: <u>SER.RI-TIC - Maite Ruiz</u>	
Data: 12:36 A: SER.RI-TIC - Maite Ruiz El Remitent us ha xifrat aquest missatge fent servir un dels vostres certificats digitals. No obstant, el Mozilla Thunderbird no ha pogut trobar aquest certificat i la seua clau privada corresponent. Possibles solucions: • Si teniu una targeta intel·ligent, si us plau, inseriu-la ara. • Si utilitzeu una nova màquina, o un nou perfil del Mozilla Thunderbird, caldrà que recupereu el vostre certificat i clau privada des d'una còpia de seguretat. Les còpies de seguretat dels certificats normalment tenen l'extensió «p12».	Respon-a: <u>maite.ruiz@ury.cat</u>	<u>.</u>
A: <u>SER.RI-TIC - Malte Ruiz</u> El Mozilla Thunderbird no pot desxifrar aquest missatge El remitent us ha xifrat aquest missatge fent servir un dels vostres certificats digitals. No obstant, el Mozilla Thunderbird no ha pogut trobar aquest certificat i la seua clau privada corresponent. Possibles solucions: • Si teniu una targeta intel·ligent, si us plau, inseriu-la ara. • Si utilitzeu una nova màquina, o un nou perfil del Mozilla Thunderbird, caldrà que recupereu el vostre certificat i clau privada des d'una còpia de seguretat. Les còpies de seguretat dels certificats normalment tenen l'extensió «p12».	Data: 12:36	
El remitent us ha xifrat aquest missatge fent servir un dels vostres certificats digitals. No obstant, el Mozilla El remitent us ha xifrat aquest missatge fent servir un dels vostres certificats digitals. No obstant, el Mozilla Thunderbird no ha pogut trobar aquest certificat i la seua clau privada corresponent. Possibles solucions: • Si teniu una targeta intel·ligent, si us plau, inseriu-la ara. • Si utilitzeu una nova màquina, o un nou perfil del Mozilla Thunderbird, caldrà que recupereu el vostre certificat i clau privada des d'una còpia de seguretat. Les còpies de seguretat dels certificats normalment tenen l'extensió «pl2».	A: SER.RI-TIC - Maite Ruiz	
	El Mozilla Thunderbird no pot desxifrar aquest missat El remitent us ha xifrat aquest missatge fent servir un dels vostres certificats digitals. No obstant, el Mozilla Thunderbird no ha pogut trobar aquest certificat i la seua clau privada corresponent. Possibles solucions: • Si teniu una targeta intel·ligent, si us plau, inseriu-la ara. • Si utilitzeu una nova màquina, o un nou perfil del Mozilla Thunderbird, caldrà que recupereu el vostre certifi clau privada des d'una còpia de seguretat. Les còpies de seguretat dels certificats normalment tenen l'exter «p12».	tge icat i Isió

Figura 21

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

