UNIVERSITAT POLITÈCNICA DE CATALUNYA	INFORMACIÓ GENERAL			
PROJECTE: Manuals d'us de signatura electrònica Versió: 1.4				
TÍTOL: Signatura electrònica amb IBM Lotu MS Windows XP	s Notes 7 i Codi Referència:			
RESUM:	Data Publicació: 19/11/2008			

PROCEDIMENT

Signatura electrònica amb IBM Lotus Notes 7 i MS Windows XP

PREPARAT PER:	REVISAT PER:	APROVAT PER:
Nom:	Nom:	Nom:
Data:	Data:	Data:

	UNIVERSITAT POLITÈCNICA De catalunya
PROJ	ECTE: Manuals d'us de signatura e
,	

INFORMACIÓ GENERAL

PROJECTE: Manuals d'us de signatura electrònica	Versió: 1.4
TÍTOL: Signatura electrònica amb IBM Lotus Notes 7 i MS Windows XP	Codi Referència:
RESUM:	Data Publicació: 19/11/2008

Versió	Parts que canvien	Descripció del canvi	Data del canvi
1.0	Tot	Creació del document	19/11/08
1.1	Tot	Modificació document inicial	22/12/08
1.2	Tot	Configuració signatura correu	14/01/09
1.3	Certificats CRL i OCSP	Certificats CRL i OCSP	16/01/09
1.4	Tot	Revisió	26/01/09

ÍNDEX

1	Objectiu i abast4
2	Prerequisits4
3	Configuració de signatura electrònica amb IBM Lotus Notes 7 i Windows XP5
4	Enviament de missatges13
4.1	Signats13
4.2	Xifrats18
5	Recepció de missatges20
5.1	SignatsiError! Marcador no definido.
5.2	XifratsiError! Marcador no definido.
6	Referències24

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 XP 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 <u>https://www.upc.edu/identitatdigital/certificat_digital/programari-certificat-digital/descarrega-de-programari</u>. Per obtenir els detalls d'instal·lació d'aquest software, es pot accedir a la següent adreça web <u>https://www.upc.edu/identitatdigital/certificat_digital/programari-certificat-digital/Guia_Basica_Instalacio.pdf/view</u>
- 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 <u>https://www.upc.edu/identitatdigital/certificat_digital/programari-certificat-digital/Guia_Basica_Instalacio.pdf/view</u>

3 <u>Configuració de signatura electrònica amb IBM Lotus</u> <u>Notes 7 i Windows XP</u>

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.

Nom Comom - Safata d'entrada - IBM Lotus Notes		
Etver Edita Visualitza Crea Accions Ajuda		
Nort		
Tanca Control+W		
Desa Control+5	▼ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	
Desa com a versió nova		
Desa automàticament	•	
Propietats del document		-
Base de dades	espon 🔹 Respon a tothom 🔹 Remet 🔹 Suprimeix Seguiment 🔹 Carpeta 👻 Copia a 🔹 Xat 👻 Eines 🗨 t	Mos Ż
Replicació		
Mòbil	I^ ^ ∪ata ∨ Hora Mida ▼ Assumpte ^	
Missatgeria instantania	,	
Adjunta		
Importa		
Exporta		
Format de pàgina		
Visualització prèvia d'impressió		
Imprimeix Control+P		
Dreferències	·3	
Seguretat	Seguretat de l'usuari	
ciries 2	Bioqueja la visualitzacio F5	
Tanca totes les pestanyes de les finestres obertes	Canvia TLD	
Desa l'estat de la finestra		
Nejeta l'estat desat de la finestra		
Surt del Notes		
Seguiment T		Þ
el Carulli/UPC	Visualització prèvia 🔺	
	A Contractions A Contractions	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.

🔴 No	Nom Cognom - Safata d'entrada - IBM Lotus Notes		đΧ
Fitxer	er Edita Visualitza Crea Accions Ajuda		
	🕽 🖬 🍅 📲 😤 🥵 🛛 🦧 🛍 🗋 🕹 🗍 오 주	ᢗᢗѶѶ҄҄ѿ ҫ҇҇ѩѿ҄ҿ ҇ѩ҄Ӎ҇҇ҲЁ	
Adre	dreça	▼ ↓ ↓ ↓ ↓ ↓ ⊗ @ @ Q [†] ▼	
1			
	🚱 Benvinguts 💽 Nom Cognom - Safata d'entrada 🗙		
	Seguretat de l'usuari	? 🗙 🚽	Haa +
R	per a Ús de l	a targeta intel·ligent amb el Notes	MUS <
6	Jeguietat basica 1		
9	Carl La vostra identitat		
	Els vostres noms		
5	La vostra targeta intel·ligent	Habilita l'inici de sessió amb la targeta intel·ligent	
	🚰 🗄 Identitat d'altres Si utilit:	eu una targeta intel·ligent, convé que la tingueu sempre a mà. D'aquesta manera es redueixen les	
5	possibi	tats d'ús inadequat o robatori de la identitat del Notes i de la informació privada emmagatzemada a la	
5	T 🗄 🗋 💝 🗉 Dades del Notes	ració de la targeta intel·ligent	
	🛛 🖻 🖗 Correu		
a	· · ·		
N			
57	7		
S			
		Detalls de la configuració	
		D'acord Tanca	
	Seguiment -		•
	el Carulli/UPC	Visualització prévia 🔺	
		▲] (🖘 ▲) [Oficina ▲]	-

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)

Configuració de la targeta i	ntel·ligent	? ×		
Les targetes intel·ligents i altres testimonis criptogràfics aporten seguretat addicional a l'entorn del Notes. Per a utilitzar les funcions de seguretat d'una targeta intel·ligent, necessiteu una targeta intel·ligent compatible i un lector de targetes intel·ligents connectat al sistema.				
El programari del controlador de la l Heu de proporcionar el nom de fitxe Eltxer controlador de la targeta inte	argeta intel·ligent permet que el Notes es comuniqui amb el lector de targetes inte er del controlador de la targeta intel·ligent proporcionat pel fabricant. Higent C:\Archivos de programa\Gemalto\Classic Client\BIN\gclib.dll	el·ligents.		
<activclient 5.4=""></activclient>	c:\winnt\system32\acpkcs211.dll	~		
<a-trust a-sign="" client="" v1.2.2.1=""> <belgian eid=""></belgian></a-trust>	c:\winnt\system32\asignp11.dll c:\winnt\system32\Belgium Identity Card PKCS11.dll	~		
<		>		
	2 Continua. Cano	cel·la		

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).

Seguretat de l'usuari		? ×
 Seguretat bàsica La vostra identitat Els vostres noms Els vostres certificats La vostra targeta intel·ligent Identitat d'altres 	Os de la targeta intel·ligent amb el Notes L'ús d'una targeta intel·ligent o un testimoni criptogràfic amb el Notes ofereis protecció per a l'ID del Notes. Per als ID del Notes compatibles amb targetes intel·ligents, cal proporcionar la targeta en iniciar la sessió i mentre s'usa el Notes. En iniciar la sessió, haureu d'introduir el PIN de la targeta intel·ligen testimoni crintonràfic en lloc d'una contracenva del Notes. Habilta l'inici de sessió amb la targeta intel·ligent Si utilizeu una targeta intel·ligent, convé que la tingueu sempre a mà. D'aquesta manera es redueixen	< més 3 t o del les
Image: Accions d'altres Image: Image: Accions d'altres Image: I	possibilitats d'ús inadequat o robatori de la identitat del Notes i de la informació privada emmagatzemac targeta. Configuracio seguretat Fabricant de la targeta Gemplus Número de sèrie de la 0040001E56CC036C	
	1 Detalls de la configuració	Identificació targeta

Figura 4. Configuració de 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 el administradors del sistema, perque podria causar el bloqueix permanent de l'access al IBM Lotus Notes.

3.5 Un cop creada la configuració de seguretat per utilitzar la targeta xip, tornarem al menu *"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).

🛑 Nom Cognom - Safata d'entrada - IBM Lotus Notes	
(Ritxer) Edita Visualitza Crea Accions Ajuda	
Nou 1 Tanca Control+W Desa Control+S Desa automàticament Propietats del document	Ს ଫ ଐ ଐ ଓ ಈ – എ ଲ. ାଲ୍ ♠ ୦. 🗃 ▼ ✑ • ୦ - ⊘ ֎ ୦. ♥
Base de dades P Replicació Mòbil Mòbil Missatgeria instantània	Respon a tothom Remet Suprimeix] Seguiment Carpeta Copia a Xat Eines Mostra els Accord Ac
Adjunta Importa Exporta	
Format de pàgina Visualització prèvia d'impressió Imprimeix Control+P	
Preferències Seguretat 2 Eines	Preferencies de l'usuari 3 Preferencies d'ubicacio Auxiliar pre si aneconfiguració del client
Tanca totes les pestanyes de les finestres obertes Desa festat de la finestra Neieta festat desat de la finestra Surt del Notes	Preferències de la barra d'eixes Preferències de la barra d'estat
Seguiment▼ a el Carull/UPC	Visualització prèvia 🔺
	▲][=> ▲][/// ▲][Oficina ▲][= ▲]

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.

Preferències de l'usuari					? ×
B Opcions bàsiques	Configuració				
A H Internacional	Llibretes d'adreces locals		Editor de missa	tges alternatiu	
	names.nsf	Navega	Сар	_	
🔁 🗉 Correu	Enviament				
General 1	Desa el correu que s'enviï		🔽 Signa el co	orreu que s'envii 2	
Internet	Desa sempre una còpia 🛛 💌		Xifra el cor	reu que s'envii	
🏈 🗉 Missatgeria instantània	📕 Xifra la còpia desada del cor	reu que s'enviï			
Ports	Remissió				
Replicació	🔽 Afegeix automàticament el p	refix de remissio	ó a l'assumpte		
	Recepció				
	Comprova si hi ha correu no	u cada 15	minuts		
	Quan arribi correu nou				
	Actualitza automàticament la	i safata d'entra	da 🥅 Mostra u	ın missatge emergent	
	I Reprodueix un so Na	vega 🔽 M	fostra una icona	a la safata del sistema	
			3	D'acord	Cancel·la

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.





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.

- <u> </u>					
Els meus documents					
El meu ordinador	General Detalles Ruta de certificación				
	Información del certificado				
Paperera de reciclatge	Este certificado está destinado a los siguientes propó: •Prueba su identidad a un equipo remoto •Protege los mensajes de correo electrónico	itos:		gemalto [*]	
Lotus Notes 7	* Más info. en declaración de entidades emisoras de certificado		Gódigo NIP:	Inicio de sesión	
Nozila Firefox	Enviado a: CPISR-1 C NOM COGNOM		CPACE C NOM COGNOM		
	Válido desde 24/10/2008 hasta 24/10/2012				
Thunderbird	Instalar certificado Declaració	n del emisor			
		D'acord 2 Mc	strar detalles Eliminar	Predeterminado	
_	Administración software Diagnóstico/Ayuda		Exportar Eliminar todos	Registrar todos	
📇 Inicia	🖉 🙋 🥹 🦈 👸 Classic Client ToolBox 👘 Certi	cado			ES 🔇 🜒 🍇 😻

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 <u>http://ocsp.catcert.net</u> (pas 2) per realitzar la verificació de l'estat del certificat, tal i com es pot apreciar a la figura 9.

ertificado		?
General Deta	lles Ruta de certificación	
Mostrar: <t< td=""><td>odos></td><td>*</td></t<>	odos>	*
Campo		Valor 🔥
Tipo de c Identifica Identifica Dasos de Acceso a Inoronal	ertificado Netscape ador de clave de asunto ador de clave de entidad emisora l certificado la información de entidad emisora 5.5.7.1.3 o distribusión CPI	Autenticación del clier fa c4 66 ad 98 d7 c8 2 Id. de clave=48 9f 8d [1]Directiva de certific [1]Acceso a informaci 20 0a 20 00 06 06 04
[1]Acceso a i	nformación de autoridad	
Método de (1.3.6.1.5.5. Nombre al 2 Direccio	e acceso=Protocolo de estado de (7.48.1) Fernativo: ón URL=http://ocsp.catcert.net	certificado en línea
	Modificar propiedades	Copiar en archivo D'acord

Figura 9. Propietats del certificat.

 "Puntos de distribución CRL" (pas 1) on ens indica les direccions url <u>http://epscd.catcert.net/crl/ec-ur.crl</u> i <u>http://epscd2.catcert.net/crl/ec-ur.crl</u> (pas 2) utilitzades com a punt de descàrrega de la llista de certificats revocats, tal i com es pot apreciar a la figura 10.

eral Detalles Ruta de certificación	
strar: <todos></todos>	*
Tampo	Valor 🔥
Acceso a la información de entidad emisora	[1]Acceso a informaci 20.05 20.08 06 06 04
Puntos de distribución CRL	[1]Punto de distribució
oso de la clave Algoritmo de identificación Huella digital	rimia digital (60) sha1 9d 47 45 87 8e 2e f6 i
) 	<u> </u>
Punto de distribución CRL Nombre del punto de distribución: Nombre complete: Dirección URL=http://epscd.catcert.ne Dirección URL=http://epscd2.catcert.r	et/crl/ec-ur.crl het/crl/ec-ur.crl

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 haber configurat la signatura electrònica de tots el 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 *"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 electrónic 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).

Lotus Notes	×
Introduïu el	D'acord 2
Targeta GemiSAFE	Cancel·la

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 <u>https://www.upc.edu/identitatdigital/certificat digital/gestio-pin-i-puk/desbloqueig targeta.pdf/view</u>

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).

Correu sortint: Configura	ació de certificats per a	signatura d	l'estil d'Internet (S/MI 🤗 🗙
Certificat de signatura			
Per enviar correu signat a per que contingui l'adreça de con Seleccioneu un certificat de s	sones que no utilitzen el Notes reu electrònic d'Internet. signatura per utilitzar lo per a ac	, cal que tingue	u un certificat de signatura d'Internet
Tipus Emès per a Q		Emès per Q	
CPISR-1 C NOM CO)GNOM	EC-UR 1	
r Seleccioneu element			
Emès per a	CPISR-1 C NOM COGNOM		Detalls avançats
Adreces de correu representades en aquest certificat	NOM.COGNOM@UPC.EDU NOM.COGNOM@UPC.EDU;	=Q0818003F	
-		2	D'acord Cancel·la

Figura 13. Sel·lecció 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 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 <u>https://www.upc.edu/identitatdigital/nou certificat digital esborrany/programari-certificat-digital/Guia Basica Instalacio.pdf/view</u>

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 -Certificació Aaència Catalana de que podrà trobar а 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 de Agència Catalana 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.

🛞 No	om Cognor	n - Safata d'entra	ada - IBM Lotu	Notes					T B
Fitxer	Edita Vis	ualitza Crea Accio	ins Ajuda						
	∎Ġ∙í	/ 🖙 😓 😞	1 B C B	<u> </u>] ♡ 주 주 수 🏷	°) 🖪 🗘 🗆 9	i); 🗠 🖷 🌢			
Adre	iça					•	(⊐ + ⊑) + 😡 (34 0. +	
18			C ()		C ()				
<u>м</u> Г	E Benvin	guts ();;;;) Nom Logn	om - Safata d'entra	da 🗙 阕 Nom Lognom	Safata d'entrada 🗙	۲ <u>ــــــــــــــــــــــــــــــــــــ</u>			- ¹
0	Co	rreu 🔻	Missatge no	J Respon 🔻 Respo	in a tothom 💌 R	emet 🕶 🛛 Sup	rimeix Seguime	nt ·][Carpeta ·] Copia a ▼][Xat •	Eines 🕶 🚺 Mostra els
	peranto	in cognom		Qui ^	∧ Data ∨	Hora	Mida ~ 4	Preferències	
3	3	Safata d'entrad	٤ *	McDuff Teems	02/01/2009	14:38	2.374	Aregeix l'emissor a la llibreta d'adrece Bloqueia el correu de l'emissor	
0		Esborranys En ústa	*	Instituto Lean	07/01/2009	17:42	167.855	Crea norma ràpida	oyota sufrir
61		Enviais Seguiment						Marca/desmarca el document com a v	vençut
		Correu no desitjat						Fora de l'oficina Paràmetres d'arxivament	
~	1	Paperera.						Missatge nou - Utilitzant un imprès	
~ .	•	visualitzacions	3					Normes de correu	
2		Preferències							
6	÷	Correu Cale	ndari i tasca	Accés i delegació					D'acord
9		[control] our		locos rucio gacio j					Canaalla
-	·	Opcions bà:	siques Capça	ilera Signatura Se	eguiment Marc	atge de miss	atges		Canceria
		Configuraci	ó de l'usuari						
0-1		Aquest fitxer	de correu perta	v a: Nom Cognom/U	PC			Canvia	
		(Feu servir e	I vostre nom jeri	irquic, per exemple, Jo	an Domènech/Or	ganització)			
		Gestioneu le	s vostres preferi	ncies de seguretat del	correu: Segur	etat de l'usuai	n		
		Correcció o	rtogràfica						
		Comprov	a automàticam	int la ortografia dels m	ssatges de correi	u abans d'env	iar-los		
	Seguir	Suprimeix/e	limina preferènc	ia per a la visualització	Enviats				
	el Carul								
) [S'ha: S	Fregunta-r	n no sempre_*						
-	Inicio	Supressió ti	emporal						
		Temps de v	enciment de la :	upressió temporal en	hores: 48				
		Advertimer	nt sobre missatg	e sense tema					
		🗖 No avisi	s si el terna s'ha	deixat en blanc abans	d'enviar un miss	atge			



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.

Preferències	<u>?</u> ×
Correu Calendari i tasca Accés i delegació	D'acord
Opcions bàsiques Capçalera Signatura Seguiment Marcatge de missatges	Cancel·la
La vostra signatura pot ser text, una imatge o un fitxer HTML	
2 🔽 Afegeix automàticament una signatura a la part final dels meus missatges de correu de sortida	
Utilitza: • Text C Fitzer HTML o d'imatges	
Signatura:	

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.

Preferències	? ×
Correu Calendari i tasca Accés i delegació	2 D'acord
Opcions bàsiques Capçalera Signatura Seguiment Marcatge de missatges	Cancel·la
La vostra signatura pot ser text, una imatge o un fitxer HTML	
V Afegeix automàticament una signatura a la part final dels meus missatges de correu de sontida	
Utilitza: © Text C Fitzer HTML o d'imatges	
NOTA IMPORTANT: Si a l'hora de llegir ac NOTA IMPORTANTE: Si a l'alee este mensaje IMPORTANT: If you get a message notifyir	



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.

Preferències	? ×
Correu Calendari i tasca Accés i delegació	D'acord
Opcions bàsiques Capçalera Signatura Seguiment Marcatge de missatges	Cancel·la
La vostra signatura pot ser text, una imatge o un fitxer HTML	
✓ Afegeix automàticament una signatura a la part final dels meus missatges de correu de sortida Utilitze: C Text 1 C Fitcer HTML o d'imatges Fitcer. 2 Ubicació on s'ha guardat l'arxiu	

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.

10000
8
19

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 cuadre de diàleg de la figura 19.

rror de xifratge del correu	?
Si opteu per continuar amb l'enviament, els destinataris següents rebran una còpia del missatge sense xifrar:	Envia-ho <u>C</u> ancel·la l'enviament
nom.cognom@domini.cat	
 El xifratge del correu ha fallat per a aquest destin No s'ha pogut trobar el certificat d'Internet d'aqui	atari perquè: est destinatari al directori. N
s'ha enviat cap entrada amb una adreça d'Intern una de coincident que no contenia cap certifical	et coincident o se n'ha trob : d'Internet utiltizable.

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 <u>Recepció de missatges</u>

5.1 Signats

En el cas de rebre missatges 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

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.

Si no hi ha cap tipus de conflicte amb les claus publiques de l'emissor o el certificat utilitzat per signat 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).

Certificador	Nom Cognom/LIPC
Servidor	Local
Nom del subjecte:	CN=CPISR-1 C NOM COGNOM/XX=11111111A/TIT
Noms alternatius del su	ubjecte
Empremta digital	43FB 78F6 F4D8 8453 50B4 D97E B8D0 4C20
Empremta digital Data de venciment	43FB 78F6 F4D8 8453 50B4 D97E B8D0 4C20 18/11/2018 12:16:44

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.

🛑 Nom Cognom - Safata d'entrada - IBM Lotus Notes	
Fitxer Edita Visualitza Crea Accions Ajuda	
Nou 1	' ራ ራ 🏷 🏠 🖶 🗕 🖶 🖷 🏟 🔍 🗮
Tanca Control+W	▼ ↓ ↓ ↓ ↓ ↓ ⊗ @ Q ⁴ ▼
Desa Control+S	
Desa com a versio nova	
Desa automaticament	
Propietats del document	
Base de dades	🕐 💌 Respon a tothom 🔻 Remet 👻 Suprimeix Seguiment 👻 Carpeta 👻 Copia a 👻 Xat 👻 Eines
Replicacio	A Data Y Hora Mida Y Assumpte A
Micratovia instantinia	2001/2000 10:00 12:00 complete
	- 23/01/2009 19:00 12:833 correu signat
Adjunta	
Importa	r 23/01/2009 19:00 14.158 RE: test
Exporta	
Format de pàgina	
Visualització prèvia d'impressió	r 23/01/2009 19:00 12.898 Correu signat
Imprimeix Control+P	
Preferències 2	3 10 707
Seguretat >	Seguretat de l'usuari
Eines +	Bloqueja la visualització F5
Tanca totes les pestanyes de les finestres obertes	Canvia IID 12.944 Correu signat
Desa l'estat de la finestra	
Nejeta l'estat desat de la finestra	
Surt del Notes	
G-2	
Sequiment*	
el Canullid IPC	Visualització pràvia 🔺
	I () () () () () () () () () (
🛃 Inicia 👘 🤌 🐼 🕲 🐣 📵 IBM Lotus Notes	🔲 Nom Cognom - Safat ES 💎

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.

Seguretat de l'usuari		? ×
Seguretat bàsica	Identitat de persones i serveis Les persones i els serveis s'identifiquen miljançant certificats. Podeu decidir en quins certificats podeu confiar com a identificació correcta i eliminar la confiança de qualsevol certificat sosphós. Els certificats voltizen per a protegir les comunicacions: per exemple, necessitareu els certificats d'altres persones per a enviar-los correu xifrat o per a protegir les commexions amb els serveis.	
Persones, Serveis Entitats B ⊕ Accions d'altres C ⊕ Dades del Notes Correu	Cerca el nom al directori i a la libreta d'adreces Certificats La columna Confiança mostra si es confia en el certificat o no. És possible que l'administrador hagi pres la decisió en nom vostre.	
	Confiança Certificat emès a nom de 4 Limitacions > No s'ha trobat el certificat de xiñatge de correu.	
	Literats der certricat Literats sorre la conjunça Suprimeix el certricat Upcont avançades 5 D'acord	Tanca

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 sur 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 <u>Referències</u>

- Informació sobre què és un certificat <u>http://www.catcert.cat/web/cat/0_0_quees.jsp</u>
- Preguntes freqüents sobre el funcionament dels certificats <u>http://www.catcert.cat/web/cat/0 0 1 preguntes.jsp</u>
- Web de l' Identitat digital UPC

https://www.upc.edu/identitatdigital/

 Espai de preguntes i respostes més freqüents de l' Identitat digital UPC <u>https://www.upc.edu/identitatdigital/altres</u>