Universitat de Lleida
Web de la universitat de Lleida [http://www.udl.cat/]
Pl. de Víctor Siurana, 1 E-25003 Lleida | Tel. +34 973 70 20 00

3. FUNCIONAMENT DE LA SIGNATURA ELECTRÒNICA

La targeta UdL és l'objecte contenidor del certificat digital (del PDI, PAS i estudiantat) que, un cop inserit en el lector del teclat (o en un d'extern) permetrà que el navegador (lector de correu, visor de documents PDF, office, etc.) signi els tràmits, documents i usos de l'administració electrònica.

La signatura electrònica mitjançant un certificat digital es basa en la criptografia asimètrica i en l'ús d'un parell de claus úniques i irrepetibles.

La criptografia asimètrica és el mètode matemàtic emprat per generar una clau privada i una clau pública, amb les quals podem codificar i descodificar informació mitjançant unes fórmules matemàtiques anomenades algorismes.

La clau privada és absolutament secreta i serveix per signar documents, missatges o tràmits amb garantia d'integritat, autentificació, confidencialitat i no repudi.

La clau pública s'ha de lliurar al receptor del document, missatge o tràmit per a que aquest pugui verificar l'autenticitat de l'emissor i de la seua tramesa.

La clau pública també serveix per xifrar, metre que la clau privada serveix per desxifrar.

La signatura electrònica permet quatre operacions bàsiques: signar, xifrar, verificar i identificar.

SIGNAR I XIFRAR

Jo disposo de ...	Que jo utilitzo per a ...	Jo t'envio el missatge o document ...	Tu reps el missatge o document ...
la meua clau privada	**signar** un missatge o document	signat, que inclou la meua clau pública	signat, que verifiques amb la meua clau pública

la teua clau pública, que he rebut en un missatge o document signat per tu	**xifrar** un missatge o document	xifrat	xifrat, que desxifres amb la teua clau privada

VERIFICAR I VALIDAR

Jo disposo de ...	Que jo utilitzo per ...	Consultant la ...	Mitjançant ...
la teua clau pública, que he rebut amb un missatge o un document signat	**verificar** la validesa de la teua signatura electrònica	llista de revocació o CRL (“Certificate Revocation List”) és la llista de certificats donats de baixa (invàlids) per l’Autoritat de Certificació CATCert	una configuració adequada del meu navegador, visor PDF, eina de verificació específica (com **PSIS** ://testvalidacio.catcert.cat/psiswebclie), o consultant directament la **llista de revocació en la web de la CATCert** http://epscd.catcert.cat/crl/ec-ur.crl

IDENTIFICAR

Jo lliuro ...	Que ...	Que em permet ...	I que pot ser ...
la meua clau pública, amb els missatges de correu que envio o els documents que signo	m’**identifica** com a subscriptor i posseïdor de la clau privada d’identificació i signatura	la generació de la signatura electrònica reconeguda	verificada


[#]