

# PROCEDIMENT DE L'ÚS DEL PROGRAMA D'ENCRIPTACIÓ DE DADES GPG4WIN

Gpg4win és un paquet de xifrat de correu electrònic i arxius per a la majoria de les versions de Microsoft Windows, que utilitza criptografia de clau pública GnuPG per al xifrat de dades i signatures digitals.

La creació original de Gpg4win va ser secundat per l'Oficina Federal per a la Seguretat de la Informació d'Alemanya. No obstant això Gpg4win i totes les eines que s'inclouen són de programari lliure i de codi obert, i és en general l'opció no propietària de la vida privada recomanada per als usuaris de Windows.

### Legislació

La Llei orgànica de Protecció de Dades de Caràcter Personal 03/2018 de 5 de desembre (LOPD), té per objecte protegir i garantir les llibertats i els drets fonamentals de les persones físiques, el seu honor i intimitat personal i familiar.

La LOPD estableix unes obligacions en relació a la protecció de dades de caràcter personal continguts en fitxers automatitzats i no automatitzats (en paper) que posseeixen empreses i administracions públiques, i que són tractats per aquestes amb diferents finalitats.

Després de l'anàlisi d'impacte dut a terme pel IBESTAT, en uns certs tractaments realitzats per aquest, s'ha identificat la necessitat d'implementar salvaguardes que protegeixin la informació gestionada d'aquelles amenaces que, després de la pertinent anàlisi de riscos, suposin un risc elevat per a les diferents dimensions de la seguretat. Entre aquestes salvaguardes i en relació amb la present instrucció, destaca la implementació de polítiques de xifratge de la informació a fi de garantir la confidencialitat d'aquesta.

La **criptografia asimètrica** (en anglès *asymmetric key cryptography*), també anomenada **criptografia de clau pública** (en anglès *public key cryptography*) o **criptografia de dues claus**<sup>1</sup> (en anglès *two-key cryptography*), és el mètode <u>criptogràfic</u> que usa un parell de claus per a l'enviament de missatges. Les dues claus pertanyen a la mateixa persona que rebrà el missatge. Una clau és pública i es pot lliurar a qualsevol persona, l'altra clau és privada i el propietari ha de guardar-la de manera que ningú tingui accés a ella. A més, els mètodes criptogràfics garanteixen que aquesta parella de claus només es pot generar una vegada, de manera que es pot assumir que no és possible que dues persones hagin obtingut casualment la mateixa parella de claus.

Si una persona que emet un missatge a un destinatari, usa la clau pública d'aquest últim per a xifrar-lo; una vegada xifrat, només la clau privada del destinatari podrà desxifrar el missatge, ja que és l'únic que hauria de conèixer-la. Per tant s'aconsegueix la *confidencialitat* de l'enviament del missatge, és *extremadament difícil que el desxifri algú excepte el destinatari*.

<sup>&</sup>lt;sup>1</sup> <u>https://ca.wikipedia.org/wiki/Criptografia\_de\_clau\_p%C3%BAblica</u>



Qualsevol, usant la clau pública del destinatari, pot xifrar-li missatges; els que seran desxifrats pel destinatari usant la seva clau privada.

Si el propietari del parell de claus usa la seva clau privada per a xifrar un missatge, qualsevol pot desxifrar-lo utilitzant la clau pública del primer. En aquest cas s'aconsegueix la *identificació i autenticació* del remitent, ja que se sap que només podia haver estat ell qui va emprar la seva clau privada (tret que un tercer l'hagi obtingut). Aquesta idea és el fonament de la <u>signatura</u> digital, on jurídicament existeix la presumpció que el signant és efectivament l'amo de la clau privada.

Els 'sistemes de xifratge de clau pública' o 'sistemes de xifratge asimètrics' es van inventar amb la finalitat d'evitar per complet el problema de l'intercanvi de claus dels <u>sistemes de xifratge</u> <u>simètrics.</u> Amb les claus públiques no és necessari que el remitent i el destinatari es posin d'acord en la clau a emprar. Tot el que es requereix és que, abans d'iniciar la comunicació secreta, cadascun ha d'aconseguir la clau pública de l'altre i cuidar cadascun la seva clau privada. És més, aquestes mateixes claus públiques poden ser usada per qualsevol que desitgi comunicar-se amb algun d'ells sempre que s'utilitzi correctament la clau pública de cadascun.



## Creació i enviament de clau pública en Gpg4win

Una vegada instal·lat i reiniciat el sistema, podem anar a la barra de tasques de Windows (on es troba el rellotge del sistema) i li donem a la icona que simbolitza un cap vermell.

Aquesta icona ens permet obrir l'eina Kleopatra per a la gestió dels certificats i per a encriptar/desencriptar els fitxers.

Li donem al botó dret sobre aquesta icona i ens mostra la finestra següent:



Seleccionem l'opció d'obrir el gestor de certificat.

Archivo       Ver       Certificados       Herramientas       Preferencias       Ventana       Ayuda         Image: Cirrar       Im	
Importance	
	ls
Bienvenido a Kleopatra Gpg4win-3.1.16	
Kleopatra es una interfaz para el software de cifrado <u>GnuPG</u> .	
Para la mayoría de las acciones necesita una clave pública (certificado) o su propia clave privada.	
<ul> <li>La clave privada no es necesaria para descifrar o firmar.</li> <li>Otras personas pueden usar la clave pública para verificar su identidad o cifrar para usted.</li> </ul>	
Puede aprender más sobre esto en la <u>Wikipedia</u> .	
Nuevo par de daves	

En obrir el programa trobats dues principals opcions, la de generar un nou parell de claus (que ens permet generar la clau publica que podrem compartir i la clau privada que conté la contrasenya que ens permetrà desencriptar els fitxers que ens enviïn amb la publica).



I l'opció d'Importar, que ens permet importar al nostre repositori les claus publiques d'altres persones/entitats, per a poder fer la tasca d'encriptar els fitxers que els hem d'enviar amb la seguretat necessària.

En seleccionar l'opció de generar un nou parell de claus, s'obrirà un assistent per a poder crear la nostra clau publica que utilitzarem per a encriptar fitxers que vagin destinats a nosaltres, ens demanarà el nom que volem que surti, la nostra adreça de correu electrònic i després li podrem assignar una clau privada que només coneixerem nosaltres en principi i ens servirà per a obrir i desencriptar el fitxer que ens enviïn.

		?	×
← Asisten	te de creación del par de claves		Ī
Introdu	izca detalles		
Por favor parámetro	, introduzca sus detalles personales debajo. Si desea más control sobre lo os, pulse el botón «Configuración avanzada».	s	
Nombre:	Usuario		(opcional)
Correo:	Usuario@CAIB.ES		(opcional)
	Proteger la clave generada con una frase de contraseña.		
	Usuario <usuario@caib.es></usuario@caib.es>	ava	nzada
	Crear	С	ancel

Una vegada creada la clau publica que compartirem sortirà en el llistat de "Certificats", el millor és exportar la clau pública i enviar-la a qui ens encriptarà dades ja que en realitzar el procés indiqués que el faci amb les nostres dades i només nosaltres podrem visualitzar el contingut amb la nostra clau.

큤 Kleopatra					-	n x
Archivo Ver Certificados	Herramientas Prefere	ncias Ventana Ayu	da			
Firmar/Cifrar Descifrar/verific	ar Importar Expo	E⊒ E⊒ rtar Certificar B	Q úsqueda en el servidor	. Certificados Bl	c de notas Sn	nartCards
Buscar <alt+q></alt+q>				Todos los certifica	idos	~ <b>1</b>
Todos los certificados	Certificados importados	Certificados importado	IS			8
Nombre	e	Corre	0	ID de los usuarios	Válido desde	Válido h
IBESTAT (Institut d'Esta	adística de les Ille info	o@ibestat.caib.es		certificado	11/07/2012	
	$\searrow$					
٢						>



Ens col·loquem damunt de la clau que volem exportar i amb el botó dret li donem a exportar, ens creés un fitxer amb extensió "ASC", i és el que hem d'enviar perquè ens puguin encriptar amb la nostra clau, si aquesta persona rep aquesta clau publica nostra, l'importés en el seu joc de claus i quan hagi d'encriptar alguna cosa per a nosaltres ho farà amb aquesta clau pública.

### **Desencriptar fitxers encriptats**

Per a desencriptar només cal anar al fitxer en concret, i li donem al botó dret, després a l'opció de:

Descifrar y verificar.

llavors ens demanarà la clau privada associada a aquest fitxer que serà la que vam posar al principi en crear el parell de claus.

#### Encriptar dades amb claus publiques

Per a poder enviar fitxers encriptats a algú, hem de disposar de la seva clau pública perquè només ell pugui desencriptar el contingut amb la clau privada associada.

Per a importar la clau pública d'algú procedirem a donar-li doble clic al fitxer que ens envien amb extensió "ASC" i tot seguit ens mostra automàticament la següent finestra:

🗇 Res	ultado de la importación del certificado - Kleopatra	?	Х
1	Detalles del resultado de la importación de G: \Informatica\Privat\Claves PGP\IBESTAT\IBESTAT\IBESTAT (Institut d'Estadística de les Illes Balears)_incluida_l. Número total procesado; 2 Importado: 0 Claves sin ID de usuario: 1 Sin cambios: 1 Claves secretas procesadas: 1 Claves secretas sin cambios: 2	a_privad	la.asc:
	I	OK	

En obrir la interface de Kleopatra, ens apareix ja el certificat (clau publica), que hem importat i ja podem utilitzar-la per a encriptar els fitxers a enviar i que només el destinatari amb la seva clau privada podrà desencriptar.



🗇 Kle	opatra	Certificados	Herramien	tas Pr	eferencias	Ventana (	lyuda			_		×
Firmar/C	Difrar	Lo Descifrar/verific	car Impo	ntar	Exportar	Certificar	Búsqu	Q leda en el servidor	Certificados	Eloc de notas	SmartCar	rds
Busca	ar <alt Todos la</alt 	+Q>	Certificado	s importa	dos Cert	ificados import	tados		Todos los certifi	cados	~	<b>1</b>
	DECTAT	Nombr	e adíctica da l		info@ibor	Co	orreo		ID de los usuario	s Válido deso	de Válid	o hi
				ß								
<												>

El procés per a encriptar és més senzill, simplement ens col·loquem damunt del fitxer a encriptar i premem el botó dret, en aparèixer el menú contextual seleccionarem

		Firmar con AutoFirma		
IBE_AENA_AEROPO		Assistent de signatura electrònica		
		Encrypt to PGP		
	Q	search with grepWin		
	10	AES Encrypt		
	2	Edit with Notepad++		
	٥	Firmar v cifrar		
		Tilliai y cillai	63	
		Más opciones de GpgEX		>



🗇 Firmar/cifrar archivos - Kleopatra				
Firmar o cifra	r archivos			
Probar autenticidad (fir	mar)			
Firmar como:	IBESTAT <info@ibestat.caib.es> (certificado, creado: 11/07/2012)</info@ibestat.caib.es>		$\sim$	
Cifrar				
Cifrar para mí:	☑ IBESTAT <info@ibestat.caib.es> (certificado, creado: 11/07/2012)</info@ibestat.caib.es>		$\sim$	
Cifrar para otros:	stadística de les Illes Balears) <info@ibestat.caib.es> (certificado, OpenPGP, creado:</info@ibestat.caib.es>	11/07/	2012)	
	4 Por favor, introduzca un nombre o dirección de correo			
Cifrar con contrase	rña. Cualquiel persona con la que comparta la contraseña podrá ver los datos.			
Salida				
Cifrar o firmar cada	a archivo por separado.			
/Informatica	/Public/BACKUP Historicos/AENA/AENA AEROPORTS/IBE_AENA_AEROPORTS_2016.xls.gpg	€		
	Cifrar	Cano	el	

Hem d'indicar la clau publica del destinatari, i posteriorment indicar-li el directori de sortida on se situés el fitxer encriptat.

### PGPtool

Existeix una alternativa al programa Gpg4win, i és una eina anomenada PGPtool, el seu funcionament és molt similar a l'anterior, però és mes lleuger i senzill d'utilitzar.



Aquest programa requereix tenir instal·lat en el sistema el JAVA RUNTIME ENVIRONMENT +18, per a funcionar.



Per a crear des d'aquest programa la clau publica i privada, es realitza a través del corresponent menú:

🖭 PGPT	Tool	
PGPTool	Key ring	Actions
	Ор	en PGP keys list
	Im	oort PGP Key
	Imp	oort PGP Key from clipboard
Previous	Cre	ate PGP key 🔁 -e
💽 Creat	e PGP key	×
	Full name	
	Email	
P	assphrase	
Passphra	se (again)	
		Create Cancel

La pàgina per a la seva descàrrega i instruccions d'ús es troba disponible en:

https://pgptool.github.io