



CRIPTOGRAFIA

Clau Asimètrica

(Clau pública)

Recordem....CRIPTOGRAFIA SIMÈTRICA

Els principals problemes dels sistemes de xifratge simètric:

→ L'intercanvi de claus

- ◆ Quin canal de comunicació segur han usat per a transmetre's les claus?
- ◆ Més fàcil per a l'atacant intentar interceptar una clau que provar totes les possibles combinacions.

→ El nombre de claus que es necessiten

- ◆ Per a n persones que necessiten comunicar-se entre si, es necessiten $n(n-1)/2$ claus diferents
90 persones -> 4.005 claus 300 persones -> 44.850 claus 6000 persones -> 17.997.000 claus
- ◆ Funciona amb un grup reduït de persones

→ Fortalesa de la clau

- ◆ **Principi de Kerckhoffs** i
- ◆ La responsabilitat de la fortalesa de la clau recau sobre l'usuari

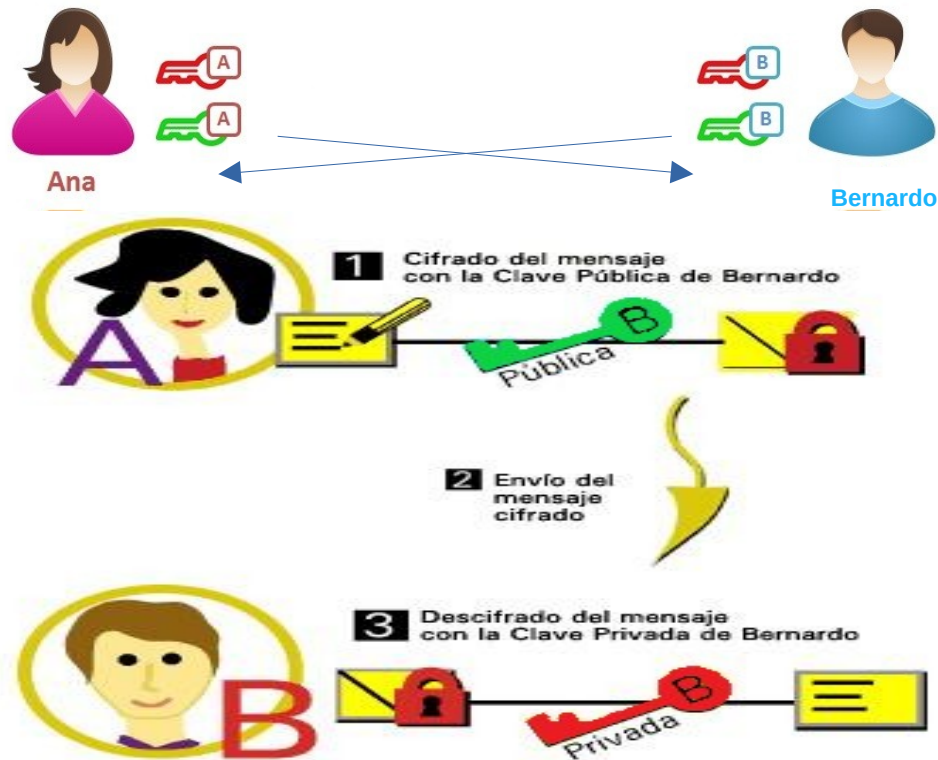
CRIPTOGRAFIA DE CLAU ASIMÈTRICA

Cada usuari del sistema ha de tindre una parella de claus

- **Clau pública:** coneguda per tothom
- **Clau privada:** custodiada per el propietari i no se donarà a conèixer mai a ningú que no siga el propietari
- **Les claus no les decideixen els usuaris.** : Les calcula un algorisme

Video:

Asymmetric Encryption : Simply explained



CRIPTOGRAFIA DE CLAU ASIMÈTRICA

Claus

- Parella de claus complementàries: el que xifra una, sols ho pot desxifrar l'altra i viceversa
- Aquestes claus s'obtenen mitjançant mètodes matemàtics complicats de manera que per raons de còmput és impossible conèixer una clau a partir d'una altra.

Avantatges

- Se sol xifrar amb una clau i desxifrar amb una altra

Desavantatges

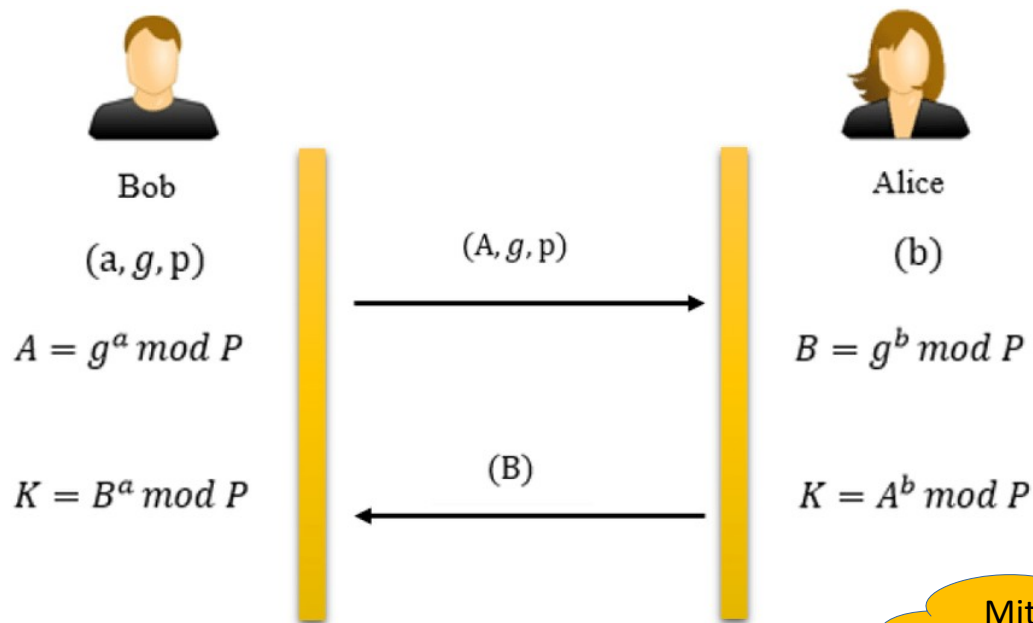
- Per a una mateixa longitud de clau el missatge es necessita **major temps** de procés
- Les claus han de ser de **major grandària** que les simètriques, es recomanen claus públiques de **1024 bits com a mínim**
- El missatge xifrat ocupa més espai que l'original

Algorismes de tècniques de clau asimètrica:

- **Diffe-Hellman, RSA, ECC, ElGamal...**

XIFRAT ASIMÈTRIC

Diffie-Hellman (Key exchange protocol) [video](#)



Bob calcula a, g, p , i A
Bob envia g, p i A (no envia a)

Alice calcula b, B i K
(K es calcula en dades que no han sigut transmeses)
Alice envia B

Bob, amb B , calcula K
(K es calcula en dades que no han sigut transmeses)

Bob i Alice saben K ,
 K no s'ha enviat en cap moment
 K no es pot calcular per una altra part, degut a les propietats matemàtiques de les operacions utilitzades.

K serà la clau de sessió

Mitjançant A, g, p, B
NO es pot calcular K

XIFRAT ASIMÈTRIC

RSA(Rivest, Shamir y Adleman, algorisme de xifrat asimètric)

Generación de claves

1. Seleccionar dos números primos: p, q
2. Calcular: $n = p * q$
3. Calcular: $z = (p - 1) * (q - 1)$
4. Seleccionar un entero k que cumpla:
 $\text{gcd}(z, k) = 1; 1 < k < z$
gcd: greatest common divisor (máximo común divisor)
5. Elegir j de modo que cumpla:
 $k * j = 1 \pmod{z}$

En la práctica: elegir un j entero que verifique
 $j = (1+x*z)/k$
para algún valor entero de k

Clave Pública:

(n, k)

Clave Privada:

(j)

XIFRAT ASIMÈTRIC

RSA(Rivest, Shamir y Adleman, algorisme de xifrat asimètric)

Cifrado y descifrado	
<p>Texto cifrado: C, que verifica: $M^k = C \pmod{n}$</p> <p>Que puede calcularse así: $C = M^k \% n$ (donde '%' calcula el módulo)</p>	<p>Texto plano: M, que verifica: $C^j = M \pmod{n}$</p> <p>Que puede calcularse así: $M = C^j \% n$ (donde '%' calcula el módulo)</p>

COMPARATIVA CRIPTOGRAFIA SIMÈTRICA I ASIMÈTRICA

Atributo	Clave simétrica	Clave asimétrica
Años en uso	Miles	Menos de 50
Velocidad	Rápida	Lenta
Uso principal	Cifrado de grandes volúmenes de datos	Intercambio de claves Firma digital
Claves	Compartidas entre emisor y receptor	Privada: sólo conocida por 1 persona. Pública: conocida por todos.
Intercambio de claves	Difícil de intercambiar por un canal inseguro	La clave pública se comparte por cualquier canal. La privada nunca se comparte
Longitud de claves	56 bits (vulnerable) 256 bits (seguro)	1024 bits mínimo
Algoritmos	DES, 3DES, Blowfish, IDEA, AES	Diffie-Hellman, RSA, DSA, ElGamal
Servicios de seguridad	Confidencialidad Integridad Autenticación	Confidencialidad Integridad Autenticación, No repudio

CRIPTOGRAFIA ASIMÈTRICA

Pràctica

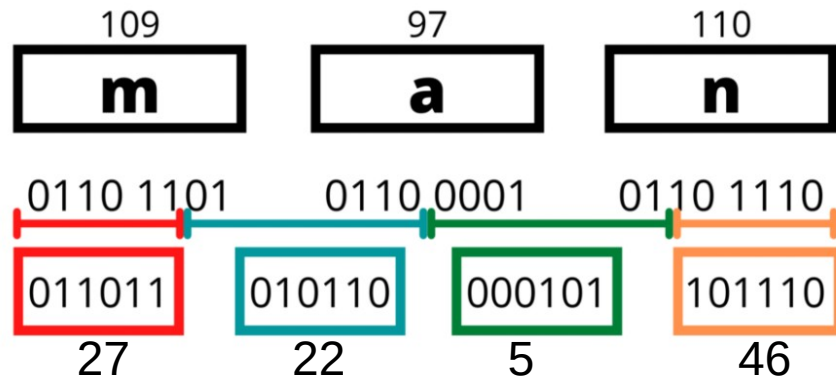
Instal·lar extensió per a Chrome FlowCrypt

- 1. Generar claus i compartir la clau pública.**
- 2. Enviar un correu xifrat a un company que tinga instal·lada la extensió.**
- 3. Enviar un correu xifrat(simètric) a un compte que no tinga instal·lada la extensió.**
- 4. Enviar un correu incloguent parts no xifrades.**

XIFRAT ASIMÈTRIC – Base64 - $2^6=64$

Els xifrats moderns treballen a nivell de bit. (Les claus també)

Caracteres ASCII de control			Caracteres ASCII imprimibles					
00	NULL	(carácter nulo)	32	espacio	64	@	96	`
01	SOH	(inicio encabezado)	33	!	65	A	97	a
02	STX	(inicio texto)	34	"	66	B	98	b
03	ETX	(fin de texto)	35	#	67	C	99	c
04	EOT	(fin transmisión)	36	\$	68	D	100	d
05	ENQ	(consulta)	37	%	69	E	101	e
06	ACK	(reconocimiento)	38	&	70	F	102	f
07	BEL	(timbre)	39	'	71	G	103	g
08	BS	(retroceso)	40	(72	H	104	h
09	HT	(tab horizontal)	41)	73	I	105	i
10	LF	(nueva línea)	42	*	74	J	106	j
11	VT	(tab vertical)	43	+	75	K	107	k
12	FF	(nueva página)	44	,	76	L	108	l
13	CR	(retorno de carro)	45	-	77	M	109	m
14	SO	(desplaza afuera)	46	.	78	N	110	n
15	SI	(desplaza adentro)	47	/	79	O	111	o
16	DLE	(esc.vínculo datos)	48	0	80	P	112	p
17	DC1	(control disp. 1)	49	1	81	Q	113	q
18	DC2	(control disp. 2)	50	2	82	R	114	r
19	DC3	(control disp. 3)	51	3	83	S	115	s
20	DC4	(control disp. 4)	52	4	84	T	116	t
21	NAK	(conf. negativa)	53	5	85	U	117	u
22	SYN	(inactividad sínc)	54	6	86	V	118	v
23	ETB	(fin bloque trans)	55	7	87	W	119	w
24	CAN	(cancelar)	56	8	88	X	120	x
25	EM	(fin del medio)	57	9	89	Y	121	y
26	SUB	(sustitución)	58	:	90	Z	122	z
27	ESC	(escape)	59	;	91	[123	{
28	FS	(sep. archivos)	60	<	92	\	124	
29	GS	(sep. grupos)	61	=	93]	125	}
30	RS	(sep. registros)	62	>	94	^	126	~
31	US	(sep. unidades)	63	?	95	_		
127	DEL	(suprimir)						

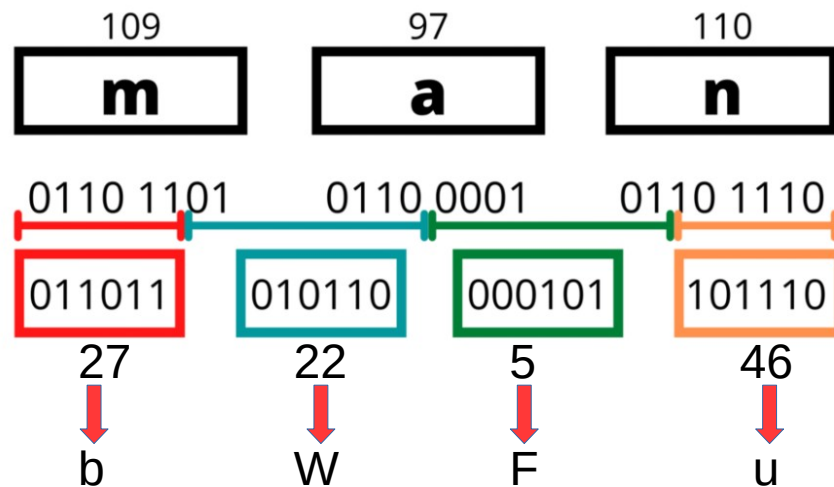


Perquè usar la codificació BASE64 ??
Per permetre la transferència i l'emmagatzematge de dades binàries a través de mitjans que podrien no ser capaços de manejar dades binàries directament

XIFRAT ASIMÈTRIC – Base64 - $2^6=64$

64 → ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-

Base64 Index Table							
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/



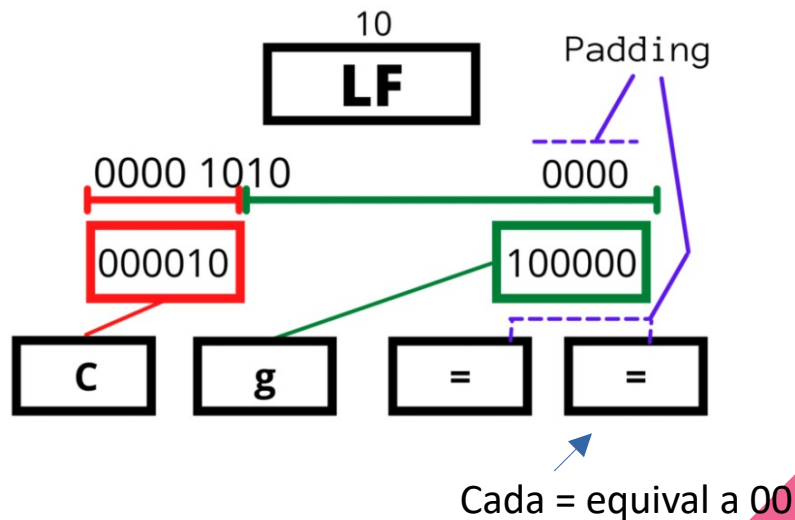
De moment quadra, $8 \times 3 = 24$
I $24/6 = 4$ símbols en base64

XIFRAT ASIMÈTRIC – Base64 - $2^6=64$

64 → ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/,

Base64 Index Table							
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Quan no es múltiple de 6 → Farcit / Padding



XIFRAT ASIMÈTRIC – Base64 - $2^6=64$

64 → ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-

H SA==
Ho SG8=
Hol SG9s
Hola SG9sYQ==
Hola SG9sYSA=
Hola M SG9sYSBN

H son 8 bits, fins a proper múltiple de 6 (12) falten 4 ceros , ==
Ho son 16 bits, fins al proper múltiple de 6(18) falten 2 ceros, =
Hol son 24 bits, fins al proper múltiple de 6(24) no falten ceros

Cada = equival a 00

...

...

Hola Mundo SG9sYSBNdW5kbw==

H	o	l	a	
01001000	01101111	01101100	01100001	
010010	000110	111101	101100	011000 010000
S	G	9	s	Y Q = =

et sents capaç de fer una funció en python
que arreplegue una cadena i
retorne el nombre de zeros a afegir?



XIFRAT ASIMÈTRIC

PGP (Pretty Good Privacy)

- Programa més popular d'encryptació i de creació de claus públiques i privades per a seguretat en documents i aplicacions informàtiques
- Es considera híbrid

GPG o (GNU Privacy Guard)

- Eina per a xifratge i signatures digitals
- Reemplaçament de PGP, és programari lliure llicenciat baix GPL

Comando: gpg

opcions : **-c (xifrat simètric)** Genera un arxiu amb extensió .pgp
-d (desxifrat)



```
(kali㉿kali)-[~]  
$ gpg -c fichero
```

Exemple: **gpg -c arxiu**
gpg -d arxiu.gpg

¿ ... Ha funcionat bé ?

¿ On estan les claus asimètriques ?

XIFRAT ASIMÈTRIC

OpenSSL

- ➔ Projecte de programari lliure consistent en un robust paquet d'eines d'administració i biblioteques relacionades amb la criptografia, que subministren funcions criptogràfiques a altres paquets com OpenSSH i navegadors web.
- ➔ Xifra (simètrica) , Xifra (asimètric), Hash, Signatura, Certificats digitals, PKI, conversió entre formats, monitoratge de la connectivitat d'un Servidor Web Segur, Comprovació d'expiració de certificats, generar contrasenyes aleatòries.

XIFRAT ASIMÈTRIC

GPG (GNU Privacy Guard)

1 Generar parell de claus per a xifrat asimètric: `gpg --gen-key` o `gpg --full-generate-key`

Durant el procés de generació se'ns aniran fent diverses preguntes:

- ➔ Tipus de xifratge. L'opció DSA and ElGamal ens permet encriptar i signar **escollim 1**
- ➔ Grandària de les claus. Per defecte es recomana 3072 (a major grandària més seguretat) **=>4096**
- ➔ Temps de validesa de la clau. 0 indicarà que no caduqui mai. **(NO RECOMANAT !!!) posa termini**
- ➔ Frase de pas (o passphrase) Contrasenya que ens assegurarà que ningú més que nosaltres mateixos podrà usar aquesta clau GPG

2 Comprovar les claus

- ➔ Vore les claus públiques disponibles: `gpg --list-keys` `(-k` o `--list-public-keys)`
- ➔ Vore les claus privades `gpg --list-secret-keys` `(-K)`

XIFRAT ASIMÈTRIC

GPG (GNU Privacy Guard)

3 Com vore la ClauID

gpg --list-key --keyid-format SHORT

```
(kali㉿kali)-[~]  
$ gpg --list-keys --keyid-format SHORT  
/home/kali/.gnupg/pubring.kbx  
-----  
pub   rsa4096/190B11F1 2023-10-11 [SC]  
      E11FFDFF1705FAD2EA5810CCCA7D692D190B11F1  
uid    [ultimate] practica gpg (SC) <practica@gpg.es>  
sub    rsa4096/505AC2A8 2023-10-11 [E]
```

La ClauID és molt important !! , ja que s'utilitzarà per a qualsevol operació sobre les nostres claus o sobre les claus dels altres.

Compte, perquè hi ha dos !! (o quatre !!)

XIFRAT ASIMÈTRIC

GPG (GNU Privacy Guard)

¿Perquè hi ha dos?

```
(kali㉿kali)-[~]  
$ gpg --list-keys --keyid-format SHORT  
/home/kali/.gnupg/pubring.kbx  
-----  
pub   rsa4096/190B11F1 2023-10-11 [SC]  
      E11FFDFF1705FAD2EA5810CCCA7D692D190B11F1  
uid           [ultimate] practica gpg (SC) <practica@gpg.es>  
sub   rsa4096/505AC2A8 2023-10-11 [E]
```

Hi ha una clau mestra i una subclau.

La clau mestra s'utilitza per a [SC] Sign , Cert

La subclau s'utilitza per a [E] Encrypt

4. Esborrar claus

- ➔ Esborrar la clau privada: **gpg --delete-secret-key ClaveID**
- ➔ Esborrar la clau pública: **gpg --delete-key ClaveID**

En este
ordre

XIFRAT ASIMÈTRIC

PGP (GNU Privacy Guard)

5. Distribució de la clau pública (dos opcions):

- 1) Pujar-la a un servidor de claus públiques (pe El servidor pgp de rediris)
- 2) Els servidors solen estar interconnectats

gpg --send-keys --keyserver pgp.rediris.es ClaveID

- Per buscar les claus públiques en el servidor

gpg --keyserver NombreDelServidor --search-keys ClaveID/nombre/email

- Per descarregar la clau pública del servidor

gpg --keyserver NombreDelServidor --recv-keys ClaveID

- 2) Enviar-la per correu o en suport portable (pendrive, CD/DVD ...)

La bolquem en un fitxer de text

gpg --armor --output fichero --export ClaveID



Fem servir este

6. Fer una còpia de la nostra clau privada per a poder recuperar-la:

gpg --armor --output fichero --export-secret-key ClaveID

XIFRAT ASIMÈTRIC

GPG (GNU Privacy Guard)

7 Importar la clau bolcada en un fitxer

```
gpg --import fichero
```

8. Eliminar claus distribuïdes en servidors (¡¡ no es poden esborrar !!)

Si s'ha oblidat la contrasenya o hem perdut la clau privada o considerem que està compromesa podem generar un certificat de revocació i pujar-lo al servidor de claus

(es recomana generar aquest certificat al final del procés de generació de claus)

```
gpg -o revocacion.asc --gen-revoke ClaveID
```

1) Crear certificat de revocació :

```
gpg -o revocacion.asc --gen-revoke claveID
```

2) Revocar la clau (importació a la nostra relació de claus)

```
gpg --import revocacion.asc
```

3) Comunicar a els servidors que la nostra clau ja no és vàlida

```
gpg --keyserver NombreDelServidor --send-key ClaveID
```

XIFRAT ASIMÈTRIC

GPG (GNU Privacy Guard)

CONFIDENCIALITAT

9. Encriptar un fitxer amb la clau pública (del destinatari)

```
gpg --encrypt --recipient clavelD documento.txt
```

```
gpg -e -r clavelD documento.txt
```

```
gpg -e -r nom@mail.net documento.txt
```

```
gpg -e -r nom@mail.net -o doc.xifrat documento.txt
```

10. Desencriptar un fitxer amb la clau privada (el que rep)

```
gpg -d documento.txt.gpg
```

```
gpg -d -o doc.desxifrat documento.txt.gpg
```

Manual de GPG: xifra, signa i envia dades de manera segura

XIFRAT ASIMÈTRIC

GPG (GNU Privacy Guard)

AUTENTICIDAD

11. Signar fitxer

```
gpg -u XXXXXXXXX --output documento-firmado.sig --clearsign documento-sin-firmar
```

```
gpg -u XXXXXXXXX --output documento-firmado.sig --sign documento-sin-firmar
```

12 (el que rep) “Verifica” un fitxer amb la clau PÚBLICA del que envia

```
gpg -d documento-firmado.sig
```

```
gpg --verify documento-firmado.sig
```

[Manual de GPG: xifra, signa i envia dades de manera segura](#)

XIFRAT ASIMÈTRIC

GPG (GNU Privacy Guard)

MANTENIMENT

13. Modificació de la passphrase de la clau privada

Busca informació sobre el comando **gpg** utilitzant la ferramenta **man** de linux

Sobre com canviar la passphrase de la teua clau privada

Activitat:

Canvia la passphrase de la teua clau privada i exporta-la
Compara amb la clau exportada previament

Activitat:

Busca com utilitzar gpg per crear un nombre aleatori
Busca com utilitzar gpg per crear un nombre primer (primo)

XIFRAT ASIMÈTRIC

GPG (GNU Privacy Guard)

MANTENIMENT

14. Modificació de la passphrase de la clau privada

Busca informació sobre el comando **gpg** utilitzant la ferramenta **man** de linux

Sobre com canviar la data de caducitat de la teua clau privada

Activitat:

Canvia la data d'expiració de la teua clau privada i exporta-la

Compara amb la clau exportada previamente

CRIPTOGRAFIA HÍBRIDA

Utilitza els dos algorismes:

→ **Algorisme de clau pública**

◆ Per al xifratge en l'enviament de la clau simètrica (petita quantitat d'informació). Més segur

→ **Algorisme de clau simètrica**

◆ Per al xifratge del missatge. Es redueix el cost computacional

→ **Eines SW que usen els algorismes anteriors:**

◆ **PGP , GPG , OpenSSL**

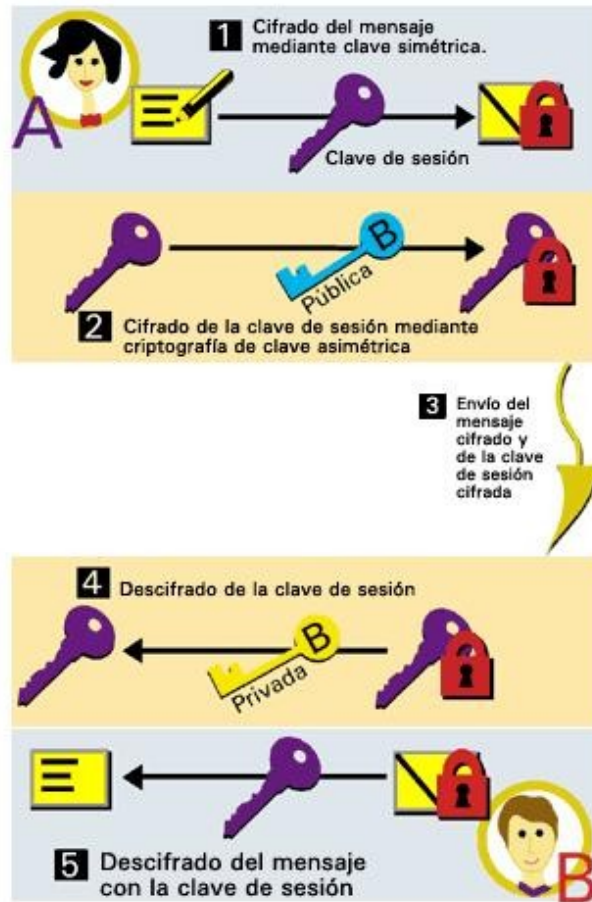
→ **Protocols de comunicació que usen els algorismes anteriors**

◆ **SSH, SSL y TLS**

CRIPTOGRAFIA HÍBRIDA

PROCÉS:

- **A** i **B** tenen els seus parells de claus respectives
- **A** escriu un missatge a **B**. El xifra amb el sistema de **criptografia de clau simètrica**. La clau que utilitza s'anomena **clau de sessió** i se genera aleatòriament. Per enviar la **clau de sessió** de forma segura, esta se xifra amb la clau pública de **B**, utilitzant per tant **criptografia de clau asimètrica**
- **B** rep el missatge xifrat amb la **clau de sessió** i esta mateixa xifrada amb la seua clau pública. Per a realitzar el procés invers, en primer lloc utilitza la seua **clau privada** per a desxifrar la **clau de sessió** una vegada obtinguda la clau de sessió ja pot desxifrar el missatge



El diagrama ilustra el proceso de criptografía híbrida de Diffie-Hellman entre Ana y Bob:

- Generación de Clave de Sesión (CS):** Ana y Bob generan sus propias claves privadas (A y B) y las combinan para crear una clave de sesión compartida (CS) que se genera aleatoriamente en el emisor.
- Intercambio de Claves Públicas:** Ana y Bob intercambian sus claves públicas (A y B) a través de un canal seguro, etiquetado como "Cifrado de Clave Pública".
- Cifrado del Mensaje:** Ana toma su "Mensaje en claro" y lo cifra utilizando la clave de sesión (CS) generada, etiquetado como "Cifrado del mensaje Con Clave de Sesión".
- Envío del Mensaje Cifrado:** El "Mensaje cifrado" (representado por una cadena binaria) es enviado a Bob.
- Descifrado del Mensaje:** Bob utiliza la clave de sesión (CS) para descifrar el mensaje, etiquetado como "Descifrado del mensaje utilizando la Clave de Sesión descifrada".
- Cifrado de la Clave de Sesión:** Ana cifra la clave de sesión (CS) con la clave pública de Bob (B) para enviarla de forma segura, etiquetado como "Cifrado de Clave de Sesión con Clave Pública de Bob".
- Descifrado de la Clave de Sesión:** Bob recibe la clave de sesión cifrada y la descifra con su clave privada (B) para recuperar la clave de sesión original, etiquetado como "Descifrado de Clave de Sesión con Clave Privada de Bob".

El diagrama concluye con la etiqueta "@C.R.S."



SIGNATURA DIGITAL

→ **Permet al receptor d'un missatge:**

- ◆ Verificar l'autenticitat de l'origen de la informació (**autenticació**)
- ◆ Verificar que la informació no ha estat modificada des de la seva generació (**integritat**)

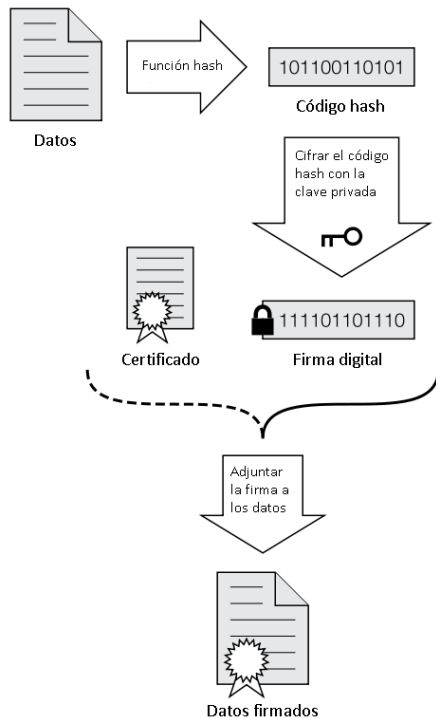
→ **L'emissor del missatge signat no pot argumentar que no ho va fer (**no repudi**)**

- Una **signatura digital** està destinada al mateix propòsit que una manuscrita, però la manuscrita és senzilla de falsificar, mentre que la digital és impossible mentre no es descobreixi la **clau privada** del signant
- La **signatura digital** és un xifratge del missatge que s'està signant però utilitzant la **clau privada** en lloc de la pública

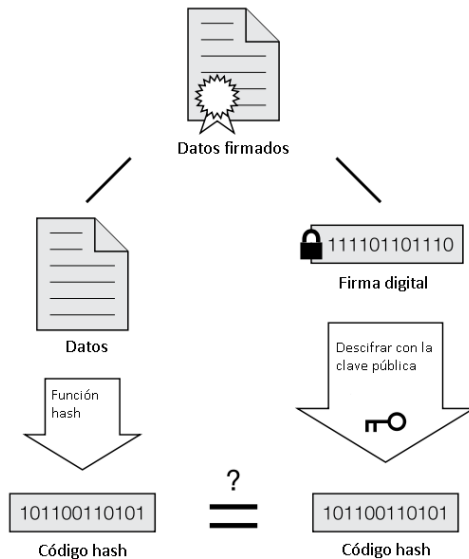
Signatura digital = resultat de xifrar amb clau privada el resum de dades a signar, fent ús de les funcions resum o **hash**

SIGNATURA DIGITAL

Firma Digital



Comprobación de una Firma



Si los códigos hash coinciden, la firma es válida

SIGNATURA DIGITAL

Exemple - Suposició

Anna i Bernat tenen els seus **parells de claus** respectives. Anna escriu un missatge a Bernat. És necessari que Bernat pugui verificar que realment és Anna qui ha enviat el missatge, per tant, Anna ha d'enviar-lo signat:

1. Anna **resumeix** el missatge o dades mitjançant una funció **hash**.
2. **Xifra** el resultat de la funció **hash** amb la seva clau privada. D'aquesta manera obté la seva signatura digital.
3. Envia a Bernat el **missatge** original juntament amb la **signatura**. Bernat rep el missatge al costat de la signatura digital. Haurà de comprovar la validesa d'aquesta per a donar per bo el missatge i reconèixer a l'autor del mateix (**integritat i autenticació**).
4. **Desxifra** el resum del missatge mitjançant la clau pública d'Anna.
5. Aplica al missatge la funció **hash** per a obtenir el **resum**.
6. **Compara** el resum rebut desxifrat, amb l'obtingut a partir de la funció **hash**.
7. Si són iguals, Bernat pot estar segur que qui ha enviat el missatge (és Anna) i que aquest no ha estat modificat.

SIGNATURA DIGITAL

Però

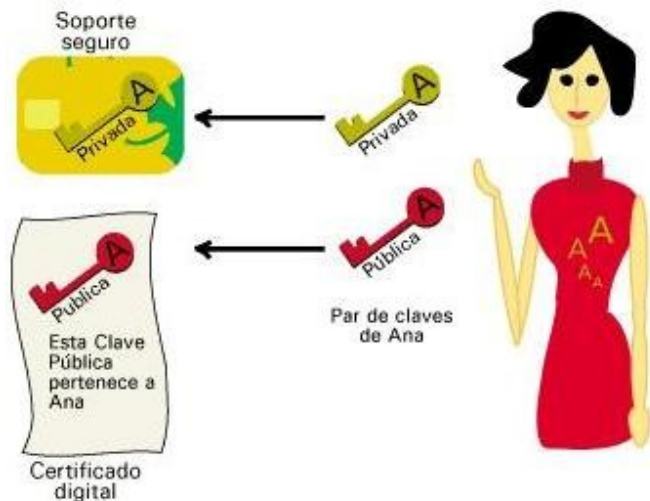
Que passa si **C**arles genera un parell de claus amb el nom d'**A**нна, i les usa per a enviar un missatge a **B**ernat?

Bernat creu que el missatge és d'**A**нна, i no té manera de comprovar si realment el missatge és d'**A**нна o no.

CERTIFICAT DIGITAL

Les operacions de xifratge i signatura digital només són eficaces si es garanteix que les claus privades són úniques.

- ➔ Per a garantir la **unicitat de les claus privades** se sol recórrer a:
 - ◆ Suports físics (targetes intel·ligents p.e. DNle, que impossibiliten la duplicació de les claus)
 - ◆ protegides per un número personal o PIN
- ➔ Per a assegurar que una determinada clau pública pertany a un usuari concret
 - ◆ **Certificats digitals**



CERTIFICAT DIGITAL

CERTIFICAT DIGITAL=document electrònic (arxiu) que associa una clau pública amb la identitat del seu propietari

Conté


- ➔ Informació sobre la identitat del seu propietari (nom, adreça ,email)
- ➔ La **clau pública** del titular (opcional: la **clau privada**)
- ➔ Altres atributs
 - àmbit d'ús de la clau
 - núm serie, versió, algorismes,
 - dates de validesa, data d'emissió, data de caducitat
 -
- ➔ La identitat de la entitat certificadora que l'ha emés
- ➔ La signatura digital de l'autoritat certificadora, a Espanya, p.e. **La casa de moneda i timbre**

CERTIFICAT DIGITAL


CERTIFICAT DIGITAL=document electrònic (arxiu) que associa una clau pública amb la identitat del seu propietari

- ➔ El format estàndard de certificats digitals és **X.509**, la seva distribució és possible realitzar-la:
 - ◆ Amb **clau privada** (sol tindre extensió .pfx o .p12) mes segur i destinat a un us privat d'exportació i importació com mètode de còpia segura
 - ◆ Sols amb la **clau pública** (sol ser extensió .cer o .crt), destinat a la distribució no segura , per a que altres entitats puguin verificar la identitat en els arxius o missatges signats
- ➔ **Aplicacions**: banca online, l'administració pública etc

UTILITATS DE CERTIFICATS


 dnielectronico.es/PortalDNle/

dnielectronico.es


 La connexió és segura

 Galetes


1 en


 Configuració del lloc web


Testificar la veracitat d'un lloc web

En els navegadors web quan visitem un lloc segur (**https**) es mostra un **cademat**  que té un formulari de dades d'enviament de credencials o dades privades que se deuen enviar de forma segura es mostra un **cademat** que ens permetrà veure el seu certificat digital i la entitat certificadora

Esbrina qui és la entitat certificadora dels següents llocs web , i la validesa dels seus certificats.

 ceice.gva.es/es/

 bbva.es/personas.html

 dnielectronico.es/PortalDNle/

UTILITATS DE CERTIFICATS

Testificar la veracitat d'un document

En alguns visors de documents, com per exemple , de documents tipus **pdf**, es mostra un segell de verificació i un botó de panell de firma per vore les propietats del certificat amb el qual ha estat signat.

Si el document signat ha estat alterat, s'indica en el segell.



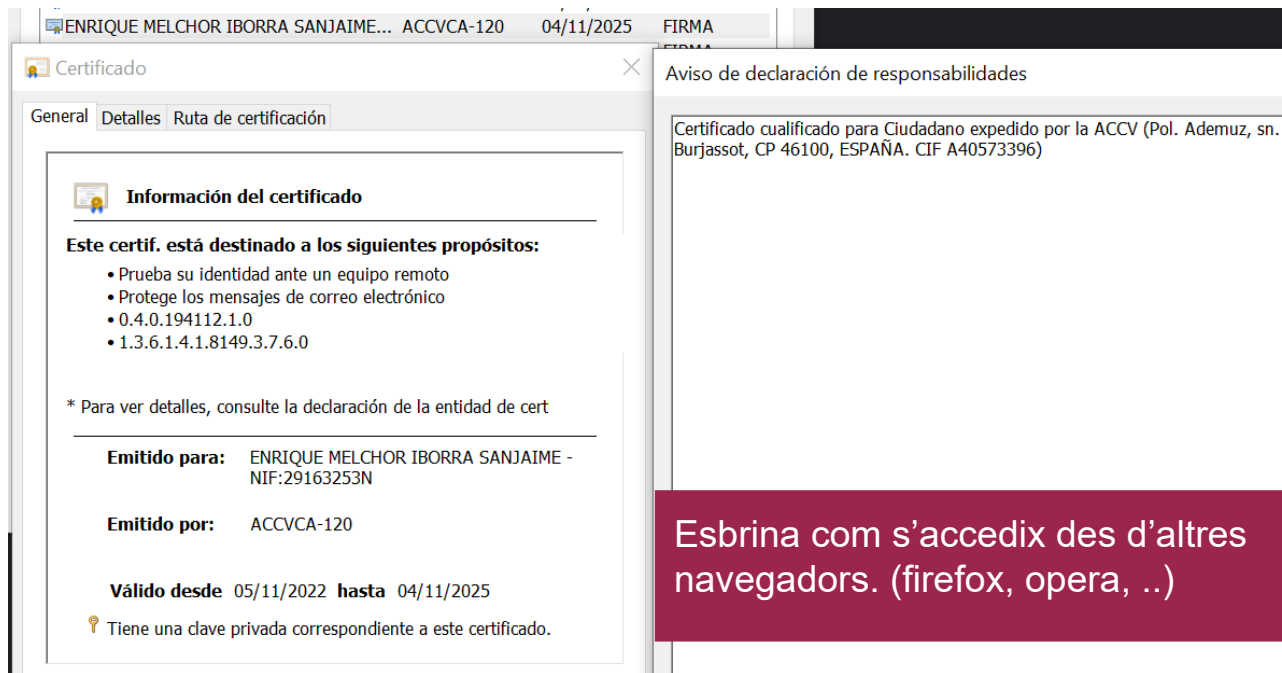
Hay al menos una firma no válida.

The screenshot shows a PDF viewer interface. At the top, a light blue status bar contains a green checkmark icon on the left and the text "Firmado y todas las firmas son válidas." in the center. On the right side of this bar is a button labeled "Panel de firma". Below the status bar, the document header includes the logo of IES Sant Vicent Ferrer, its address (Parc Salvador Castell, 16, 46680 Algemesí), the course information (CICLE: ASIX, MODALITAT: SEMIPRESENCIAL, MÒDUL: SAD), and the logo of the Generalitat Valenciana. Below the header, the text "Activitat: doble signatura PDF" is displayed. At the bottom, there is a red rectangular area with a white ribbon-like graphic.

UTILITATS DE CERTIFICATS

Instal·lar / Vore certificats del SO, navegadors web o clients de correu

chrome : Configuración/ Privacidad y Seguridad/Seguridad/Gestionar certificados/Gestionar certificados importados



Esbrina com s'accedix des d'altres navegadors. (firefox, opera, ..)

TERCERES PARTS DE CONFIANÇA

La validesa d'un certificat és la confiança que la clau pública continguda en el certificat pertany a l'usuari indicat en el certificat

- ➔ La manera de confiar en el certificat d'un usuari és mitjançant la **confiança en terceres parts**. La idea consisteix en el fet que dos usuaris puguin confiar directament entre si, tots dos tenen relació amb una tercera part i que aquesta pugui donar fe de la fiabilitat dels dos
- ➔ Es podrà tenir confiança en el certificat digital d'un usuari al qual prèviament no coneixem si aquest certificat està **avalat per una tercera part en la qual si confiem**.
- ➔ La forma en què aquesta tercera part avalarà que el certificat és de fiar és mitjançant la seva signatura digital sobre el certificat

La **tercera part confiable** (**TPC Tercera Part Confiable o TTP Trusted Third Party**) que s'encarrega de la signatura digital dels certificats dels usuaris en un entorn de clau pública es coneix amb el nom de **Autoritat de Certificació (AC)**

TERCERES PARTS DE CONFIANÇA

El model de confiança basat en **Terceres Parts Confiables** es la base de la definició de les **Infraestructures de Clau Pública (ICP o PKI Public Key Infrastructures)** formades per :

- **Autoritat de certificació (CA)**: emet i elimina els certificats digitals
- **Autoritat de registre (RA)**: controla la generació dels certificats, processa les peticions i comprova la identitat dels usuaris, mitjançant el requeriment de la identificació personal oportuna
- **Autoritats de repositori**: emmagatzemen els certificats emesos i eliminats
- **Software** per a l'ús de certificats
- **Política de seguretat** en les comunicacions relacionades amb la gestió de certificats

TERCERES PARTS DE CONFIANÇA

Infraestructures de Clau Pública (ICP o PKI Public Key Infraestructures) formades per :

Autoritat de certificació (CA): Autoritat de registre (RA):

Esbrina qui és l'Autoritat de registre i l'Autoritat de certificació de:






bbva, caixabank.cat, bancosantander.es

Després comprova que estes autoritats es troven instal·lades en el teu navegador (SO)

Gestionar certificados

Administra la configuración y los certificados HTTPS/SSL

Certificados

Propósito planteado: <Todos>		
Entidades de certificación intermedias Entidades de certificación raíz de confianza Editores de		
Emitido para	Emitido por	Fecha de ...
 Symantec Enterprise Mobile R...	Symantec Enterprise Mobile Root for ...	15/03/2032
 VeriSign Universal Root Certif...	VeriSign Universal Root Certification ...	02/12/2037
 AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	01/01/2030
 ACCRAIZ1	ACCRAIZ1	31/12/2030
 Certum CA	Certum CA	11/06/2027

DNIE

El **Document Nacional d'Identitat (DNI)** emès per la Direcció General de la Policia (Ministeri de l'interior)

El document electrònic ha d'oferir les mateixes certeses que el document físic:

- ➔ **Acreditar** electrònicament i sense possibilitat de dubte la **identitat** de persona
- ➔ **Signar** digitalment documents electrònics, atorgant-los una **validesa jurídica** equivalent a la que els proporciona la signatura manuscrita

DNI 4.0



Esbrina de quina versió és el teu DNI

DNIE

El Document Nacional d'Identitat electrònic (**DNle**) incorpora un petit circuit integrat (xip) capaç de guardar de manera segura, mitjançant mesures específiques de seguretat per a impedir la seva falsificació.

La informació que conté és:

- Un **certificat electrònic per autenticar** la personalitat del ciutadà
- Un **certificat electrònic per a signar** electrònicament amb la mateixa validesa jurídica que la signatura manuscrita
- Certificat de l'Autoritat de Certificació emissora
- Claus per a la seva utilització
- La plantilla biomètrica per a la impressió dactilar

Per a utilitzar el DNle es necessari:

- Maquinari específic: lector de targetes que compleixi és estàndard ISO-7816
- Programari específic: controladors o mòduls criptogràfics que permetin
- l'accés a xip de la targeta
 - ◆ **Windows** : Crtyptographic Sevice Provider (CSP)
 - ◆ **GNU/Linux** : mòdul criptogràfic PKC#11

Certificat digital

Que es pot fer amb el certificat digital? [punxa ací](#)

- Presentació i liquidació d'impostos.
- Presentació de recursos i reclamacions.
- Emplenament de les dades del cens de població i habitatges.
- Consulta i inscripció en el padró municipal.
- Consulta de multes de circulació.
- Consulta i tràmits per a sol·licitud de subvencions.
- Consulta d'assignació de col·legis electorals.
- Actuacions comunicades.
- Signatura electrònica de documents i formularis oficials.
- Sol·licitar treball

[On es pot utilitzar el certificat](#)

Certificat digital

On es pot obtenir el certificat digital?

CA

- FNMT-Ceres, creada per la Fábrica Nacional de Moneda y Timbre
- IZENPE: l'autoritat de certificació impulsada per el Govern Basc i les Diputacions Forals
- ACCV, Autoritat de Certificació de la Comunitat Valenciana
- CATCert, Agència Catalana de Certificació

RA Consulta la [página de la agencia tributaria](#) i selecciona el servei electrònic de confiança que necessites sol·licitar.

Servicios electrónicos de confianza cualificados

<Seleccionar Servicio>
<Seleccionar Servicio>
<Todos>
Servicio de expedición de certificados electrónicos cualificados de firma electrónica
Servicio de expedición de certificados electrónicos cualificados de sello electrónico
Servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web
Servicio de expedición de sellos electrónicos cualificados de tiempo

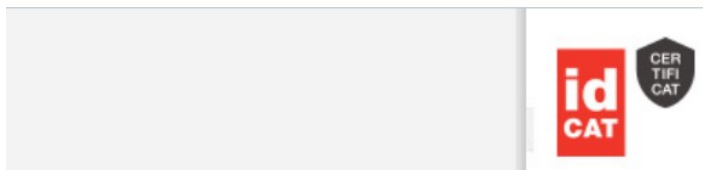
Certificat digital

- FNMT-Ceres, creada per la Fábrica Nacional de Moneda y Timbre
- IZENPE: la autoritat de certificació impulsada per el Govern Basc i les Diputacions Forals
- ACCV, Autoritat de Certificació de la Comunitat Valenciana < > ↺ ☐ | 🔒 www.accv.es



- CATCert, Agència Catalana de Certificación

🔒 www.idcat.cat/idcat/ciutada/menu.do



Certificat digital

¿Que tipus de certificats digital existeixen?

- Persona física (com es ve expedint en l'actualitat).
- Representants de persones jurídiques que siguin administradors únics o solidaris.
- Representants de persones jurídiques.
- Representant d'entitats sense personalitat jurídica.
- Certificat d'empleat públic
- Certificat de component (ssl/tls) [més info](#)

Suports:

- Software / instal·lables [Com instal·lar](#)
- DNle
- Targetes
- Dispositiu USB
- Cl@ve

Certificat digital

Formats de codificació dels certificats (exporta Importar)

- PEM

Format de text, xifrat Base64

Utilitza extensions .cer .crt .pem .key

- DER

Format binari

Utilitza extensions .cer .der

- P7B

Format Base64

Utilitza extensions .p7b .p7c

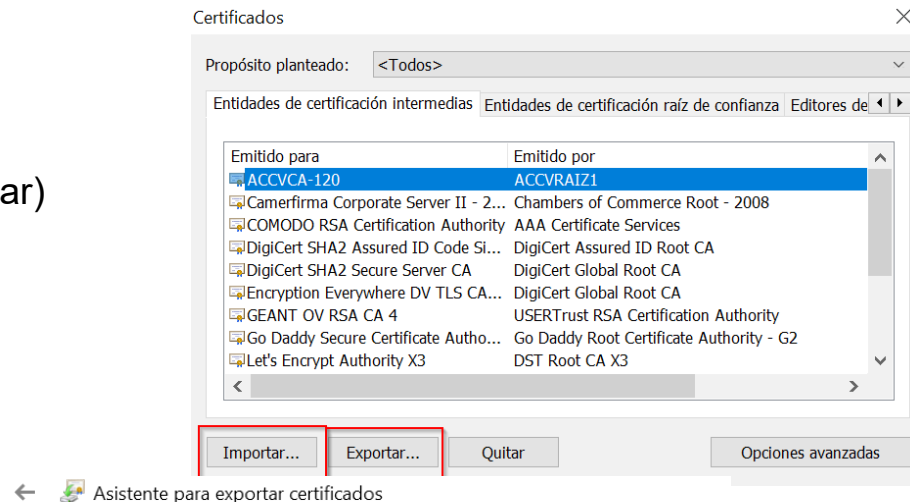
No contenen clau privada

- PFX/P12

Format binari

Utilitza extensions .pfx .p12

Conté la clau privada



Formato de archivo de exportación

Los certificados pueden ser exportados en diversos formatos de archivo.

Seleccione el formato que desea usar:

☒ DER binario codificado X.509 (.CER)

☐ X.509 codificado base 64 (.CER)

☐ Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)

☐ Incluir todos los certificados en la ruta de certificación (si es posible)

☐ Intercambio de información personal: PKCS #12 (.PFX)

Email encriptat

Pràctica

Envia'm un correu de gmail encriptat amb la contrasenya : SVF2023

Utilitza l'extensió Mailvelope

CERTIFICATS DIGITALS

Suggerència



Pràctica

Obtenir un certificat digital que acredite la nostra identitat.

1. **Triar que tipus de certificat sol·licitarem. Per a això farem una primera recerca sobre els certificats i mètodes disponibles al nostre país.**
2. **Sol·licitar el certificat elegit i justificar l'elecció.**
3. **Identificar-se i explicar el mètode utilitzat.**
4. **Instal·lar el certificat si és necessari.**
5. **Utilitzar el certificat.**
6. **Exportar el certificat a un mitjà extern.**