ACTIVITAT FORMATIVA	MP: SMX-6 - Seguretat informática
	UF4: **Seguretat activa**

GPG

SMX-6-UF4-2 - GPG (Privat)

Introducció

A SMX-6-UF4-1 - Criptografia hem après les tècniques bàsiques de la criptografia.

Però perquè una tecnologia sigui útil s'ha de poder utilitzar amb facilitat.

Per això ara farem servir **GPG** (la versió lliure de **PGP**).

transfer.sh

Si transfer.sh no funciona pots fer servir oshi.at

```
touch hello.txt
curl -T hello.txt https://oshi.at
```

PGP

Pretty Good Privacy o **PGP** (en català *privadesa bastant bona*) és un programa desenvolupat a principis dels anys 90.

La seva finalitat és protegir la informació distribuïda a través d'Internet mitjançant l'ús de criptografia de clau pública, així com facilitar l'autenticació de documents gràcies a les signatures digitals.

Avui en dia Symantec és el propietari del producte.

El problema és que té una llicència comercial.

GPG

GNU Privacy Guard (**GnuPG** o **GPG**) és un programa lliure que fa el mateix que PGP.

La primera versió és de finals dels anys 1990.

S'utilitza moltíssim més que PGP perquè és gratuït, sobretot a nivell de software.

OpenPGP

OpenPGP és un estàndard de finals dels anys 1990 que s'ha anat actualitzant.

S'utilitza sobretot per encriptar correu electrònic.

GPG compleix completament aquest estàndard.

Com que és anterior a l'ús generalitzat de GPG té el nom d'OpenPGP.

Crea una màquina gpg per aquesta activitat:

```
> .\box.exe start gpg

> New-wsl gpg
> Connect-wsl gpg
```

Clau GPG

Generar una clau

El primer que hem de fer es generar una clau GPG.

Per generar les claus asimètriques necessitem entropía, per això instal.lem el paquet `haveged` perquè es generin més ràpid:

```
sudo apt update
sudo apt install -y haveged
```

Per generar la clau PGP fem servir el flag `--full-generate-key.`

Important!. Enlloc de "`David <david@himitsu>`" has de fe servir el teu identificador!

Per exemple **`maria`**`@himitsu` (teu nom).

```
box@gpg:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection?
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072)
Requested keysize is 3072 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: David
Email address: david@himitsu
Comment:
You selected this USER-ID:
    "David <david@himitsu>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

Caducitat del certificat :

- El **valor predeterminat** de la caducitat del teu certificat és **mai**.
- Si algú té accés a la clau privada del teu certificat pot fer coses amb el teu `USER-ID`.
- Quan passa això pots utilitzar el teu certificat de revocació per revocar el certificat.
- El problema es que molts cops exit
- aquest certificat de revocació s'ha perdut.
- Per això és millor que la clau caduqui al cap d'un temps determinat.

Password :

- El certificat està protegit per la contrasenya que et demanen
- Si perds la contrasenya no la pots recuperar !

Digues (O)kay i amb les dades que has introduït es genera un certificat:

```
gpg: /home/box/.gnupg/trustdb.gpg: trustdb created
gpg: key 942EAF368FE1CF35 marked as ultimately trusted
gpg: directory '/home/box/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/box/.gnupg/openpgp-revocs.d/094C7FF6B373
8DAF0AE828CC942EAF368FE1CF35.rev'
public and secret key created and signed.

pub   rsa3072 2023-11-15 [SC]
      094C7FF6B3738DAF0AE828CC942EAF368FE1CF35
uid                      David <david@himitsu>
sub   rsa3072 2023-11-15 [E]

box@gpg:~$
```

S'HA CREAT UN CERTIFCAT

Llistar Clau secreta

Amb l'ordre `gpg --list-secret-keys` pots veure que la teva clau GPG s'ha incorporat a la base de dades local gpg:

```
box@gpg:~$ gpg --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/home/box/.gnupg/pubring.kbx
-----------------------------
sec   rsa3072 2023-11-15 [SC]
      094C7FF6B3738DAF0AE828CC942EAF368FE1CF35
uid           [ultimate] David <david@himitsu>
ssb   rsa3072 2023-11-15 [E]

box@gpg:~$
```

Exportar

Si vols guardar la clau GPG l'has d'exportar:

```
box@gpg:~$ gpg --output david.asc --armor --export-secret-keys --export-option
s export-backup david
box@gpg:~$
box@gpg:~$ curl --upload-file david.asc https://transfer.sh/david.asc
https://transfer.sh/mf[redacted]/david.ascbox@gpg:~$
```

Editar

Un certificat es por editar per canviar la data de caducitat, la contrasenya, signar o revocar claus i eliminar correus electrònics i fotos.

```
box@gpg:~$ gpg --edit-key david
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

sec  rsa3072/942EAF368FE1CF35
     created: 2023-11-15  expires: never       usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/CB9017BE358F62C1
     created: 2023-11-15  expires: never       usage: E
[ultimate] (1). David <david@himitsu>

gpg>
```

Amb la comanda `help` tinc una llista de totes les ordres disponibles (també puc demanar ajuda a ChatGPT)

```
gpg> help
quit        quit this menu
save        save and quit
help        show this help
fpr         show key fingerprint
grip        show the keygrip
list        list key and user IDs
```

Per exemple puc modificar la data de caducitat:

```
gpg> expire
Changing expiration time for the primary key.
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 50y
Key expires at Thu Nov  2 11:41:57 2073 UTC
Is this correct? (y/N) y                    ARA

sec  rsa3072/942EAF368FE1CF35
     created: 2023-11-15  expires: 2073-11-02  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/CB9017BE358F62C1
     created: 2023-11-15  expires: never       usage: E
[ultimate] (1). David <david@himitsu>       ABANS

gpg> quit
Save changes? (y/N) N   POTS GUARDAR (O NO) ELS CANVIS FETS
Quit without saving? (y/N) y
box@gpg:~$
```

Importar

En la propera activitat SMX-6-UF4-3 - Certificats veurem que tots els sistemes operatius tenen instal.lats per defecte un conjunt de certificats de confiança més o menys comuns.

GPG no funciona així, sinó que, tu has d'importar expressament aquelles claus públiques en què tu confies.

Amb l'opció `--import` puc importat la clau pública que algú altre a adjuntat al correu que he rebut o que està al seu lloc web.

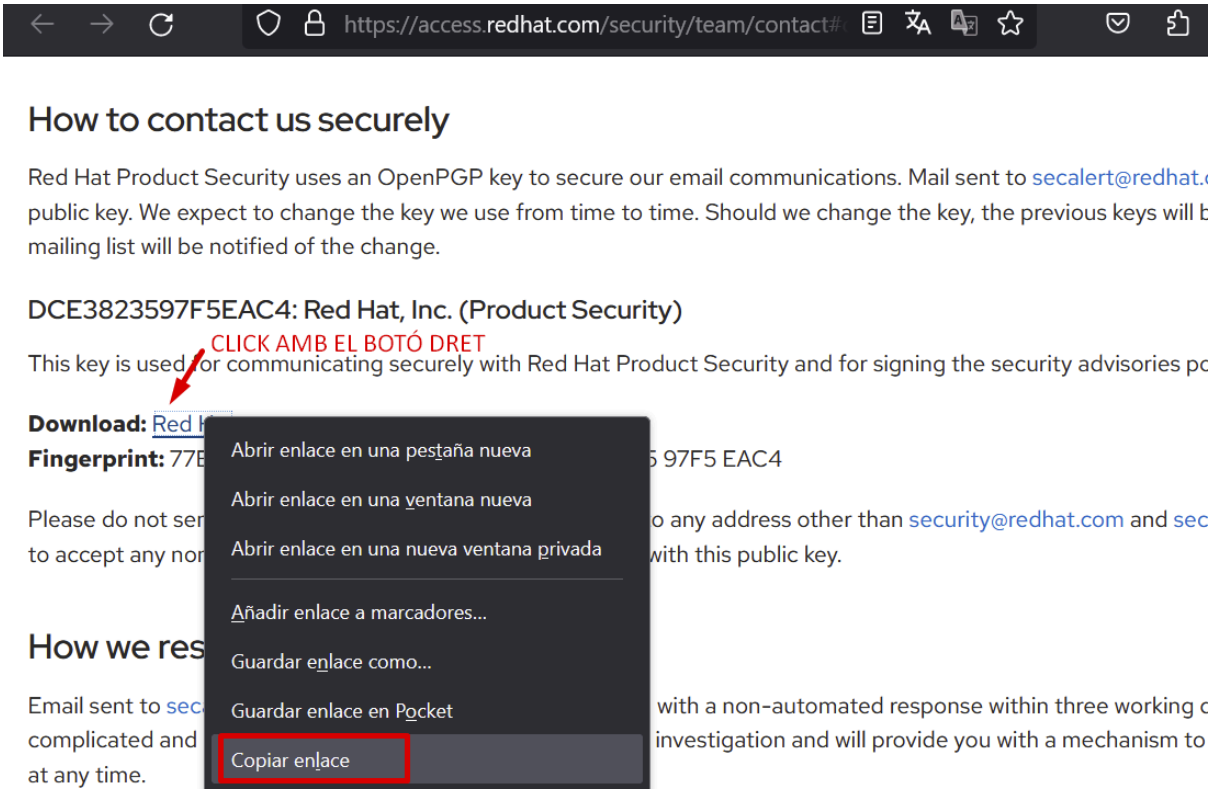
Red Hat

Per exemple si vull contacta de manera segura amb RedHat per notificar una alerta de seguretat, normalment hauré d'incloure informació sensible.

El que haig de fer és:

1. Importar la seva clau PGP tal com s'explica a Security contacts and procedures - Red Hat Customer Portal
2. Encriptar el missatge amb la seva clau PGP i enviar el missatge encriptat a l'adreça secalert@redhat.com.

Copio l'enllaç de la clau pública PGP de la pàgina web:



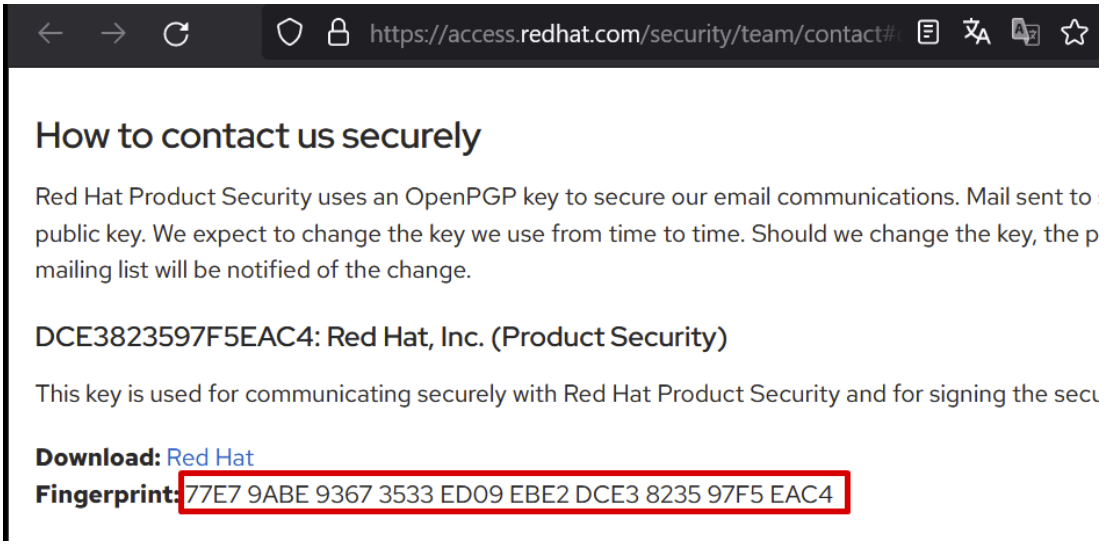
Ja puc importar la clau pública:

```
box@gpg:~$ wget -q https://access.redhat.com/security/data/97f5eac4.txt -O redha
t.txt
box@gpg:~$
box@gpg:~$ gpg --import redhat.txt
gpg: key DCE3823597F5EAC4: public key "Red Hat, Inc. (Product Security) <secaler
t@redhat.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
box@gpg:~$
box@gpg:~$ gpg --list-keys
/home/box/.gnupg/pubring.kbx
----------------------------
pub   rsa3072 2023-11-15 [SC]
      094C7FF6B3738DAF0AE828CC942EAF368FE1CF35
uid           [ultimate] David <david@himitsu>
sub   rsa3072 2023-11-15 [E]

pub   rsa4096 2017-10-31 [SC]
      77E79ABE93673533ED09EBE2DCE3823597F5EAC4
uid           [ unknown] Red Hat, Inc. (Product Security) <secalert@redhat.com>
sub   rsa4096 2017-11-01 [E]

box@gpg:~$
```

Amb l'opció `--fingerprint` puc veure el hash de de la clau pública GPG:

```
box@gpg:~$ gpg --fingerprint redhat
pub   rsa4096 2017-10-31 [SC]
      77E7 9ABE 9367 3533 ED09  EBE2 DCE3 8235 97F5 EAC4
uid           [ unknown] Red Hat, Inc. (Product Security) <secalert@redhat.com>
sub   rsa4096 2017-11-01 [E]

box@gpg:~$
```

I la puc comparar amb la de la pàgina web per assegurar-me que és correcte:

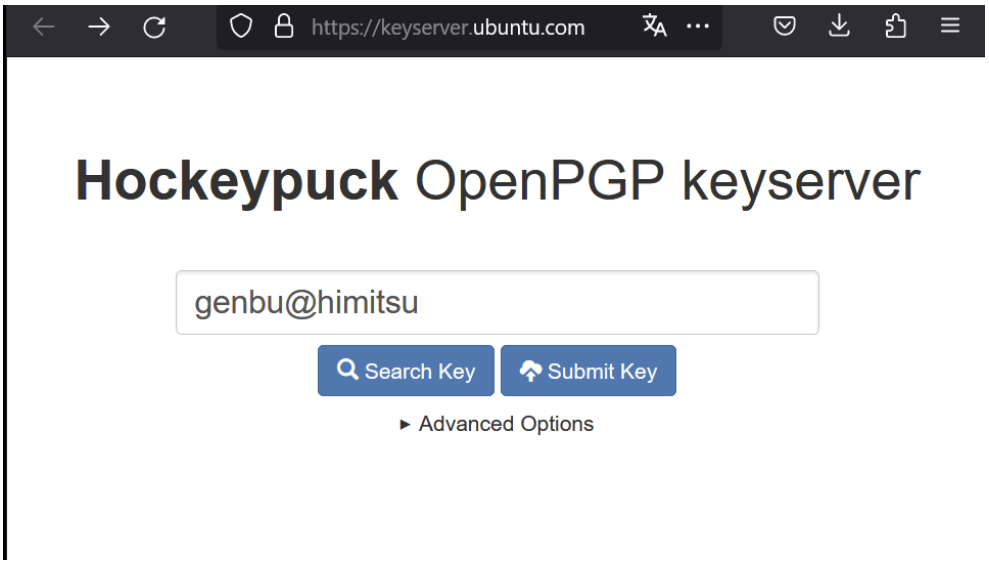


Més endavant explicarem com encriptar el missatge.

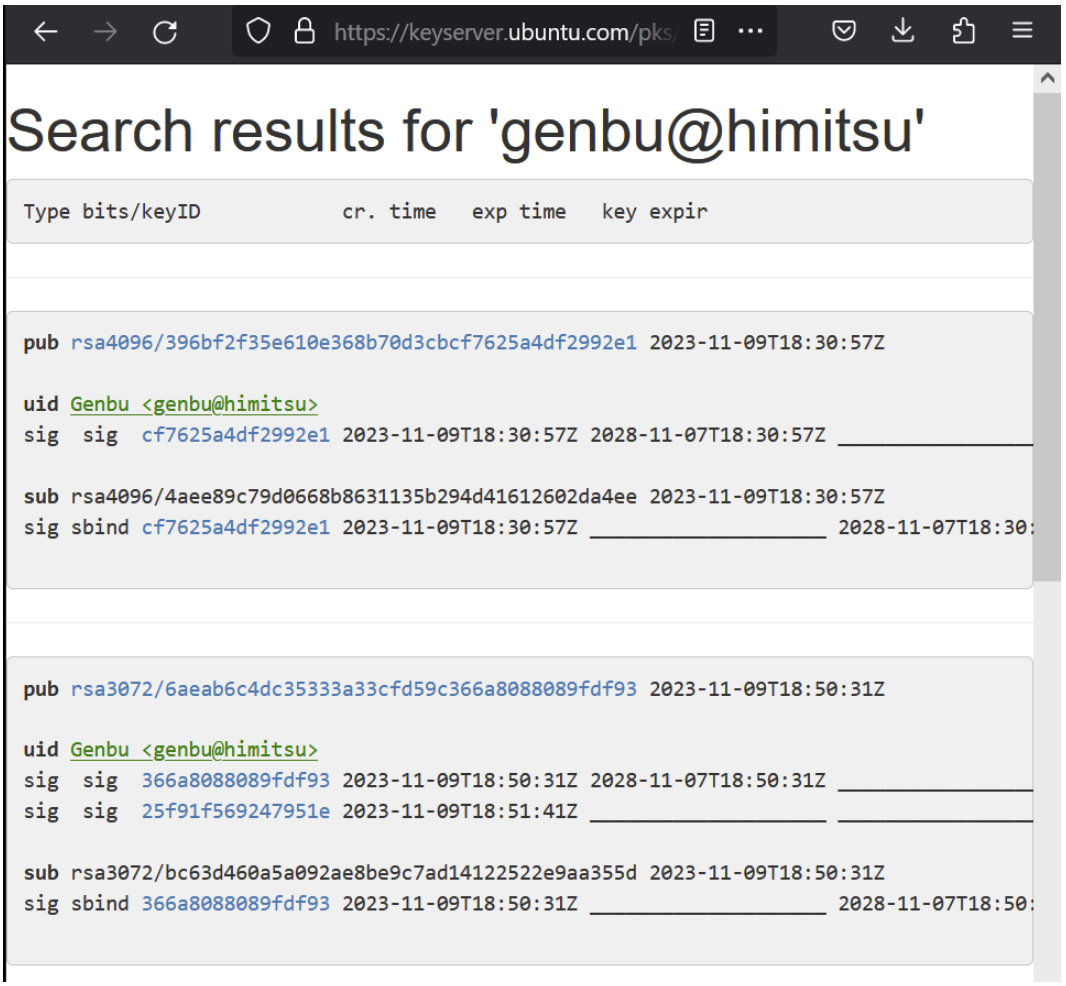
Ubuntu

També hi ha la possibilitat que la persona amb qui voleu comunicar-vos hagi penjat la seva clau pública a un servidor de claus públiques.

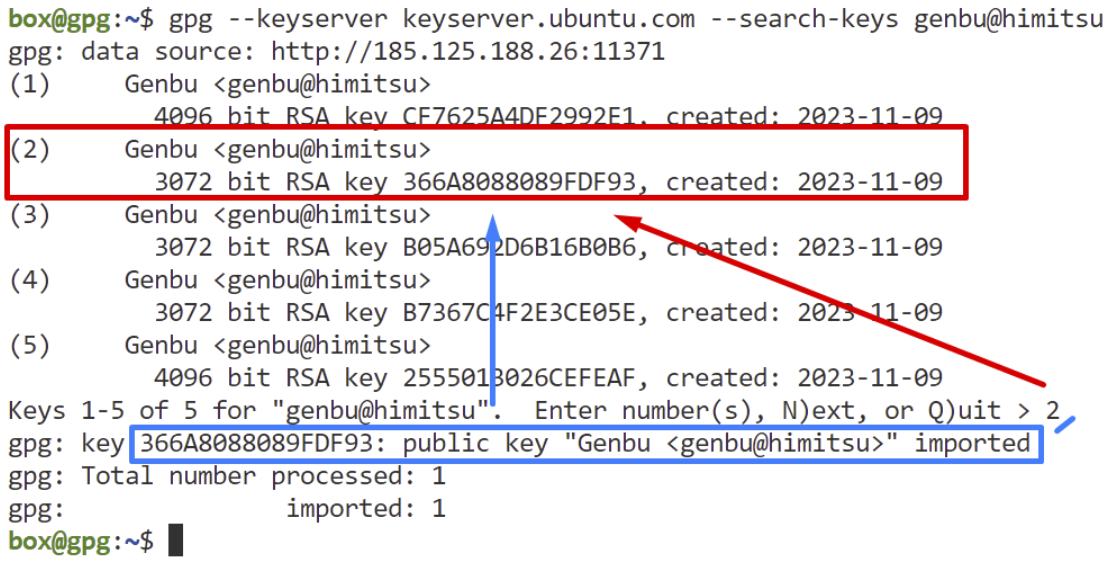
Pots buscar claus públiques PGP pel nom o adreça de correu electrònic en el servidor d'Ubuntu a través de la seva página web: https://keyserver.ubuntu.com/



Pots veure les claus públiques GPG del domini xtec.dev que estan publicades en aquest servei :



També pots buscar claus públiques GPG desde la línia de comandes i importar la que vulguis:



Pots veure que la clau pública s'ha importat:

```
box@gpg:~$ gpg --list-keys
/home/box/.gnupg/pubring.kbx
----------------------------
pub   rsa3072 2023-11-15 [SC]
      094C7FF6B3738DAF0AE828CC942EAF368FE1CF35
uid           [ultimate] David <david@himitsu>
sub   rsa3072 2023-11-15 [E]

pub   rsa3072 2023-11-09 [SC] [expires: 2028-11-07]
      6AEAB6C4DC35333A33CFD59C366A8088089FDF93
uid           [ unknown] Genbu <genbu@himitsu>
sub   rsa3072 2023-11-09 [E] [expires: 2028-11-07]

box@gpg:~$
```

També podem borra una clau pública importada:

```
box@gpg:~$ gpg --delete-keys genbu
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


pub  rsa3072/366A8088089FDF93 2023-11-09 Genbu <genbu@himitsu>

Delete this key from the keyring? (y/N) y
box@gpg:~$
```

List

Ja saps de SMX-6-UF4-1 - Criptografia que les claus asimètriques són dues: la púbica i la privada.

Com has vist abans, quan fas servir l'opció `--list-keys` gpg et torna una llista de totes les claus públiques.

```
box@gpg:~$ gpg --list-keys
/home/box/.gnupg/pubring.kbx
----------------------------
pub   rsa3072 2023-11-15 [SC]
      094C7FF6B3738DAF0AE828CC942EAF368FE1CF35
uid           [ultimate] David <david@himitsu>
sub   rsa3072 2023-11-15 [E]

pub   rsa4096 2017-10-31 [SC]
      77E79ABE93673533ED09EBE2DCE3823597F5EAC4
uid           [ unknown] Red Hat, Inc. (Product Security) <secalert@redhat.com>
sub   rsa4096 2017-11-01 [E]

box@gpg:~$
```

Si només vols una llista de les claus privades has de fer servir l'opció `--list-secret-keys` :

```
box@gpg:~$ gpg --list-secret-keys
/home/box/.gnupg/pubring.kbx
----------------------------
sec   rsa3072 2023-11-15 [SC]
      094C7FF6B3738DAF0AE828CC942EAF368FE1CF35
uid           [ultimate] David <david@himitsu>
ssb   rsa3072 2023-11-15 [E]

box@gpg:~$
```

Verificar i signar

Si vols, pots crear una clau GPG amb el nom i l'adreça de correu d'algú altre.

De la mateixa manera qualsevol pot crear una clau GPG amb el teu nom i correu electrònic.

Verificar

Tal com hem vist amb RedHat podem verificar la identitat del certificat perquè l'empremta de la clau GPG està en la seva pàgina web.

DCE3823597F5EAC4: Red Hat, Inc. (Product Security)

This key is used for communicating securely with Red Hat Product Security and for signing the security advisor

Download: Red Hat
Fingerprint: 77E7 9ABE 9367 3533 ED09 EBE2 DCE3 8235 97F5 EAC4

Please do not send messages encrypted with this public key to any address other than security@redhat.com an accept any non-security-related email which is encrypted with this public key.

Signar

Si estas conforme amb la validació de la clau GPG pots signar la clau per indicar a PGP que has verificat que la clau GPG pertany a RedHat:

Per signar una clau que has importat, escriu:

```
box@gpg:~$ gpg --sign-key redhat

pub  rsa4096/DCE3823597F5EAC4
     created: 2017-10-31  expires: never       usage: SC
     trust: unknown       validity: unknown
sub  rsa4096/B8914F503278E012
     created: 2017-11-01  expires: never       usage: E
[ unknown] (1). Red Hat, Inc. (Product Security) <secalert@redhat.com>


pub  rsa4096/DCE3823597F5EAC4
     created: 2017-10-31  expires: never       usage: SC
     trust: unknown       validity: unknown
 Primary key fingerprint: 77E7 9ABE 9367 3533 ED09  EBE2 DCE3 8235 97F5 EAC4

     Red Hat, Inc. (Product Security) <secalert@redhat.com>

Are you sure that you want to sign this key with your
key "David <david@himitsu>" (942EAF368FE1CF35)

Really sign? (y/N) y

box@gpg:~$
```

Al signar una clau també estàs ajudant a donar validesa a la clau pública PGP que has signat.

Si algú confía en la teva clau pública PGP també confiará en la clau pública que has signat.

Pots exportar la clau pública signada i enviar-la al propietari, en aquest cas RedHat:

```
box@gpg:~$ gpg --output redhat.asc --export --armor redhat
box@gpg:~$ cat redhat.asc | head -5
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFn41kMBEACpJL82mKFBTnr4RyCsEseKhMrKaytD19woOwlGSlwFGFsdLKLw
1jtI2ETqjmIIkZ5uNMB0n9xb1h6azgTZdjADGLRjLcMInxGjw/0wlvhXOlXdea/G
Klj0YXikdpgINUiMTb5Pyir7K6YQPI27nVk5KTAx3rCA9js7/Br71F+V++PuPud1
box@gpg:~$
```

A RedHat no li fa falta, però podria importar la teva signatura per donar més credibilitat a la seva clau GPG.

Quan rebin aquesta nova clau signada, la poden importar, afegint la informació de signatura que heu generat a la seva base de dades GPG.

Exportar

Una clau PGP només té sentit si altres la poden fer servir la clau pública i confien en ella.

Lloc web

Perquè tothom pugui fer servir la meva clau pública PGP la puc exportar a un fitxer en format text i pujar-la al meu lloc web:

```
box@gpg:~$ gpg --output david.asc --export --armor david
box@gpg:~$
box@gpg:~$ cat david.asc | head -n 5
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGVUrJcBDACe9rLcKdry1rzuHb4ZrAWva4d8fX6aNsHecdQ6O5u+fGAvvjmo
OyRxbij67BzYN+1IjyxzKnBpIlnHRbyp1fXe21fYhvwIPv//AtGJRjh+9cuATvxq
WoqjUBGnjUp6WJNuCJOe02MGU3ypoXlksinh+76EoMePLrDOH1M/pUIYozcPdk6K
box@gpg:~$
```

Fas servir l'opció **`--armor`** perquè exporti la clau pública PGP en format text.

De la mateixa manera que fa RedHat també has de posar l'empremta:

```
box@gpg:~$ gpg --fingerprint david
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   1  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1  valid:   1  signed:   0  trust: 1-, 0q, 0n, 0m, 0f, 0u
pub   rsa3072 2023-11-15 [SC]
      094C 7FF6 B373 8DAF 0AE8  28CC 942E AF36 8FE1 CF35
uid           [ultimate] David <david@himitsu>
sub   rsa3072 2023-11-15 [E]

box@gpg:~$
```

Servidor de claus

La clau pública es pot pujar a un servidor de claus perquè estigui fàcilment disponible:

- https://keyserver.ubuntu.com/
- https://keys.openpgp.org/
- https://pgp.mit.edu/

Amb l'identificador de la teva clau, pots pujar-la directament amb el client `gpg`.

```
box@gpg:~$ gpg --list-keys --keyid-format SHORT david
pub   rsa3072/8FE1CF35 2023-11-15 [SC]
      094C7FF6B3738DAF0AE828CC942EAF368FE1CF35
uid         [ultimate] David <david@himitsu>
sub   rsa3072/358F62C1 2023-11-15 [E]

box@gpg:~$ gpg --send-keys --keyserver keyserver.ubuntu.com 8FE1CF35
gpg: sending key 942EAF368FE1CF35 to hkp://keyserver.ubuntu.com
box@gpg:~$
```

La teva clau ja està disponible a https://keyserver.ubuntu.com/.

També pots verificar des del shell:

```
box@gpg:~$ gpg --search-keys --keyserver keyserver.ubuntu.com david@himitsu
gpg: data source: http://185.125.188.26:11371
(1)     David <david@himitsu>
          3072 bit RSA key 942EAF368FE1CF35, created: 2023-11-15
Keys 1-1 of 1 for "david@himitsu".  Enter number(s), N)ext, or Q)uit > Q
gpg: error searching keyserver: Operation cancelled
gpg: keyserver search failed: Operation cancelled
box@gpg:~$
```

La clau s'acabarà sincronitzant amb altres servidor de claus PGP.

El problema és pots posar el que vulguis en aquest servidor, ningú ho verifica.

Si tu pots, tothom pot, per tant no et pots fiar de cap identitat que importis d'un servidor públic a menys que algú et confirmi que es autèntic:

- La persona t'ha confirmat personalment que és la seva clau GPG.
- La clau està firmada per una clau GPG en que tu confies.

😟

Confiança (trust)

Només has d'importar una clau pública GPG si confies en ella.

Normalment, confies en ella perquè l'has obtingut de la pàgina web oficial o algú de confiança ha firmat aquella clau GPG.

Per exemple:

- A l'activitat SMX-6-UF4-3 - Certificats veurem que hi ha empreses de confiança que es dediquen a verificar identitats i crear certificats signats per aquestes empreses certificadores de confiança.
- El teu DNI és vàlid perquè la policia és qui d'identifica i firma el teu DNI.

Grup de confiança

Si ets el responsable d'un grup, d'una empresa o d'una associació la teva tasca pot ser signar les claus GPG dels membres del grup, de tal manera que tothom pugui acceptar els certificats dels altres sense tenir que verificar la identitat de l'altre o coneixe't personalment.

Però com que les persones no volen esforçar-se massa aviat descobriràs que gpg no es fa servir de manera habitual, excepte en el software perquè ho fan màquines i és una solució molt útil.

Per exemple: Google Linux Software Repositories

En parlarem més endavant, però de moment anem a crear una organització secreta !

himitsu (秘密)

Himutsu (秘密) és una organització secreta.

Important!. Tu has de fer el mateix però amb la teva organització secreta ! 😎

Ningú es coneix, però tothom sap que pot confiar en aquelles claus que estan firmades per `sensei@himitsu`.

Sensei va crear la seva clau GPG de `sensei@himitsu` :

```
box@gpg:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.



GnuPG needs to construct a user ID to identify your key.

Real name: Sensei
Email address: sensei@himitsu
Comment:
You selected this USER-ID:
    "Sensei <sensei@himitsu>"
```

El hash de la nova clau GPG de `sensei@himitsu` és:

3805 C4FE E186 2024 8DE8 9D7D 71AD 7E33 5AF2 FAA0

```
box@gpg:~$ gpg --fingerprint sensei
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   2  signed:   1  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: depth: 1  valid:   1  signed:   0  trust: 1-, 0q, 0n, 0m, 0f, 0u
pub   rsa3072 2023-11-15 [SC]
      3805 C4FE E186 2024 8DE8  9D7D 71AD 7E33 5AF2 FAA0
uid           [ultimate] Sensei <sensei@himitsu>
sub   rsa3072 2023-11-15 [E]

box@gpg:~$
```

Però com que no li ha donat temps d'actualitzar tot el demés, de moment has de fer servir l'antiga clau de `sensei@himitsu` per seguir l'exercici:

😇

```
box@pgp:~$ gpg --fingerprint sensei
pub   rsa4096 2023-11-09 [SC] [expires: 2073-10-27]
      4F7E A4A0 D5DC 9C81 DD7C  D453 F2BD 23B0 7EA5 56B6
uid           [ultimate] Sensei <sensei@himitsu>
sub   rsa4096 2023-11-09 [E] [expires: 2073-10-27]

box@pgp:~$
```

Com que la teva organització té 3 membres que no es coneixen entre ells **has de crear les seves claus GPG amb un password temporal**, signar les claus i enviar a cada un la seva clau GPG.

El primer que has de fer és generar les **tres claus** amb `gpg --full-generate-key`

El resultat ha de ser aquest:

```
box@pgp:~$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   5  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 5u
gpg: next trustdb check due at 2025-11-07
/home/box/.gnupg/pubring.kbx
---------------------------
pub   rsa4096 2023-11-08 [SC] [expires: 2025-11-07]
      ACC0B16219F09AFEE7E3B377B0D394F00D613201
uid           [ultimate] David de Mingo <ddemingo@xtec.cat>
sub   rsa4096 2023-11-08 [E] [expires: 2024-11-07]

pub   rsa4096 2023-11-09 [SC] [expires: 2073-10-27]
      4F7EA4A0D5DC9C81DD7CD453F2BD23B07EA556B6
uid           [ultimate] Sensei <sensei@himitsu>
sub   rsa4096 2023-11-09 [E] [expires: 2073-10-27]

pub   rsa3072 2023-11-09 [SC] [expires: 2025-11-08]
      C5BA5036AD8A46830ECF19C1B05A692D6B16B0B6
uid           [ultimate] Genbu <genbu@himitsu>
sub   rsa3072 2023-11-09 [E] [expires: 2025-11-08]

pub   rsa3072 2023-11-09 [SC] [expires: 2025-11-08]
      C4C1D3A433937E6ED58B09D4D221E91485435F62
uid           [ultimate] Suzaku <suzaku@himitsu>
sub   rsa3072 2023-11-09 [E] [expires: 2025-11-08]

pub   rsa3072 2023-11-09 [SC] [expires: 2025-11-08]
      3FD5C10946FD5E7737131A9F7A47550B0C5B75F9
uid           [ultimate] Byakko <byakko@himitsu>
sub   rsa3072 2023-11-09 [E] [expires: 2025-11-08]

box@pgp:~$
```

Com que tenim varies claus hem de configurar gpg perquè faci servir la de sensei@himitsu:

```
box@pgp:~$ gpg --list-keys --keyid-format SHORT sensei
pub   rsa4096/7EA556B6 2023-11-09 [SC] [expires: 2073-10-27]
      4F7EA4A0D5DC9C81DD7CD453F2BD23B07EA556B6
uid           [ultimate] Sensei <sensei@himitsu>
sub   rsa4096/DEEC7452 2023-11-09 [E] [expires: 2073-10-27]

box@pgp:~$ echo "default-key 7EA556B6" > .gnupg/gpg.conf
box@pgp:~$
```

Ja podem signar totes les claus del grup himitsu:

```
box@pgp:~$ gpg --sign-key genbu

sec  rsa3072/B05A692D6B16B0B6
     created: 2023-11-09  expires: 2025-11-08  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/1769BD2F508EBBF3
     created: 2023-11-09  expires: 2025-11-08  usage: E
[ultimate] (1). Genbu <genbu@himitsu>

gpg: using "7EA556B6" as default secret key for signing

sec  rsa3072/B05A692D6B16B0B6
     created: 2023-11-09  expires: 2025-11-08  usage: SC
     trust: ultimate      validity: ultimate
 Primary key fingerprint: C5BA 5036 AD8A 4683 0ECF  19C1 B05A 692D 6B16 B0B6

     Genbu <genbu@himitsu>

This key is due to expire on 2025-11-08.
Are you sure that you want to sign this key with your
key "Sensei <sensei@himitsu>" (F2BD23B07EA556B6)

Really sign? (y/N) y

box@pgp:~$
```

Pots veure que la clau GPG de Genku està firmada per Sensei:

```
box@pgp:~$ gpg --list-keys --keyid-format SHORT genbu
pub   rsa3072/6B16B0B6 2023-11-09 [SC] [expires: 2025-11-08]
      C5BA5036AD8A46830ECF19C1B05A692D6B16B0B6
uid         [ultimate] Genbu <genbu@himitsu>
sub   rsa3072/508EBBF3 2023-11-09 [E] [expires: 2025-11-08]

box@pgp:~$ gpg --list-sig 6B16B0B6
pub   rsa3072 2023-11-09 [SC] [expires: 2025-11-08]
      C5BA5036AD8A46830ECF19C1B05A692D6B16B0B6
uid           [ultimate] Genbu <genbu@himitsu>
sig 3        B05A692D6B16B0B6 2023-11-09  Genbu <genbu@himitsu>
sig          F2BD23B07EA556B6 2023-11-09  Sensei <sensei@himitsu>
sub   rsa3072 2023-11-09 [E] [expires: 2025-11-08]
sig          B05A692D6B16B0B6 2023-11-09  Genbu <genbu@himitsu>

box@pgp:~$
```

A continuació has d'exportar les claus de Genbu, Suzaku i Byakko:

```
box@pgp:~$ gpg --output genbu.asc --armor --export-secret-keys --export-options
export-backup genbu
```

Ja pots enviar les claus a cada membre del grup (no s'han de conèixer entre ells).

Opció 1: Una manera segura és a través de https://transfer.sh/ :

```
box@pgp:~$ curl --upload-file genbu.asc https://transfer.sh/genbu.asc
https://transfer.sh/KRN3oKClnq/genbu.ascbox@pgp:~$
```

Opció 2: Ja pots pujar les claus del grup himetsu a https://keyserver.ubuntu.com/

```
box@pgp:~$ gpg --list-keys --keyid-format SHORT himitsu
pub   rsa4096/7EA556B6 2023-11-09 [SC] [expires: 2073-10-27]
      4F7EA4A0D5DC9C81DD7CD453F2BD23B07EA556B6
uid         [ultimate] Sensei <sensei@himitsu>
sub   rsa4096/DEEC7452 2023-11-09 [E] [expires: 2073-10-27]

pub   rsa3072/6B16B0B6 2023-11-09 [SC] [expires: 2025-11-08]
      C5BA5036AD8A46830ECF19C1B05A692D6B16B0B6
uid         [ultimate] Genbu <genbu@himitsu>
sub   rsa3072/508EBBF3 2023-11-09 [E] [expires: 2025-11-08]

pub   rsa3072/85435F62 2023-11-09 [SC] [expires: 2025-11-08]
      C4C1D3A433937E6ED58B09D4D221E91485435F62
uid         [ultimate] Suzaku <suzaku@himitsu>
sub   rsa3072/3C6B890B 2023-11-09 [E] [expires: 2025-11-08]

pub   rsa3072/0C5B75F9 2023-11-09 [SC] [expires: 2025-11-08]
      3FD5C10946FD5E7737131A9F7A47550B0C5B75F9
uid         [ultimate] Byakko <byakko@himitsu>
sub   rsa3072/46A3FC57 2023-11-09 [E] [expires: 2025-11-08]

box@pgp:~$ gpg --send-keys --keyserver keyserver.ubuntu.com 7EA556B6
gpg: sending key F2BD23B07EA556B6 to hkp://keyserver.ubuntu.com
box@pgp:~$ gpg --send-keys --keyserver keyserver.ubuntu.com 6B16B0B6
gpg: sending key B05A692D6B16B0B6 to hkp://keyserver.ubuntu.com
box@pgp:~$ gpg --send-keys --keyserver keyserver.ubuntu.com 85435F62
gpg: sending key D221E91485435F62 to hkp://keyserver.ubuntu.com
box@pgp:~$ gpg --send-keys --keyserver keyserver.ubuntu.com 0C5B75F9
gpg: sending key 7A47550B0C5B75F9 to hkp://keyserver.ubuntu.com
box@pgp:~$
```

Confiança (Trust)

Important!. Ara treballaras amb Himutsu (秘密) no amb la teva organització

Torna a configurar per defecte el teu usuari normal:

```
box@pgp:~$ gpg --list-keys --keyid-format SHORT ddemingo
pub   rsa4096/0D613201 2023-11-08 [SC] [expires: 2025-11-07]
      ACC0B16219F09AFEE7E3B377B0D394F00D613201
uid         [ultimate] David de Mingo <ddemingo@xtec.cat>
sub   rsa4096/A91B6632 2023-11-08 [E] [expires: 2024-11-07]

box@pgp:~$ echo "default-key 0D613201" > .gnupg/gpg.conf
box@pgp:~$
```

USER-ID

Imagina't que vols enviar un missatge a `genbu@himitsu.`

Les instruccions són molt senzilles:

1. **Importa la clau GPG de genbu@himitsu** que està a https://keyserver.ubuntu.com/
2. Encripta el missatge amb la clau GPG de Genbu (després expliquem com)
3. Puja el missatge a https://transfer.sh
4. Publica la URL de transfer.sh a https://etherpad.wikimedia.org/p/himitsu

En principi sembla molt fàcil:

```
box@pgp:~$ gpg --search-keys --keyserver keyserver.ubuntu.com genbu@himitsu
gpg: data source: http://185.125.188.26:11371
(1)     Genbu <genbu@himitsu>
          4096 bit RSA key CF7625A4DF2992E1, created: 2023-11-09
(2)     Genbu <genbu@himitsu>
          3072 bit RSA key 366A8088089FDF93, created: 2023-11-09
(3)     Genbu <genbu@himitsu>
          3072 bit RSA key B05A692D6B16B0B6, created: 2023-11-09
(4)     Genbu <genbu@himitsu>
          3072 bit RSA key B7367C4F2E3CE05E, created: 2023-11-09
(5)     Genbu <genbu@himitsu>
          4096 bit RSA key 2555013026CEFEAF, created: 2023-11-09
Keys 1-5 of 5 for "genbu@himitsu".  Enter number(s), N)ext, or Q)uit > 
```

Però resulta que hi ha 5 `genbu@himitsu` 🤨!!

Algú està intentat hackejar l'organització Himutsu (秘密)

Quin és l'autèntic 🤔?)

Baixem les 5 claus a veure quina és la bona:

```
box@pgp:~$ gpg --search-keys --keyserver keyserver.ubuntu.com genbu@himitsu
gpg: data source: http://185.125.188.26:11371
(1)     Genbu <genbu@himitsu>
          4096 bit RSA key CF7625A4DF2992E1, created: 2023-11-09
(2)     Genbu <genbu@himitsu>
          3072 bit RSA key 366A8088089FDF93, created: 2023-11-09
(3)     Genbu <genbu@himitsu>
          3072 bit RSA key B05A692D6B16B0B6, created: 2023-11-09
(4)     Genbu <genbu@himitsu>
          3072 bit RSA key B7367C4F2E3CE05E, created: 2023-11-09
(5)     Genbu <genbu@himitsu>
          4096 bit RSA key 2555013026CEFEAF, created: 2023-11-09
Keys 1-5 of 5 for "genbu@himitsu".  Enter number(s), N)ext, or Q)uit > 1 2 3 4 5
gpg: key 2555013026CEFEAF: public key "Genbu <genbu@himitsu>" imported
gpg: key B7367C4F2E3CE05E: public key "Genbu <genbu@himitsu>" imported
gpg: key B05A692D6B16B0B6: public key "Genbu <genbu@himitsu>" imported
gpg: key 366A8088089FDF93: public key "Genbu <genbu@himitsu>" imported
gpg: key CF7625A4DF2992E1: public key "Genbu <genbu@himitsu>" imported
gpg: Total number processed: 5
gpg:               imported: 5
box@pgp:~$ 
```

Com que ja tenim nocions de seguretat és fàcil de saber quin és la clau GPG autèntica.

Mirem les signatures, a veure quina clau PGP està firmada per `sensei@himitsu` :

```
box@pgp:~$ gpg --list-signatures genbu
pub   rsa4096 2023-11-09 [SC] [expires: 2028-11-07]
      893FC1196C4932BBBCCA98C52555013026CEFEAF
uid           [ unknown] Genbu <genbu@himitsu>
sig 3        2555013026CEFEAF 2023-11-09  Genbu <genbu@himitsu>
sub   rsa4096 2023-11-09 [E] [expires: 2028-11-07]
sig          2555013026CEFEAF 2023-11-09  Genbu <genbu@himitsu>

pub   rsa3072 2023-11-09 [SC] [expires: 2028-11-07]
      CEF19250B4A28A84EEB07D7CB7367C4F2E3CE05E
uid           [ unknown] Genbu <genbu@himitsu>
sig 3        B7367C4F2E3CE05E 2023-11-09  Genbu <genbu@himitsu>
sub   rsa3072 2023-11-09 [E] [expires: 2028-11-07]
sig          B7367C4F2E3CE05E 2023-11-09  Genbu <genbu@himitsu>
```

Cap està firmada !! I ara que faig 🙄 ??

Millor que mirar Google o ChatGPT és seguir llegint (és molt difícil trobar la solució).

Per defecte, quan et baixes una clau d'un servidor públic, només la baixa amb la seva signatura.

Si vols les altres signatures has d'afegir l'opció `--keyserver-options no-self-sigs-only` ja que per defecte l'opció és `self-sigs-only` .

Actualizo les claus:

```
box@pgp:~$ gpg --refresh-keys --keyserver-options no-self-sigs-only  --keyserver keyserver.ubu
ntu.com
gpg: refreshing 6 keys from hkp://keyserver.ubuntu.com
gpg: key CF7625A4DF2992E1: "Genbu <genbu@himitsu>" not changed
gpg: key 366A8088089FDF93: 1 signature not checked due to a missing key
gpg: key 366A8088089FDF93: "Genbu <genbu@himitsu>" 1 new signature
gpg: key B05A692D6B16B0B6: 1 signature not checked due to a missing key
gpg: key B05A692D6B16B0B6: "Genbu <genbu@himitsu>" 1 new signature
gpg: key B7367C4F2E3CE05E: "Genbu <genbu@himitsu>" not changed
gpg: key 2555013026CEFEAF: "Genbu <genbu@himitsu>" not changed
gpg: key B0D394F00D613201: "David de Mingo <ddemingo@xtec.cat>" not changed
gpg: Total number processed: 6
gpg:              unchanged: 4
gpg:         new signatures: 2
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2025-11-07
box@pgp:~$
```

I torno a mirar les signatures:

```
box@pgp:~$ gpg --list-signatures genbu
pub   rsa4096 2023-11-09 [SC] [expires: 2028-11-07]
      893FC1196C4932BBBCCA98C52555013026CEFEAF
uid           [ unknown] Genbu <genbu@himitsu>
sig 3        2555013026CEFEAF 2023-11-09  Genbu <genbu@himitsu>
sub   rsa4096 2023-11-09 [E] [expires: 2028-11-07]
sig          2555013026CEFEAF 2023-11-09  Genbu <genbu@himitsu>

pub   rsa3072 2023-11-09 [SC] [expires: 2028-11-07]
      CEF19250B4A28A84EEB07D7CB7367C4F2E3CE05E
uid           [ unknown] Genbu <genbu@himitsu>
sig 3        B7367C4F2E3CE05E 2023-11-09  Genbu <genbu@himitsu>
sub   rsa3072 2023-11-09 [E] [expires: 2028-11-07]
sig          B7367C4F2E3CE05E 2023-11-09  Genbu <genbu@himitsu>

pub   rsa3072 2023-11-09 [SC] [expires: 2025-11-08]
      C5BA5036AD8A46830ECF19C1B05A692D6B16B0B6
uid           [ unknown] Genbu <genbu@himitsu>
sig 3        B05A692D6B16B0B6 2023-11-09  Genbu <genbu@himitsu>
sig          F2BD23B07EA556B6 2023-11-09  [User ID not found]
sub   rsa3072 2023-11-09 [E] [expires: 2025-11-08]
sig          B05A692D6B16B0B6 2023-11-09  Genbu <genbu@himitsu>

pub   rsa3072 2023-11-09 [SC] [expires: 2028-11-07]
      6AEAB6C4DC35333A33CFD59C366A8088089FDF93
uid           [ unknown] Genbu <genbu@himitsu>
sig 3        366A8088089FDF93 2023-11-09  Genbu <genbu@himitsu>
sig          25F91F569247951E 2023-11-09  [User ID not found]
sub   rsa3072 2023-11-09 [E] [expires: 2028-11-07]
```

FIRMAT PER UN USUARI DESCONEGUT

Importa la clau de Sensei

Com que les claus del membres del grup Himitsu estan firmades per `sensei@himitsu` millor importo la clau de Sensei:

```
box@pgp:~$ gpg --search-keys --keyserver keyserver.ubuntu.com sensei@himitsu
gpg: data source: http://185.125.188.26:11371
(1)     Sensei <sensei@himitsu>
          4096 bit RSA key F2BD23B07EA556B6, created: 2023-11-09
(2)     Sensei <sensei@himitsu>
          3072 bit RSA key 25F91F569247951E, created: 2023-11-09
Keys 1-2 of 2 for "sensei@himitsu".  Enter number(s), N)ext, or Q)uit > 1 2
gpg: key 25F91F569247951E: public key "Sensei <sensei@himitsu>" imported
gpg: key F2BD23B07EA556B6: public key "Sensei <sensei@himitsu>" imported
gpg: Total number processed: 2
gpg:               imported: 2
box@pgp:~$
```

Com que sabem que la clau autentica té el hash (“fingerprint”) `4F7EA4A0D5DC9C81DD7CD453F2BD23B07EA556B6` podem saber quina és la clau GPG autèntica:

```
box@pgp:~$ gpg --list-keys sensei
pub   rsa3072 2023-11-09 [SC] [expires: 2073-10-27]
      32128CD8D596083CFD89F83825F91F569247951E
uid           [ unknown] Sensei <sensei@himitsu>
sub   rsa3072 2023-11-09 [E] [expires: 2073-10-27]

pub   rsa4096 2023-11-09 [SC] [expires: 2073-10-27]
      4F7EA4A0D5DC9C81DD7CD453F2BD23B07EA556B6
uid           [ unknown] Sensei <sensei@himitsu>
sub   rsa4096 2023-11-09 [E] [expires: 2073-10-27]

box@pgp:~$
```

AUTÉNTICA

Tothom pot posar el nom que vulgui a la seva clau GPG, per això gpg utilitza hash curts per identificar les claus amb precissió:

```
box@pgp:~$ gpg --list-keys --keyid-format SHORT  sensei
pub   rsa3072/9247951E 2023-11-09 [SC] [expires: 2073-10-27]
      32128CD8D596083CFD89F83825F91F569247951E
uid         [ unknown] Sensei <sensei@himitsu>
sub   rsa3072/1BF0A030 2023-11-09 [E] [expires: 2073-10-27]

pub   rsa4096/7EA556B6 2023-11-09 [SC] [expires: 2073-10-27]
      4F7EA4A0D5DC9C81DD7CD453F2BD23B07EA556B6
uid         [ unknown] Sensei <sensei@himitsu>
sub   rsa4096/DEEC7452 2023-11-09 [E] [expires: 2073-10-27]

box@pgp:~$
```

AUTENTICA

Signo la clau bona:

```
box@pgp:~$ gpg --list-keys --keyid-format SHORT  sensei
pub   rsa3072/9247951E 2023-11-09 [SC] [expires: 2073-10-27]
      32128CD8D596083CFD89F83825F91F569247951E
uid         [ unknown] Sensei <sensei@himitsu>
sub   rsa3072/1BF0A030 2023-11-09 [E] [expires: 2073-10-27]

pub   rsa4096/7EA556B6 2023-11-09 [SC] [expires: 2073-10-27]
      4F7EA4A0D5DC9C81DD7CD453F2BD23B07EA556B6
uid         [ unknown] Sensei <sensei@himitsu>
sub   rsa4096/DEEC7452 2023-11-09 [E] [expires: 2073-10-27]

box@pgp:~$ gpg --sign-key 7EA556B6

pub  rsa4096/F2BD23B07EA556B6
     created: 2023-11-09  expires: 2073-10-27  usage: SC
     trust: unknown       validity: unknown
sub  rsa4096/98D1F018DEEC7452
```

Borro la falsa:

```
box@pgp:~$ gpg --list-keys --keyid-format SHORT  sensei
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   1  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1  valid:   1  signed:   1  trust: 1-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2025-11-07
pub   rsa3072/9247951E 2023-11-09 [SC] [expires: 2073-10-27]
      32128CD8D596083CFD89F83825F91F569247951E
uid         [ unknown] Sensei <sensei@himitsu>
sub   rsa3072/1BF0A030 2023-11-09 [E] [expires: 2073-10-27]

pub   rsa4096/7EA556B6 2023-11-09 [SC] [expires: 2073-10-27]
      4F7EA4A0D5DC9C81DD7CD453F2BD23B07EA556B6
uid         [  full  ] Sensei <sensei@himitsu>
sub   rsa4096/DEEC7452 2023-11-09 [E] [expires: 2073-10-27]

box@pgp:~$ gpg --delete-keys 9247951E
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Importa la clau de Genbu

Ara ja podem tornar a mirar de nou les claus de Genbu:

```
box@pgp:~$ gpg --list-signatures --keyid-format SHORT genbu
pub   rsa4096/26CEFEAF 2023-11-09 [SC] [expires: 2028-11-07]
      893FC1196C4932BBBCCA98C52555013026CEFEAF
uid         [ unknown] Genbu <genbu@himitsu>
sig 3        26CEFEAF 2023-11-09  Genbu <genbu@himitsu>
sub   rsa4096/EEDCCF3B 2023-11-09 [E] [expires: 2028-11-07]
sig          26CEFEAF 2023-11-09  Genbu <genbu@himitsu>

pub   rsa3072/2E3CE05E 2023-11-09 [SC] [expires: 2028-11-07]
      CEF19250B4A28A84EEB07D7CB7367C4F2E3CE05E
uid         [ unknown] Genbu <genbu@himitsu>
sig 3        2E3CE05E 2023-11-09  Genbu <genbu@himitsu>
sub   rsa3072/AA25893C 2023-11-09 [E] [expires: 2028-11-07]
sig          2E3CE05E 2023-11-09  Genbu <genbu@himitsu>

pub   rsa3072/6B16B0B6 2023-11-09 [SC] [expires: 2025-11-08]
      C5BA5036AD8A46830ECF19C1B05A692D6B16B0B6
uid         [  undef ] Genbu <genbu@himitsu>
sig 3        6B16B0B6 2023-11-09  Genbu <genbu@himitsu>
sig          7EA556B6 2023-11-09  Sensei <sensei@himitsu>
sub   rsa3072/508EBBF3 2023-11-09 [E] [expires: 2025-11-08]
sig          6B16B0B6 2023-11-09  Genbu <genbu@himitsu>

pub   rsa3072/089FDF93 2023-11-09 [SC] [expires: 2028-11-07]
      6AEAB6C4DC35333A33CFD59C366A8088089FDF93
uid         [ unknown] Genbu <genbu@himitsu>
sig 3        089FDF93 2023-11-09  Genbu <genbu@himitsu>
sig          9247951E 2023-11-09  [User ID not found]
sub   rsa3072/E9AA355D 2023-11-09 [E] [expires: 2028-11-07]
```

AQUESTA ÉS LA BONA

AQUESTA FIRMA ÉS FALSA

Signo la clau bona de Genbu:

```
box@pgp:~$ gpg --sign-key 6B16B0B6

pub  rsa3072/B05A692D6B16B0B6
     created: 2023-11-09  expires: 2025-11-08  usage: SC
     trust: unknown       validity: undefined
sub  rsa3072/1769BD2F508EBBF3
     created: 2023-11-09  expires: 2025-11-08  usage: E
[  undef ] (1). Genbu <genbu@himitsu>
```

Borro les altres:

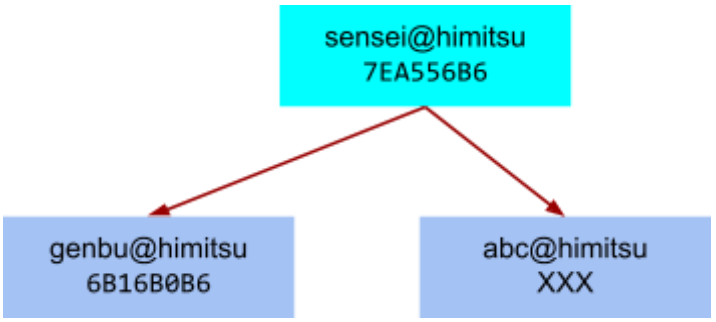
```
box@pgp:~$ gpg --delete-keys 26CEFEAF 2E3CE05E 089FDF93 DF2992E1
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


pub  rsa4096/2555013026CEFEAF 2023-11-09 Genbu <genbu@himitsu>

Delete this key from the keyring? (y/N) y

pub  rsa3072/B7367C4F2E3CE05E 2023-11-09 Genbu <genbu@himitsu>

Delete this key from the keyring? (y/N) y

pub  rsa3072/366A8088089FDF93 2023-11-09 Genbu <genbu@himitsu>

Delete this key from the keyring? (y/N) y

pub  rsa4096/CF7625A4DF2992E1 2023-11-09 Genbu <genbu@himitsu>

Delete this key from the keyring? (y/N) y
box@pgp:~$
```

Web of Trust

Com veurem també a SMX-6-UF4-3 - Certificats la validesa d'un certificat depèn de qui l'ha firmat.

I si no confies en qui ha signat aquest certificat llavors has de mirar qui ha firmat el certificat del que ha firmat el certificat.

I vas fent així fins que trobes un certificat en que tu confies.



En el nostre cas és el de Sensei amb fingerprint: `4F7EA4A0D5DC9C81DD7CD453F2BD23B07EA556B6`

A partir d'aquest clau de confiança es pot construir un conjunt de claus validades per Sensei.

Tu confies en la **clau genbu@himitsu** amb **ID `6B16B0B6`** (i no en les altres) perquè està **firmada per sensei@himitsu** encara que no coneguis a "Genbu"

Així és com funcionen tots els certificats, i perquè tots els hackers intenten obtenir el control dels certificats de confiança que firmen els altres certificats.

Aquesta és la lliçó que havies d'apendre.

🙂

USER-ID

Com hem vist abans la majoria dels llocs posen en la seva pàgina web un enllaç directe a la clau i el fingerprint.

Sensei podria haver posat directament la `KEY-ID` de la seva clau que com ja saps és `7EA556B6`

Llavors podries baixar la seva clau directament amb aquesta `KEY-ID`:

```
box@pgp:~$ gpg --receive-keys --keyserver keyserver.ubuntu.com 7EA556B6
gpg: key F2BD23B07EA556B6: "Sensei <sensei@himitsu>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
box@pgp:~$
```

Però no ho fa perquè pensa que qui contacti amb ell ha de demostrar uns mínims coneixements de seguretat.

Xifrar i desxifrar missatges

Xifrar i desxifrar missatge amb GPG és molt senzill.

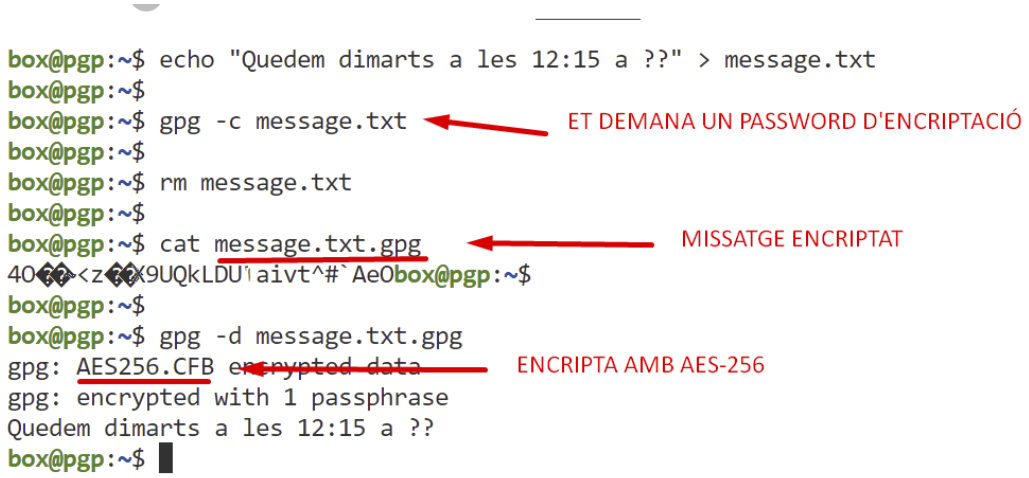
El que és difícil es garantir l'autenticitat dels missatges perquè moltes persones i organitzacions els hi agrada mentir per treure profit personal.

Ja hem vist com podem garantir l'autenticitat dels missatges amb la xarxa de confiança de claus firmades.

Xifratge simètric

Xifrar i desxifrar un fitxer amb **gpg** és molt més fàcil que amb `openssl` perquè has d'escriure menys 👍

gpg ja decideix per tu!

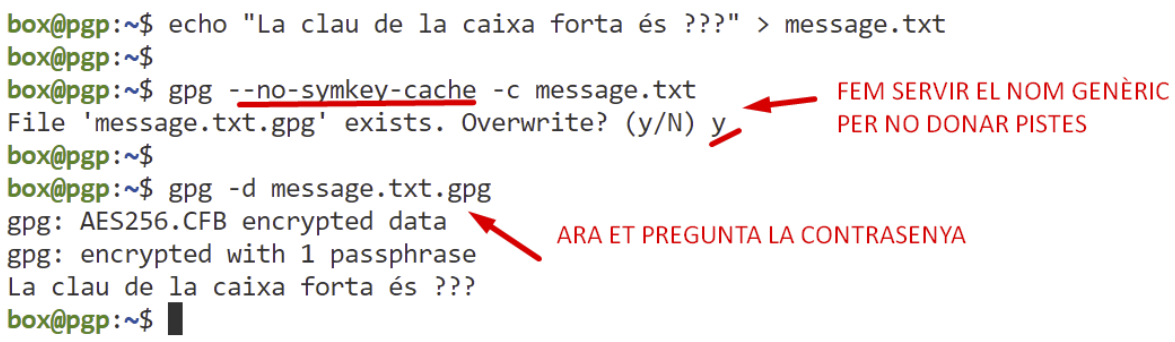


La única diferència és que openssl fa servir el flag `-e` (encrypt) i pgp el flag `-c` (cipher)

I que per desxifrar no t'ha demanat la contrasenya 😳!

Com PGP sap per experiència que la gent no se'n recorda de les contrasenyes al cap d'un minuts, fa servir una memòria "**cache**" per intentar desxifrar el missatge sense demanar-te la contrasenya.

Si no vols que faci això pots fer servir el flag `--no-symkey-cache`.



Com pots veure per defecte el missatge desxifrat només apareix per pantalla.

Això es fa per no deixar rastre del missatge desxifrat perquè com veurem a SMX-6-UF4-4 - Recuperació de fitxers un fitxer es pot recuperar encara que s'hagi borrat del disc dur.

I si no t'has oblidat de borrar-lo encara més fàcil 🤨!

Però, que has de fer si vols guardar el missatge desencriptat en un fitxer perquè és un video o un pdf per exemple?

Amb el flag `-o` (output) li dius a pgp el nom del fitxer.

```
box@pgp:~$ echo "El resultat del partit serà ..." > message.txt
box@pgp:~$
box@pgp:~$ gpg -c message.txt
File 'message.txt.gpg' exists. Overwrite? (y/N) y
box@pgp:~$
box@pgp:~$ rm message.txt
box@pgp:~$
box@pgp:~$ gpg -o message.txt -d message.txt.gpg
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
box@pgp:~$
box@pgp:~$ cat message.txt
El resultat del partit serà ...
box@pgp:~$
```

Xifratge asimètric

Enviar un missatge

Com ja saps de SMX-6-UF4-1 - Criptografia, per enviar un missatge el que fem és:

1. Encriptar el missatge amb una clau simètrica d'un sol ús
2. Encriptar la clau simètrica amb la clau pública del destinatari.
3. Enviar el missatge encriptat amb la la clau simètrica encriptada.

Massa feina amb openssl, millor PGP que ho fa tot per nosaltres !

Si vull enviar un missatge a `genbu@himitsu` amb `pgp` :

```
box@pgp:~$ echo -n "鳥が巣を離れました" | gpg -e -o message.gpg -r genbu
box@pgp:~$
box@pgp:~$ cat message.gpg
i/P
   VSnUYd  S#9ZX>Ct
*)uK/ĉ(,uDX$
jnHc-*4W5.Q6qZzcx3J)3-\B?xE@9c>ǩ(-QVB!2'7?UlT[krrX(c  4V.!Mb^Ym}ZA+C.4S+e@{
)o
6^ibox@pgp:~$
```

En aquest cas fais servir el flag `-e` (o `--encrypt`).

Amb el flag `-r` (o `--recipient`) indico el destinatari del missatge.

Si vull crear un missatge amb més d'un destinatari puc afegir més `-r` :

```
box@pgp:~$ echo -n "鳥が巣を離れました" | gpg -e -o message.gpg -r genbu
 -r sensei
box@pgp:~$
```

I si no poso destinatari gpg em pregunta per ell:

```
box@pgp:~$ echo -n "鳥が巣を離れました" | gpg -e -o message.gpg
You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID.  End with an empty line: genbu

Current recipients:
rsa3072/1769BD2F508EBBF3 2023-11-09 "Genbu <genbu@himitsu>"

Enter the user ID.  End with an empty line:  ENTER
File 'message.gpg' exists. Overwrite? (y/N) y
box@pgp:~$
```

Desencriptar: **gpg -d arxiu**

Crear un usuari de proves

Has enviat un missatge a genbu, però com pot saber genbu que aquest missatge és original?

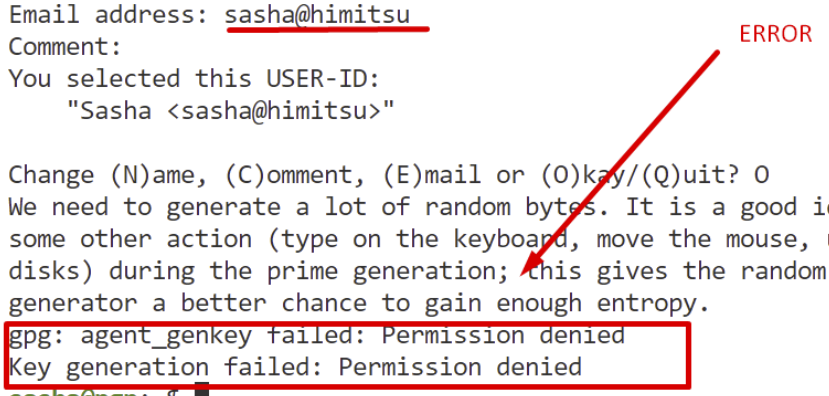
El que hem de fer és fer proves en el nostre ordinador per aprendre a fer servir gpg.

Crea un nou usuari `sasha` (o qualsevol altre nom) a la màquina virtual i canvia a aquest usuari:

```
box@pgp:~$ sudo su sasha
sasha@pgp:/home/box$ cd
sasha@pgp:~$
```

Crea una clau GPG per a l'usuari `sasha@himitsu` :

```
GnuPG needs to construct a user ID to identify your key.

Real name: Sasha
Email address: sasha@himitsu
Comment:
You selected this USER-ID:
    "Sasha <sasha@himitsu>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: agent_genkey failed: Permission denied
Key generation failed: Permission denied
sasha@pgp:~$
```



gpg dóna error perquè el terminal és de box, no de `sasha` i GPG ha avortat l'acció en lloc de continuar.

Això sol passar si executem comandes sobre SSH.

Però millor crea una altra màquina, serà més fàcil i pedagògic 🤔 !

```
box.exe create sasha
box.exe start sasha
box.exe ssh sahsa
```

A continuació crea una clau gpg per a **sasha** :

```
box@sasha:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/box/.gnupg' created
gpg: keybox '/home/box/.gnupg/pubring.kbx' created


GnuPG needs to construct a user ID to identify your key.

Real name: Sasha
Email address: sasha@himitsu
Comment:
You selected this USER-ID:
    "Sasha <sasha@himitsu>"
```

Puja la clau pública a `keyserver.ubuntu.com` :

```
box@sasha:~$ gpg --list-keys --keyid-format SHORT himitsu
pub   rsa3072/845862E8 2023-11-15 [SC]
      66CD2E060A7F693F63DA436E6AE7A13E845862E8
uid         [ultimate] Sasha <sasha@himitsu>
sub   rsa3072/5ED94219 2023-11-15 [E]

box@sasha:~$ gpg --send-keys --keyserver keyserver.ubuntu.com 845862E8
gpg: sending key 6AE7A13E845862E8 to hkp://keyserver.ubuntu.com
box@sasha:~$
```

Crea un etherpad a https://pad.riseup.net/ amb la ID de la clau gpg de sasha:

https://pad.riseup.net/p/**845862e8**.

Per defecte el pad s'elimina al cap de 60 dies si no hi ha activitat.

Seguretat

El procediment que faras sevir et pot semblar una mica complicat, però és el més segur.

Quan tu envies un missatge encriptat per correu ningú pot llegit el missatge, però no pots amagar que has enviat un missatge a aquella persona.

Quan envies missatges amb WhatsApp o Telegram, el missatge està codificat, però les empreses saben amb qui parles, quan parles, etc.

I això és molta informació perquè "digues-me amb qui vas i et diré qui ets".

A la llarga hauras d'apendre a programar en Python en el futur si vols dedicar-te a la ciberseguretat per automatizar aquestes tasques.

També conectarte a través d'una VPN com ASIX-11-UF2-4 - Wireguard

Envia un missatge a sasha

Torna a la màquina gpg !

Enlloc d'enviar un missatge a `genbu` ara li envias a `sasha`.

1.- Torna a la màquina gpg, importa la clau de sasha i signa la clau

Com que no som molt originals i és segur que molts haureu creat un clau `sasha@himitsu`, importa directament la clau amb **la ID** :

```
box@gpg:~$ gpg --receive-keys --keyserver keyserver.ubuntu.com 845862e8
gpg: key 6AE7A13E845862E8: public key "Sasha <sasha@himitsu>" imported
gpg: Total number processed: 1
gpg:               imported: 1
box@gpg:~$
box@gpg:~$ gpg --sign-key sasha

pub  rsa3072/6AE7A13E845862E8
     created: 2023-11-15  expires: never       usage: SC
     trust: unknown       validity: unknown
sub  rsa3072/F706AE965ED94219
     created: 2023-11-15  expires: never       usage: E
[ unknown] (1). Sasha <sasha@himitsu>


pub  rsa3072/6AE7A13E845862E8
     created: 2023-11-15  expires: never       usage: SC
     trust: unknown       validity: unknown
 Primary key fingerprint: 66CD 2E06 0A7F 693F 63DA  436E 6AE7 A13E 8458 62E8

     Sasha <sasha@himitsu>

Are you sure that you want to sign this key with your
key "David <david@himitsu>" (942EAF368FE1CF35)

Really sign? (y/N) y

box@gpg:~$
```

2. - Encripta un missatge per a sasha

```
box@gpg:~$ echo "El 09/01/2023 apareixerà de nou un estel" | gpg -e -o message.txt
 -r sasha
gpg: checking the trustdb
gpg: no ultimately trusted keys found
gpg: F706AE965ED94219: There is no assurance this key belongs to the named user

sub  rsa3072/F706AE965ED94219 2023-11-15 Sasha <sasha@himitsu>
 Primary key fingerprint: 66CD 2E06 0A7F 693F 63DA  436E 6AE7 A13E 8458 62E8
      Subkey fingerprint: 893A BEB2 3A2E 0E40 B660  647F F706 AE96 5ED9 4219

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
box@gpg:~$
```

4.- Puja a https://transfer.sh el missatge per sasha

si no funciona transfer.sh podeu feu servir:

```
touch hello.txt
```

```
box@cert:~$ curl -T hello.txt https://oshi.at
```

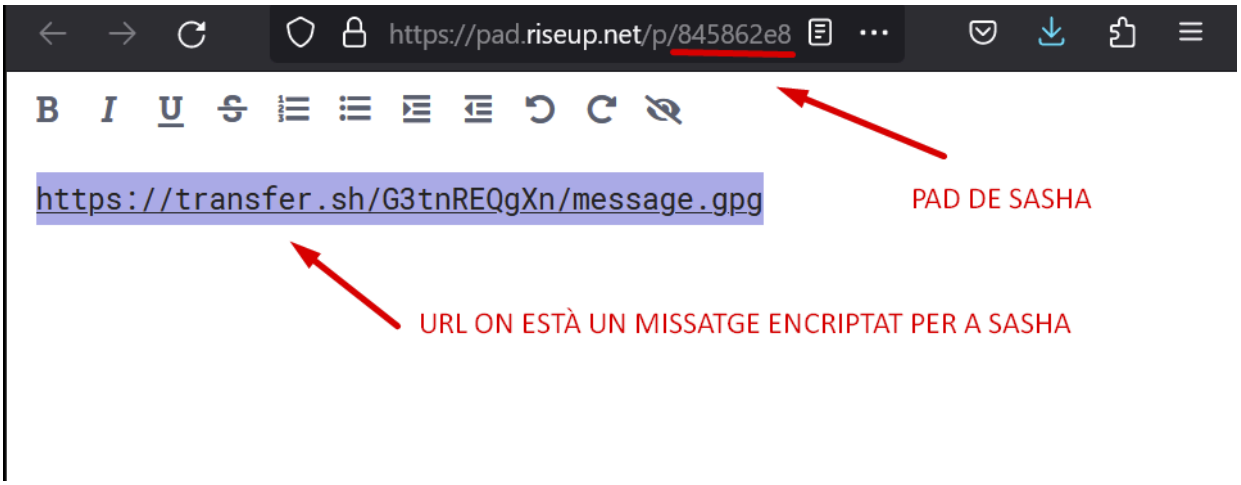
```
box@gpg:~$ curl --upload-file message.txt https://transfer.sh/message.gpg
https://transfer.sh/G3tnREQgXn/message.gpgbox@gpg:~$
```

URL ON ESTÀ EL MISSATGE ENCRIPTAT

El fitxer que has pujat s'elimina en 14 dies.

5.- Posa la URL que t'ha donat `transfer.sh` al pad de Sasha.

Saps quin és el pad per la ID de la clau gpg de Sasha.



Sasha llegeix el teu missatge

Torna a la màquina sasha !

1.- Sasha de tant en tant mira el seu pad (és la seva bústia)

Com que ha trobat un nou missatge, el baixa a la seva màquina.

```
box@sasha:~$ wget https://transfer.sh/G3tnREQgXn/message.gpg
--2023-11-21 10:31:46--  https://transfer.sh/G3tnREQgXn/message.gpg
Resolving transfer.sh (transfer.sh)... 144.76.136.153, 2a01:4f8:200:1097::2
Connecting to transfer.sh (transfer.sh)|144.76.136.153|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 502 []
Saving to: ‘message.gpg’

message.gpg          100%[===================>]     502  --.-KB/s    in 0s

2023-11-21 10:31:46 (110 MB/s) - ‘message.gpg’ saved [502/502]

box@sasha:~$
```

2.- A continuació ha de desencriptar el missatge:

```
box@sasha:~$ gpg -d message.gpg
gpg: encrypted with 3072-bit RSA key, ID F706AE965ED94219, created 2023-11-15
      "Sasha <sasha@himitsu>"
El 09/01/2023 apareixerà de nou un estel
box@sasha:~$
```

NOMÉS SASHA POT LLEGIR AQUEST MISSATGE !

3.- Encara que només ell pot llegir el missatge no sap qui l'ha creat perquè el missatge només s'ha encriptat, no signat 😣 !

Envia un missatge a Sasha (signat)

Torna a la màquina gpg !

1. - Encripta un missatge per a sasha amb l'opció de signar `-s :`

```
box@gpg:~$ rm message.txt
box@gpg:~$
box@gpg:~$ echo "El 09/01/2023 apareixerà de nou un estel, que tornarà a il.lumina
r el cel només per tu" | gpg -e -s -o message.txt -r sasha
gpg: F706AE965ED94219: There is no assurance this key belongs to the named user

sub  rsa3072/F706AE965ED94219 2023-11-15 Sasha <sasha@himitsu>
 Primary key fingerprint: 66CD 2E06 0A7F 693F 63DA  436E 6AE7 A13E 8458 62E8
      Subkey fingerprint: 893A BEB2 3A2E 0E40 B660  647F F706 AE96 5ED9 4219

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
gpg: signing failed: Inappropriate ioctl for device
gpg: [stdin]: sign+encrypt failed: Inappropriate ioctl for device
box@gpg:~$
```

ERROR!

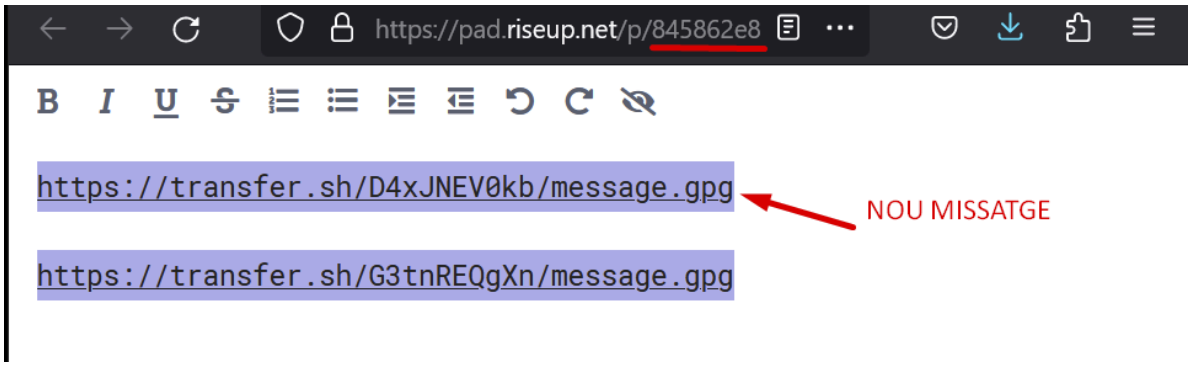
Si apareix aquest error has de exportar aquesta variable :

```
export GPG_TTY=$(tty)
```

Ja pots encriptar i signar:

```
box@gpg:~$ echo "El 09/01/2023 apareixerà de nou un estel, que tornarà a il.lumina
r el cel només per tu" | gpg -e -s -o message.txt -r sasha
gpg: F706AE965ED94219: There is no assurance this key belongs to the named user

sub  rsa3072/F706AE965ED94219 2023-11-15 Sasha <sasha@himitsu>
 Primary key fingerprint: 66CD 2E06 0A7F 693F 63DA  436E 6AE7 A13E 8458 62E8
      Subkey fingerprint: 893A BEB2 3A2E 0E40 B660  647F F706 AE96 5ED9 4219

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
box@gpg:~$
```

2.- Ja pots pujar el nou missatge a https://transfer.sh/ i publicar la nova URL al pad de Sasha:



Sasha llegeix el nou missatge

Torna a la màquina sasha !

1.- Llegeix el nou missatge

```
box@sasha:~$ rm message.gpg
box@sasha:~$
box@sasha:~$ wget https://transfer.sh/D4xJNEV0kb/message.gpg
--2023-11-21 10:54:47--  https://transfer.sh/D4xJNEV0kb/message.gpg
Resolving transfer.sh (transfer.sh)... 144.76.136.153, 2a01:4f8:200:1097::2
Connecting to transfer.sh (transfer.sh)|144.76.136.153|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1007 []
Saving to: ‘message.gpg’

message.gpg          100%[===================>]    1007  --.-KB/s    in 0.001s

2023-11-21 10:54:47 (1.13 MB/s) - ‘message.gpg’ saved [1007/1007]

box@sasha:~$
```

2.- Desencripta el missatge:

```
box@sasha:~$ gpg -d message.gpg
gpg: encrypted with 3072-bit RSA key, ID F706AE965ED94219, created 2023-11-15
      "Sasha <sasha@himitsu>"
El 09/01/2023 apareixerà de nou un estel, que tornarà a il.luminar el cel només pe
r tu                    EL MISSATGE ESTÀ SIGNAT
gpg: Signature made Tue Nov 21 10:49:04 2023 UTC
gpg:                using RSA key 094C7FF6B3738DAF0AE828CC942EAF368FE1CF35
gpg: Can't check signature: No public key
box@sasha:~$
                        PERÒ NO TENS IMPORTADA LA CLAU PÚBLICA DE QUI HA ESCRIT
                        EL MISSATGE
```

Digues a sasha on pot trobar la teva clau pública

Torna a la màquina gpg !

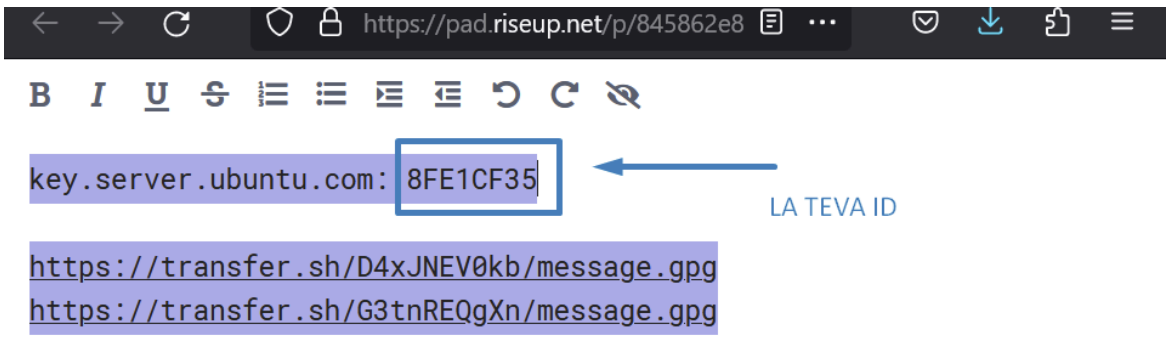
1.- Pots veure a la màquina gpg que la teva clau RSA és la que Sasha veu que s'ha fet servir per firmar el missatge:

```
box@gpg:~$ gpg --list-keys
/home/box/.gnupg/pubring.kbx
----------------------------
pub   rsa3072 2023-11-15 [SC]
      094C7FF6B3738DAF0AE828CC942EAF368FE1CF35
uid           [ unknown] David <david@himitsu>
sub   rsa3072 2023-11-15 [E]

pub   rsa3072 2023-11-15 [SC]
      66CD2E060A7F693F63DA436E6AE7A13E845862E8
uid           [ unknown] Sasha <sasha@himitsu>
sub   rsa3072 2023-11-15 [E]

box@gpg:~$
```

2.- Mira quina és la `ID` de la teva clau:

```
box@gpg:~$ gpg --list-keys --keyid-format SHORT david
pub   rsa3072/8FE1CF35 2023-11-15 [SC]
      094C7FF6B3738DAF0AE828CC942EAF368FE1CF35
uid         [ unknown] David <david@himitsu>
sub   rsa3072/358F62C1 2023-11-15 [E]

box@gpg:~$
```

3.- Pública al pad de sasha la `ID` de la teva clau i que està a https://keyserver.ubuntu.com/.



(CONTINUA)

A partir d'aquí continua tu sol.

1.- Sasha ha d'importar la teva clau, i enviar-te un missatge de resposta al teu pad.

2.- Tu has de llegir el missatge de Sasha.

3.- Com ja saps com funciona gpg, ja pots enviar un missatge encriptat al pad de `genbu@himitsu`.

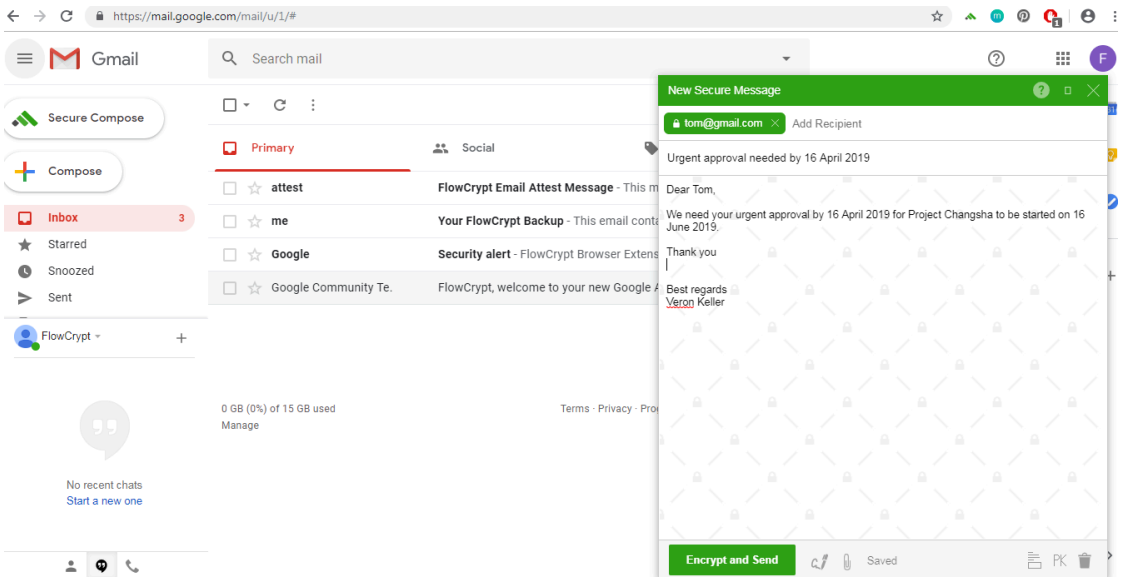
Flowcrypt

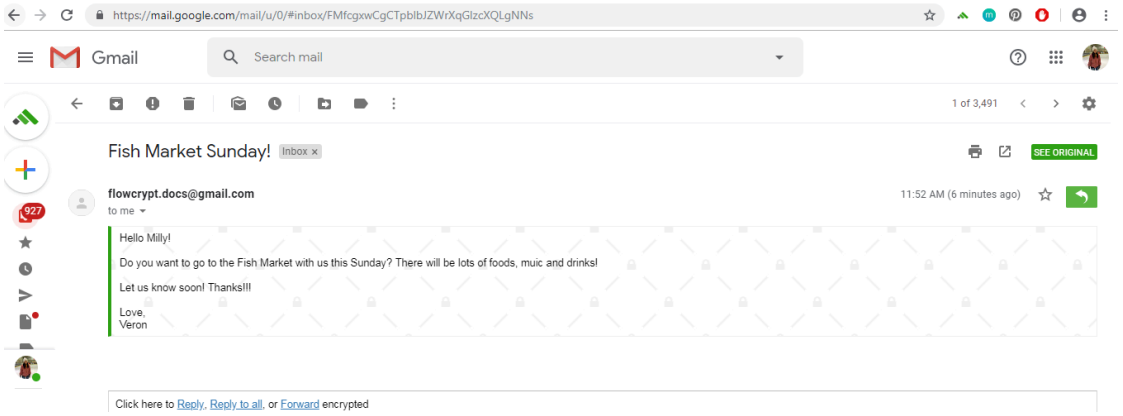
Com ja saps perquè la gent faci servir criptografia aquesta ha de ser molt fàcil de fer servir o que la persona estigui molt interesada.

FlowCrypt és un programa de xifratge de correu electrònic que s'integra molt fàcilment amb Gmail.

FlowCrypt utilitza OpenPGP per xifrar els missatges amb claus a les quals només tens accés tu i el teu destinatari.

Captures de pantalla de l'extensió del navegador FlowCrypt





- https://flowcrypt.com/docs/guide/setup/install.html
- https://flowcrypt.com/docs/guide/send-and-receive/overview.html

Envia amb Flowcrypt un correu encriptat al correu electrònic d'un altre alumne.