



TL;DR

Steg-för-steg genomgång av hur man skapar en pgp-nyckel med subnycklar för signering och kryptering med GnuPG v 2.2.x



https://cdimage.kali.org/kali-2019.1a/kali-linux-light-2019.1a-amd64.iso https://docs.kali.org/downloading/kali-linux-live-usb-install



Det bör dock gå bra att följa merparten av instruktionerna förutsatt att du har GPG v2.2.x på någon linux eller mac-distribution med Bash som skal. Till Workshopen finns en labmaskin

lab.cert.sunet.se

Konton och lösenord finns på

https://www.cert.sunet.se/ws/accounts

4



Om du vill byta tangenbordslayout Applications -> Settings -> Keyboard

2		Keyboard	1	+ = ×
@ 2	Keyboa Edit keyb	ard oard settings an	d application shor	tcuts
Behavio	or Applic	ation Shortcuts	Layout	
🗌 Us	e system (defaults		
Keyb	oard mo	del		
Ge	eneric 105	-key PC (intl.)		Å
Chan	nge layou	t option	Compose key	
-		* *	-	* *
Keyb	oard layo	out		
La	yout	Variant		*
En	nglish (US)			+
	Add	Edit	Delete	
Help	>			Close

Välj fliken layout Klicka på Add



Välj önskad layout. Jag väljer Swedish utan döda tangenter.

@ 2	Keyboard	◆ □ ×
@ Keyl 2 Edit k	poard eyboard settings and application short	cuts
Behavior Ap	olication Shortcuts Layout	
🗌 Use syste	em defaults	
Keyboard	nodel	
Generic	105-key PC (intl.)	▲ ▼
Change lay	yout option Compose key	
-	* -	▲ ▼
Keyboard	ayout	
Layout	Variant	
English (US)	
Swedish	Swedish (no dead keys)	
Add	Edit Delete	
Help		Close

Nu borde man kunna växla layout, men jag har inte fått det att fungera. Radera därför "English (US)"

Avsluta med [Close]



Starta en terminal



Terminal redo att börja

Förkrav är att ha skapat en partition på 100MB

För att hitta rätt device:

DEVICE=\$(df /run/live/medium |tail -1|cut -d " " 1); DEVICE=\${DEVICE%%[0-9]*} parted \$DEVICE print

Skapa monteringspunkt /mnt/usb Montera /dev/sdb3 på monteringspunkt /mnt/usb

Terminal - root@kali: /mnt/usb/GPGDIR.Say	• -	o ×
File Edit View Terminal Tabs Help		
<pre>root@kal1:/mnt/usb# export GNUPGHOME=\$(mktemp -d /mnt/usb/GPGDIR.XXX) root@kali:/mnt/usb# cd \$GNUPGHOME</pre>		Î
<pre>root@kali:/mnt/usb/GPGDIR.Say# gpglist-keys</pre>		
gpg: WARNING: unsate permissions on homedir '/mnt/usb/GPGDIR.Say' gpg: DBG: locking for '/mnt/usb/GPGDIR.Say/pubring.kbx.lock' done via O	EXCL	
<pre>gpg: keybox '/mnt/usb/GPGDIR.Say/pubring.kbx' created</pre>		
gpg: DBG: locking for '/mnt/usb/GPGDIR.Say/trustdb.gpg.lock' done via O gpg: /mnt/usb/GPGDIR_Say/trustdb_gpg: trustdb_created	_EXCL	
<pre>root@kali:/mnt/usb/GPGDIR.Say#</pre>		
Ĩ		
<u>۵</u>		
		~

Skapa en katalog för den nya nyckeln och lagra namnet i omgivningsvariabel GNUPGHOME

gpg --list-keys

- Listar nycklar i nyckelring.
- Finns ingen nyckelring skapas en ny, tom sådan
- Viktigt test för att se att vi har en fräsch installation

Varning för att rättigheterna på GNUPGHOME är osäkra, vilket vi kan ignorera nu när vi kör i en isolerad miljö.

Skapa en gpg.conf med lämpliga värden så att vi får bästa möjliga nycklar keyid-format short för att lättare kunna arbeta med nycklarna

Terminal - root@kali: /mnt/usb/GPGDIR.Say	÷		×
File Edit View Terminal Tabs Help			
<pre>root@kali:/mnt/usb/GPGDIR.Say# gpgfull-generate-keyexpert gpg: WARNING: unsafe permissions on homedir '/mnt/usb/GPGDIR.Say' gpg (GnuPG) 2.2.12; Copyright (C) 2018 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.</pre>			^
<pre>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) (7) DSA (set your own capabilities) (8) RSA (set your own capabilities) (9) ECC and ECC (10) ECC (sign only) (11) ECC (set your own capabilities) (13) Existing key</pre>			
Your selection? 8			v

Dags att generera vår masternyckel.

Kommando: gpg –full-generate-keys –expert

Välj RSA-nyckel (set your own capabilities). Val: 8

Primärnyckel har normalt sett tre egenskaper

- Sign. Signera dokument
- Certify. Signera nycklar
- Encrypt. Krytpera dokument

Vi skall bara ha Certify och behöver därför ta bort S(ign) och E(ncrypt) Val: S

Terminal - root@kali: /mnt/usb/GPGDIR.Say	+ ×
File Edit View Terminal Tabs Help	
(10) ECC (sign only) (11) ECC (set your own capabilities) (13) Existing key Your selection? 8	*
Possible actions for a RSA key: Sign Certify Encrypt Authenticate Current allowed actions: Sign Certify Encrypt	
 (S) Toggle the sign capability I (E) Toggle the encrypt capability (A) Toggle the authenticate capability (Q) Finished 	
Your selection? S	
Possible actions for a RSA key: Sign Certify Encrypt Authenticate Current allowed actions: Certify Encrypt	
 (S) Toggle the sign capability (E) Toggle the encrypt capability (A) Toggle the authenticate capability (0) Einiched 	
Your selection? E	

Här syns att Sign är borttaget och nu skall Encrypt bort också

Val: E

Terminal - root@kali: /mnt/usb/GPGDIR.Say	+ _ = ×
File Edit View Terminal Tabs Help	
<pre>(A) Toggle the authenticate capability (Q) Finished</pre>	Â
Your selection? S	
Possible actions for a RSA key: Sign Certify Encrypt Authenticate Current allowed actions: Certify Encrypt	
 (S) Toggle the sign capability I (E) Toggle the encrypt capability (A) Toggle the authenticate capability (Q) Finished 	
Your selection? E	
Possible actions for a RSA key: Sign Certify Encrypt Authenticate Current allowed actions: Certify	
 (S) Toggle the sign capability (E) Toggle the encrypt capability (A) Toggle the authenticate capability (Q) Finished 	
Your selection? Q	

Nu ser vi att det bara är Certify kvar och vi kan avsluta valet av egenskaper.

Val: Q

Nu är det dags att välja nyckellängd.

Enligt NIST är 2048 bara tillräckligt fram till 2030. 3072 skall räcka, 4096 ger inte så mycket extra skydd, men kräver mer beräkningskraft än 3072. Val: 3072

Nu skall vi välja giltighetstid.

Viktigt att veta att vi alltid kan förlänga giltighetstid, så att sätta detta är ett extra skydd om nyckel och revokeringscertifikat skulle gå förlorade. Välj ett så lågt värde som ni anser är hanterbart. Vi väljer 2 år i den här övningen. Val: 2y

Nu skall vi välja giltighetstid.

Viktigt att veta att vi alltid kan förlänga giltighetstid, så att sätta detta är ett extra skydd om nyckel och revokeringscertifikat skulle gå förlorade. Välj ett så lågt värde som ni anser är hanterbart. Vi väljer 2 år i den här övningen. Val1: 2y

Val2: y

Terminal - root@kali: /mnt/usb/GPGDIR.Say	• =	×
File Edit View Terminal Tabs Help		
Your selection? Q RSA keys may be between 1024 and 4096 bits long. What keysize do you want? (3072) 3072 Requested keysize is 3072 bits Please specify how long the key should be valid. 0 = key does not expire <pre></pre> <pre></pre> <pr< td=""><td></td><td>*</td></pr<>		*
Real name: SUNET CERT Email address: cert@cert.sunet.se Comment: You selected this USER-ID: "SUNET CERT <cert@cert.sunet.se>" Change (N)ame, (C)omment, (E)mail or (0)kay/(Q)uit? 0</cert@cert.sunet.se>		~

Sätt en identitet på nyckeln. Real name och Email address bör sättas även om Email address är det enda som krävs.

Val 1: <Namn på ditt team>

Val 2: <epost till ditt team>

Val 3: <tomt>

Val 4: O

Välj en bra passphrase för din nyckel. Det här är enda skyddet som återstår om någon kommer åt din hemliga nyckel.

Terminal - root@kali: /mnt/usb/GPGDIR.Say	÷	
File Edit View Terminal Tabs Help		
Real name: SUNET CERT Email address: cert@cert.sunet.se Comment: You selected this USER-ID: "SUNET CERT <cert@cert.sunet.se>"</cert@cert.sunet.se>		*
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: DBG: locking for '/mnt/usb/GPGDIR.Say/pubring.kbx.lock' done via O_ gpg: DBG: locking for '/mnt/usb/GPGDIR.Say/trustdb.gpg.lock' done via O_ gpg: key F888EC71 marked as ultimately trusted gpg: directory '/mnt/usb/GPGDIR.Say/openpgp-revocs.d' created gpg: revocation certificate stored as '/mnt/usb/GPGDIR.Say/openpgp-revoc DDE265DDC793D65442FD28730692F888EC71.rev' public and secret key created and signed.	EXCL EXCL s.d/7	DAC
pub rsa3072/F888EC71 2019-04-02 [C] [expires: 2021-04-01] 7DACDDE265DDC793D65442FD28730692F888EC71		
<pre>root@kali:/mnt/usb/GPGDIR.Say#</pre>		

Efter en stund är nyckeln klar (rör på musen om det går långsamt)

Vi ser att vi har en nyckel utan undernycklar och att den bara har egenskapen Certify [C]

Kort nyckelid efter nyckellängden rsa3072/F888EC71

Vi ser här att en revokeringsnyckel har skapats automatiskt

Början på revokeringsfilen. Den här kan vara bra att skriva ut på papper och förvara i kassaskåp bredvid USB-stickan med den hemliga nyckeln. Skulle alla digitala kopior vara förstörda kan man (mödosamt) återskapa den och revokera en förlorad nyckel.

Dags att lägga till fler identiteter (behövs bara om ni har fler identiteter som skall använda samma nyckel)

Kommando: gpg -edit-key <NYCKELID>

Terminal - root@kali: /mnt/usb/GPGDIR.Say	+ - • ×
File Edit View Terminal Tabs Help	
7DACDDE265DDC793D65442FD28730692F888EC71 uid [ultimate] SUNET CERT <cert@cert.sunet.se></cert@cert.sunet.se>	^
<pre>root@kali:/mnt/usb/GPGDIR.Say# gpgedit-key F888EC71 gpg: WARNING: unsafe permissions on homedir '/mnt/usb/GPGDIR.Say' gpg (GnuPG) 2.2.12; Copyright (C) 2018 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.</pre>	
Secret key is available.	
<pre>sec rsa3072/F888EC71 created: 2019-04-02 expires: 2021-04-01 usage: C trust: ultimate validity: ultimate [ultimate] (1). SUNET CERT <cert@cert.sunet.se></cert@cert.sunet.se></pre>	
gpg> adduid Real name: SUNET CERT abuse Email address: abuse@cert.sunet.se Comment: You selected this USER-ID: "SUNET CERT abuse <abuse@cert.sunet.se>" Change (N)ame, (C)omment, (E)mail or (0)kay/(Q)uit? 0</abuse@cert.sunet.se>	

Extra identiteter läggs till med **adduid** Val: <Namn på identiteten> Val: <epost för identiteten> Val: <tomt> Val: O

		[3613]@kali		↑ _ X	
	Dacaphra			(
1 🖬 1	Passpilla	50.			
	Please enter "SUNET CERT 3072-bit RSA created 2019	the passphrase to unloc r <cert@cert.sunet.se>9 key, ID F888EC71, -04-02.</cert@cert.sunet.se>	k the OpenPG	P secret key:	
	Password:	••••••			
	Save in pa	assword manager			
			Cancel	OK	

Då vi skall ändra nyckeln så krävs att vi anger lösenordsfras. Senare i exempeln visas inte denna uttryckligen, men du förutsätts fylla i den när så behövs.

Vid behov lägg till ytterligare identiteter.

Vid behov lägg till ytterligare identiteter.

Välj den uid som skall vara primär.

Val 1: uid 1

Val 2: primary

Terminal - root@kali: /mnt/usb	0	> _	1 8	3
File Edit View Terminal Tabs Help				
"SUNET abuse <abuse@sunet.se>"</abuse@sunet.se>				^
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O				
<pre>sec rsa3072/F888EC71 created: 2019-04-02 expires: 2021-04-01 usage: C trust: ultimate validity: ultimate [ultimate] (1). SUNET CERT <cert@cert.sunet.se> [unknown] (2) SUNET CERT abuse <abuse@cert.sunet.se> [unknown] (3) SUNET abuse <abuse@sunet.se></abuse@sunet.se></abuse@cert.sunet.se></cert@cert.sunet.se></pre>				
gpg> uid 1				
<pre>sec rsa3072/F888EC71 created: 2019-04-02 expires: 2021-04-01 usage: C trust: ultimate validity: ultimate [ultimate] (1)* SUNET CERT <cert@cert.sunet.se> [unknown] (2) SUNET CERT abuse <abuse@cert.sunet.se> [unknown] (3) SUNET abuse <abuse@sunet.se> </abuse@sunet.se></abuse@cert.sunet.se></cert@cert.sunet.se></pre>				
gpg> primary				
gpg> quit Save changes? (y/N) y				~

Här ser vi nu att nyckeln har tre identiteter och vi kan avsluta och spara.

Terminal - root@kali: /mnt/usb	÷ =	o x
File Edit View Terminal Tabs Help		
<pre>root@kali:/mnt/usb# gpglist-keys gpg: WARNING: unsafe permissions on homedir '/mnt/usb/GPGDIR.Say' /mnt/usb/GPGDIR.Say/pubring.kbx</pre>		^
<pre>pub rsa3072/F888EC71 2019-04-02 [C] [expires: 2021-04-01] 7DACDDE265DDC793D65442FD28730692F888EC71 uid [ultimate] SUNET CERT <cert@cert.sunet.se> uid [ultimate] SUNET CERT abuse <abuse@cert.sunet.se> uid [ultimate] SUNET abuse <abuse@cert.se></abuse@cert.se></abuse@cert.sunet.se></cert@cert.sunet.se></pre>		
root@kali:/mnt/usb#		÷

Listar vi nyckeln ser vi de nya identiterna och att vi automatiskt fått [ultimate] trust för dem.

Den vi valde som primary listas först.

Terminal - root@kali: /mnt/usb	6	> -	×	
File Edit View Terminal Tabs Help				
/mnt/usb/GPGDIR.Say/pubring.kbx			ſ	
<pre>pub rsa3072/F888EC71 2019-04-02 [C] [expires: 2021-04-01] 7DACDDE265DDC793D65442FD28730692F888EC71 uid [ultimate] SUNET CERT <cert@cert.sunet.se> uid [ultimate] SUNET CERT abuse <abuse@cert.sunet.se> uid [ultimate] SUNET abuse <abuse@cert.se></abuse@cert.se></abuse@cert.sunet.se></cert@cert.sunet.se></pre>				
<pre>root@kali:/mnt/usb# gpgexpertedit-key F888EC71 gpg: WARNING: unsafe permissions on homedir '/mnt/usb/GPGDIR.Say' gpg (GnuPG) 2.2.12; Copyright (C) 2018 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.</pre>				
Secret key is available. sec rsa3072/F888EC71 created: 2019-04-02 expires: 2021-04-01 usage: C trust: ultimate validity: ultimate				
<pre>[ultimate] (1). SUNET CERT <cert@cert.sunet.se> [ultimate] (2) SUNET CERT abuse <abuse@cert.sunet.se> [ultimate] (3) SUNET abuse <abuse@sunet.se> gpg></abuse@sunet.se></abuse@cert.sunet.se></cert@cert.sunet.se></pre>				

Nu är det dags att skapa subnycklar för kryptering och signering.

Kommando: gpg -expert -edit-key <KEYID>

Skapa en subnyckel med egenvalda egenskaper

Val 1:8

Vi är nöjda med Sign och Encrypt på nyckeln. Vi vill ha en 3072 bitar lång nyckel med 1 års giltighetstid.

Den kortarte tiden är för att detta är en nyckel som skall delas och användas på maskiner anslutna till nätet.

Val 1: Q

Val 2: 3072

Val 3: 1y

Val 4: y

Val 5: y

Terminal - root@kali: /mnt/usb	÷	• ×
File Edit View Terminal Tabs Help		
0 = key does not expire		^
<n> = key expires in n days</n>		
<n>w = key expires in n weeks</n>		
<n>m = key expires in n months</n>		
<pre><n>y = key expires in n years</n></pre>		
Key is valid for? (0) ly		
Key expires at Thu 02 Apr 2020 10:53:47 AM UTC		
Is this correct? (y/N) y		
Really create? (y/N) y		
we need to generate a lot of random bytes. It is a good idea to perform		
some other action (type on the keydoard, move the mouse, utilize the		
dependent a better chance to gain enough entropy		
generator a better chance to gain enough entropy.		
sec_rsa3072/F888EC71		
created: 2019-04-02 expires: 2021-04-01 usage: C		
trust: ultimate validity: ultimate		
ssb rsa3072/0B8DD705		
created: 2019-04-03 expires: 2020-04-02 usage: SE		
[ultimate] (1). SUNET CERT <cert@cert.sunet.se></cert@cert.sunet.se>		
<pre>[ultimate] (2) SUNET CERT abuse <abuse@cert.sunet.se></abuse@cert.sunet.se></pre>		
[ultimate] (3) SUNET abuse <abuse@sunet.se></abuse@sunet.se>		

Terminal - root@kali: /mnt/usb	* = • ×
File Edit View Terminal Tabs Help	
<n> = key expires in n days</n>	<u>^</u>
<n>w = key expires in n weeks</n>	
<n>m = key expires in n months</n>	
<n>y = key expires in n years</n>	
Key is valid for? (0) ly	
Key expires at Thu 02 Apr 2020 10:53:47 AM UTC	
Is this correct? (y/N) y	
Really create? (y/N) y	
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.	
sec rsa30/2/+888EU/1	
created: 2019-04-02 expires: 2021-04-01 usage: C	
trust: utilimate validity: utilimate	
SSD [Sd30/2/00000/03 croated, 2010 04 02 expires, 2020 04 02 usage, SE	
Createu: 2019-04-03 expires: 2020-04-02 usage: Se	
[ultimate] (1). SUNET CERT ACCOLUCET.SUNET.Sev	
[ultimate] (2) SUNET CLAT abuse sabuse(cert.sunet.se)	
[uttimate] (3) SONET abuse Cabuse@sunet.se>	
apas quit	
Save changes? (v/N) v	
our containg control ()/ (i)	

Avlsuta och spara nyckeln.

För att vi och andra skall kunna använda nycklarna måste den publika delen exporteras och publiceras. Både master och subnycklar exporteras. Kommando: gpg –armor –export <KEYID> > /mnt/usb/<KEYID>-pub.asc --armor : Konvertera binär nyckel till portabelt ASCII format

--export : Exportera publik nyckel

För att vi skall kunna arbeta med signering och kryptering måste vi ha tillgång till de privata subnycklarna, men inte den privata masternyckeln. Här exporterar vi endast subnycklarna.

Kommando: gpg –armor –export-secret-subkeys <KEYID> > /mnt/usb/<KEYID>-subsec.asc

-- armor : Konvertera binär nyckel till portabelt ASCII format

-- export-secret-subkeys : Exportera bara de hemliga subnycklarna.

För att enkelt kunna använda USB-stickan och generera nya nycklar i framtiden skapar vi ett litet skript som kan köras för att välja rätt nyckelring. För att använda denna nästa gång räcker det att skriva ". /mnt/usb/gpgsetup.sh"

Dags för en demonstration av hur man kan arbeta med endast subnycklar. Sätt upp en ny GNUPG-katalog

Kommando: export GNUPGHOME=\$(mktemp -d /tmp/GNUPG.XXX)

Kommando: gpg –list-keys

Importera den publika nyckeln

Kommando: gpg --import <path-to-public-key>

Terminal - root@kali: /mnt/usb File Edit View Terminal Tabs Help root@kali:/mnt/usb# gpgimport /mnt/usb/F888EC71-sub-sec.asc gpg: key 28730692F888EC71: "SUNET CERT <cert@cert.sunet.se>" not changed gpg: To migrate 'secring.gpg', with each smartcard, run: gpgcard-status gpg: key 28730692F888EC71: secret key imported gpg: Total number processed: 1 gpg: unchanged: 1 gpg: secret keys read: 1 gpg: secret keys imported: 1</cert@cert.sunet.se>
File Edit View Terminal Tabs Help root@kali:/mnt/usb# gpgimport /mnt/usb/F888EC71-sub-sec.asc gpg: key 28730692F888EC71: "SUNET CERT <cert@cert.sunet.se>" not changed gpg: To migrate 'secring.gpg', with each smartcard, run: gpgcard-status gpg: key 28730692F888EC71: secret key imported gpg: Total number processed: 1 gpg: unchanged: 1 gpg: secret keys read: 1 gpg: secret keys imported: 1</cert@cert.sunet.se>
<pre>root@kali:/mnt/usb# gpgimport /mnt/usb/F888EC71-sub-sec.asc gpg: key 28730692F888EC71: "SUNET CERT <cert@cert.sunet.se>" not changed gpg: To migrate 'secring.gpg', with each smartcard, run: gpgcard-status gpg: key 28730692F888EC71: secret key imported gpg: Total number processed: 1 gpg: unchanged: 1 gpg: secret keys read: 1 gpg: secret keys imported: 1</cert@cert.sunet.se></pre>
root@kali:/mnt/usb#

Importera de privata subnycklarna

Kommando: gpg -import <path-to-secret-subkeys>

Terminal - root@kali: /mnt/usb	÷	• ×
File Edit View Terminal Tabs Help		
<pre>root@kali:/mnt/usb# gpglist-keys /tmp/GNUPG.x05/pubring.kbx</pre>		Â
<pre>pub rsa3072 2019-04-02 [C] [expires: 2021-04-01]</pre>		
root@kali:/mnt/usb#		
		~

Här ser vi att de importerade nycklarna. [unknown] betyder att vi inte sagt att vi litar på dessa.

Terminal - root@kali: /mnt/usb	+ _ = ×
File Edit View Terminal Tabs Help	
<pre>root@kali:/mnt/usb# gpgedit-key F888EC71 gpg (GnuPG) 2.2.12; Copyright (C) 2018 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.</pre>	A
Secret subkeys are available.	
<pre>pub rsa3072/28730692F888EC71 created: 2019-04-02 expires: 2021-04-01 usage: C trust: unknown validity: unknown ssb rsa3072/BE9224410B8DD705</pre>	

Först måste vi se till att vi litar på nycklarna.

Kommando: gpg –edit-key <KEYID>

Sätt ultimate trust . Ultimate används normalt bara för dina egna nycklar så i praktiken kanske det skall vara "I trust fully" då det kan vara någon av dina kollegor som signerat.

gpg kommando: trust

Val 1: 5

Val 2: y

Avsluta. Notera att du inte behöver spara. Anledningen är att trust sparas i en separat fil och inte påverkar själva nyckeln.

Terminal - root@kali: /mnt/usb	+ _ = ×
File Edit View Terminal Tabs Help	
<pre>root@kali:/mnt/usb# gpglist-keyskeyid-format short appa. checking the tructdb</pre>	^
<pre>gpg: cnecking the trustab 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 2021-04-01 /tmp/GNUPG.x05/pubring.kbx</pre>	
<pre>pub rsa3072/F888EC71 2019-04-02 [C] [expires: 2021-04-01] 7DACDDE265DDC793D65442FD28730692F888EC71 uid [ultimate] SUNET CERT <cert@cert.sunet.se> uid [ultimate] SUNET CERT abuse <abuse@cert.sunet.se> uid [ultimate] SUNET abuse <abuse@sunet.se> sub rsa3072/0B8DD705 2019-04-03 [SE] [expires: 2020-04-02]</abuse@sunet.se></abuse@cert.sunet.se></cert@cert.sunet.se></pre>	
root@kali:/mnt/usb#	

Nu ser vi att vi har [ultimate] trust på identiteterna.

Dags att kryptera ett hemligt meddelande och spara det i filen hemligt.pgp

Ni får byta cert@cert.sunet.se mot en av de identiteter ni valt för er teamnyckel. Kommando: gpg –s –e –r cert@cert.sunet.se

- -s : Signera meddelandet
- -e : Kryptera meddelandet
- -r abuse@cert.sunet.se : Kryptera för denna mottagare

Här ser vi att det är en PGP RSA krypterad fil

Terminal - root@kali: /mnt/usb	• - 0	×
File Edit View Terminal Tabs Help		
<pre>File Edit View Terminal Tabs Help root@kali:/mnt/usb# gpg -d hemligt.pgp gpg: encrypted with 3072-bit RSA key, ID BE9224410B8DD705, created 2019 "SUNET CERT <cert@cert.sunet.se>" Hemligt meddelande gpg: Signature made Wed 03 Apr 2019 01:09:37 PM UTC gpg: using RSA key 9359E8167D8FC7F8D3214269BE9224410B8DD gpg: Good signature from "SUNET CERT <cert@cert.sunet.se>" [ultimate] gpg: aka "SUNET CERT abuse <abuse@cert.sunet.se>" [ultimate] root@kali:/mnt/usb#</abuse@cert.sunet.se></cert@cert.sunet.se></cert@cert.sunet.se></pre>	-04-03 705 mate]	
		~

Här ser vi att vi kan avkryptera filen med nyckeln för <abuse@sunet.se> och att den är signerad av <abuse@sunet.se>

Kommando: gpg –d hemligt.php

-d : Dekryptera