

El manual del KGpg

Jean-Baptiste Mardelle

Rolf Eike Beer

Traductor: Albert Astals Cid

Traductor: Antoni Bella



El manual del KGpg

Índex

1	Introducció	5
2	Com començar	6
3	Com usar KGpg	8
3.1	Com generar una clau	8
3.2	Com revocar una clau	9
3.3	Com encriptar les vostres dades	10
3.3.1	Com encriptar un fitxer des del Konqueror o Dolphin	10
3.3.2	Com encriptar un text amb la miniaplicació de KGpg	10
3.3.3	Com encriptar text des de l'editor de KGpg	10
3.4	Com desencriptar les vostres dades	11
3.4.1	Com desencriptar un fitxer des del Konqueror o el Dolphin	11
3.4.2	Com desencriptar text amb la miniaplicació de KGpg	11
3.4.3	Com desencriptar un text des de l'editor	11
3.5	Gestió de claus	11
3.5.1	Gestor de claus	12
3.5.2	Propietats de la clau	13
3.5.3	Firmar les claus	13
3.6	Treballar amb els servidors de claus	16
3.6.1	Comunicació amb els servidors de claus	16
3.6.2	Resultat de la cerca en el servidor de claus	17
3.7	Com configurar KGpg	17
3.7.1	Encriptatge	18
3.7.2	Desencriptatge	19
3.7.3	Aparença	19
3.7.4	Opcions de GnuPG	19
3.7.5	Servidors de claus	19
3.7.6	Miscel·lània	19
4	Crèdits i llicència	20

Resum

El KGpg és una interfície gràfica simple per GnuPG (<https://gnupg.org>).

Capítol 1

Introducció

KGpg és una interfície simple de GnuPG, una potent utilitat d'enciptatge. GnuPG (també conegut com a «gpg») està inclòs a la majoria de distribucions i hauria d'estar instal·lat al vostre sistema. Podeu obtenir l'última versió a <https://gnupg.org>.

Amb KGpg podreu encriptar i desencriptar els vostres fitxers i correus electrònics, permetent una comunicació molt més segura. Un mini «com es fa» sobre encriptació amb gpg està disponible al [lloc web de GnuPG](#).

Amb KGpg, no necessiteu recordar les opcions i ordres de gpg. Es pot fer gairebé tot amb uns quants clics de ratolí.

Capítol 2

Com començar

Aquesta és una llista dels components principals de KGpg:

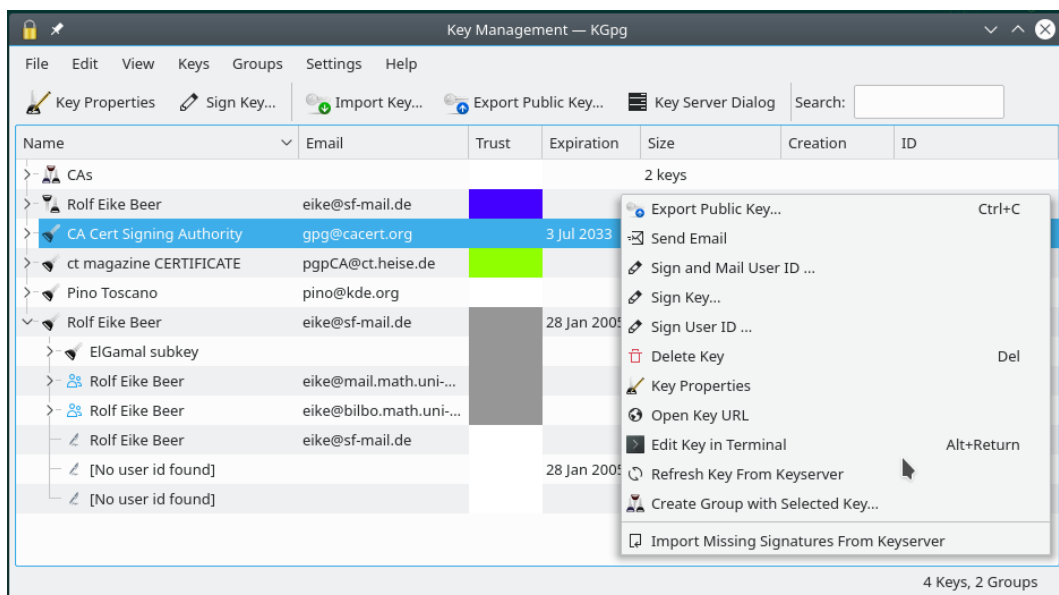
Icona de la safata del sistema



Quan iniciu KGpg, apareixerà una icona a la safata del sistema. Un clic amb el botó esquerre del ratolí obrirà la finestra del gestor de claus, mentre que un clic amb el botó dret del ratolí obrirà un menú que us permetrà un ràpid accés a algunes característiques importants. Si preferiu altres opcions podeu canviar l'acció del botó esquerre del ratolí a mostrar l'editor o inhabilitar completament la icona de la safata del sistema usant el [diàleg de configuració](#).

Si us plau, tingueu en compte que la icona de KGpg a la safata del sistema està marcada com «inactiva» gairebé tot el temps. Com la miniaplicació de safata del sistema sol ocultar les icones inactives, la de KGpg no es mostrarà fins que ho requeriu explícitament. Per a més detalls, consulteu la documentació de Plasma.

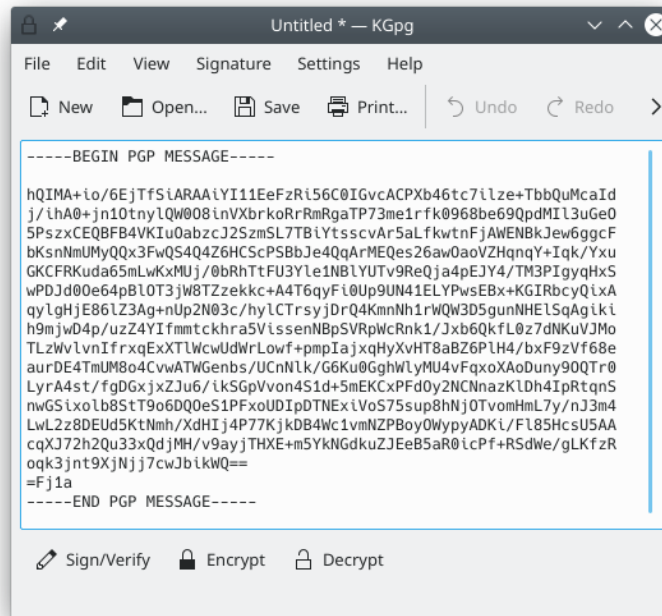
Finestra de gestió de claus



El manual del KGpg

Aquest és el lloc central per a gestionar les vostres claus. Per a obrir la [finestra del gestor de claus](#), feu clic amb el botó esquerre del ratolí sobre la miniaplicació de KGpg. Podeu importar, exportar, signar i editar les vostres claus. Gran part de les accions es poden realitzar amb un clic del botó esquerre del ratolí sobre una clau.

Finestra de l'editor



És un editor de text simple, on podeu escriure o enganxar text per a encriptar/desencriptar. Per a obrir l'[editor](#), feu clic amb el botó dret del ratolí sobre la miniaplicació de KGpg.

Integració amb el gestor de fitxers

El KGpg està integrat en el Konqueror i el Dolphin. Això vol dir que quan feu clic dret a sobre d'un fitxer, podreu escollir **Accions** → **Encripta un fitxer** per a encriptar-lo. El podreu desencriptar amb un clic del botó esquerre del ratolí.

Capítol 3

Com usar KGpg

Hi ha dues formes d'encriptar les vostres dades:

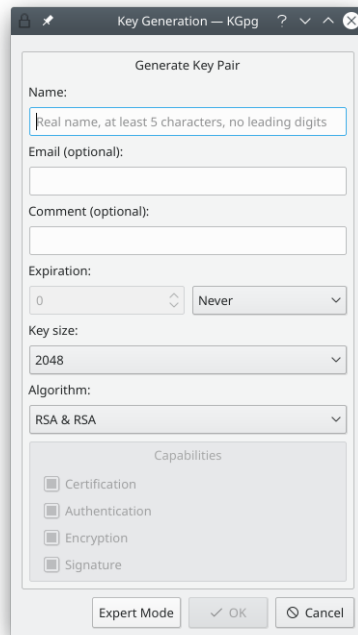
- Encriptatge simètric: Les vostres dades s'encripten amb una contrasenya. Qualsevol que disposi d'un ordinador amb gpg podrà descriptar el vostre missatge si li doneu la contrasenya. Per a realitzar un encriptatge simètric, escolliu l'opció «Encriptatge simètric» al quadre d'opcions quan se us demani per una clau d'encriptatge.
- Encriptar amb clau: Primer haureu de crear el vostre parell de claus (la clau secreta i la clau pública) i proporcionar una frase de pas. Deseu la vostra clau secreta en un lloc segur, i intercanvieu la vostra clau pública amb els vostres amics. Després, si desitgeu enviar un missatge encriptat a l'Àlex, haureu d'encriptar el missatge amb la clau pública de l'Àlex. Per a descriptar el missatge, el destinatari necessitarà la clau secreta de l'Àlex i la seva frase de pas.

L'encriptació amb clau és una mica més complicat (haureu d'intercanviar claus amb els vostres amics), però més segur. Recordeu que si encipteu un missatge amb la clau d'una altra persona, no el podreu descriptar. Tan sols podreu descriptar els missatges que hagin estat enciptats amb la vostra clau pública.

3.1 Com generar una clau

Si no teniu cap clau, la primera vegada que l'inicieu, KGpg mostrarà automàticament una finestra emergent amb el diàleg per a la generació de claus. També podeu accedir-hi mitjançant el Gestor de claus de **Claus** → **Genera parell de claus**.

El manual del KGpg



Simplement introduïu el vostre nom, adreça de correu electrònic i feu clic a **D'acord**. Això generarà una clau gpg estàndard. Si desitgeu més opcions, podeu fer clic en el botó de **Mode expert**, el qual us oferirà una Konsole amb totes les opcions de gpg.

Moltes persones juguen amb la seva primera clau, generen identificadors d'usuari incorrectes, afegeixen comentaris dels quals després se'n penedeixen o simplement obliden la seva frase de pas. Per a evitar que aquestes claus tinguin validesa il·limitada sol ser una bona idea limitar la seva vida a uns 12 mesos. Podeu modificar la vida de la vostra clau secreta més endavant utilitzant la [finestra de propietats de la clau](#).

3.2 Com revocar una clau

Un parell de claus que ha expirat es pot tornar a un estat funcional, sempre que tingueu accés a la clau privada i a la frase de pas. Per a tornar llegible una clau inusable necessitareu revocar-la. La revocació es porta a terme mitjançant l'afegit d'una signatura de revocació especial a la clau.

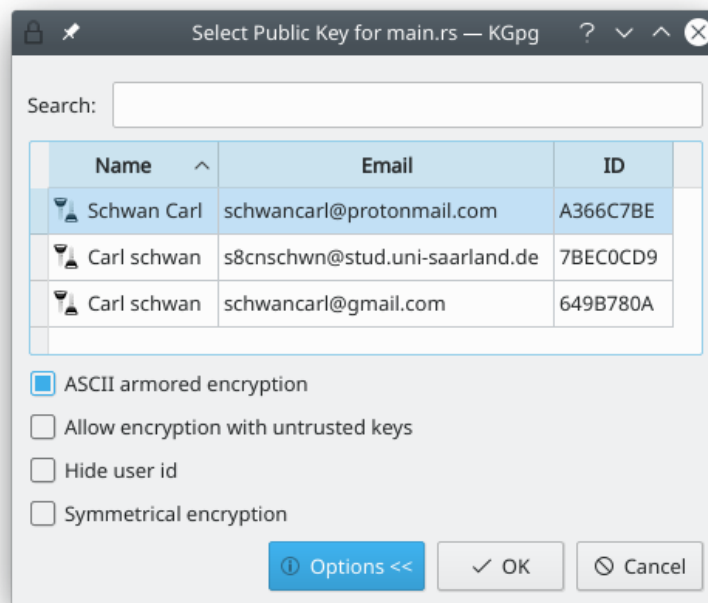
Aquesta signatura de revocació es pot crear juntament amb la clau. En aquest cas, s'emmagatzema en un fitxer a part. Aquest fitxer podrà ser importar més endavant al clauer i després afegit a la clau inusable. Si us plau, tingueu en compte que per a la importació d'aquesta signatura a la clau no és necessària la contrasenya. Per tant, hauríem d'emmagatzemar aquesta signatura de revocació en un lloc segur, en general diferent del parell de claus. És un bon consell utilitzar un lloc separat del vostre ordinador, o bé copiar-la a un dispositiu d'emmagatzematge extern com una memòria USB o imprimir-la.

Si no heu creat una revocació separada en la creació de la clau podeu crear una signatura de revocació en qualsevol moment escollint **Clau** → **Revoca la clau**, opcionalment important-la al vostre clauer immediatament.

3.3 Com encriptar les vostres dades

3.3.1 Com encriptar un fitxer des del Konqueror o Dolphin

Feu clic amb el botó dret del ratolí sobre el fitxer que voleu encriptar. Escolliu **Accions** → **Encripta el fitxer** en el menú emergent. Se us mostrarà el diàleg de selecció de la clau pública. Escolliu la clau del destinatari i feu clic a **Encripta**. El fitxer encriptat es desarà amb una extensió `.asc` o `.pgp`, depenent de si havíeu escollit **Encriptatge en armadura ASCII** o no. Els fitxers encriptats en ASCII només utilitzen caràcters llegibles per a representar les dades resultants en fitxers que són més robustos quan es copia tot o s'envien per correu, però són un terç més grans.



3.3.2 Com encriptar un text amb la miniaplicació de KGpg

Podeu encriptar el contingut del porta-retalls seleccionant l'element **Encripta el porta-retalls** en el menú de la miniaplicació. En canvi, si escolliu **Signa el porta-retalls** llavors se signarà el text contingut en el mateix. Ambdues accions importaran el contingut actual del porta-retalls a una [finestra de l'editor](#), realitzant l'acció requerida i enganxant el contingut altra vegada a l'editor.

3.3.3 Com encriptar text des de l'editor de KGpg

És tan simple com fer clic a sobre del botó **Encripta**. Llavors se us mostrarà el diàleg per a la selecció de la clau pública. Escolliu la vostra clau i feu clic a **D'acord**. El missatge encriptat apareixerà a la finestra de l'editor.

Normalment, només podreu encriptar fitxers amb les claus en què confieu. Atès que a vegades sols voldreu enviar una nota confidencial a certes persones, haureu de ser conscient de tenir una clau GPG per a la que pugueu establir l'opció **Permet l'encriptatge amb claus que no siguin de confiança**.

Per a assegurar-vos que podeu desencriptar qualsevol fitxer que heu encriptat, fins i tot si ho heu fet amb la clau d'un altre, podeu utilitzar les opcions **Encripta sempre amb** i **Encripta fitxers amb**, que estan disponibles en la [configuració de KGpg](#).

Per a més informació quant a les opcions d'enciptatge **Armadura ASCII**, **Permet l'enciptatge amb claus que no siguin de confiança** i **Enciptatge simètric**, si us plau, consulteu la documentació o [pàgines del manual](#) de gpg.

3.4 Com descriptar les vostres dades

3.4.1 Com descriptar un fitxer des del Konqueror o el Dolphin

Feu clic esquerre en el fitxer que voleu descriptar. Introduïu la vostra frase de pas i es descriptarà. També podeu arrossegar un fitxer de text enciptat a la finestra de l'editor de KGpg. Aquest us demanarà la frase de pas i obrirà el fitxer descriptat amb l'editor de KGpg. Fins i tot podeu arrossegar-hi fitxers remots! També podeu usar **Fitxer** → **Descripta el fitxer** i escollir un fitxer a descriptar.

3.4.2 Com descriptar text amb la miniaplicació de KGpg

També podeu descriptar el contingut del porta-retalls amb l'entrada **Descripta el porta-retalls** del menú de la miniaplicació del KGpg. Es mostrarà una [finestra de l'editor](#) amb el text descriptat.

3.4.3 Com descriptar un text des de l'editor

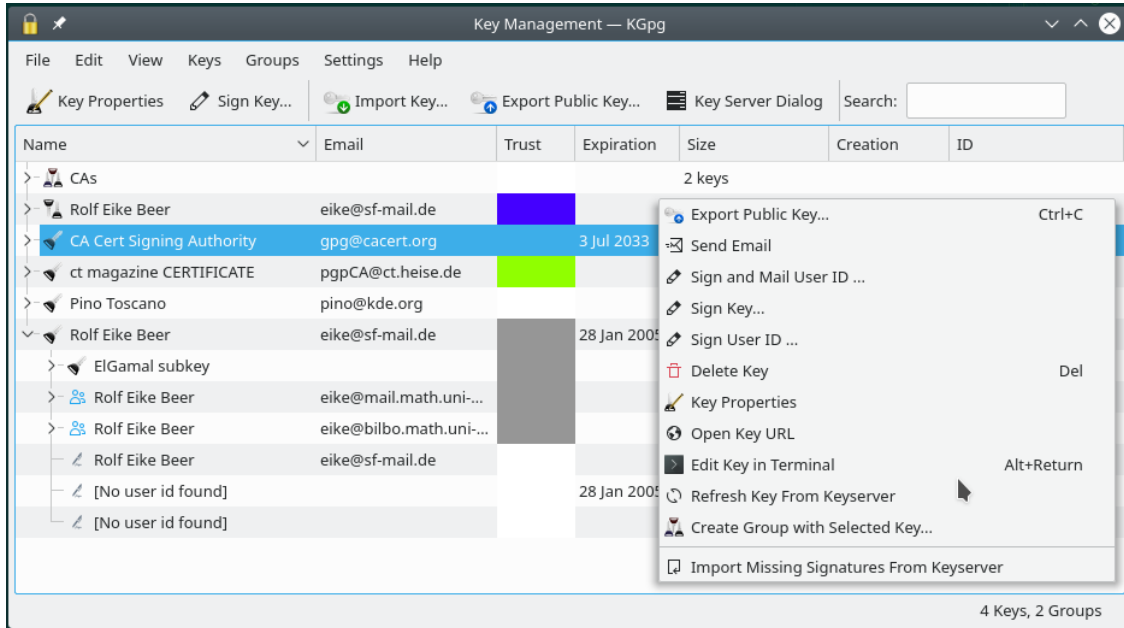
Copieu o arrossegueu i deixeu-hi anar el text que voleu descriptar, i feu clic a sobre del botó **Descripta**. Se us demanarà la frase de pas.

3.5 Gestió de claus

Totes les opcions bàsiques per a la gestió de claus poden realitzar-se a través de KGpg. Per a obrir la finestra de gestió de claus feu clic amb el botó esquerre del ratolí a la miniaplicació de KGpg. La majoria d'opcions estan disponibles amb un clic dret sobre una clau. Per a importar/exportar claus públiques, podeu utilitzar arrossegar i deixar anar o les dreceres del teclat de copiar/enganxar.

Podeu exportar una clau pública a través del correu electrònic, al porta-retalls, a un servidor de claus o a un fitxer local. Utilitzeu les opcions en el diàleg d'exportació per a exportar-ho tot, exportar sense atributs (identificacions amb foto) o exportar una clau neta, és a dir, la clau incloent les seves subclaus, però excloent totes les signatures.

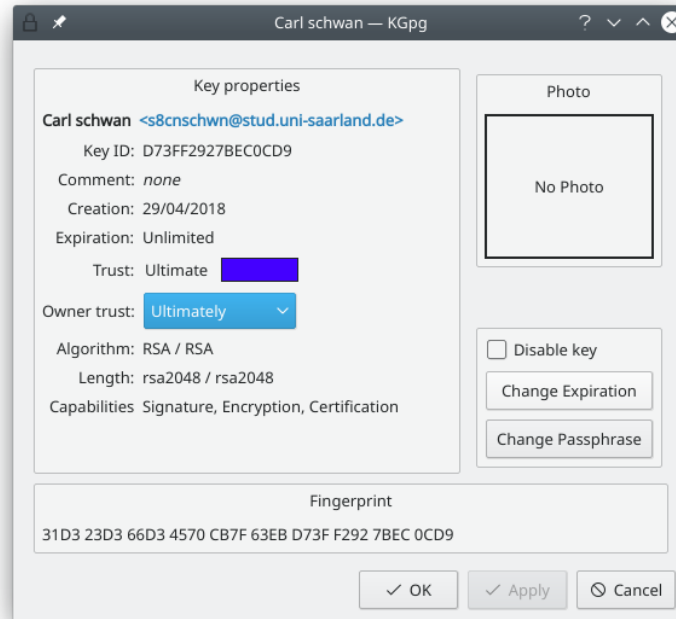
3.5.1 Gestor de claus



En aquest exemple podeu veure un grup de claus que conté dues claus, dos parells de claus i tres claus públiques. La tercera columna mostra la confiança que teniu en les claus. El primer parell de claus és de confiança total i també és la clau per omisió (lletra negreta), mentre que el segon ja ha expirat. Dues de les claus públiques són de confiança completa, mentre que l'última posseeix una confiança marginal. L'última clau està expandida, i mostra la seva subclau ElGamal, una identitat d'usuari addicional, ambdues de confiança marginal, i algunes de les seves signatures.

Les signatures permeten navegar pel vostre anell de claus. Si feu doble clic sobre una signatura o una clau mostrada com a membre d'un grup, anireu directament a la seva clau primària corresponent.

3.5.2 Propietats de la clau



Mentre que el gestor de claus us permet accions generals amb una o més claus, grups de claus o signatures, la finestra de propietats de la clau us proporciona accés a una única clau. La podeu obtenir prement la tecla **Retorn** en el gestor de claus o fent doble clic sobre la clau.

En aquesta finestra podeu canviar la frase de pas de la clau i la caducitat de les vostres claus secretes. També podeu establir el valor de confiança en el propietari, per a cadascuna de les claus.

Aquest valor indica quanta confiança diposeu en el propietari d'aquesta clau per a verificar correctament la identitat de les claus que signa. Tenint en compte la confiança en el propietari, gpg crea la vostra pròpia xarxa de confiança. Confieu en les claus que heu signat. Si assigneu confiança en aquestes persones, també confiareu en les claus que hagin signat sense la necessitat que també les signeu.

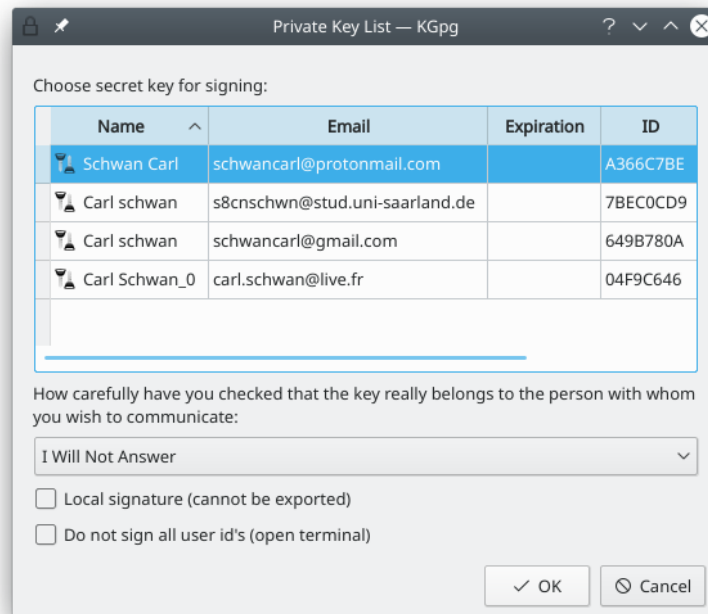
3.5.3 Firmar les claus

Quan signeu una clau d'una altra persona (a la que anomenarem Alícia) esteu anunciant que esteu segur que aquesta clau realment pertany a aquesta persona i que la clau és de confiança. Per descomptat, hauríeu de comprovar-ho. Això sol significar que us heu trobat amb Alícia, que almenys heu comprovat el seu carnet d'identitat i heu obtingut d'ella l'empremta digital completa de la seva clau o una còpia d'aquesta. A continuació heu tornat a casa i heu signat la clau de l'Alícia. Normalment, pujareu més tard la clau recentment signada a un [servidor de claus](#) perquè tothom sàpiga que heu comprovat que la clau i el seu propietari són de confiança. Alícia probablement farà el mateix, de manera que ambdós tindreu les vostres claus signades per l'altra persona. Si un de vosaltres no té el carnet d'identitat a mà, tampoc hi haurà cap problema si la signatura es fa en una única direcció.

Però penseu en el que succeeix si Alícia viu a l'altre extrem del món. Us hi comuniquem amb regularitat, però no hi ha cap possibilitat que us veieu en un futur immediat. Com confiar en la seva clau?

Quan selecciona la seva clau i després seleccioneu **Signa la clau...** obtindreu el diàleg que us permetrà triar les opcions amb que us agradaria signar aquesta clau.

El manual del KGpg



En primer lloc, podeu triar la clau que utilitzareu per a signar la clau. Llavors podeu introduir el grau de confiança amb el que heu comprovat que realment és la persona que diu ser. Aquesta informació serà emmagatzemada juntament amb la signatura, per la qual cosa és una guia per a tots els altres que puguin necessitar la signatura (tornarem a això més endavant). I després ve l'opció que us ajuda si no us podeu trobar amb Àlicia en persona: **Signatura local (no es pot exportar)**. Quan activeu aquesta opció es crearà una versió especial de la signatura que mai sortirà del vostre anell de claus, ni tan sols per accident.

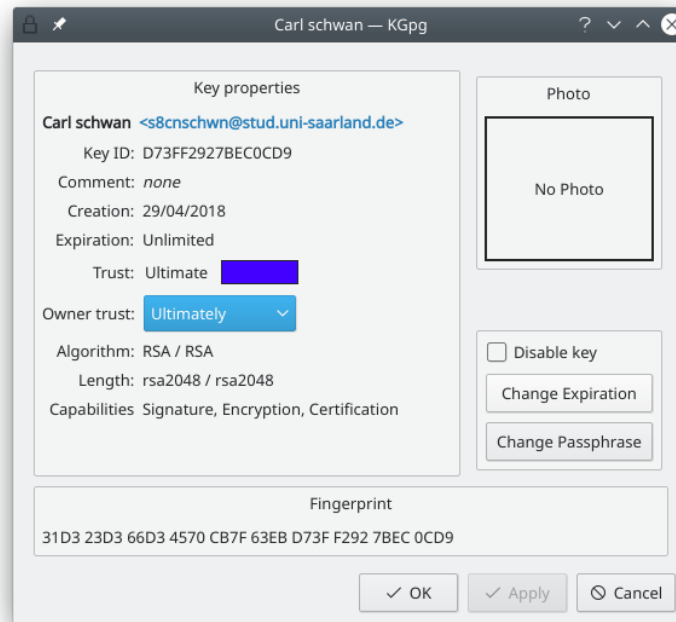
Però. Per què és important la cura amb què s'ha comprovat la identitat d'Àlicia? Qui ha de tenir cura? Hi ha una manera diferent de resoldre el vostre problema amb la identitat d'Àlicia. Si no podeu visitar-la a curt termini penseu en Trent. Sabeu que Trent també té un parell de claus. I és un rodamon, en un continent diferent almenys dues vegades al mes. Si teniu sort potser cau a prop d'Àlicia aviat. D'aquesta manera us podeu reunir amb en Trent per a signar les vostres respectives claus. A continuació, enviareu una nota a Àlicia dient que Trent viatjarà aviat a la seva ciutat i li demanareu si es pot reunir amb ell per a signar les claus. Quan tot això hagi passat, ja sabíeu que la clau d'en Trent és de confiança i Trent sap que la clau d'Àlicia és de confiança. Si confieu en Trent que ha verificat acuradament la identitat d'Àlicia, aleshores també podeu confiar en la seva clau.

Aquestes relacions entre les claus i els seus propietaris formen el que s'anomena una xarxa de confiança. Dins d'aquesta xarxa hi ha alguns valors importants que defineixen el fiable que és una clau en particular. El primer és la cura amb què s'ha comprovat la identitat del propietari de la clau. Aquest és el valor que hem vist a la finestra de selecció de la clau secreta. Per exemple, probablement sabeu com verificar el vostre carnet d'identitat local, però en un país completament diferent pot ser difícil de comprovar. Per tant, es podria dir que heu revisat acuradament la identitat de Trent, perquè heu vist el seu carnet d'identitat i s'assembla molt al vostre. No obstant això, Trent, tot i que ha vist tant el document d'identitat i la llicència de conduir de l'Àlicia podria dir que només ha fet una lleugera identificació, ja que no està absolutament segur quant als documents en aquesta part del món.

El valor d'importància és la quantitat de confiança en l'altra persona per a verificar documents. Sabeu que en Trent és bo en això. Però George, per exemple, no és algú al que qualificaríeu d'intel·ligent. Ja que gairebé no va mirar el vostre carnet d'identitat quan us vàreu reunir amb ell per a signar una clau. Esteu segur que en George és la persona que pretén ser perquè vàreu comprovar acuradament els seus documents. Però, segons sembla, ell no és igual de minuciós en el control d'altres persones pel que tindreu un alt nivell de confiança en la clau d'en George,

El manual del KGpg

però una confiança molt baixa en la seva signatura. Si obriu les **proprietats** d'una clau trobareu el camp **Confiança en el propietari**. Aquesta serà la confiança que teniu en el propietari de la clau quan ell signa claus. Aquest valor no s'exportarà, és totalment una preferència personal vostra.



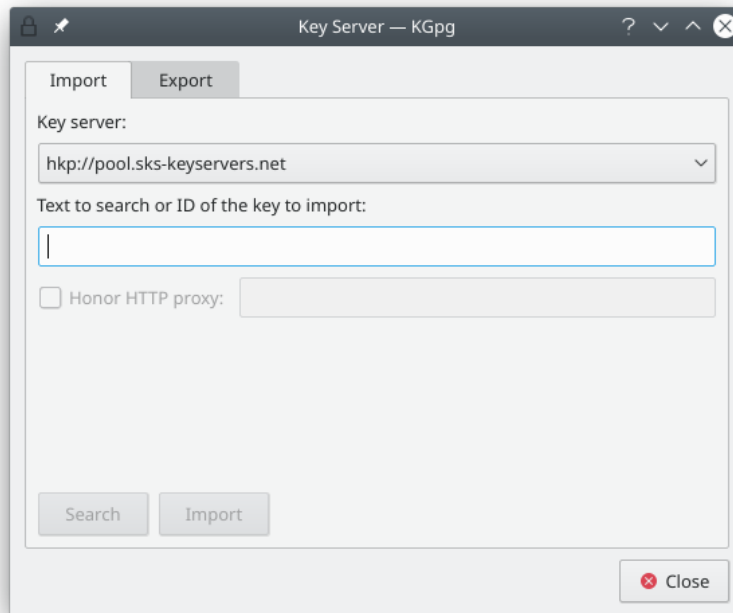
Ara hauríeu de tenir una idea de com es construeix la xarxa de confiança, per a què serveixen els valors de confiança en el propietari i la clau, i per què cal tenir sempre molta cura en verificar les identitats: Altres persones podran donar-vos la seva confiança. Però encara hi ha un element en el procés que està sense verificar: Les adreces de correu electrònic de les claus que signeu. Creant una nova identitat d'usuari en la vostra clau amb l'adreça de correu electrònic d'Àlicia o Trent només us caldran alguns clics del ratolí. Heu comprovat que Trent és el veritable propietari de la seva clau. Però ningú ha comprovat fins ara que Trent realment controla les adreces de correu electrònic de les seves identitats d'usuari.

Si escolliu **Signa i envia l'ID de l'usuari...** des del menú haureu tancat aquest forat. La idea és que signeu la clau com de costum i després es dividirà en trossos. Cada peça només contindrà una identitat d'usuari de la clau d'en Trent i la vostra signatura. Aquesta serà encriptada amb la clau d'en Trent i enviada només a l'adreça de correu electrònic proporcionada en aquesta identitat. En Trent només podrà importar la signatura al seu anell de claus si rep aquest correu i el descripta. No pugeu les vostres signatures, ja que li pertoca a ell. Si la vostra signatura es mostra en un servidor de claus, podeu estar segur que en Trent realment controla tant la seva clau com l'adreça de correu electrònic que vàreu signar. Les signatures que realitzeu en aquest procés no formaran part del vostre anell de claus. De manera que després de signar les claus d'en Trent encara es mostraran com a no de confiança en el vostre anell de claus. Una vegada en Trent rebí el correu i hagi importat la vostra signatura al seu anell de claus podreu pujar-les a un servidor de claus. En actualitzar la seva clau des del servidor obtindreu les noves signatures. Encara que aquest principi pot semblar un inconvenient, no garanteix que li donareu confiança a la seva identitat, la que ell controla. Només les signatures que apareixen en un servidor de claus són les que tothom, inclòs vostè, podeu estar segur que realment controla l'adreça de correu electrònic corresponent.

3.6 Treballar amb els servidors de claus

3.6.1 Comunicació amb els servidors de claus

La part pública d'un parell de claus normalment s'emmagatzema en un servidor de claus. Aquests servidors permeten que qualsevol persona cerqui una clau pertanyent a una determinada persona o adreça de correu electrònic. Les signatures també estan emmagatzemades en aquests servidors.

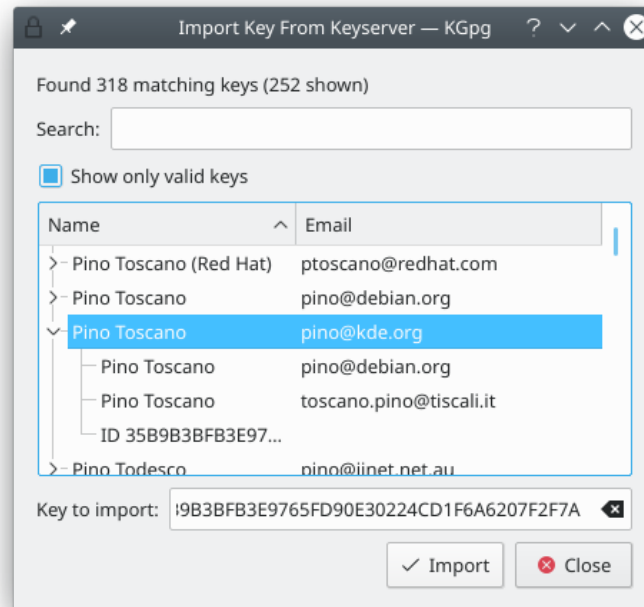


Aquest diàleg us proporciona accés als servidors de claus. Podeu cercar i importar claus des d'un servidor de claus, així com exportar a un servidor. Un exemple de cerca i importació és quan es vol escriure un correu a algú. Si el voleu encriptar, podeu cercar si aquest posseeix alguna clau pública en els servidors de claus. Si heu creat un parell nou de claus o heu signat la clau d'algú, és possible que vulgueu exportar la clau pública (possiblement amb noves signatures) a un servidor de claus.

La majoria dels servidors de claus sincronitzen les seves dades entre els altres de manera que s'obtinguin resultats similars sense importar quin servidor utilitzeu. Com que hi ha excepcions a aquesta regla podeu triar el servidor de claus a utilitzar en aquest diàleg. En general és una bona idea triar un servidor de claus per ommissió que es trobi a prop vostre (és a dir, al país o al continent), ja que generalment responen més ràpidament a les vostres consultes.

Si us plau, tingueu en compte que tot el que pugueu a un servidor de claus en general es queda allà per sempre. Aquesta és una bona raó per a limitar la vida de les vostres claus. Tingueu també en compte que els servidors a vegades són rastrejats pels generadors de correu brossa a la cerca d'adreces de correu electrònic.

3.6.2 Resultat de la cerca en el servidor de claus



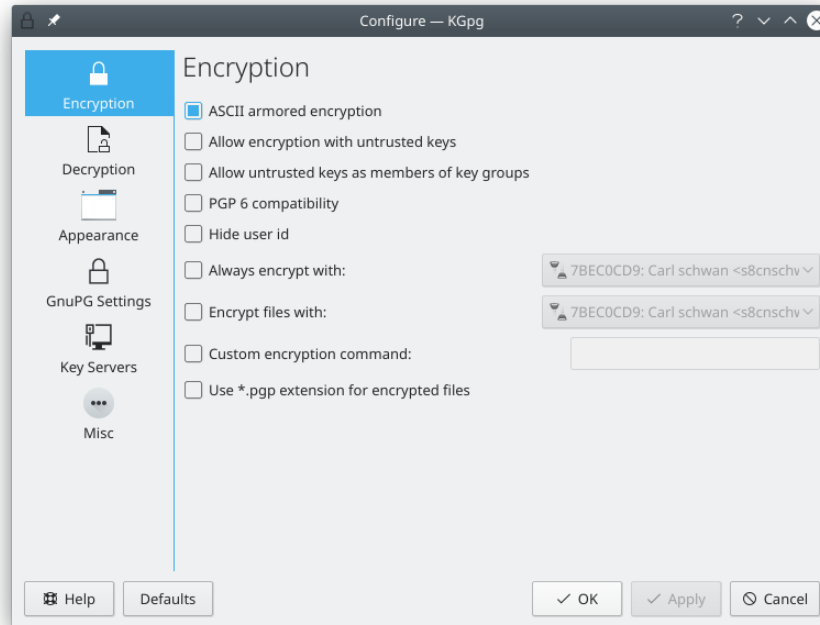
Tots els resultats d'una cerca es mostren en aquesta finestra. Aquesta imatge mostra una cerca per a les adreces «@ kde.org» i ens mostra 244 resultats. Utilitzant el camp de cerca, la llista s'ha reduït a una sola clau. Aquesta clau té dues coincidències: L'ID d'usuari primari coincideix amb la cadena de cerca, així com un dels altres identificadors d'usuari.

Podeu seleccionar una o més claus a importar. Els identificadors de les claus es mostren en el camp **Clau a importar** a la part inferior de la finestra. En fer clic a **Importa** es torna a contactar amb el servidor per a obtenir les seleccionades i incorporar-les al vostre anell de claus.

3.7 Com configurar KGpg

La configuració és accessible a través del menú de la miniaplicació de KGpg (feu clic amb el botó dret del ratolí a sobre de la miniaplicació) o a través del menú principal (**Arranjament** → **Configura KGpg**). Podreu establir-hi els paràmetres per omisió per a l'encrriptatge, desencriptatge, la interfície d'usuari i per a la miniaplicació. La majoria de les opcions d'encrriptatge estan directament relacionades amb gpg i estan documentades a les seves [pàgines del manual](#).

3.7.1 Encriptatge



Aquí podeu configurar opcions especials per a passar-les a GnuPG per a canviar el comportament de l'encriptatge. Per a una descripció detallada, doneu un cop d'ull al manual de GnuPG.

- **Encriptatge en armadura ASCII:** Això causa que els fitxers encriptats s'emmagatzemin en un format que fa servir caràcters ASCII imprimibles i amb línies curtes. Els fitxers emmagatzemats d'aquesta manera són més grans que els fitxers en format binari, però són més fàcils d'enviar, p. ex., per correu electrònic.
- **Permet l'encriptatge amb claus que no siguin de confiança:** Això us permet encriptar fitxers amb claus que no són de confiança.
- **Compatibilitat amb PGP 6:** Els fitxers encriptats són compatibles amb l'estàndard PGP6 antic. Això inhabilita certes característiques, de manera que només l'hauríeu d'utilitzar si és absolutament necessari.
- **Oculto l'identificador d'usuari:** Això elimina tot indicatiu del receptor en el fitxer encriptat. En cas que la transmissió sigui interceptada, ningú podrà obtenir informació sobre el destinatari a partir del fitxer. Si el receptor posseeix múltiples claus, necessitareu provar amb la que s'ha emprat.
- **Encripta sempre amb:** Totes les encriptacions seran encriptades addicionalment amb aquesta clau. Si ho establiu a una de les vostres claus privades, us assegurareu que podreu llegir totes les dades que encripteu pel preu d'obtenir missatges més llargs.
- **Encripta fitxers amb:** Es comporta com **Encripta sempre amb** per a l'encriptatge del fitxer.
- **Ordre a mida per a l'encriptatge:** Si necessiteu passar alguna opció poc usual a GnuPG, podeu especificar aquí la línia d'ordres. La majoria d'usuaris no ho necessitarà.
- **Usa l'extensió *.pgp per als fitxers encriptats:** Si marqueu aquesta opció, els fitxers encriptats s'anomenaran com el fitxer d'entrada amb l'extensió .pgp afegida, en cas contrari s'utilitzarà l'extensió .gpg.

3.7.2 Desencrptatge

Aquí podeu especificar una ordre de desencrptatge personalitzada. Aquesta opció rares vegades és necessària i només és d'utilitat per a usuaris avançats que coneixen les opcions de la línia d'ordres de GnuPG.

3.7.3 Aparença

Aquí podeu configurar la manera en què es mostra KGpg. Les opcions possibles són els colors que reflecteixen els diferents nivells de confiança de les claus en el [gestor de claus](#) i les opcions de la lletra per a l'[editor](#).

3.7.4 Opcions de GnuPG

Aquí podeu configurar quin binari gpg i quin **fitxer de configuració** i carpeta d'inici s'utilitzaran. Aquests valors són autodetectats durant el primer inici i ja haurien de funcionar.

La utilització de l'[Agent GnuPG](#) fa que el treball amb GnuPG sigui més còmode, ja que no cal introduir la contrasenya per a cada acció. Aquesta serà emmagatzemada en la memòria cau per un temps, de manera que es pugui realitzar qualsevol operació que la requereixi. Tingueu en compte que això pot permetre que altres persones facin servir les vostres claus privades si els doneu accés a la sessió.

3.7.5 Servidors de claus

Aquí podeu crear una llista de servidors de claus que se us mostraran quan obriu el [diàleg dels servidors de claus](#). Si executeu GnuPG des de la línia d'ordres, només s'usarà el servidor de claus que heu establert aquí com per omissió.

El protocol utilitzat per a la comunicació amb el servidor de claus està basat en HTTP, de manera que pren sentit en alguns entorns **Satisfer a l'intermediari HTTP quan estigui disponible**.

3.7.6 Miscel·lània

Aquesta secció permet l'establiment d'algunes característiques diferents que no encaixen en les altres seccions. Podeu configurar per exemple **Inicia KGpg automàticament en accedir al sistema**. L'opció **Usa la selecció del ratolí en comptes del porta-retalls** modifica si es pot seleccionar amb el ratolí i enganxar amb el botó del mig del ratolí o si totes les operacions es realitzaran mitjançant dreceres de teclat.

També podeu canviar si es mostrarà la icona de la safata del sistema de KGpg, i quina acció succeeix si feu clic sobre la icona amb el botó esquerre del ratolí. Si es mostra la icona de la safata del sistema es tancarà la finestra de KGpg minimitzant l'aplicació a la safata. Si no es mostra la icona de la safata del sistema KGpg sortirà de totes les finestres en tancar-se.

Capítol 4

Crèdits i llicència

KGpg

Copyright del programa (c) 2002-2003 Jean-Baptiste Mardelle bj@altern.org.

(c) 2006-2007 Jimmy Gilles jimmygilles@gmail.com

(c) 2006,2007,2008,2009,2010 Rolf Eike Beer kde@opensource.sf-tec.de

Traductors de la documentació: Albert Astals Cid aacid@kde.org i Antoni Bella antonibella5@yahoo.com

Aquesta documentació està llicenciada d'acord amb les clàusules de la [Llicència de Documentació Lliure de GNU](#).

Aquest programa està llicenciat d'acord amb les clàusules de la [Llicència Pública General de GNU](#).