Приручник за КГПГ

Жан Баптист Мардеј
Ролф Ајке Бер
превод: Драган Пантелић

Приручник за КГПГ

Садржај

Сажетак

КГПГ је просто графичко сучеље за ГнуПГ (http://gnupg.org).

Глава 1

Увод

КГПГ је једноставно сучеље за ГнуПГ, моћну алатку за шифровање. ГнуПГ (познат и као ГПГ) укључен је у већину дистрибуција и требало би да је инсталиран на вашем систему. Најновију верзију можете добавити са http://gnupg.org.

КГПГ-ом ћете моћи да шифрујете и дешифрујете фајлове и е-пошту, што омогућава много безбеднију комуникацију. Мали водич кроз шифровање ГПГ-ом доступан је на веб сајту ГнуПГ-а.

Уз КГПГ не морате да памтите ГПГ-ове опције командне линије. Скоро све се може урадити са неколико кликова мишем.

Глава 2

Први кораци

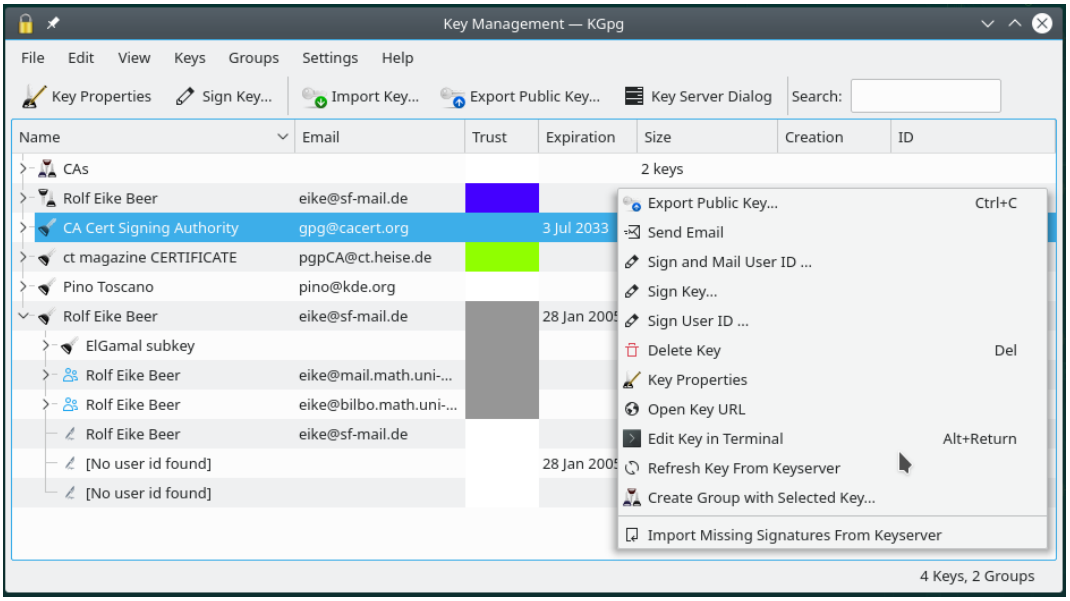
Следи списак главних компоненти КГПГ-а:

иконица системске касете

Кад покренете КГПГ, појавиће се иконица системске касете. Леви клик мишем на њу отвара менаџер кључева, а десни клик мени за брз приступ неким важним могућностима. Ако желите другачији одзив, можете задати да леви клик позива уређивач, или потпуно искључити иконицу системске касете, кроз дијалог за подешавање.

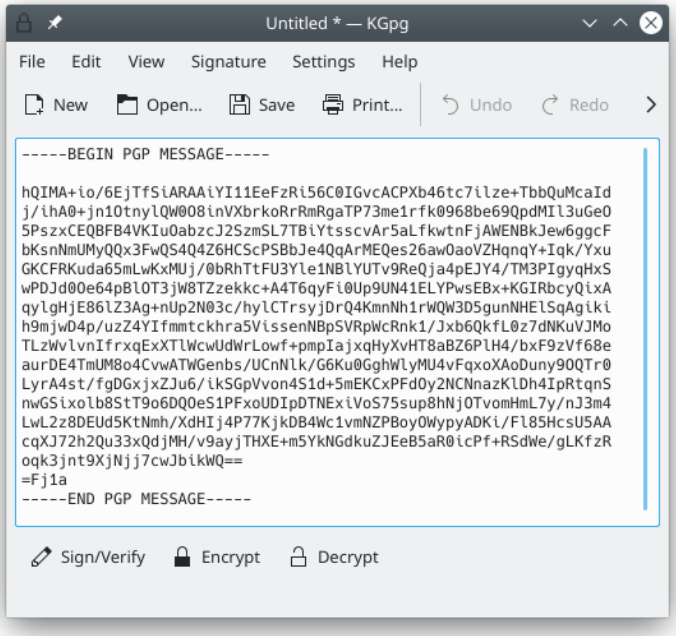
Приметите да је иконица КГПГ-а у системској касети у основи „неактивна“ све време. Пошто аплет системске касете обично сакрива неактивне иконице, иконица КГПГ-а неће бити приказана ако изричито то не затражите. За детаље погледајте документацију Плазме.

прозор менаџера кључева



Средишње место за управљање кључевима. Прозор менаџера кључева отварате левим кликом на КГПГ-ов аплет. Кључеве можете увозити, извозити, потписивати и уређивати. Већина радњи може се извршити десним кликом на кључ.

прозор уређивача



Једноставан уређивач текста у којем можете куцати или налепљивати текст ради шифровања и дешифровања. Уређивач отварате десним кликом на КГПГ-ов аплет.

уклапање у менаџер фајлова

КГПГ је уклопљен у К-освајач и Делфин. Ово значи да, пошто кликнете десним на фајл, можете да изаберете Радње → Шифруј фајл да га шифрујете. Фајл можете дешифровати левим кликом.

Глава 3

Коришћење КГПГ-а

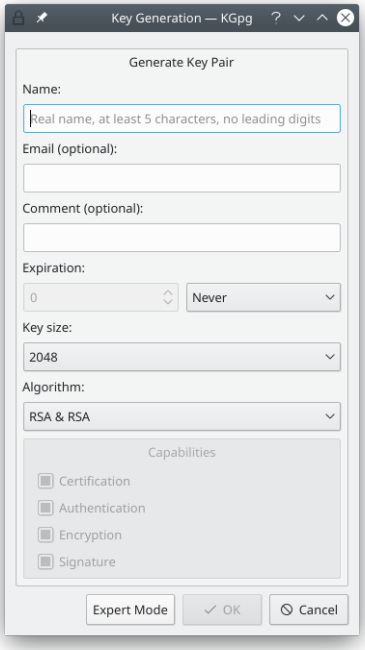
Подаци се могу шифровати на два начина:

- Симетрично шифровање. Подаци се шифрују само лозинком; свако ко има ГПГ на рачунару може дешифровати вашу поруку ако зна лозинку коју сте употребили. Симетрично шифровање захтевате опцијом Симетрично шифровање кад вам се затражи да изаберете шифрарски кључ.
- Шифровање кључем. Прво морате створити лични пар кључева (тајни и јавни кључ) заштићен лозинком. Тајни кључ задржите на скровитом месту, а јавне кључеве размените с пријатељима. Затим, ако желите да пошаљете шифровану поруку Алекси, шифрујете је Алексиним јавним кључем; за дешифровање поруке, примаоцу ће требати Алексин тајни кључ и лозинка.

Шифровање кључем је мало компликованије (морате размењивати кључеве с пријатељима), али је безбедније. Имајте у виду да ако шифрујете поруку туђим кључем, нећете моћи да је дешифрујете. Дешифровати можете само поруке које су биле шифроване и вашим јавним кључем.

3.1 Стварање кључа

Ако немате кључ, КГПГ ће по првом покретању аутоматски приказати дијалог за стварање кључева. Можете му приступити и кроз менаџер кључева, преко Кључеви → Генерисање пара кључева.



Само унесите своје име, адресу е-поште и кликните на У реду. Тиме ће бити створен стандардан ГПГ кључ. Ако желите више опција, можете кликнути на дугме Зналачки режим, што ће отворити прозор Конзоле са свим опцијама ГПГ-а.

Многи се играју са својим првим кључем: стварају лоше корисничке ИД-ове, додају коментаре због којих касније жале, или једноставно забораве лозинку. Да бисте избегли да такав кључ буде довека ваљан, обично је добра идеја да животни век ограничите на неких 12 месеци. Животни век својих тајних кључева можете накнадно изменити у прозору са својствима кључа.

3.2 Повлачење кључа

Пар кључева који је истекао може се вратити у радно стање све док имате приступ приватном кључу и лозинки. Да бисте кључ темељно учинили неупотребљивим, морате га повући. Ово се изводи додавањем кључу специјалног потписа за повлачење.

Потпис за повлачење може бити створен заједно са кључем. У том случају, складишти се у засебном фајлу. Тај фајл се касније може увести у свежањ кључева и тиме прикачити кључу, учинивши га неупотребљивим. Имајте на уму да за увоз овог потписа над кључем није потребна лозинка. Зато би потпис за повлачење требало да чувате на безбедном месту, обично неком различитом од онога где стоји пар кључева. Најбоље је да то буде негде изван вашег рачунара, тако што потпис копирате на спољашњи складишни уређај попут УСБ штапића, или га чак одштампате.

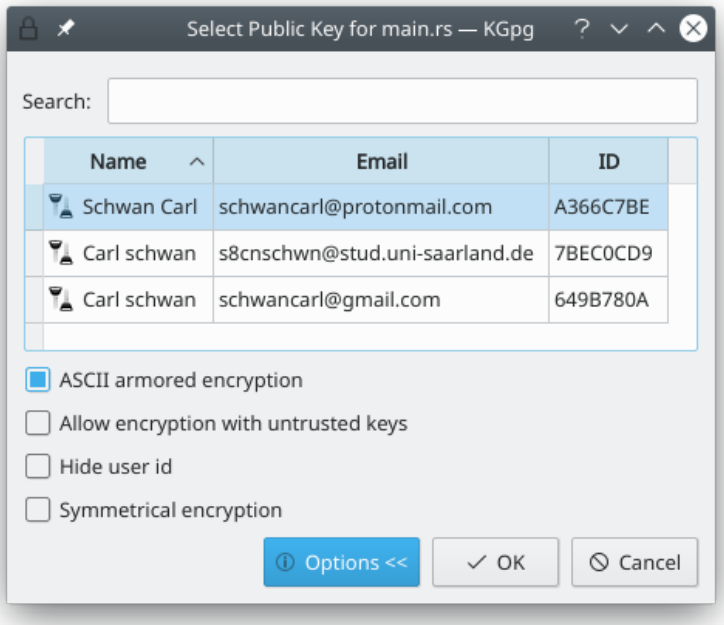
Ако потпис за повлачење нисте направили при стварању кључа, можете га направити у било ком каснијем тренутку преко Кључеви → Повуци кључ.... Тада га можете одмах и увести у свежањ кључева.

3.3 Шифровање података

3.3.1 Шифровање фајла из К-освајача или Делфина

Кликните десним на фајл који желите да шифрујете. У искачућем менију изаберите Радње → Шифруј фајл. Појавиће се дијалог који тражи избор јавног кључа. Изаберите кључ

примаоца и кликните на Шифрују. Шифровани фајл биће сачуван с наставком .asc или .g pg, у зависности од тога да ли сте или нисте изабрали Аски оклопљено шифровање. Аски шифровани фајлови представљају податке само читљивим аски знаковима, што чине такве фајлове робуснијим током копирања и слања е-поштом, али по цену да су за трећину већи.



3.3.2 Шифровање текста помоћу КГПГ-овог аплета

Садржај клипборда можете шифровати ставком Шифруј клипборд у менију аплета. Ако сте изабрали Потпиши/овери клипборд, текст ће уместо тога бити потписан. Обе радње ће увести текући садржај клипборда у прозор уређивача, извести захтевану радњу и налепити садржај назад у уређивач.

3.3.3 Шифровање текста из КГПГ-овог уређивача

Само кликните на дугме Шифруј. У дијалогу који се појави изаберите јавни кључ и кликните на У реду. У прозору уређивача појавиће се шифрована порука.

Обично можете шифровати фајлове само са кључевима који сте прогласили поузданим. Пошто понекад желите да пошаљете поверљиву поруку некој произвољној особи за коју знате да има ГПГ кључ, можете укључити опцију Дозволи шифровање непоузданим кључевима.

Да бисте обезбедили да можете дешифровати сваки фајл који сте шифровали, чак и када су шифровани нечијим туђим кључем, можете употребити опције Увек шифруј помоћу: и Шифруј фајлове помоћу: доступне у постави КГПГ-а..

За више информација о опцијама шифровања Аски оклопљено шифровање, Дозволи шифровање непоузданим кључевима и Симетрично шифровање, завирите у документацију или упутну страницу ГПГ-а.

3.4 Дешифровање података

3.4.1 Дешифровање фајла из К-освајача или Делфина

Кликните левим на фајл који желите да дешифрујете. Унесите своју лозинку и фајл ће бити дешифрован. Можете и превући шифровани фајл у КГПГ-ов прозор уређивача; тражиће

вам лозинку, и пошто је унесете, дешифровани текст ће бити отворен у уређивачу. Можете превлачити чак и удаљене фајлове! Фајл за дешифровање можете изабрати и кроз Фајл → Дешифруј фајл.

3.4.2 Дешифровање текста кроз КГПГ-ов аплет

Садржај клипборда можете дешифровати помоћу ставке менија Дешифруј клипборд у КГПГ-овом аплету. Појавиће се прозор уређивача са дешифрованим текстом.

3.4.3 Дешифровање текста из уређивача

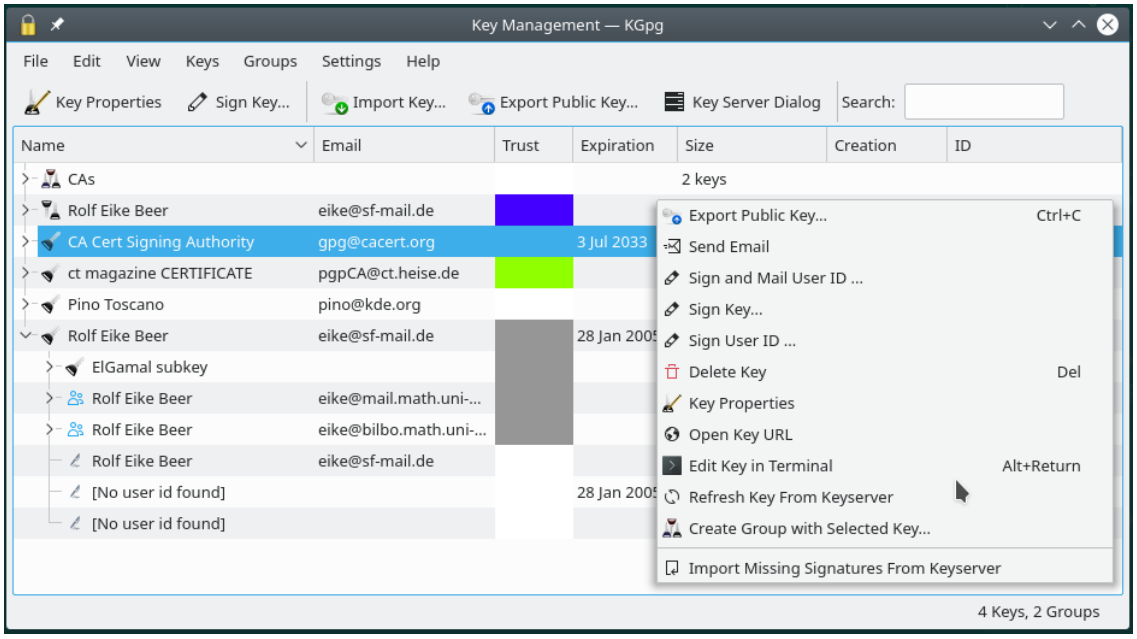
Копирајте или превуците текст који желите да дешифрујете и кликните на дугме Дешифруј. Биће вам затражена лозинка.

3.5 Управљање кључевима

Све основне радње управљања кључевима могу се извршити кроз КГПГ. Кликните левим на КГПГ-ов аплет да отворите прозор управљања кључевима. Већина радњи је доступна на десни клик на кључ. Јавне кључеве можете увозити и извозити превлачењем, или пречицама тастатуре за копирање и налепљивање.

Јавни кључ можете да извезете е-поштом, у клипборд, на сервер кључева или у локални фајл. Употребите опције извозног дијалога да извезете све, извезете без атрибута (фото ИД-ова) или да извезете чист кључ (сам кључ и његове поткључеве, али без свих потписа).

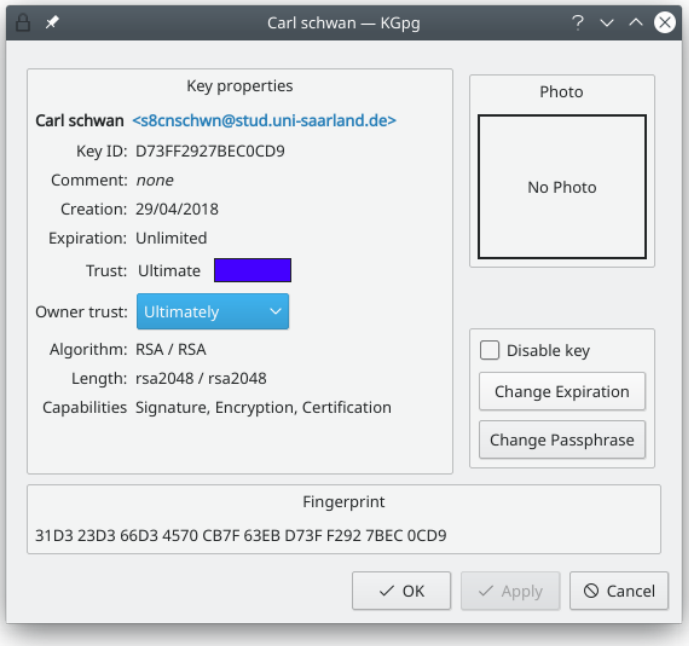
3.5.1 Менаџер кључева



У овом примеру видите групу кључева која садржи два кључа, два пара кључева и три јавна кључа. Трећа колона показује поузданост коју придајете кључевима. Први пар кључева је безусловно поуздан, а постављен је и као подразумевани кључ (подебљан фонт), док је други истекао. Од јавних кључева, два су потпуно поуздана, док је поузданост последњег кључа гранична. Последњи кључ је раширен, тако да се види Елгамалов поткључ, додатни кориснички ИД, оба такође са граничном поузданошћу, и неки од његових потписа.

Потписи омогућавају кретање кроз свежањ кључева. Двокликом на потпис, или на кључ приказан као члан групе, скачете на одговарајући примарни кључ.

3.5.2 Својства кључа



Док менаџер кључева омогућава извођење општих радњи над једним или више кључева, групама кључева и потписима, прозор својстава кључа даје приступ појединачном кључу. Можете га отворити притиском на Enter у менаџеру кључева или двокликом на кључ.

У овом прозору можете да мењате лозинке и истицања својих тајних кључева. За било који кључ можете да поставите поузданост власника.

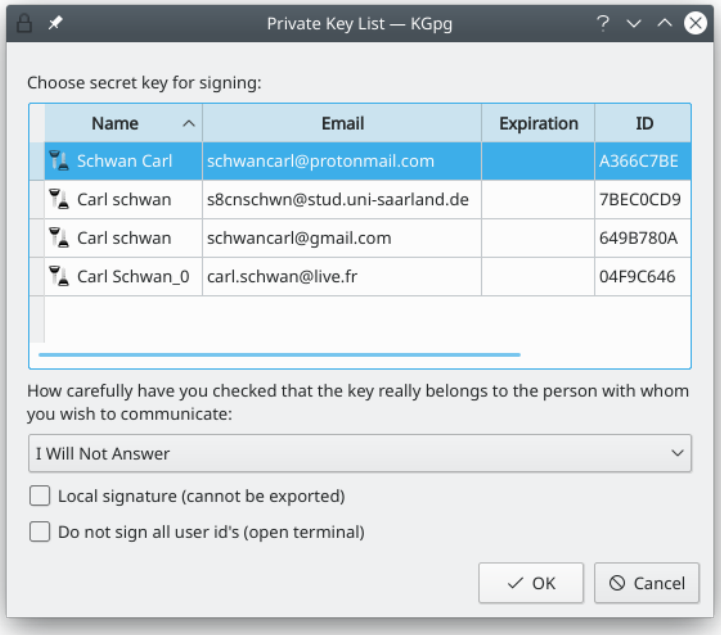
Вредност поузданости говори колико верујете власнику кључа да ће исправно оверавати идентитет кључева које потписује. На основу поузданости власникâ, ГПГ гради вашу мрежу поверења. Верујете кључевима које сте потписали. Ако неку особу прогласите поузданом, веровање се кључевима које је она потписала, без потребе да лично потпишете те кључеве.

3.5.3 Потписивање кључева

Тиме што потпишете кључ неке особе (зовимо је Алиса) објављујете да сте сигурни да кључ заиста припада тој особи и да је поуздан. Наравно, треба ово заиста и да проверите. То обично значи да треба да се састанете са Алисом, погледате барем једну њену исправу, и запишете цео отисак њеног кључа или копирате кључ. Када се вратите кући, потпишете кључ. Потом ћете најчешће отпремити потписани кључ на сервер кључева, тако да сви знају да сте проверили кључ и да је његов власник поуздан. Алиса ће вероватно урадити исто, тако да ћете обоје на свом кључу имати потпис оног другог. Ако једно од вас нема исправе при себи током сусрета, то није проблем под условом да се потпише само кључ онога ко их је имао.

Али, помислите шта бива ако Алиса живи на другом крају света од вас. Редовно комуницирате с њом, али нема изгледа да ћете је видети у неко догледно време. Како онда веровати њеном кључу?

Када изаберете њен кључ па кликнете на Потпиши кључеве..., добићете дијалог са опцијама за различите начине потписивања кључа.

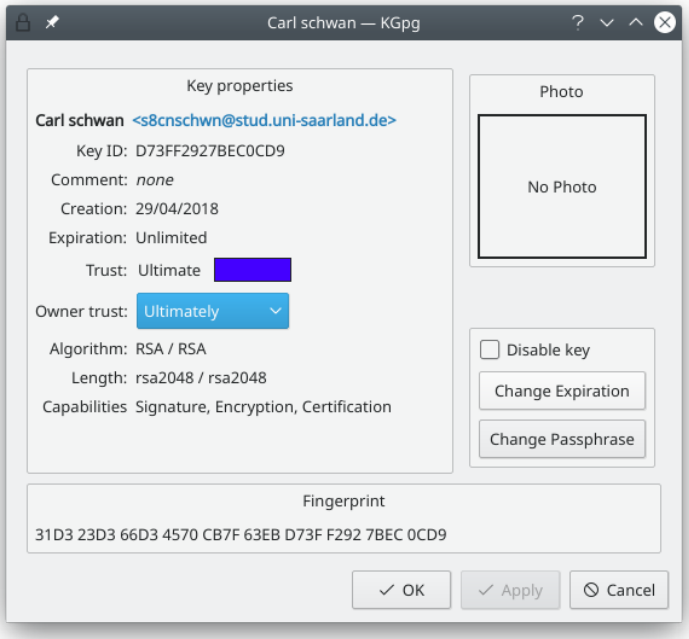


Прво можете изабрати кључ којим ћете потписати дати кључ. Затим можете навести колико сте пажљиво проверили да ли је она заиста особа за коју се издаје. Ови подаци биће ускладиштени заједно са потписом, тако да буду водиља свима онима којима би ваш потпис могао користити (више о овоме у наредном). Долазимо до опције која ће вам помоћи ако не можете да се уживо састанете са Алисом: Локални потпис (не може да се извезе). Ако је активирате биће направљена специјална верзија потписа, таква која никада, чак ни случајно, не може напустити ваш свежањ кључева.

Али зашто је важно колико сте пажљиво проверили Алисин идентитет? Кога је за то брига? Проблем са Алисиним идентитетом можете разрешити на још један начин. Ако не можете да посетите Алису у догледно време, сетите се Тоше. Знате да и Тоша има пар кључева, као и да је светски путник — свраћа на различит континент бар двапут месечно. Уз мало среће, ускоро би се могао наћи негде у близини Алисе. Зато навратите до Тоше да потпишете кључеве. Потом обавестите Алису да би Тоша могао ускоро да се нађе с њом, и питате је да ли би пристала да с њим потпише кључеве. Кад се све то заврши, знате да је Тошин кључ поуздан и да Тоша зна да је Алисин кључ поуздан. Ако верујете Тоши да је пажљиво проверио Алисин идентитет, онда и ви можете сматрати њен кључ поузданим.

Овакви односи између кључева и њихови власника образују такозвану мрежу поверења. У оквиру те мреже постоје неке важне вредности које одређују поузданост датог кључа. Прва међу њима је пажња са којом је проверен идентитет власника кључа. То је вредност коју сте видели изнад у прозору за избор приватног кључа. На пример, вероватно ћете знати како да оцените личну карту у вашој држави, али то може бити тешко са личном картом из неке далеке државе. Тада можете рећи да сте врло пажљиво проверили Тошин идентитет, јер сте видели његову личну карту која је иста као и ваша. Али Тоша, иако је видео и Алисину личну карту и возачку дозволу, може рећи да је тек површно проверио њен идентитет пошто се не разуме у докумéнта из тог дела света.

Следећа важна вредност је колико верујете другој особи да пажљиво проверава документа. Знате да је Тоша добар у томе. Али Ђура, на пример, није неко кога бисте назвали озбиљним. Једва да је погледао вашу личну карту кад сте се нашли с њим да потпишете кључеве. Сигурни сте да је Ђура заиста Ђура, пошто сте пажљиво проверили његова документа. Али делује као да га је мало брига како проверава друге људе, тако да ћете сматрати Ђурин кључ врло поузданим, али његове потписе мало поузданим. Ако отворите својства кључа, видећете поље Поузданост власника:. Оно показује колико верујете власнику кључа кад потписује друге кључеве. Ова вредност се не извози, тако да је потпуно ствар вашег личног избора.



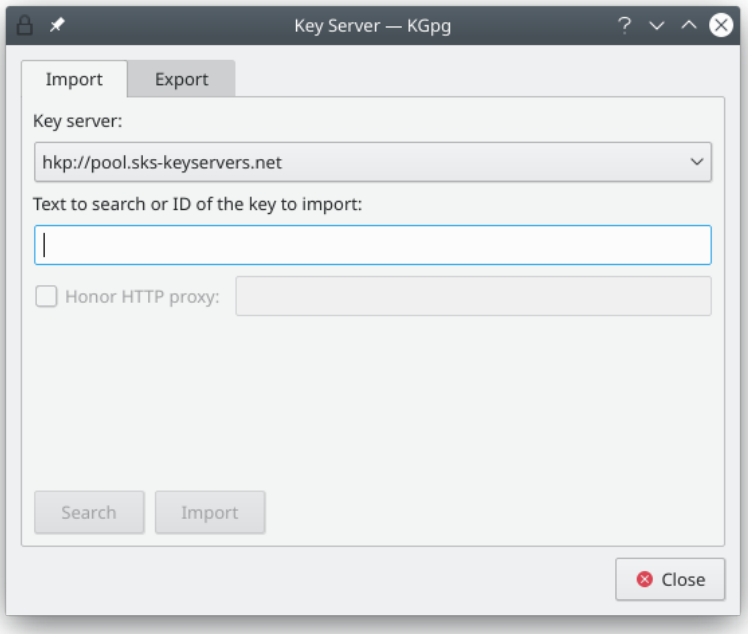
До сада би требало да сте стекли основно разумевање о изградњи мреже поверења, чему служе вредности поузданости кључа и власника, и зашто увек треба да пазите кад проверавате идентитете — јер се други могу ослонити на вас. Међутим, преостаје још један непроверен елемент процеса: адресе е-поште у кључевима које сте потписали. Треба вам само неколико кликова мишем за стварање новог корисничког идентитета у свом кључу са Алисином или Тошином адресом е-поште. Проверили сте да је Тоша заиста власник свог кључа, али до сада нико нико није проверио да ли Тоша заиста контролише адресе е-поште својих идентитета.

Овај процеп можете затворити тако што изаберете Потпиши и пошаљи корисничке ИД-ове... из менија. Идеја је да се кључ потпише као и обично, а затим распарча. Свако парче ће садржати само један идентитет из Тошиног кључа, и ваш потпис на њему. Ово се затим шифрује Тошиним кључем и шаље само на адресу е-поште уз дати идентитет. Тоша ће моћи да увезе ваш потпис у свој свежањ кључева само ако прими и дешифрује поруку. Ви нећете отпремити своје потписе, већ је то потпуно на Тоши. Тада, ако се ваш потпис појави на серверу кључева, можете бити сигурни да су у Тошином поседу и кључ и адреса е-поште које сте потписали. Потписи које начините овако такође не постају део вашег свежња кључева, што значи да ће Тошин кључ у вашем свежњу и даље бити приказан као непоуздан пошто сте га потписали. Када Тоша прими вашу поруку, увезе потпис у свој свежањ и отпреми га на сервер, ви можете освежити његов кључ са сервера и добити нове потписе. Иако ово може звучати напорно испрва, обезбеђује да не дођете у ситуацију да прогласите поузданим неки Тошин идентитет који није под његовом контролом. Само за потписе који се појаве на серверу кључева сви, укључујући и вас, могу бити сигурни да припадајући идентитети заиста одговарају наведеним адресама е-поште.

3.6 Рад са серверима кључева

3.6.1 Комуникација са серверима кључева

Јавни део пара кључева обично се складишти на серверу кључева. Ови сервери свакоме допуштају тражење кључа одређене особе или адресе е-поште. На њима се складиште и потписи.

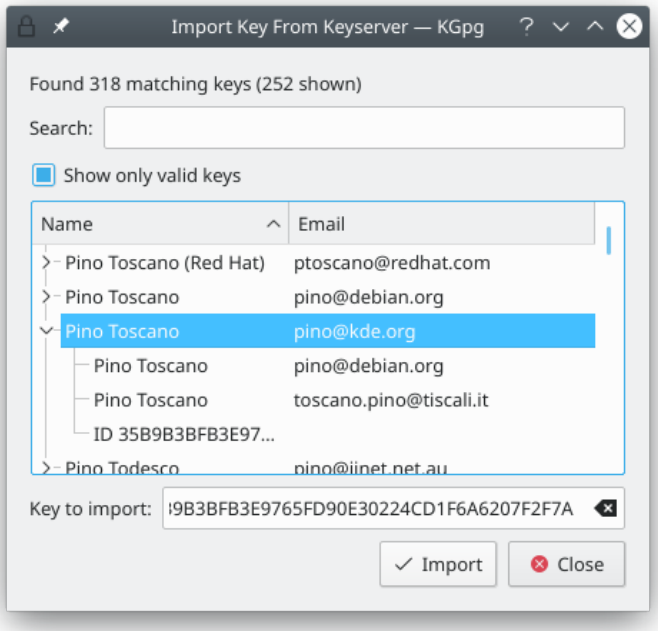


Овај дијалог даје приступ серверима кључева. Кључеве можете тражити и увозити са сервера, као и извозити кључева на њега. До претраге и увожења долази, на пример, када желите неком новом да пишете е-поштом — ако желите да шифрујете поруку тој особи, на серверима кључева можете потражити да ли она има јавни кључ. Пошто сте створили нови пар кључева, или потписали нечији кључ, можда ћете желети да извезете јавни кључ, односно нове потписе, на сервер кључева.

Већина сервера кључева међусобно синхронизују податке, тако да ћете добити сличне резултате претраге без обзира на то који сте сервер употребили. Пошто ипак постоје изузеци од овог правила, у овом дијалогу можете изабрати жељени сервер кључева. Обично је добро за подразумевани изабрати онај сервер кључева који вам је географски близу (тј. у држави или на континенту на којем сте), пошто ће се обично брже одазивати вашим упитима.

Имајте у виду да све што отпремите на сервер кључева обично тамо остаје заувек. Ово је један разлог због којег обично треба да ограничите животни век својих кључева. Пазите такође на то да спамери понекад скенирају сервере кључева ради прикупљања адресе е-поште.

3.6.2 Резултати претраге на серверу кључева



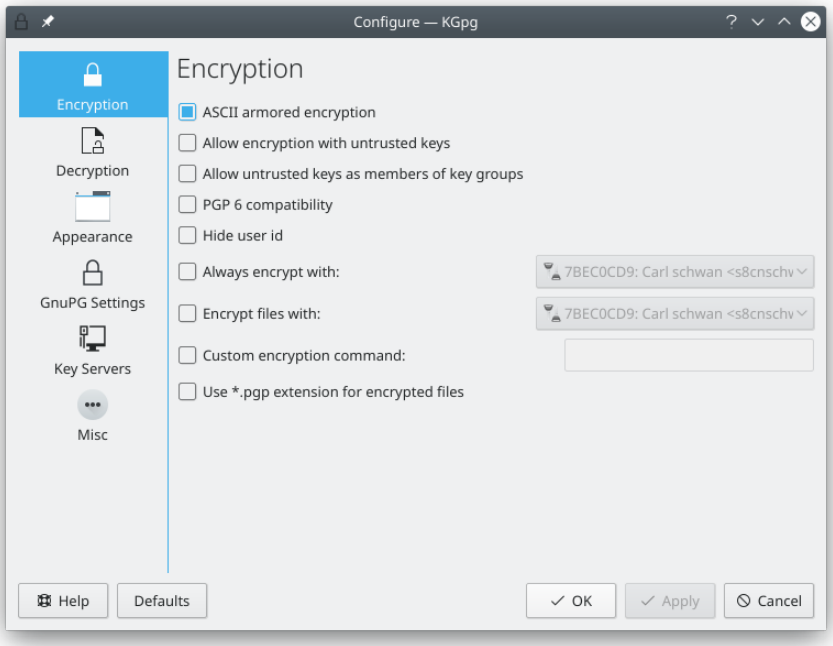
Сви резултати претраге приказују се у овом прозору. На слици се види претрага за адресама @kde.org, која је испоставила 244 резултата. Употребом поља за претрагу, списак је сведен на један кључ. Овај кључ има два поклапања: примарни и још један ИД корисника поклапају ниску претраге.

Можете изабрати више од једног кључа за увожење. ИД-ови тих кључева приказују се у пољу Кључ за увоз: при дну прозора. Кад кликнете на Увези, сервер кључева бива поново контактиран и кључеви се добављају у ваш свежањ кључева.

3.7 Подешавање КГПГ-а

Подешавању се може приступити кроз мени КГПГ-овог аплета (кликните десним на аплет) или кроз главни мени (Подешавање → Подеси КГПГ...). Можете поставити подразумеване параметре за шифровање, дешифровање, корисничко сучеље и аплет. Највећи део опција шифровања у директној су вези са ГПГ-ом и документоване су на његовој упутној страници.

3.7.1 Шифровање



Овде можете подесити специјалне опције за прослеђивање ГнуПГ-у ради измене понашања шифровања. Детаљан опис потражите у приручнику за ГнуПГ.

- Аски оклопљено шифровање: уписује шифроване фајлове у формату који користи само видљиве аски знакове у кратким редовима. Овако шифровани фајлови су већи од оних у бинарном формату, али су сигурнији при слању, нпр. е-поштом.
- Дозволи шифровање непоузданим кључевима: дозвољава шифровање фајлова непоузданим кључевима.
- Сагласност са ПГП-ом 6: шифровани фајлови сагласни су са старијим стандардом ПГП-а 6. Ово искључује извесне могућности, па га користите само ако је заиста потребно.
- Сакриј кориснички ИД: уклања све доказе о примаоцу из шифрованог фајла. У случају да пренос буде пресретнут, нико не би могао да сазна податке о примаоцу из фајла. Ако прималац има више кључева, мора ће да их испробава да би сазнао који је употребљен.
- Увек шифруј помоћу: — на свако шифровање додатно се шифрује и овим кључем. Ако ово поставите да неки од својих приватних кључева, моћи ћете да читате податке које сте шифровали за неког другог. Цена су веће поруке.
- Шифруј фајлове помоћу: — као Увек шифруј помоћу:, само за шифровање фајлова.
- Посебна наредба за шифровање: — ако треба да проследите неуобичајене опције ГнуПГ-у, овде можете задати командну линију. Већини корисника ово неће требати.
- Наставак *.pgp за шифроване фајлове: ако ово укључите, шифровани фајлови биће именовани као улазни фајл с додатим наставком .pgp. Иначе се користи наставак .gpg.

3.7.2 Дешифровање

Овде можете задати посебну наредбу за дешифровање. Ова опција је ретко потребна и може бити корисна само напреднијим корисницима, који познају опције командне линије ГнуПГ-а.

3.7.3 Изглед

Овде подешавате како ће КГПГ изгледати. На располагању су поставке боја које одражавају различите степене поузданости кључева у менаџеру кључева, или фонт у уређивачу.

3.7.4 Поставке ГнуПГ-а

Овде можете подесити који се извршни и поставни фајл ГПГ-а користи, и која је домаћа фасцикла. Ове вредности ће бити аутоматски откривене при првом покретању, и требало би да раде.

Агент ГнуПГ-а чини удобнијим рад са ГнуПГ-ом тако што вам омогућава да не уносите лозинку за сваку радњу. Лозинка се кешира у меморији на неко време, за које ће се без питања извршити сваки поступак који би иначе захтевао лозинку. Пазите, ово би могло омогућити другима да употребе ваше приватне кључеве, ако им случајно учините доступном своју сесију.

3.7.5 Сервери кључева

Овде можете одредити списак сервера кључева који вам даје дијалог за сервер кључева. Ако извршавате ГнуПГ из командне линије, користиће се само сервер кључева који овде поставите као подразумевани.

Протокол којим се комуницира са серверима кључева заснован је на ХТТП-у, тако да у неким окружењима има смисла укључити Поштуј ХТТП прокси када је доступан.

3.7.6 Разно

Ова секција омогућава постављање неких могућности које се не уклапају у друге секције. На пример, можете укључити Аутоматски покрени КГПГ по пријављивању. Опција Бирање мишем уместо клипборда одређује да ли се бира мишем и налепљује средњим дугметом миша или се све радње изводе пречицама с тастатуре.

Можете одредити да ли се приказује иконица системске касете КГПГ-а, и која се радња изводи кад на њу кликнете левим дугметом миша. Ако се иконица приказује, затварање прозора минимизоваће КГПГ у касету; у супротном, КГПГ ће бити напуштен по затварању свих прозора.

Глава 4

Заслуге и лиценца