KGpg käsiraamat

Jean-Baptiste Mardelle
Rolf Eike Beer
Tõlge eesti keelde: Marek Laane

Sisukord

Kokkuvõte

KGpg on GnuPG (http://gnupg.org) lihtne graafiline kasutajaliides.

Peatükk 1

Sissejuhatus

KGpg on võimsa krüptimisvahendi GnuPG lihtne kasutajaliides. GnuPG (kannab ka nimetust gpg) on kaasas enamiku distributsioonidega ning peaaegu kindlalt paigaldatud ka sinu süsteemi. Uusima versiooni leiab aadressilt http://gnupg.org.

KGpg abil saab oma faile ja kirju krüptida ning lahti krüptida, mis võimaldab märksa turvalisemat sihtlemist. Lühike õpetus (HOWTO) gpg vahendusel krüptimise kohta asub GnuPG veebileheküljel.

KGpg kasutamisel ei ole sugugi vaja meeles pidada gpg arvukaid käsureavõtmeid ja muud sellist, peaaegu kõik on võimalik ära teha mõne hiireklõpsuga.

Peatükk 2

Alustamine

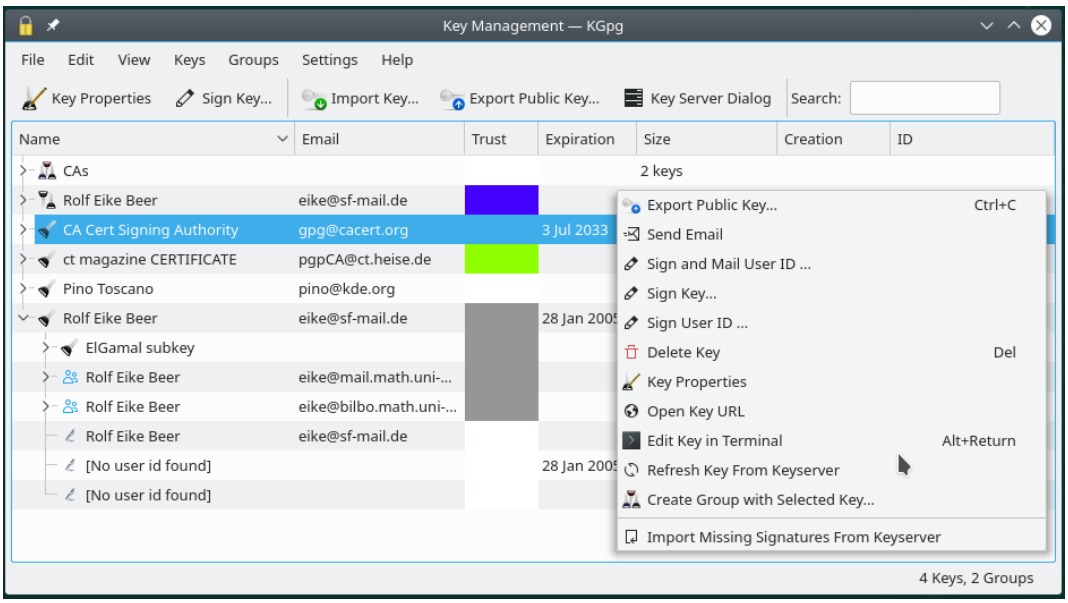
KGpg põhikomponendid on sellised:

Süsteemse doki ikoon

KGpg käivitamisel ilmub kõigepealt ikoon süsteemisalve. Klõps sellel hiire vasaku nupuga avab võtmehalduri, klõps hiire parema nupuga menüü, mis võimaldab kasutada mõningaid olulisemaid rakenduse võimalusi. Kui soovid kasutada teisi võimalusi, võid hiire vasaku nupuga klõpsates avada redaktori või üldse süsteemisalve ikooni välja lülitada seadistustedialoogis.

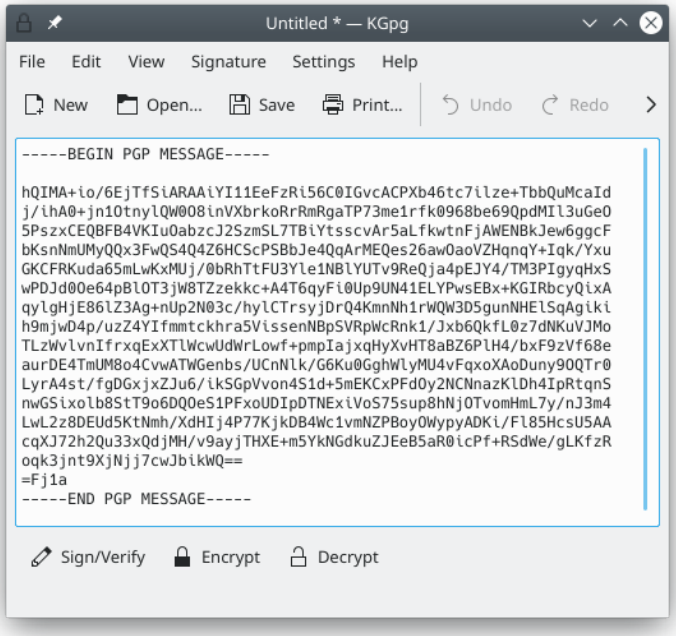
Pane tähele, et KGpg süsteemisalve ikoon on põhimõtteliselt kogu aeg ˝mitteaktiivne˝. Et süsteemisalve aplett peidab tavaliselt mitteaktiivsed ikoonid, siis ei näe KGpg ikooni enamasti, kuni sa seda spetsiaalselt ei kasuta. Täpsemalt kõneleb sellest Plasma käsiraamat.

Võtmehalduri aken



See on keskne koht, kus oma võtmeid hallata. Võtmehalduri avamiseks klõpsa KGpg apletil hiire vasaku nupuga. Siin saab võtmeid importida, eksportida, signeerida ja redigeerida. Enamik tegevusi on võimalik sooritada võtmel hiire vasaku nupuga klõpsates.

Redaktoriaken



See on üsna lihtne tekstiredaktor, kuhu saab teksti kirjutada või asetada ning seejärel krüptida või lahti krüptida. Redaktori avamiseks tee KGpg apletil klõps hiire parema nupuga.

Lõimimine failihalduriga

KGpg on põimitud Konquerori ja Dolphini. See tähendab, et kui klõpsad failil hiire parema nupuga, saad näiteks faili krüptida hüpikmenüü käsuga **Toimingud** → **Krüpti fail**. Sama hõlpsalt saab hiire vasaku nupuga klõpsates faili lahti krüptida.

Peatükk 3

KGpg kasutamine

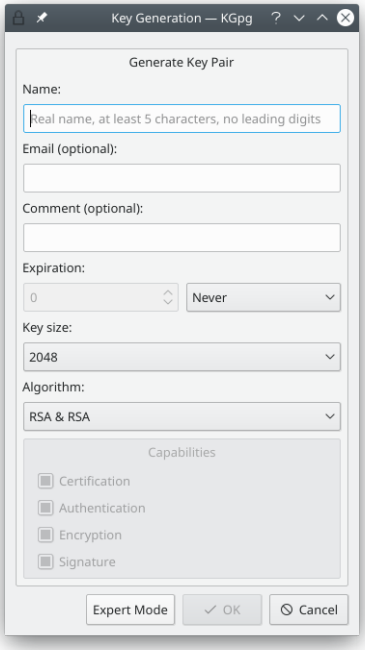
Andmete krüptimiseks on olemas kaks viisi:

- Sümmeetriline krüptimine: andmed krüptitakse ainult parooliga. Kõik, kes kasutavad gpg-ga arvutit, võivad sinu kirja lahti krüptida, kui vaid annad neile teada parooli. Sümmeetrilise krüptimise kasutamiseks vali siis, kui sul palutakse valida krüptovõti, võimalus ˝sümmeetriline krüptimine˝.
- Võtmega krüptimine: esmalt tuleb luua võtmepaar (salajane ja avalik võti) ning määrata paroolifraas. Hoia salajane võti turvalises kohas ning levita oma avalikku võtit tuttavate ja sõprade seas. Kui soovid nüüd saata näiteks krüptitud kirja Aleksile, pead kirja krüptima Aleksi avaliku võtmega. Kirja lahtikrüptimiseks vajab saaja Aleksi salajast võtit ja paroolifraasi.

Võtmega krüptimine on mõnevõrra keerukam (sõpradega tuleb võtmeid vahetada), kuid seeeest turvalisem. Pea meeles, et kui krüptid kirja kellegi teise võtmega, ei suuda sa seda enam lahti krüptida. Lahti krüptida saad ainult neid kirju, mis on krüptitud sinu avaliku võtmega.

3.1 Võtme genereerimine

Kui sul võtit ei ole, avab KGpg kohe esimesel käivitamisel automaatselt võtme genereerimise dialoogi. Selle saab avada ka võtmehalduris menüükäsuga **Võtmed** → **Genereeri võtmepaar**.



Anna siin lihtsalt oma nimi, e-posti aadress ja klõpsa nupule **OK**. Nüüd genereeritakse tavaline gpg võti. Kui soovid tingimusi ja omadusi täpsemalt määrata, vali **ekspertrežiim**, mis avab Konsolei akna koos kõigi gpg valikutega.

Paljud proovivad oma esimese võtmega mitmeid asju, loovad kehvi kasutaja ID-id, lisavad kommentaare, mida nad hiljem kahetsevad, või lihtsalt unustavad oma paroolifraasi. Esimest korda avalikku võtit luues oleks mõttekas piirata selle eluiga näiteks 12 kuuga. Oma salajaste võtmete eluiga saab hiljem muuta võtme omaduste dialoogis.

3.2 Võtme tühistamine

Aegunud võtmepaari saab taas kasutusele võtta, kui on ligipääs privaatvõtmele ja paroolifraasile. Et muuta võti kindlalt kasutuskõlbmatuks, tuleb see tühistada. Selleks lisatakse võtmele spetsiaalne tühistamisallkiri.

Tühistamisallkirja võib luua koos võtmega. Sel juhul salvestatakse see eraldi faili, mille võib hiljem importida võtmerõngasse, millega see lisatakse võtmele ja muudetakse viimane kasutuskõlbmatuks. Palun pane tähele, et allkirja importimisel võtmesse ei ole parool nõutav. Seepärast tuleks tühistamisallkiri salvestada turvalisse, reeglina võtmepaarist erinevasse kohta. Soovitatav on salvestada see arvutist eraldi, näiteks kopeerida välisele salvestile (USB-pulk või midagi muud) või lausa trükkida.

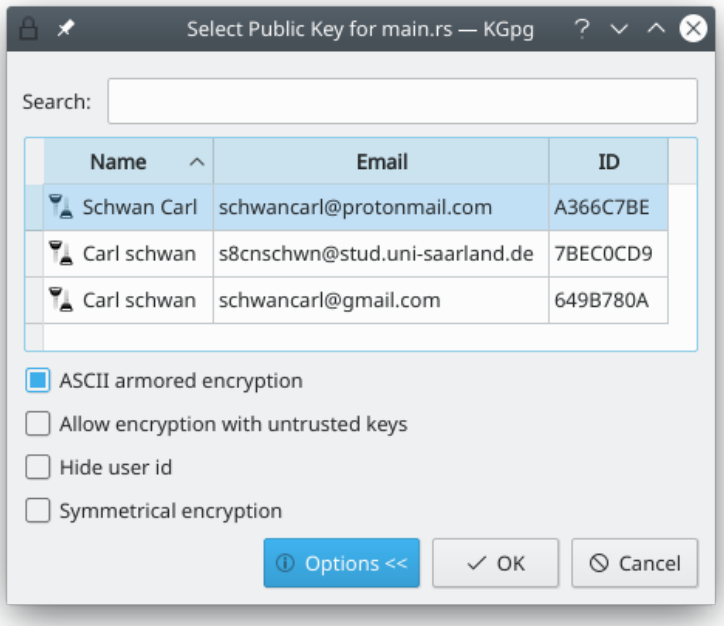
Kui sa ei loonud eraldiseisvat tühistust võtme loomisel, saab tühistamisallkirja alati luua menüükäsuga **Võtmed** → **Tühista võti**, kusjuures võib selle ka kohe importida võtmerõngasse.

3.3 Andmete krüptimine

3.3.1 Faili krüptimine Konqueroris või Dolphinis

Klõpsa failil, mida soovid krüptida, hiire parem nuppga. Vali hüpikmenüüst **Tegevused** → **Krüpti fail**. Seejärel ilmub avaliku võtme valimise dialoog. Vali seal saaja võti ning klõpsa nupule **Krüpti**. Krüptitud fail salvestada sõltuvalt sellest, kas valid **ASCII krüptimise** või mitte,

laiendiga `.asc` või `.gpg`. ASCII krüptingus failid kasutavad andmete esitamiseks ainult loetavaid märke, mis annab tulemuseks töökindlamad failid, kui neid kopeerida või e-kirjaga saata, kuid on samas kolmandiku võrra suuremad.



3.3.2 Faili või teksti krüptimine KGpg apleti abil

Lõikepuhvri sisu saab krüptida, kui valida apleti menüüs käsk **Krüpti lõikepuhver**. Kui aga valida **Allkirjasta lõikepuhver**, tekst hoopis allkirjastatakse. Mõlemal juhul imporditakse lõikepuhvri aktiivne sisu redaktori aknasse, sooritatakse vajalik toiming ning asetatakse sisu tagasi redaktorisse.

3.3.3 Teksti krüptimine KGpg redaktoris

Siin piirdub kõik vaid klõpsuga nupule **Krüpti**. Seejärel ilmub avaliku võtme valimise dialoog. Vali võti ja klõpsa taas nupule **OK**. Krüptitud kiri ilmub redaktori aknasse.

Tavaliselt saab faile krüptida ainult võtmega, mida sa usaldad. Et aga mõnikord võib olla vaja saata konfidentsiaalne tekst mõningatele juhuslikumatele inimestele, kelle kohta sa siiski tead, et neil on GPG võti olemas, saab siin valida ka võimaluse **Krüptimise lubamine mitteusaldusväärsete võtmetega**.

Tagamaks, et sa saad lahti krüptida iga faili, mille oled krüptinud, isegi kui need on krüptitud kellegi teise võtmega, saab dialoogis KGpg seadistamine valida võimalusi **Alati krüptitakse võtmega** ja **Failid krüptitakse võtmega**.

Rohkem infot krüptimise selliste valikute kohta, nagu **ASCII pakend**, **krüptimise lubamine mitteusaldusväärsete võtmetega** ja **sümmeetriline krüptimine** leiab gpg dokumentatsioonist või man-lehekülgedelt.

3.4 Andmete lahtikrüptimine

3.4.1 Faili lahtikrüptimine Konqueroris või Dolphinis

Klõpsa hiire vasaku nupuga failil, mida soovid lahti krüptida. Anna paroolifraas ja see krüptitaksegi lahti. Krüptitud tekstifaili võib lohistada ka KGpg redaktori aknasse. Seejärel küsitakse paroolifraasi ja kui see on õige, avatakse lahtikrüptitud tekst KGpg redaktoris. Sinna võib kukutada isegi võrgufaile! Samuti võib kasutada menüükäsku **Fail** → **Krüpti fail lahti** ja valida, millist faili soovid lahti krüptida.

3.4.2 Teksti lahtikrüptimine KGpg apleti abil

Lõikepuhvri sisu saab lahti krüptida, kui valida KGpg apleti menüüs **Krüpti lõikepuhver lahti**. Selle peale ilmub redaktori aken lahtikrüptitud tekstiga.

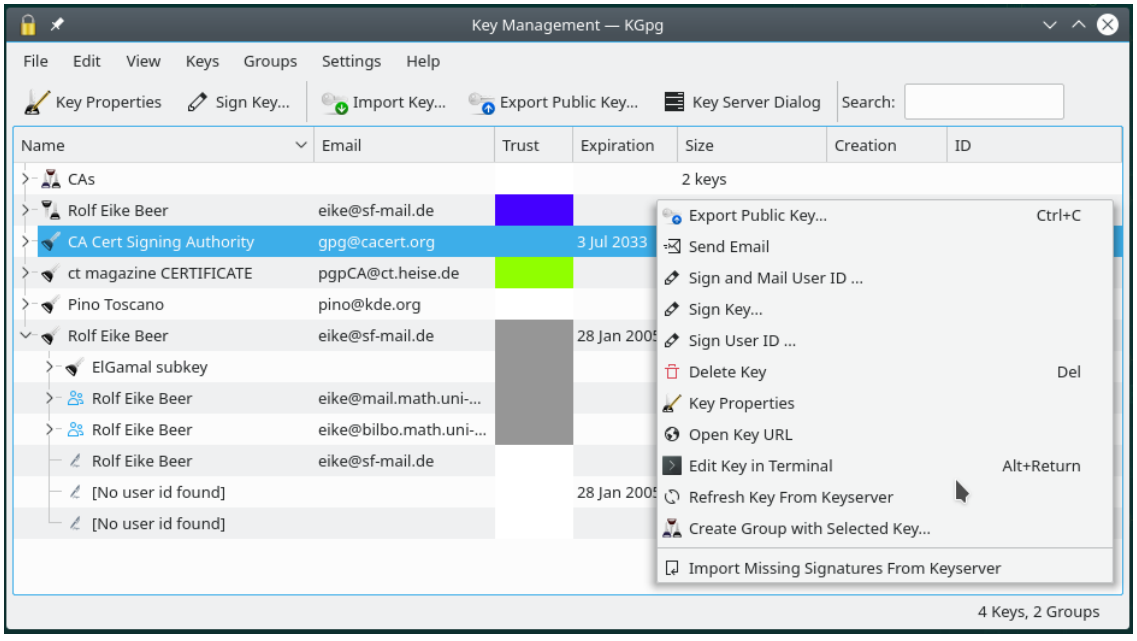
3.4.3 Teksti lahtikrüptimine redaktoris

Kopeeri või lohista tekst, mida soovid lahti krüptida, ning klõpsa nupule **Krüpti lahti**. Seejärel küsitakse paroolifraasi.

3.5 Võtmehaldur

KGpg võimaldab sooritada kõik peamised võtmete haldamisega seotud operatsioonid. Võtmehalduri avamiseks tee hiire vasaku nupuga klõps KGpg apletil. Enamik valikud on saadaval hiire parema nupu klõpsuga võtmel. Avaliku võtme importimiseks või eksportimiseks võib selle kas lohistada või kiirklahvidega kopeerida/asetada.

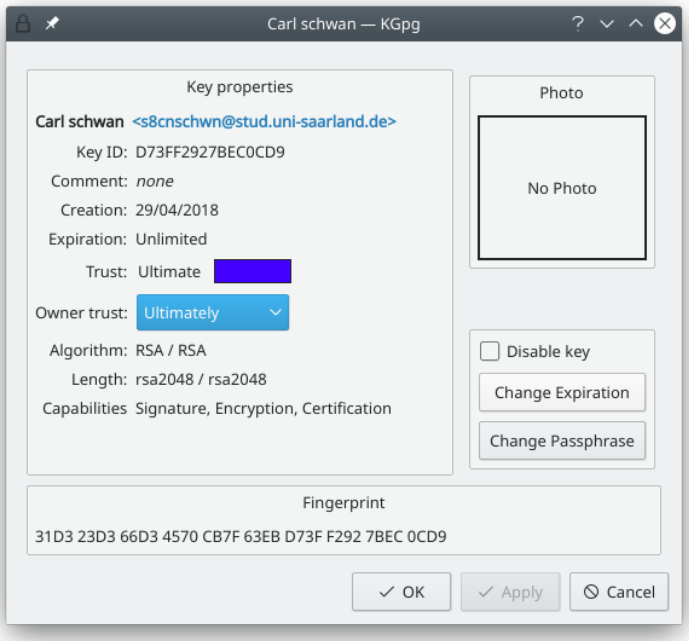
3.5.1 Võtmehaldur



Antud näites on näha võtmegrupp, mis koosneb kahest võtmest, kahest võtmepaarist ja kolmest avalikust võtmest. Kolmas veerg näitab võtmete usaldusväärsust. Esimene võtmepaar on äärmiselt usaldusväärne ning ühtlasi vaikimisi võti (rasvane kiri), teine aga juba aegunud. Kaks avalikku võtit on täielikult usaldusväärsed, viimane aga põgusalt usaldusväärne. Viimane võti on avatud:näha on selle ElGamali alamvõti, kasutaja ID, mis mõlemad on samuti põgusalt usaldusväärsed, ning mõned allkirjad.

Allkirjad võimaldavad liikuda võtmerõngas. Topeltklõpsuga allkirjal või võtmel, mis kuulub gruppi, saab otse hüpata vastavale primaarvõtmele.

3.5.2 Võtme omadused



Kui võtmehalduris saab võtta midagi ette ühe või mitme võtme, võtmegrupi või allkirjaga, siis võtme omaduste aknas saab tegelda konkreetse võtmega. Selle akna saab avada võtmehalduris klahvi Enter vajutades või topeltklõpsu tehes.

Selles aknas saab muuta paroolifraasi ja oma salajaste võtmete aegumist. Kõigi võtmete puhul saab määrata ka omaniku usaldusväärsuse.

See näitab, mil määral usaldad selle võtme omanikku tema allkirjastamisel kasutatud võtmete identiteedi kontrollimisel. Omaniku usaldusväärsuse arvestamisega loob gpg sinu isikliku usaldusvõrgu. Sa usaldad võtmeid, mille oled allkirjastanud. Kui omistad neile isikutele samuti usaldusväärsuse, usaldad ka võtmeid, millega nad allkirjastavad, ilma et sa oleksid eelnevalt ka nende võtmeid allkirjastanud.

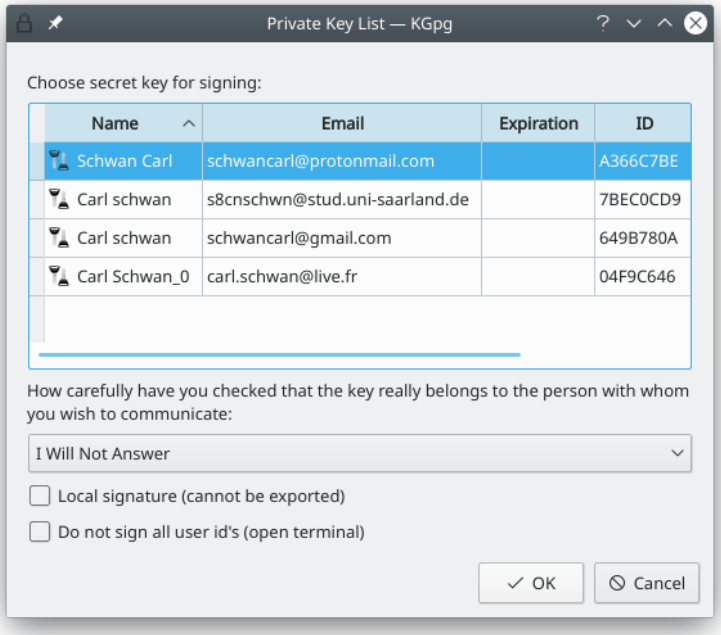
3.5.3 Võtmete allkirjastamine

Kui allkirjastad kellegi teise (ütleme näiteks Alice'i) võtme, annad teada, et oled kindel, et see võti kuulub tõepoolest sellele isikule ja et seda võtit võib usaldada. Loomulikult tuleks seda kindlasti kontrollida. See tähendab enamasti, et sa oled Alice'iga kohtunud, kontrollinud vähemalt tema isikutunnistust ning saanud tema võtme koopia või täieliku võtme sõrmejälje. läinud seejärel koju ja allkirjastanud selle võtme. Tavaliselt järgneb sellele allkirjastatud võtme laadimine võtmeserverisse, mille järel kõik teavad, et sa oled seda võtit kontrollinud ja pead omanikku

usaldusväärseks. Alice teeb tõenäoliselt sama, nii et sel juhul olete mõlemad vastastikku teineteise võtmed allkirjastanud. Kui ühel ei juhtu olema näiteks isikutunnistust kaasas, pole ka viga, kui see toimub ühepoolselt.

Aga mis siis, kui Alice elab teises maailma otsas? Sa suhtled temaga pidevalt, aga sul pole vähimatki võimalust teada niipea näha. Kuidas siis tema võtit usaldada+

Kui valid tema võtme ja seejärel käsu **Allkirjasta võti...**, ilmub dialoog, kus saab valida tingimused, kuidas võti allkirjastada.



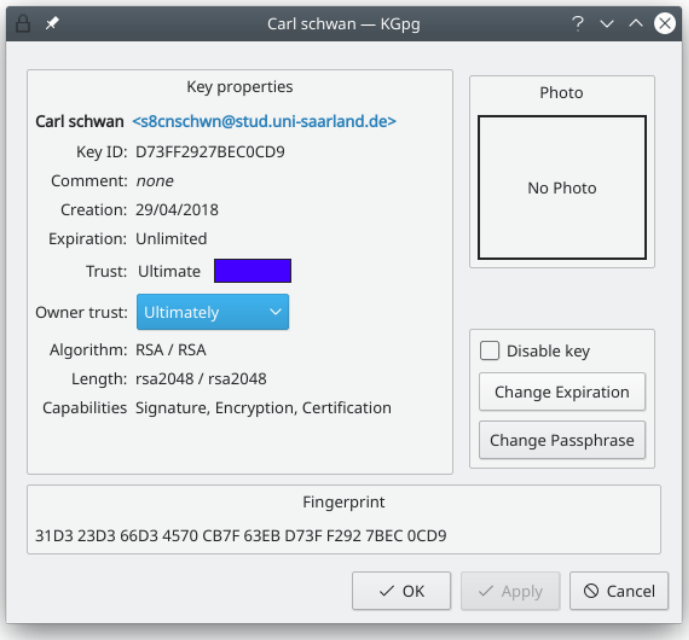
Kõigepealt saad valida võtme, mida kasutada võtme allkirjastamiseks. Siis saab valida, kui hoolikalt oled kontrollinud, et tegemist on ikka isikuga, keda ta väidab ennast olevat. See salvestatakse koos allkirjaga, andes niisiis märku kõigile, kellel võib seda allkirja vaja minna (sellest lähemalt allpool). Siis tulebki valik, mis on abiks, kui sa ei saa Alice'iga isiklikult kohtuda: **Kohalik allkiri (ei saa eksportida)**. Selle valimisel luuakse eriline allkiri, mis ei saa mitte kunagi isegi juhuslikult pääseda kaugemale kui sinu võtmerõngas.

Aga miks on üldse oluline, kui hoolikalt sa oled kontrollinud Alice'i identiteeti? Kes sellest ikka hoolib? Igal juhul saab Alice'i identiteedi probleemi lahendada ka teisiti. Kui sa ei saa ise Alice'it niipea külastada, siis tuleb appi Trent. Sa tead, et Trentil on samuti võtmepaar. Ja Trent on tõeline maailmarändur, kes satub vähemalt paar korda kuus mõnele teisele mandrile. Hea õnne korral satub ta peagi ka Alice'i lähedale. Niisiis, lähed Trentiga kohtuma, et võtmed allkirjastada. Seejärel saadad Alice'ile teate, et Trent satub peagi tema lähedusse ja palud, kas ta ei saaks Trentiga kohtuda, et võtmed allkirjastada. Pärast seda tead, et Trenti võtit saab usaldada, ning Trent teab, et Alice'i võtit saab usaldada. Kui sa usud, et Trent on hoolikalt kontrollinud Alice'i identiteeti, võid niisiis usaldada ka Alice'i võtit.

Niisuguseid suhteid võtmete ja nende omanike vahel nimetatakse usaldusvõrguks. Selles võrgus valitsevad teatavad olulised väärtused, mis määravad, kui usaldusväärne on konkreetne võti. Kõigepealt see, kui hoolikalt on kontrollitud võtmeomaniku identiteeti. See on väärtus, mida võis näha eespool salajase võtme valimise aknas. Näiteks on usutav, et sa tead, kui usaldusväärsed on sinu enda maa isikutunnistused, aga teiste riikide puhul on seda juba raskem kontrollida. Seega võid öelda, et oled kontrollinud hoolikalt Trenti isikutunnistust ja see paistis täiesti sinu enda isikutunnistuse moodi. Aaa kuigi Trent nägi Alice'i isikutunnistust ja autojuhiluba, võib öelda, et ta kontrollis Alice'i identiteeti vaid pealiskaudselt, sest ta ei saa olla absoluutselt kindel, millised peavad just välja nägema selle maailma nurga dokumendid.

Järgmine oluline väärtus on see, mil määral sa usaldad teist isikut dokumentide kontrollimisel. Sa

tead, et Trent on selles päris hea. Aga näiteks George'i ei söanda keegi targaks nimetada. Ta heitis vaevu pilgu sinu isikutunnistusele, kui te võtmete allkirjastamiseks kohtusite. Sa oled kindel, et George on tõepoolest George, sest kontrollisid hoolikalt tema dokumente. Kuid tema ei paistnud kontrollimisest eriti välja tegevat. Niisiis võid väga usaldada George'i võtit, aga väga vähe tema allkirju. Kui avad võtme omadused, leiab seal välja **Omaniku usaldusväärsus**. See näitabki seda, mil määral sa usaldad võtme omanikku, kui ta võtmeid allkirjastab. Seda väärtust ei ekspordita, see on puhtalt sinu enda jaoks.



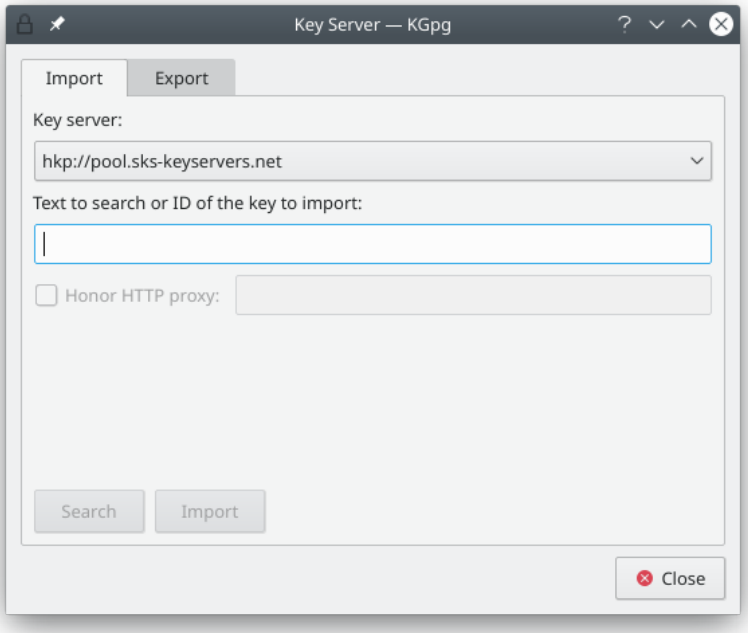
Nüüd peaks sul olema ettekujutus, kuidas näeb välja usaldusvärk, mida tähendavad omaniku ja võtme usaldusväärtused ja miks tuleb alati olla identiteedi kontrollimisel väga hoolas: teised inimesed võivad tugineda sinu hinnangutele. Üks element on siiski veel lahtine: allkirjastatud võtmete e-posti aadressid. Uue kasutajaidentiteedi loomine sinu võtmes Alice'i või Trenti e-posti aadressiga nõuab vaid paari hiireklõpsu. Sa oled kontrollinud, et Trenti võti kuulub tõepoolest talle. Aga seni ei ole keegi kontrollinud, et Trent kontrollib tegelikult ka tema kasutajaidentiteedi e-posti aadresse.

Sellest saab üle, kui valida menüüst käsk **Allkirjasta ja saada kasutaja ID...** Selle mõte seisab sellest, et sa allkirjastad võtme nagu tavaliselt, aga siis jagatakse see osadeks. Iga osa sisaldab ainult ühte Trenti võtme kasutajaidentiteeti ja sinu allkirja sellele. See krüptitakse Trenti võtmega ja saadetakse ainult identiteedis leiduvale e-posti aadressile. Ainult siis, kui Trent saab selle kirja kätte ja suudab selle lahti krüptida, saab ta selle allkirja importida oma võtmerõngasse. Mitte sina ei laadi oma allkirju üles, see on vaid tema teha. Kui sinu allkiri ilmub võtmeserverisse, võid olla kindel, et Trent kontrollib tõepoolest nii võtit kui e-posti aadressi, mille sa allkirjastasid. Allkirjad, mida sa selle käigus andsid, ei muutu sinu võtmerõnga osaks. Seega ka pärast seda, kui sa oled allkirjastanud Trenti võtme, näidatakse seda sinu võtmerõngas ebausaldusväärsena. Kui Trent saab sinu kirja ja impordib sini allkirja oma võtmerõngasse, võib ta need laadida võtmeserverisse. Kui värskendad oma võtit võtmeserverist, saad sealt uued allkirjad. See võib esialgu tunduda üsna ebamugav, aga asja mõte on see, et sa ei näeks kogemata usaldusväärsena mõnda tema identiteeti, mida ta tegelikult ei kontrolli. Ainult allkirjad, mis ilmuvad võtmeserveris, on allkirjad, mille puhul kõik, sealhulgas sa ise, võivad olla kindlad, et just tema kontrollib vastavat e-posti aadressi.

3.6 Võtmeserverite kasutamine

3.6.1 Suhtlemine võtmeserveritega

Võtmepaari avalik osa on tavaliselt salvestatud võtmeserverisse. Need serverid võimaldavad kõigl otsida konkreetse isiku või e-posti aadressiga seotud võtit. Serveritesse on salvestatud ka allkirjad.

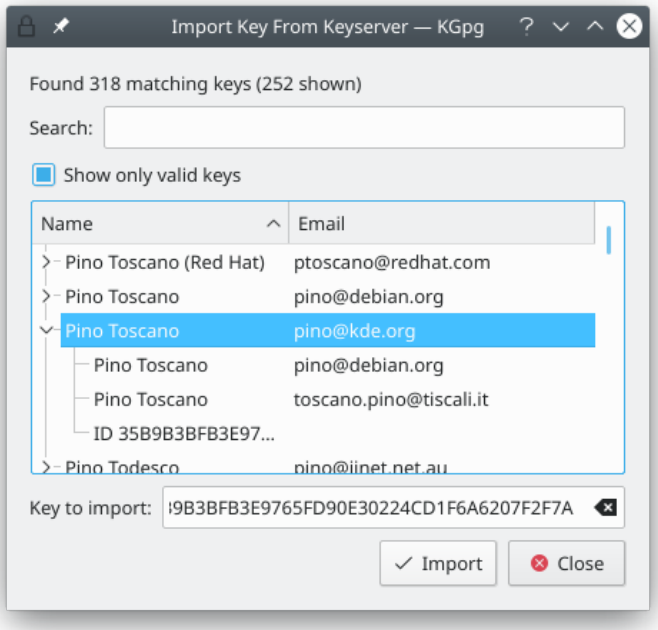


See dialoog võimaldab kasutada võtmeservereid. Siin saab otsida võtmeserveris võtmeid ja neid importida, samuti eksportida võtmeid serverisse. Otsimisel ja importimisel on mõtet näiteks siis, kui soovid kirjutada kirja kellelegi, kellega pole varem suhelnud. Kui soovid oma kirja uuele kontaktile krüptida, võid otsida, kas tal on võtmeserverites avalik võti. Kui oled loonud uue võtmepaari või allkirjastanud kellegi teise võtme, võib aga olla mõttekas eksportuda avalik võti (soovi korral koos uute allkirjadega) võtmeserverisse.

Enamik võtmeservereid sünkroniseerib oma andmed, nii et otsimine annab sõltumata serverist sama tulemuse. Et igal reeglil on alati erandeid, saab dialoogis siiski ka määrata, millist võtmeserverit kasutada. Tavaliselt on mõttekas valida vaikimisi võtmeserveriks mõni füüsiliselt lähemal asuv (oma riigis või vähemalt samal mandril), sest need vastavad enamasti päringutele kiiremini.

Palun arvesta, et üldiselt jääb kõik, mis on laaditud võtmeserverisse, sinna igaveseks. Seepärast ongi mõttekas piirata oma võtmete eluiga. Samuti tasub arvestada, et mõnikord kammivad võtmeservereid aadresside leidmiseks läbi rämpsposti levitajad.

3.6.2 Võtmeserveri otsingu tulemused



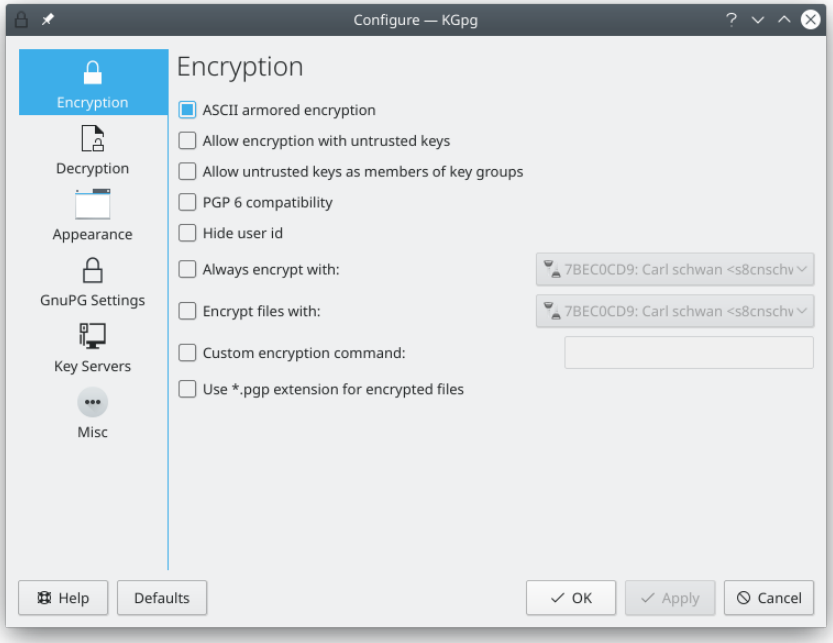
Selles aknas näeb kõiki otsingutulemusi. Pildilt näeb, et otsing ˝@kde.org˝ on andnud 224 tulemust. Otsinguvälja kasutades on nimekirja piiratud, nii et näha on vaid üks võti. Sel on kaks sobivust: otsingule vastab nii primaarne kasutaja ID ise kui ka üks teiste kasutajate ID-dest.

Importimiseks võib valida kas ainult ühe või ka rohkem võtmeid. Nende võtmete ID-sid näeb akna allosas väljal **Imporditavad võtmed**. Klõpsuga nupule **Impordi** võetakse taas ühendust võtmeserveriga ja võtmed tõmmatakse sinu võtmerõngasse.

3.7 KGpg seadistamine

Seadistamise manu pääseb KGpg apletilt (klõps hiire parema nupuga apletil) või põhimenüüst (**Seadistused** → **KGpg seadistmaine**). Seal saab määrata vaikeväärtused krüptimisele, lahtikrüptimisele, kasutajaliidesele ja apletile. Enamik krüptimisvalikuid on otseselt seotud gpg-ga ning nende parima seletuse leiab gpg man-leheküljelt.

3.7.1 Krüptimine



Siin saab seadistada spetsiaalseid GnuPG-le edastatavaid valikuid, mis muudavad krüptimise käiku. Täpsemalt kõneleb neist GnuPG manuaal.

- **ASCII pakendis krüptimine**: krüptitud failid salvestatakse vormingus, is kasutab ainult ASCII sümboleid ning lühikesi ridu. Sel moel salvestatud failid on suuremad kui binaarfailid, aga neil näiteks e-postiga lihtsam saata.
- **Krüptimise lubamine mitteusaldusväärsete võtmetega**: see lubab krüptida faile võtmetega, mida sa pole märkinud usaldusväärseks.
- **PGP 6 ühilduvus**: krüptitud failid ühilduvad vanema PGP6 standardiga. See tühistab teatud omadused, mistõttu seda tasuks kasutada ainult siis, kui seda on tõepoolest vaja.
- **Kasutaja ID peitmine**: kõrvaldab krüptitud failist kõik viited saajale. Kui keegi peaks ülekande hõivama, ei saa ta vähemalt teada, kes on faili saaja. Kui saaja kasutab mitut võtit, peab ta proovima, millist sellise ülekande puhul kasutati.
- **Alati krüptitakse kasutades**: kõik krüptimised krüptitakse lisaks määratud võtmega. Kui määrad siin mõne oma privaatvõtmetest, tuleks kontrollida, et saad lugeda kõiki andmeid, mida oled krüptinud.
- **Failid krüptitakse kasutades**: käitub samamoodi nagu **Alati krüptitakse kasutades** failide krüptimise puhul.
- **Kohandatud krüptimise käsk**: kui sul on tarvis määrata GnuPG-le mingeid tavapärasest erinevaid võtmeid, siis saab vastava käsu anda siin. Enamasti ei ole seda vaja.
- **Krüptitud failidel kasutatakse laiendit .pgp**: selle märkimisel nimetatakse krüptitud failid sisendfailiks laiendiga `.pgp`, vastasel juhul kasutatakse laiendit `.gpg`.

3.7.2 Lahtikrüptimine

Siin saab määrata kohandatud lahtikrüptimise käsu. Seda läheb harva tarvis ning see on mõeldud eelkõige kogenud kasutajatele, kes tunnevad hästi GnuPG käsurea võtmeid.

3.7.3 Välimus

Siin saab seadistada KGpg välimust. Määrata saab värve, mis tähistavad võtme erinevat usaldusväärsust võtmehalduris, ning redaktoris kasutatavaid fonte.

3.7.4 GnuPG seadistused

Siin saab määrata, millist gpg binaarfaili ning **seadistusfaili** ja kodukataloogi kasutatakse. Need väärtused tuvastatakse automaatselt esmakäivitamise ajal ning peaksid üldjuhul sobima.

GnuPG agendi kasutamine muudab GnuPG-ga töötamise hõlpsamaks, sest siis pole vaja iga toimingu jaoks anda uuesti parooli. See salvestatakse mõneks ajaks mällu ning kõik parooli nõudvad toimingud sooritatakse aega viitmata. Pane siiski tähele, et see võib võimaldada teistel kasutada sinu privaatvõtmeid, kui neil avaneb ligipääs sinu seansile.

3.7.5 Võtmeserverid

Siin saab paika panna võtmeserverite nikekirja, mida näidatakse, kui avad võtmeserveri dialoogi. Kui käivitad GnuPG käsurealt, kasutatakse ainult siin vaikimisi serveriks määratud võtmeserverit.

Võtmeserveritega suhtlemiseks kasutatakse HTTP põhist protokolli, mistõttu mõnes keskkonnas tasuks märkida valik **HTTP puhverserveri kasutamine, kui võimalik**.

3.7.6 Muu

Siin saab määrata mõningaid asju, mis ei sobi mujale. Näiteks saab sisse lülitada valiku **KGpg käivitatakse automaatselt sisselogimisel**. Valik **Lõikepuhver kasutab hiirega valimist** muudab seda, kas valik toimub hiirega ja asetamine hiire keskmise nupuga või sooritatakse kõik toimingud kiirklahvide abil.

Samuti saab muuta seda, kas KGpg ikooni näidatakse süsteemses salves või mitte ning mis juhtub siis, kui ikoonil klõpsata hiire vasaku nupuga. Kui süsteemses salves näidatakse ikooni, võrdub KGpg akna sulgemine selle minimeerimisega süsteemsesse salve. Kui ikooni ei näidata, lõpetatakse KGpg töö kõigi akende sulgemisel.

Peatükk 4

Autorid ja litsents

KGpg