Het handboek voor KGpg

Jean-Baptiste Mardelle
Rolf Eike Beer
Vertaler/Nalezer: Jaap Woldringh
Vertaler/Nalezer: Freek de Kruijf

Het handboek voor KGpg

Inhoudsopgave

Samenvatting

KGpg is een eenvoudige grafische interface voor GnuPG http://gnupg.org

Hoofdstuk 1

Inleiding

KGpg is een eenvoudige interface voor GnuPG, een krachtig hulpmiddel voor encryptie. GnuPG (ook bekend als gpg) wordt meegeleverd bij de meeste distributies en moet op uw systeem worden geïnstalleerd. U kunt de laatste versie hier: http://gnupg.org verkrijgen.

Met KGpg kunt u uw bestanden en emails versleutelen en ontcijferen, waardoor een veel veiliger communicatie mogelijk wordt. U kunt een mini Howto voor gpg vinden op GnuPG's website.

Met KGpg is het niet nodig de gpg-opdrachten en -opties te onthouden. Bijna alles kunt u doen met enkele muisklikken.

Hoofdstuk 2

Wij beginnen

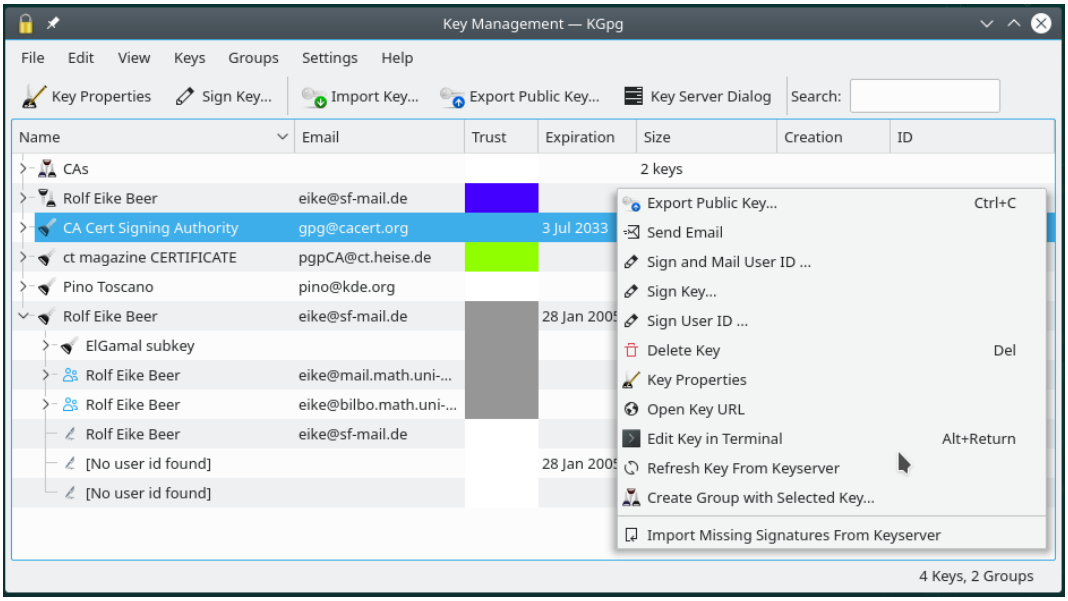
Hier is een lijst van de voornaamste onderdelen van KGpg:

Pictogram in het systeemvak

Als u KGpg start verschijnt er een pictogram (een hangslotje) in het systeemvak. Een linkermuisknop-klik opent het venster van het Sleutelbeheer, een rechtermuisknop-klik opent een menu waarin u snel enkele belangrijke eigenschappen kunt vinden. Als u aan andere opties de voorkeur geeft dan kun u de rechtermuisknop actie wijzigen om de bewerker te tonen of het pictogram in het systeemvak volledig uit te schakelen met de instellingen-dialoog.

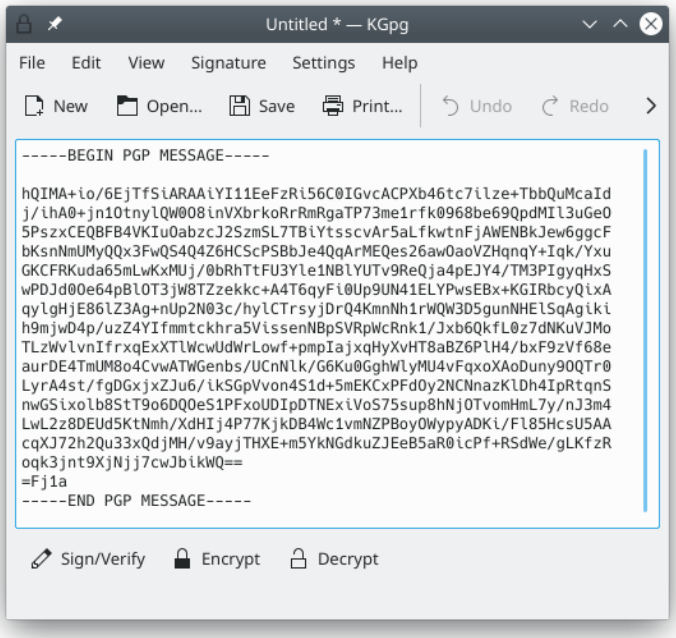
Merk op dat het pictogram van KGpg in het systeemvak in principe altijd als ˝inactief˝ is gemarkeerd. Omdat het systeemvak-applet gewoonlijk inactieve pictogrammen zal verbergen zal ook die van KGpg niet worden getoond totdat u daar expliciet om vraagt. Voor details gaarne in de Plasma-documentatie kijken.

Venster van het Sleutelbeheer



Dit is de centrale plaats voor het beheer van uw sleutels. U kunt het Sleutelbeheervenster openen met de linkermuisknop op het applet van KGpg. U kunt hier uw sleutels importeren, exporteren, ondertekenen, en bewerken. De meeste acties kunt u activeren met een rechtermuisknop-klik op een sleutel.

Het venster Bewerken



Dit venster bevat een eenvoudige tekstverwerker waarin u tekst kunt typen of plakken die u wilt versleutelen of ontcijferen. Om de bewerker te openen, klik met de rechtermuisknop op het applet van KGpg.

Bestandsbeheerder-integratie

KGpg is in Konqueror en Dolphin geïntegreerd. Dit betekent dat als u op een bestand rechtsklikt, u in een menu **Acties** → **Bestand versleutelen** kunt kiezen om het te versleutelen. Met een linkermuisknop-klik kunt u een bestand ontcijferen.

Hoofdstuk 3

KGpg gebruiken

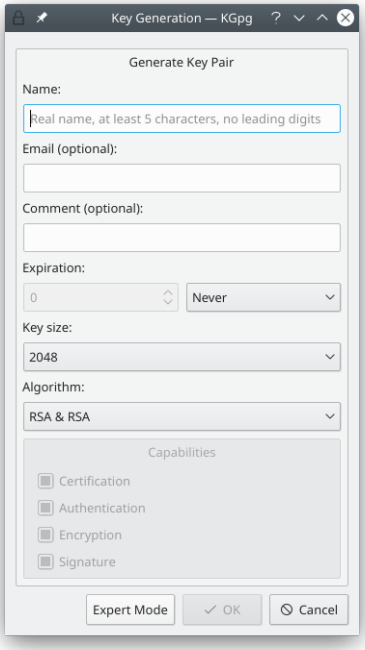
U kunt uw gegevens op twee manieren versleutelen:

- Symmetrisch versleutelen: uw gegevens worden slechts met een wachtwoord versleuteld. Iedereen die gpg op zijn computer heeft kan uw bericht ontcijferen als u hem/haar het wachtwoord geeft. Voor symmetrisch versleutelen kiest u ˝symmetrische versleuteling˝ onder de knop Opties in het venster waarin u om een sleutel wordt gevraagd.
- Versleuteling met een sleutel: eerst moet u uw sleutelpaar aanmaken (geheime en publieke sleutel) en een een wachtzin opgeven die als wachtwoord dient. Bewaar uw geheime sleutel op een veilige plek en wisselt u uw publieke sleutel uit met die van uw vrienden. Daarna, indien u een versleuteld bericht wilt sturen naar uw vriend Alex, versleutelt u dat bericht met de publieke sleutel van Alex. De ontvanger kan daarna met de geheime sleutel van Alex en zijn wachtzin het bericht ontcijferen.

Versleuteling met een sleutel is wat omslachtiger (u moet sleutels uitwisselen met uw vrienden) maar wel veiliger. Onthoud dat als u iets versleutelt met de sleutel van iemand anders, u het daarna niet zelf kunt ontcijferen. U kunt alleen berichten ontcijferen die met uw publieke sleutel zijn versleuteld.

3.1 Een sleutel aanmaken

Indien u nog geen sleutel heeft toont KGpg u automatisch een dialoogvenster voor het aanmaken van sleutels als u het programma de eerste keer start. U kunt dit venster ook oproepen met **Sleutels** → **Sleutelpaar aanmaken**.



Voer gewoon uw naam en e-mailadres in, en klik op **Ok**. Hierna wordt een standaard gpg-sleutel aangemaakt. Als u meer opties wenst, kunt u op de knop **Expertmodus** klikken, waarna u een Konsolevenster krijgt met hierin alle opties van gpg.

Veel mensen spelen een beetje met hun eerste sleutel, genereren slechte gebruiker-id's, voegen commentaar toe waar ze later spijt van hebben of vergeten eenvoudig hun wachtzin. Om zulke sleutels niet een eeuwigheid te laten bestaan is het gewoonlijk een goed idee om de leeftijd te beperken tot zo'n 12 maanden. U kunt de leeftijd van uw geheime sleutels later wijzigen met gebruik van het sleuteleigenschappenvenster.

3.2 Een sleutel intrekken

Een verlopen sleutelpaar kan teruggebracht worden in een operationele status zolang u toegang hebt tot de privé sleutel en de wachtwoordzin. Om een sleutelpaar betrouwbaar onbruikbaar te maken moet u het terugtrekken. Terugtrekken wordt gedaan door een speciale handtekening voor terugtrekken aan de sleutel toe te voegen.

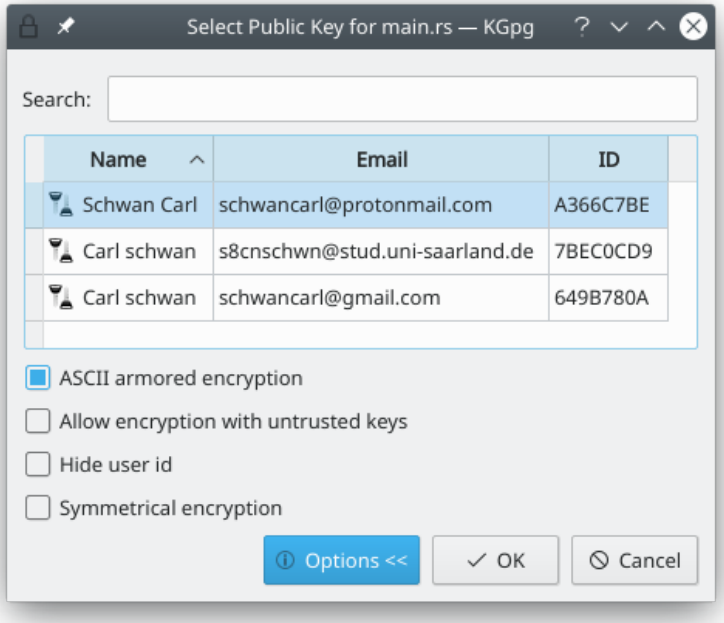
Deze handtekening voor terugtrekken kan samen met de sleutel worden aangemaakt. In dat geval wordt het als een apart bestand opgeslagen. Dit bestand kan later geïmporteerd worden in de sleutelring en wordt dan vastgeplakt aan de sleutel waarmee het onbruikbaar wordt. Merk op dat bij het importeren van deze ondertekening naar de sleutel geen wachtwoord is vereist. Daarom moet u deze ondertekening voor terugtrekken op een veilige plek opslaan, gewoonlijk een plek die verschilt van waar uw sleutelpaar is opgeslagen. Een goed advies is om een plek te kiezen die apart van uw computer is, kopieer het ofwel naar een externe opslag zoals een USB-stick of druk het af.

Als u geen handtekening voor terugtrekken hebt gemaakt bij het aanmaken van uw sleutelpaar, dan kunt u deze op elk moment aanmaken door het kiezen van **Sleutels** → **Sleutel terugtrekken**, met als optie om het onmiddellijk in uw sleutelring te importeren.

3.3 Uw gegevens versleutelen

3.3.1 Een bestand in Konqueror of Dolphin versleutelen

Klik met de rechter muisknop op het bestand dat u wilt versleutelen. Kies **Acties** → **Bestand versleutelen** in het menu dat u krijgt. U wordt daarna gevraagd om een sleutel te selecteren in het dialoogvenster voor het selecteren van de publieke sleutel. Kies de sleutel van de ontvanger en klik op **Versleutelen**. Het versleutelde bestand wordt opgeslagen met een `.asc`- of `.gpg`-extensie, dit is afhankelijk van of u **Versleutelde bestanden in ASCII opslaan** hebt gekozen of niet. In ASCII versleutelde bestanden gebruiken alleen leesbare tekens om de resulterende bestanden te representeren, die meer robuust zijn bij het rond kopiëren of het per e-mail verzenden, maar ze zijn een-derde groter.



3.3.2 Een tekst versleutelen met de applet van KGpg

U kunt de inhoud van het klembord versleutelen door het item **Klembord versleutelen** in het applet-menu te selecteren. Wanneer u **Klembord versleutelen** kiest dan zal de tekst in plaats daarvan worden ondertekend. Beide acties zal de inhoud van het huidige klembord in een tekst-bewerkervenster importeren, de gevraagde actie uitvoeren en de inhoud plakken in de bewerker.

3.3.3 Een tekst van de tekstverwerker van KGpg versleutelen

Dit doet u heel eenvoudig door op de knop **Versleutelen** te klikken. U krijgt dan het dialoog-scherm voor het kiezen van de publieke sleutel. Kies de gewenste sleutel en klik op de knop **OK**. Het versleutelde bericht verschijnt in het scherm van de tekstverwerker.

Gewoonlijk kunt u bestanden alleen met door u vertrouwde sleutels versleutelen. Omdat u soms een confidentiële notitie naar willekeurige mensen wilt sturen weest u er zich dan van bewust dat het hebben van een GPG-sleutel waarvan u de optie **versleuteling toestaan met niet vertrouwde sleutels** hebt ingesteld.

Om er zeker van te zijn dat u elk bestand dat u hebt versleuteld, zelfs als ze zijn versleuteld met de sleutel van iemand anders, kunt ontcijferen, dan kunt u de options **Altijd versleutelen met** en **Bestanden versleutelen met** gebruiken, die beschikbaar zijn in de KGpg-instellingen.

Voor meer informatie over de opties voor versleuteling, **ASCII armor** (beveiligde ASCII), **Versleuteling toestaan met niet vertrouwde sleutels** en **Symmetrische versleuteling**, kunt u het beste de gpg-documentatie of man pagina's raadplegen.

3.4 Uw gegevens ontcijferen

3.4.1 Een bestand uit Konqueror of Dolphin ontcijferen

Klik met de linker muisknop op het bestand dat u wilt ontcijferen. Voer uw sleutelzin in waarna het bestand wordt ontcijferd. U kunt ook een versleuteld tekstbestand slepen naar het venster van de tekstverwerker van KGpg. U wordt daarna naar de sleutelzin gevraagd waarna de ontcijferde tekst in dit venster is te zien. U kunt dit zelfs met bestanden doen die op een andere computer staan! Ook kunt u **Bestand** → **Bestand ontcijferen** gebruiken en een bestand kiezen dat ontcijferd moet worden.

3.4.2 Een tekst ontcijferen met de applet van KGpg

U kunt ook de inhoud van het klembord ontcijferen met het menu-item van het KGpg-applet **Klembord ontcijferen**. Er verschijnt dan een bewerkingsvenster met de te ontcijferen tekst.

3.4.3 Een tekst van de tekstverwerker ontcijferen

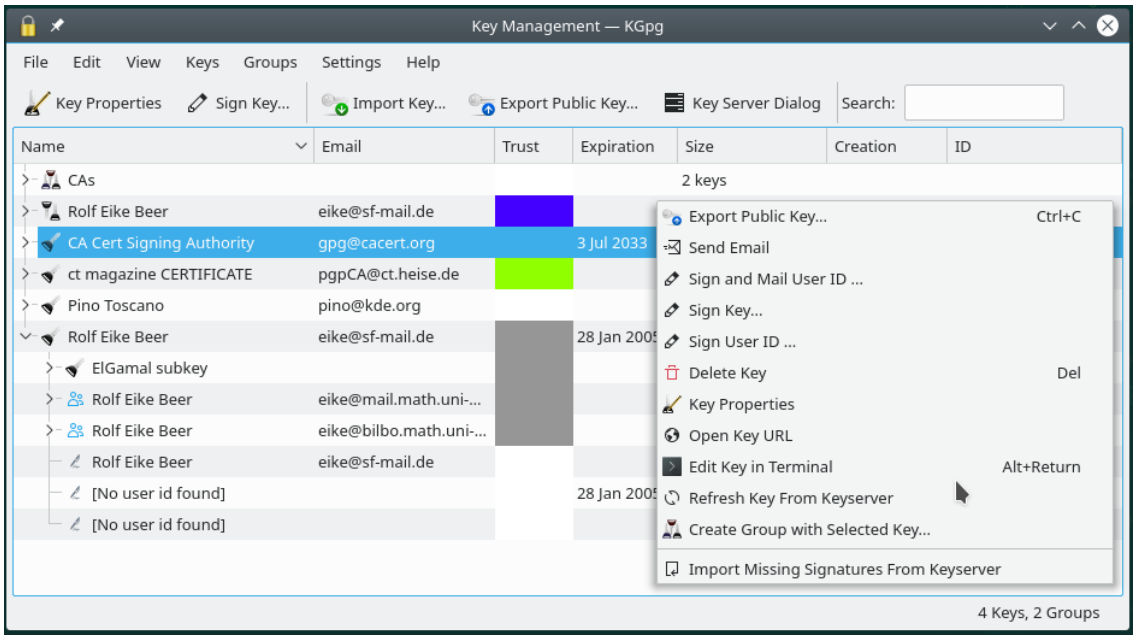
Kopiëer of versleep de tekst die u wilt ontcijferen, en klik op de knop **Ontcijferen**. U wordt gevraagd naar de sleutelzin.

3.5 Sleutelbeheer

Alle basisopties van het sleutelbeheer zijn in KGpg beschikbaar. U kunt het venster van het sleutelbeheer openen door met linkermuisknop op het applet van KGpg te klikken. De meeste opties zijn beschikbaar door rechts te klikken op een sleutel. Voor het importeren/exporteren van publieke sleutels kunt u gebruik maken van slepen en neerzetten of van de sneltoetsen voor Kopiëren/Plakken.

U kunt een publieke sleutel exporteren via e-mail, naar het klembord, naar een sleutelserver of naar een lokaal bestand. Gebruik de opties in de exportdialoog om alles, zonder attributen (foto id's) or een schone sleutel (bijv. de sleutel zelf inclusief zijn subsleutels, maar zonder alle ondertekeningen) te exporteren.

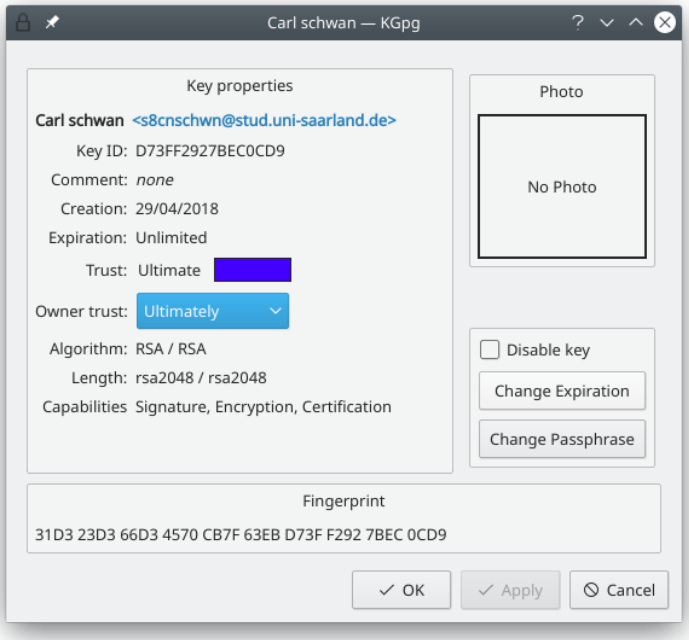
3.5.1 Sleutelbeheerder



In dit voorbeeld ziet u een sleutelgroep met twee sleutels, twee sleutelparen en drie publieke sleutels. De derde kolom toont het vertrouwen dat u hebt in de sleutels. Het eerste sleutelpaar wordt volledig vertrouwd en is ook ingesteld als de standaard sleutel (vet lettertype) terwijl de tweede niet meer geldig is. Twee van de publieke sleutels worden volledig vertrouwd terwijl het vertrouwen van de laatste sleutel marginaal is. De laatste sleutel is uitgevouwen, waarbij het zijn ElGamal-subsleutel toont, een extra gebruikers-id, beide ook met marginaal vertrouwen en enkele van zijn handtekeningen.

Handtekeningen maken het mogelijk door uw sleutelring te lopen. Dubbelklikken op een handtekening of een sleutel die getoond wordt als lid van een groep maakt direct een sprong naar de overeenkomstige primaire sleutel.

3.5.2 Sleuteleigenschappen



Terwijl de sleutelbeheerder het mogelijk maakt om algemene acties met een of meer sleutels, sleutelgroepen of handtekeningen te doen, geeft het venster met sleuteleigenschappen u toegang tot een enkele sleutel. U bereikt het door op in de sleutelbeheerder op Enter te drukken of te dubbelklikken op de sleutel.

In dit venster kunt u de wachtwoordzin van de sleutel en de vervaldatum van uw geheime sleutels wijzigen. Voor alle sleutels kunt u ook het vertrouwen in de eigenaar instellen.

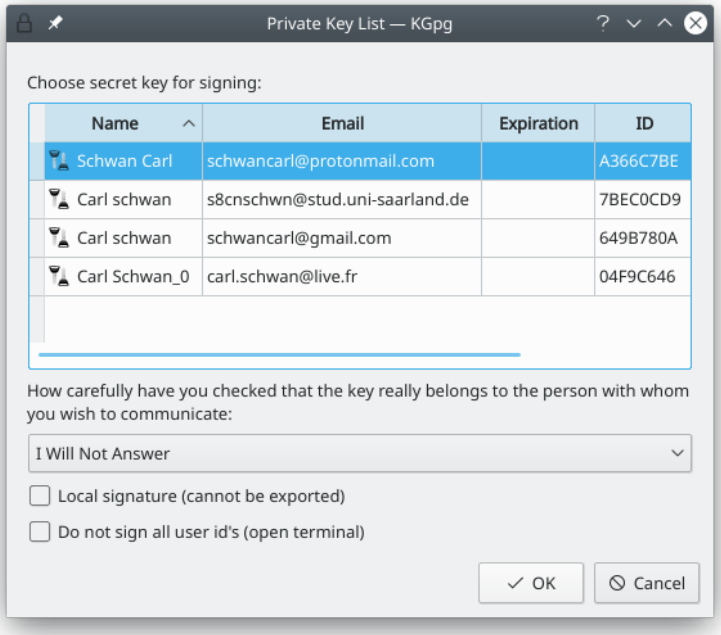
Deze waarde geeft aan hoeveel vertrouwen u hebt in de eigenaar van deze sleutel om op een juiste manier de identiteit van de sleutels die ondertekent na te gaan. Met het vertrouwen in de eigenaar creëert gpg uw eigen web van vertrouwen. U vertrouwt de sleutels die u ondertekent. Als u vertrouwen in de eigenaar toekent aan deze personen dan vertrouwt u ook de sleutels die zij hebben ondertekend zonder de noodzaak dat u eerst hun sleutels ook moet ondertekenen.

3.5.3 Sleutels ondertekenen

Wanneer u een sleutel van iemand anders ondertekent (laten we haar Alice noemen) dan betekent dat dat u er zeker van bent dat deze sleutel echt bij die persoon behoort en dat de sleutel kan worden vertrouwd. Natuurlijk moet u dat echt hebben gecontroleerd. Dit betekent gewoonlijk dat u Alice hebt ontmoet, in elk geval een identiteitskaart hebt gecontroleerd en de volledige vingerafdruk of een kopie van haar sleutel. Daarna gaat u naar huis en ondertekent die sleutel. Daarna is het gebruikelijk dat u de nieuwe ondertekende sleutel naar een sleutelserver stuurt zodat iedereen weet dat u die sleutel hebt gecontroleerd en dat de eigenaar vertrouwd kan worden. Alice zal waarschijnlijk hetzelfde doen zodat u beiden sleutels hebt door elkaar ondertekend. Als een van u geen identiteitskaart bij de hand had dan is dat geen probleem als het ondertekenen slechts in één richting is gedaan.

Maar bedenk eens wat er gebeurt als Alice aan het andere eind van de wereld woont. U communiceert regelmatig met haar maar er is geen mogelijkheid dat u haar spoedig zult zien. Hoe vertrouwt u haar sleutel?

Wanneer u haar sleutel selecteert en daarna **Sleutel ondertekenen...** dan krijgt u de dialoog die u in staat stelt om de opties te kiezen over hoe u die sleutel wilt ondertekenen.



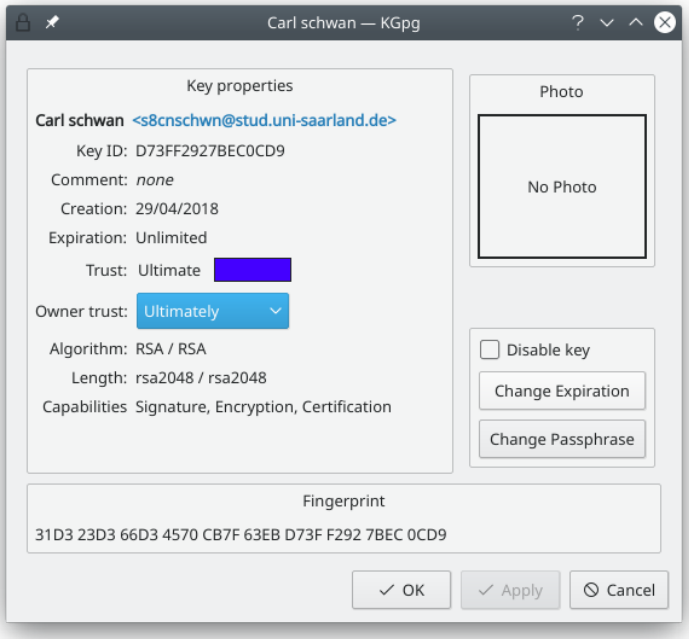
Eerst kiest u de sleutel die u wilt gebruiken om de sleutel te ondertekenen. Daarna kunt u invoeren hoe nauwkeurig u hebt gecontroleerd dat ze werkelijk de persoon is die ze pretendeert te zijn. Deze informatie zal worden opgeslagen samen met de handtekening zodat het een richtlijn is voor ieder ander wie die ondertekening nodig heeft (meer hieronder). En daarna komt de optie die u helpt als u Alice niet in persoon kunt ontmoeten: **Lokale ondertekening (kan niet worden geëxporteerd)**. Wanneer u die optie activeert dan wordt er een speciale versie van een ondertekening gemaakt die nooit, zelfs niet per ongeluk, uw sleutelring kan verlaten.

Maar waarom is het belangrijk om de identiteit van Alice nauwkeurig te controleren? Voor wie is dat belangrijk? Er zijn verschillende manieren om uw probleem met de identiteit van Alice op te lossen. Als u Alice niet spoedig kunt bezoeken denk dan aan Trent. U weet dat Trent ook een sleutelpaar heeft. En Trent is een globetrotter, die twee maal per maand een ander continent bezoekt. Als u geluk hebt dan vliegt hij spoedig naar een plaats dicht bij Alice. Dus gaat u Trent bezoeken om sleutels te ondertekenen. Daarna stuurt u een bericht naar Alice dat Trent spoedig bij haar in de buurt komt en vraagt u haar of zij hen kan ontmoeten om sleutels te ondertekenen. Nadat dit allemaal heeft plaats gevonden weet u dat de sleutel van Trent vertrouwd kan worden en Trent weet dat de sleutel van Alice vertrouwd kan worden. Als u Trent vertrouwd dat hij de identiteit van Alice goed heeft gecontroleerd dan kunt u ook haar sleutel vertrouwen.

Deze relaties tussen sleutels en hun eigenaars vormen een zo genaamd web van vertrouwen. Binnen dat web zijn enkele belangrijke waarden die bepalen hoe betrouwbaar een bepaalde sleutel is. Het eerste is hoe zorgvuldig de identiteit van de sleuteleigenaar is gecontroleerd. Dat is de waarde die u hierboven hebt gezien in het selectievenster van de geheime sleutel. U weet bijvoorbeeld hoe u de identiteitskaart van uw land moet controleren maar een uit een compleet ander land kan moeilijk worden geverifieerd. U kunt dus zeggen dat u zeer zorgvuldig de identiteit van Trent hebt gecontroleerd omdat u zijn identiteitskaart hebt gezien en deze erg veel lijkt op die van u. Maar Trent, hoewel hij de identiteitskaart en het rijbewijs van Alice heeft gezien dan kan hij zeggen dat hij slechts een oppervlakkige controle van haar identiteit heeft gedaan omdat hij niet absoluut zeker is van de documenten uit dat deel van de wereld.

De volgende belangrijke waarde is hoe veel vertrouwen u hebt dat de andere persoon de documenten heeft geverifieerd. U weet dat Trent daar goed in is. Maar bijvoorbeeld George is niet iemand waarvan je zou kunnen zeggen dat hij zorgvuldig is. Hij keek nauwelijks naar uw identiteitskaart toen u hem ontmoette voor ondertekening van sleutels. U bent er zeker van dat George de persoon is die hij voorgeeft te zijn toen u zijn documenten zorgvuldig onderzocht. Maar het kan hem niet veel schelen om echt andere mensen te controleren zodat u veel vertrouwen hebt in

de sleutel van George maar weinig in de ondertekening van George. Als u de eigenschappen van een sleutel opent dan ziet u het veld **Vertrouwen in eigenaar**. Dit is hoeveel vertrouwen u hebt in de eigenaar van de sleutel wanneer hij sleutels ondertekent. Deze waarde zal niet geëxporteerd worden, het is volledig uw persoonlijke voorkeur.



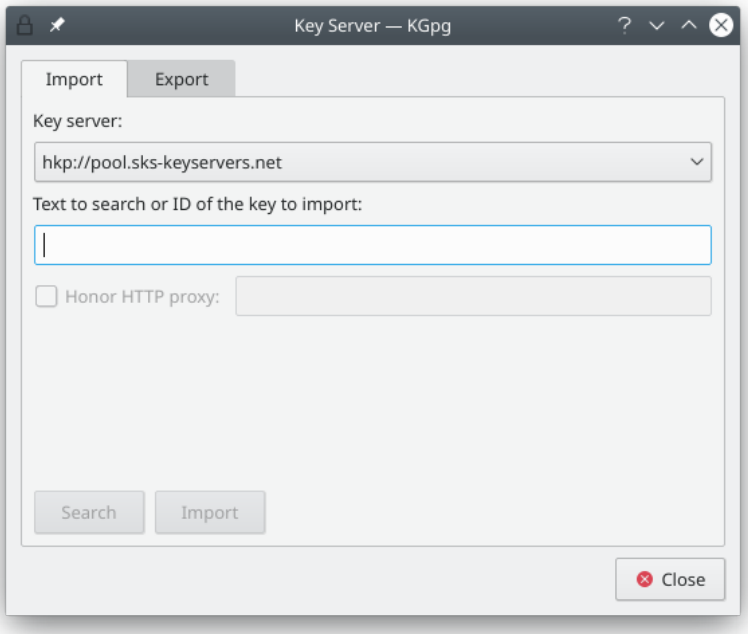
U zou nu een idee moeten hebben over hoe het web van vertrouwen is opgebouwd, waar de waarden van vertrouwen in eigenaar en sleutel voor zijn en waarom u altijd erg voorzichtig moet zijn wanneer u identiteiten controleert: andere mensen kunnen op u vertrouwen. Er is echter één element in het proces dat nog niet is geverifieerd: de e-mailadressen in de sleutels die u hebt ondertekend. Het aanmaken van een nieuwe gebruikersidentiteit in uw sleutel met het e-mailadres van Alice of Trent is slechts een paar muisklikken. U hebt geverifieerd dat Trent echt de eigenaar van deze sleutel is. maar niemand heeft tot nu toe gecontroleerd dat Trent echt de e-mailadressen van zijn gebruikersidentiteiten bezit.

Als u, in plaats daarvan, **Onderteken en stuur e-mail naar gebruikers-id ...** uit het menu kiest dan kunt u dat gat sluiten. Het idee is dat u de sleutel zoals gebruikelijk ondertekent en daarna wordt het opgedeeld in stukken. Elk stuk bevat slechts één gebruikersidentiteit van de sleutel van Trent en uw ondertekening daarin. Dit zal worden versleuteld met de sleutel van Trent en worden verzonden naar het e-mailadres in die identiteit. Alleen Trent kan dit e-mailbericht ontvangen en ontcijferen, hij kan die handtekening importeren in zijn sleutelring. U zult uw handtekeningen niet uploaden, dat is helemaal aan hem. Als uw ondertekening opduikt op een sleutelserver dan bent u er zeker van dat Trent echt de controle heeft over zijn sleutel evenals over het e-mailadres dat u ondertekende. De ondertekening die u in dit proces hebt gemaakt is geen onderdeel van uw sleutelring. Dus direct nadat u de sleutel van Trenthebt ondertekend wordt het nog steeds getoond als niet vertrouwd in uw sleutelring. Nadat Trent uw e-mail heeft ontvangen en uw ondertekening heeft geïmporteerd in zijn sleutelring kan hij ze uploaden naar een sleutelserver. Wanneer u zijn sleutel van een sleutelserver hebt ververst zult u de nieuwe handtekeningen krijgen. Hoewel dat eerst ongemakkelijk mag klinken is maakt het zeker dat u niet per ongeluk een van zijn identiteiten als vertrouwd hebt aangemerkt waarover hij geen controle heeft. Alleen de handtekeningen die opduiken op een sleutelserver zijn die waar iedereen, inclusief u, zeker van kan zijn dat hij echt de controle heeft over de bijbehorende e-mailadressen.

3.6 Werken met sleutelservers

3.6.1 Communicatie met sleutelservers

Het publieke gedeelte van een sleutelpaar is gewoonlijk op een sleutelserver opgeslagen. Deze servers stellen iedereen in staat om naar een sleutel die bij een bepaald persoon of e-mailadres hoort op te zoeken. De ondertekeningen zijn ook op deze servers opgeslagen.

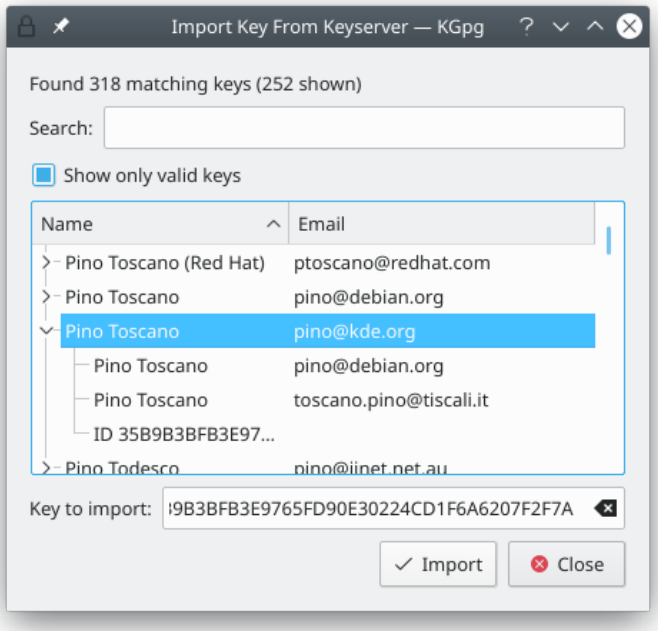


Deze dialoog geeft u toegang tot de sleutelservers. U kunt er in zoeken en sleutels importeren evenals sleutels exporteren. Een voorbeeld van het zoeken en importeren is wanneer u een e-mail naar een nieuw iemand wilt sturen. Als u de e-mail naar uw contactpersoon wilt versleutelen dan kunt u opzoeken of hij of zij een publieke sleutel heeft op de sleutelservers. Als u een nieuw sleutelpaar hebt aangemaakt of de sleutel van iemand anders hebt ondertekend, dan kunt u de publieke sleutel exporteren (mogelijk met nieuwe handtekeningen) naar een sleutelserver.

De meeste sleutelservers synchroniseren hun gegevens onderling zodat u gelijke resultaten krijgt onafhankelijk van welke server u gebruikt. Omdat er uitzonderingen op deze regel zijn kunt u de te gebruiken sleutelserver in deze dialoog kiezen. Het is in het lagemeen een goed idee om een standaard sleutelserver te kiezen die dichtbij staat (bijv. in uw land of op uw continent) omdat deze gewoonlijk sneller antwoord geveb op uw vragen.

Opmerking: alles wat u naar een sleutelserver uploadt blijft daar gewoonlijk voor eeuwig. Dat is een reden dat u de leeftijd van uw sleutels moet beperken. Merk ook op dat de sleutelservers soms worden gescand door spammers op e-mailadressen.

3.6.2 Zoekresultaten van sleutelservers



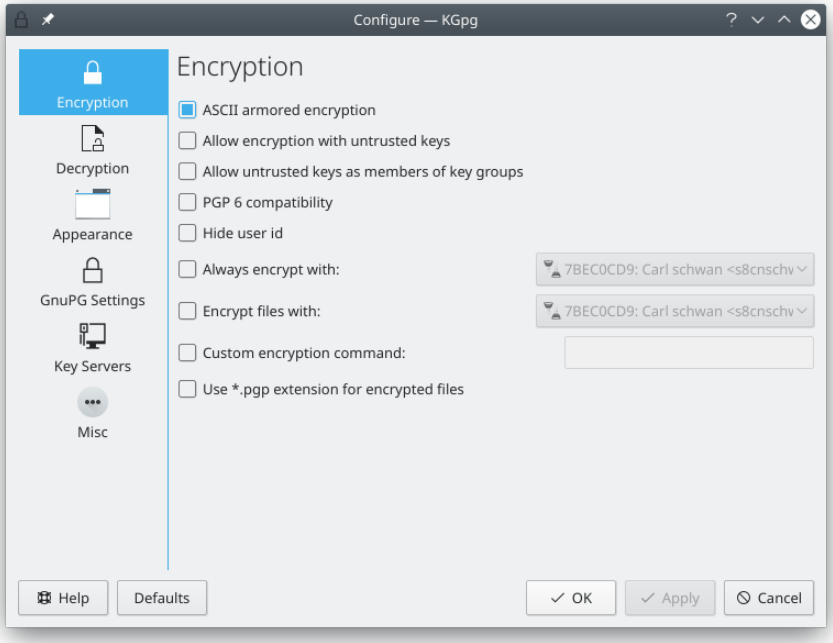
Alle resultaten van een zoekopdracht worden weergegeven in dit vesnter. Deze afbeelding toont een zoekopdracht naar adressen met ˝@kde.org˝ die tot 244 resultaten laten zien. Met het zoekveld wordt de weergegeven lijst gereduceerd tot een enkele sleutel. Deze sleutel heeft twee overeenkomsten: de primaire gebruikers-id zelf komt overeen met de zoektekst evenals een van de andere gebruiker-id's.

U kunt een of meer sleutels selecteren voor importeren. De id's van deze sleutels worden getoond in het veld **Te importeren sleutels** onderaan het venster. Wanneer u klikt op **Importeren** zal de sleutelserver opnieuw worden benaderd en de sleutels worden opgehaald naar uw sleutelring.

3.7 Het instellen van KGpg

Instellen van KGpg is mogelijk in het menu van de applet van KGpg (met rechtermuisknop op het applet klikken) of via het hoofdmenu (**Instellingen** → **KGpg instellen**). U kunt de standaard parameters instellen voor versleutelen, ontcijferen, gebruikersinterface en applet. De meeste opties hebben direct verband met gpg en zijn in de man-pagina ervan gedocumenteerd.

3.7.1 versleuteling (encryptie)



Hier kunt u speciale opties confugureren die aan GnuPG gegeven worden om het gedrag van de versleuteling te wijzigen. Voor een gedetailleerde beschrijning wordt u verwezen naar de handleiding van GnuPG.

- **Versleutelde bestanden in ASCII opslaan**: dit veroorzaakt dat versleutelde bestanden worden opgeslagen in een formaat dat alleen te printen ASCII-tekens bevat en korte regels. Bestanden die op die manier worden opgeslagen zijn groter dan de bestanden die in een binair formaat worden opgeslagen maar kunnen gemakkelijker bijv. per e-mail worden verzonden.
- **Versleuteling toestaan met niet -vertrouwde sleutels**: dit stelt u in staat om bestanden te versleutelen met sleutels die u niet vertrouwt.
- **PGP 6 compatibiliteit**: versleutelde bestanden zijn compatibel met de oudere PGP6-standaard. Dit schakelt bepaalde mogelijkheden uit, zodat u dit alleen moet gebruiken als het echt nodig is.
- **Gebruikers-id verbergen**: dit verwijdert alle bewijs van de ontvanger van het versleutelde be.tand In het geval dat de overdracht wordt afgeluisterd kan niemand de informatie over de ontvanger uit het bestand afleiden. Als de ontvanger meerdere sleutels heeft, dan moet hij proberen welke is gebruikt.
- **Altijd versleutelen met**: alle versleutelingen worden ook versleuteld met deze sleutel. Als u deze instelt voor uw privé sleutels dan kunt u later alles wat u hebt versleuteld lezen ten koste van een groter bericht.
- **Bestanden versleutelen met**: gedraagt zich voor het versleutelen van bestanden als **Altijd versleutelen met**.
- **Aangepast commando voor versleuteling**: als u ongebruikelijke opties aan GnuPG wilt meegeven, dan kunt u de commandoregel hier specificeren. De meeste gebruikers zullen dit niet nodig hebben.
- **De extensie *.pgp voor versleutelde bestanden gebruiken**: als u deze optie activeert zullen versleutelde bestanden de naam van het invoerbestand krijgen met de extensie `.pgp` toegevoegd, anders wordt de extensie `.gpg` gebruikt.

3.7.2 Ontcijfering (decryption)

Hier kunt u een eigen commando voor ontcijfering specificeren. Deze optie is zelden nodig en is alleen bruikbaar voor geavanceerde gebruikers die kennis hebben van de opties op de commandoregel van GnuPG.

3.7.3 Uiterlijk

U kunt hier de manier waarop KGpg er uit ziet instellen. Mogelijke instellingen zijn de kleuren die de verschillende niveaus van het vertrouwen in de sleutel weergeven in de sleutelbeheerder en de instellingen van het lettertype voor de editor.

3.7.4 GnuPG-instellingen

U kunt hier instellen welk gpg-uitvoerbaar bestand, welk **configuratiebestand** en welke persoonlijke map worden gebruikt. Deze waarden worden automatisch gedetecteerd bij de eerste start en zouden al moeten werken.

GnuPG-agent gebruiken maakt het werken met GnuPG comfortabeler omdat het niet nodig is om uw wachtwoord voor elke actie in te voeren. Het wordt een poosje in geheugen opgeslagen zodat elke bewerking die een wachtwoord vereist onmiddellijk gedaan kan worden. Merk op dat dit andere mensen kan toestaan om uw privé sleutels te gebruiken als u uw sessie voor hen toegankelijk maakt.

3.7.5 Sleutelservers

U kunt hier een lijst met sleutelservers aanmaken die aan u getoond worden wanneer u de sleutelserverdialoog opent. Als u GnuPG gebruikt vanaf de commandoregel zal alleen de sleutelserver, die u als standaard hebt ingesteld, hier worden gebruikt.

Het protocol dat wordt gebruikt voor de communicatie met de sleutelservers is gebaseerd op HTTP, zodat het in sommige omgeving zinvol is om **gebruik de HTTP-proxy indien beschikbaar**.

3.7.6 Diversen

Deze sectie laat u de instelling van enige verschillende mogelijkheden, die niet in de andere secties passen, zien. U kunt bijvoorbeeld **KGpg automatisch starten bij aanmelden** instellen. De optie **Muisselectie gebruiken in plaats van klembord** wijzigt of de selectie gedaan wordt met de muis en plakken door de middelste muisknop of dat alle bewerkingen gedaan worden door sneltoetsen.

U kunt ook het pictogram van KGpg in het systeemvak laten zien of niet en welke actie genomen wordt als er op het pictogram wordt geklikt met de linkermuisknop. Als het pictogram in het systeemvak wordt getoond dan wordt bij het sluiten van het KGpg-venster de toepassing geminimaliseerd naar het systeemvak. Als het pictogram niet getoond wordt zal KGpg eindigen wanneer alle vensters worden gesloten.

Hoofdstuk 4

Dankbetuigingen en Licentie