Підручник з KGpg

Jean-Baptiste Mardelle
Rolf Eike Beer
Переклад українською: Юрій Чорноіван

Підручник з KGpg

Зміст

1 Вступ 5

2 Початок роботи 6

3 Користування KGpg 8
- 3.1 Створення ключа . . . 8
- 3.2 Відкликання ключа . . . 9
- 3.3 Шифрування ваших даних . . . 9
  - 3.3.1 Шифрування файла з Konqueror або Dolphin . . . 9
  - 3.3.2 Шифрування тексту за допомогою аплету KGpg . . . 10
  - 3.3.3 Шифрування тексту з редактора KGpg . . . 10
- 3.4 Розшифрування ваших даних . . . 11
  - 3.4.1 Розшифрування файла з Konqueror або Dolphin . . . 11
  - 3.4.2 Розшифрування тексту за допомогою аплету KGpg . . . 11
  - 3.4.3 Розшифрування тексту з редактора . . . 11
- 3.5 Керування ключами . . . 11
  - 3.5.1 Засіб для керування ключами . . . 11
  - 3.5.2 Властивості ключів . . . 12
  - 3.5.3 Підписування ключів . . . 12
- 3.6 Робота з серверами ключів . . . 15
  - 3.6.1 Обмін інформацією з серверами ключів . . . 15
  - 3.6.2 Результати пошуку на сервері ключів . . . 16
- 3.7 Налаштовування KGpg . . . 16
  - 3.7.1 Шифрування . . . 17
  - 3.7.2 Розшифрування . . . 17
  - 3.7.3 Вигляд . . . 18
  - 3.7.4 Параметри GnuPG . . . 18
  - 3.7.5 Сервери ключів . . . 18
  - 3.7.6 Інше . . . 18

4 Подяки і ліцензія 19

Анотація

KGpg — це простий графічний інтерфейс до GnuPG (https://gnupg.org).

Розділ 1

Вступ

KGpg — це простий інтерфейс до GnuPG, потужного засобу для шифрування. Програму GnuPG (також відому як gpg) включено до більшості дистрибутивів, її слід встановити у вашу систему. Останню версію цієї програми ви можете знайти за адресою https://gnupg.org.

За допомогою KGpg ви зможете шифрувати і розшифровувати ваші файли і листи електронної пошти, ця програма зробить ваш обмін інформацією безпечнішим. Невеличкий список рецептів дій щодо шифрування за допомогою gpg можна знайти на вебсайті GnuPG.

Якщо ви використовуватимете KGpg, вам не потрібно буде пам'ятати всі команди і параметри командного рядка gpg. Майже всі дії можна виконати за допомогою декількох клацань кнопками миші.

Розділ 2

Початок роботи

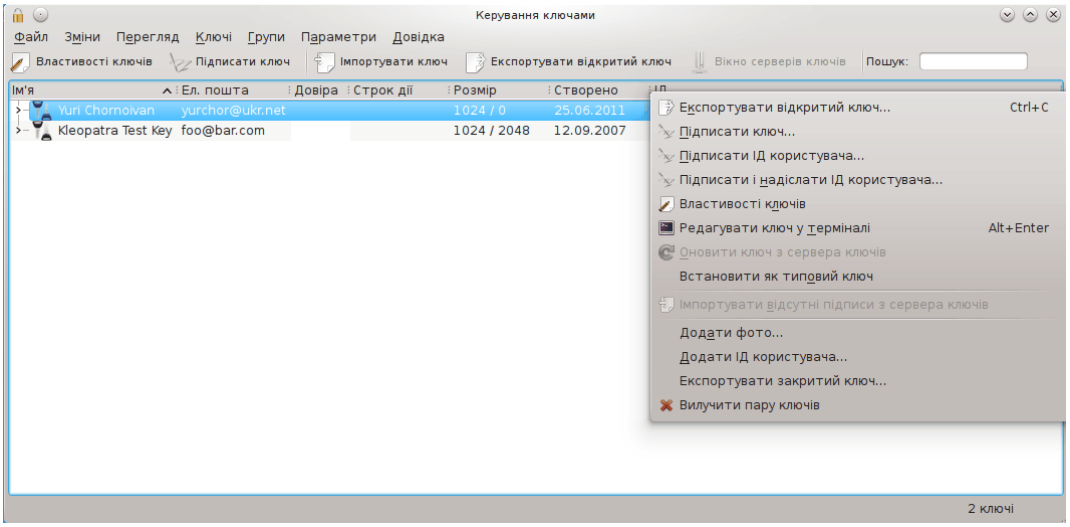
Ось список основних компонентів KGpg:

Піктограма у системному лотку

Після запуску KGpg у системному лотку з'являється його піктограма. Якщо ви наведете на неї вказівник миші і клацнете лівою кнопкою, відкриється вікно Засобу керування ключами, тоді як клацання правою кнопкою надасть вам доступ до меню, яке дозволить вам швидко доступитися до декількох важливих можливостей програми. Якщо ви бажаєте змінити параметри, наприклад дію програми у відповідь на клацання лівою кнопкою миші (наказати програмі відкривати вікно редактора або повністю вимкнути піктограму системного лотка), ви можете це зробити за допомогою діалогового вікна параметрів програми.

Будь ласка, зауважте, що піктограма системного лотка KGpg перебуватиме у стані «неактивна» майже весь час. Оскільки зазвичай у системному лотку неактивні піктограми приховуються, піктограму KGpg не буде показано, якщо ви явним чином не накажете її показувати. Щоб дізнатися більше, зверніться до документації з Плазми.

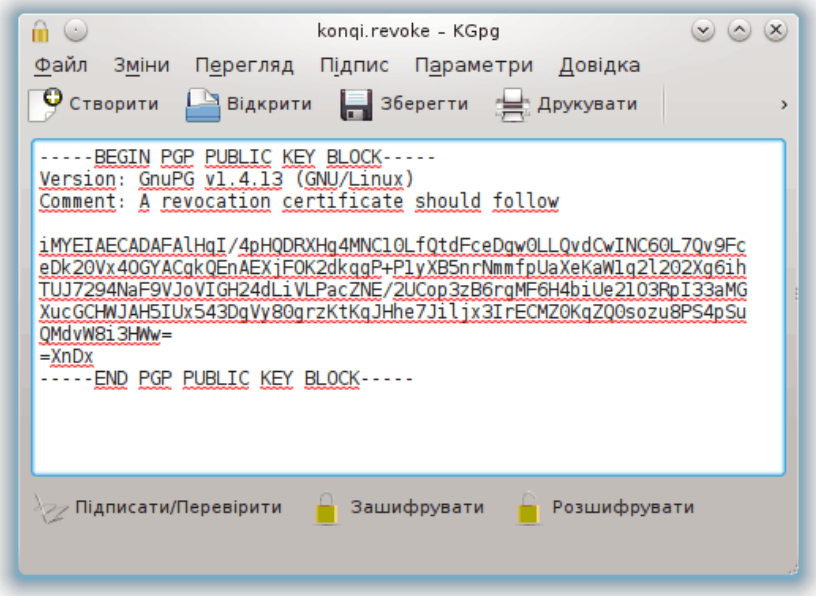
Вікно засобу керування ключами



Це основний засіб для керування вашими ключами. Щоб відкрити Вікно засобу керування ключами, наведіть вказівник миші на аплет KGpg і клацніть лівою кнопкою. За

допомогою цього вікна ви зможете імпортувати, експортувати, підписувати і змінювати ваші ключі. Більшість з цих дій можна виконати за допомогою наведення вказівника миші на запис ключа з наступним клацанням правою кнопкою миші.

Вікно редактора



Це простий текстовий редактор, у якому ви можете набрати або вставити текст, який слід зашифрувати або розшифрувати. Щоб відкрити вікно редактора, наведіть вказівник миші на аплет KGpg і клацніть правою кнопкою.

Інтеграція до засобу керування файлами

KGpg інтегровано до Konqueror і Dolphin. Це означає, що після того, як ви наведете вказівник на значок файла і клацнете правою кнопкою, ви зможете обрати з контекстного меню Дії → Зашифрувати файл, щоб зашифрувати файл. Розшифрувати файл можна наведенням на його позначку вказівника миші з наступним клацанням лівою кнопкою миші.

Розділ 3

Користування KGpg

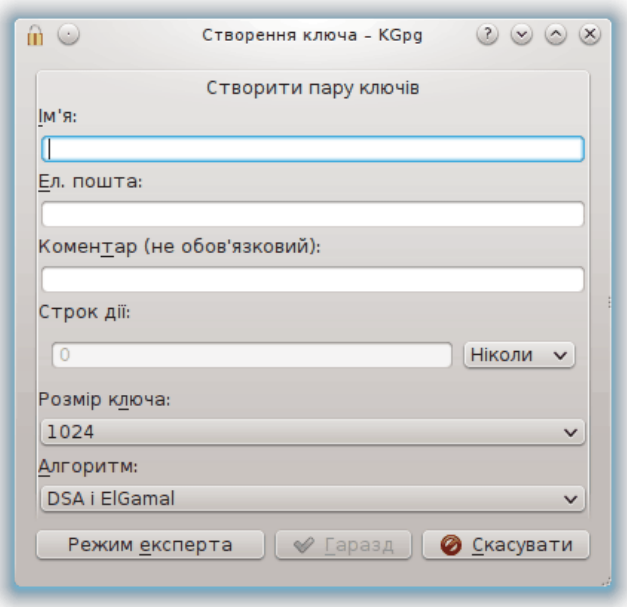
Існує два способи шифрування ваших даних:

- Симетричне шифрування: ваші дані просто шифруються за допомогою пароля. Будь-хто, на чийому комп'ютері встановлено gpg, може розшифрувати ваше повідомлення, якщо ви надасте йому чи їй пароль до нього. Щоб виконати симетричне шифрування, оберіть «симетричне шифрування» у полі параметрів, коли програма попросить вас ввести ключ шифрування.
- Шифрування ключем: спершу ви маєте створити вашу пару ключів (закритий ключ і відкритий ключ) і вказати пароль. Ваш закритий ключ слід зберігати у безпечному місці, а відкритим ключем слід поділитися з вашими друзями. Після цього, якщо ви бажатимете надіслати зашифроване повідомлення Василеві, ви повинні будете зашифрувати повідомлення відкритим ключем Василя. Щоб розшифрувати повідомлення, отримувачу знадобляться закритий ключ Василя і пароль.

Шифрування ключем трохи складніше (вам слід обмінятися ключами з вашими друзями), але воно також є безпечнішим. Запам'ятайте: якщо ви зашифруєте повідомлення чужим ключем, ви не зможете розшифрувати цю інформацію. Ви можете розшифровувати лише повідомлення, які було зашифровано вашим відкритим ключем.

3.1 Створення ключа

Якщо у вас немає ключа, KGpg автоматично відкриє діалогове вікно створення ключа під час першого запуску програми. Відкрити це вікно можна також у засобі керування ключами за допомогою пункту меню Ключі → Створити пару ключів.



У цьому вікні вам слід просто ввести ваше ім'я, адресу електронної пошти і натиснути кнопку Гаразд. Ці дії призведуть до створення стандартного ключа gpg. Якщо вам потрібен доступ до додаткових параметрів, натисніть кнопку Режим експерта: буде відкрито вікно Konsole з усіма параметрами gpg.

Багато користувачів, граючись зі своїм першим ключем, створюють погано сформовані ідентифікатори користувача, додають коментарі, про які згодом почнуть жалкувати, або просто забувають власний пароль. Щоб запобігти довічній чинності таких ключів, зазвичай, непогано обмежити строк його дії приблизно дванадцятьма місяцями. Ви можете змінити строк дії ваших закритих ключів пізніше за допомогою вікна властивостей ключа.

3.2 Відкликання ключа

Пару ключів, строк дії якої сплив, можна поновити, якщо у когось є доступ до закритого ключа і він знає пароль. Щоб надійно вилучити непотрібний ключ, вам слід його відкликати. Відкликання виконується додаванням до ключа особливого підпису відкликання.

Цей підпис відкликання можна створити разом з самим ключем. Підпис зберігатиметься у окремому файлі. Цей файл пізніше можна імпортувати до сховища ключів, а потім долучити до ключа для позначення його як непридатного до використання. Будь ласка, зауважте, що для імпортування цього підпису до ключа не потрібно вказувати пароль. Тому вам слід зберігати підпис відкликання у надійному місці, зазвичай окремо від пари ключів. Варто зберігати такий підпис на портативному пристрої зберігання даних, не з'єднаному з комп'ютером постійно, або просто надрукувати підпис на папері.

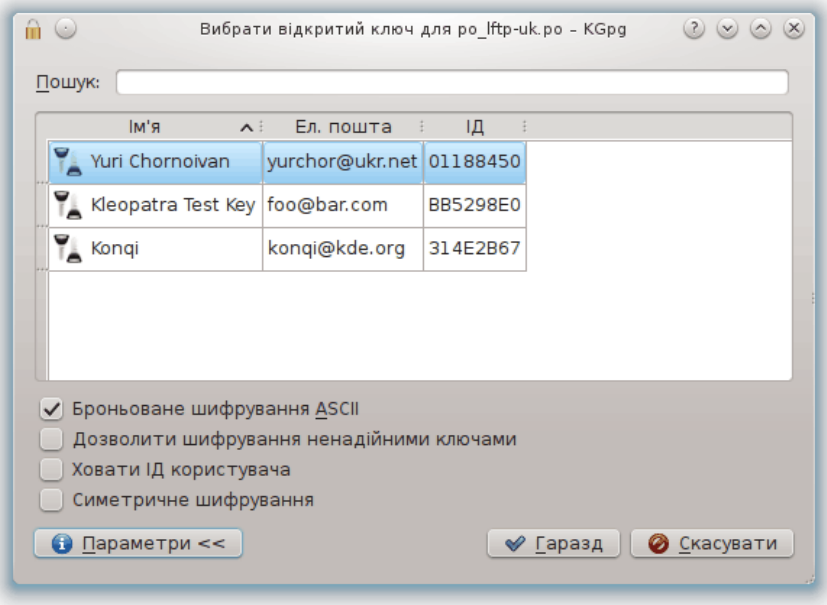
Якщо вам не створено такого підпису відкликання під час створення самого ключа, ви можете створити підпис відкликання за допомогою пункту меню Ключі → Відкликати ключ і, якщо потрібно, негайно імпортувати підпис до вашого сховища ключів.

3.3 Шифрування ваших даних

3.3.1 Шифрування файла з Konqueror або Dolphin

Наведіть вказівник миші на позначку файла, який ви бажаєте зашифрувати, і клацніть правою кнопкою. Виберіть з контекстного меню пункт Дії → Зашифрувати файл. Програма відкриє діалогове вікно вибору відкритого ключа. Оберіть ключ отримувача і натисніть кнопку

Зашифрувати. Зашифрований файл буде збережено з суфіксом .asc або .gpg, залежно від того, вибрали ви Броньоване шифрування ASCII, чи ні. У зашифрованих файлах ASCII містяться лише звичайні друковані символи, вміст таких файлів придатніший для копіювання і надсилання електронною поштою, але розмір їх приблизно на третину більший за звичайний.



3.3.2 Шифрування тексту за допомогою аплету KGpg

Ви можете зашифрувати вміст буфера, якщо оберете пункт Зашифрувати кишеню з меню аплету. Якщо ж ви оберете пункт Підписати кишеню, замість шифрування буде виконано операцію підписування тексту. За використання будь-якої з описаних вище дій поточний вміст буфера обміну даними буде імпортовано до вікна редактора, програма виконає відповідну дію і вставить отримані дані до вікна редактора.

3.3.3 Шифрування тексту з редактора KGpg

Виконати вказану вище дію дуже просто: натисніть кнопку Зашифрувати. У відповідь програма відкриє діалогове вікно вибору відкритого ключа. Виберіть потрібний ключ і натисніть кнопку Гаразд. Зашифроване повідомлення з'явиться у вікні редактора.

Зазвичай, зашифрувати файли можна лише за допомогою ключів, які ви вважаєте надійними. Оскільки іноді у вас може виникати потреба у надсиланні конфіденційного повідомлення певним випадковим особам, яким ви не бажаєте довіряти ваш ключ GPG, ви можете позначити пункт Дозволити шифрування ненадійними ключами.

Щоб забезпечити можливість розшифрування всіх файлів, які ви зашифрували, навіть якщо їх було зашифровано чужим ключем, ви можете скористатися пунктами Завжди шифрувати цим ключем і Зашифровувати файли за допомогою, які можна знайти у вікні налаштування KGpg.

Щоб дізнатися більше про параметри шифрування Броньоване шифрування ASCII, Дозволити шифрування ключами без довіри та Симетричне шифрування, зверніться до документації з gpg або сторінок довідника (man) програми.

3.4 Розшифрування ваших даних

3.4.1 Розшифрування файла з Konqueror або Dolphin

Наведіть вказівник миші на позначку файла, який ви бажаєте розшифрувати, і клацніть лівою кнопкою миші. Введіть ваш пароль і файл буде розшифровано. Крім того, ви можете перетягнути зашифрований текст і скинути його у вікно редактора KGpg. Програма запитає вас про пароль, а потім відкриє розшифрований текст у вікні редактора KGpg. Ви можете скидати у це вікно навіть нелокальні файли! Крім того, ви можете скористатися пунктом Файл → Розшифрувати файл, а потім обрати файл, який слід розшифрувати.

3.4.2 Розшифрування тексту за допомогою аплету KGpg

Крім того, ви можете розшифровувати вміст буфера за допомогою пункту меню Розшифрувати кишеню аплету KGpg. Програма відкриє вікно редактора з розшифрованим текстом.

3.4.3 Розшифрування тексту з редактора

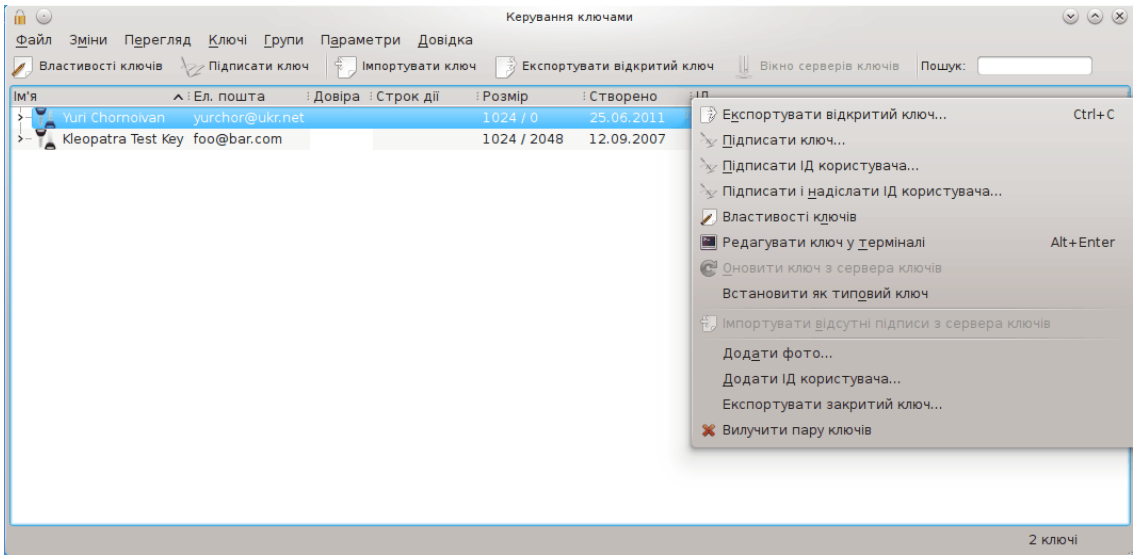
Скопіюйте або перетягніть і скиньте текст, який ви бажаєте розшифрувати, а потім натисніть кнопку Розшифрувати. Програма запитає вас про пароль.

3.5 Керування ключами

За допомогою KGpg можна виконати всі базові операції з керування ключами. Щоб відкрити вікно керування ключами, наведіть вказівник на аплет KGpg і клацніть лівою кнопкою миші. Доступ до більшості операцій можна отримати наведенням вказівника миші на запис ключа з наступним клацанням правою кнопкою миші. Для того, щоб імпортувати або експортувати відкриті ключі, ви можете скористатися перетягуванням і скиданням або клавіатурними скороченнями для копіювання або вставляння.

Відкритий ключ можна експортувати за допомогою електронної пошти на сервер ключів або до локального файла. За допомогою пунктів діалогового вікна експортування ви можете наказати програмі експортувати усі дані, експортувати без атрибутів (фотоідентифікаторів) або експортувати лише ключ, тобто ключ із підключами, але без усіх підписів.

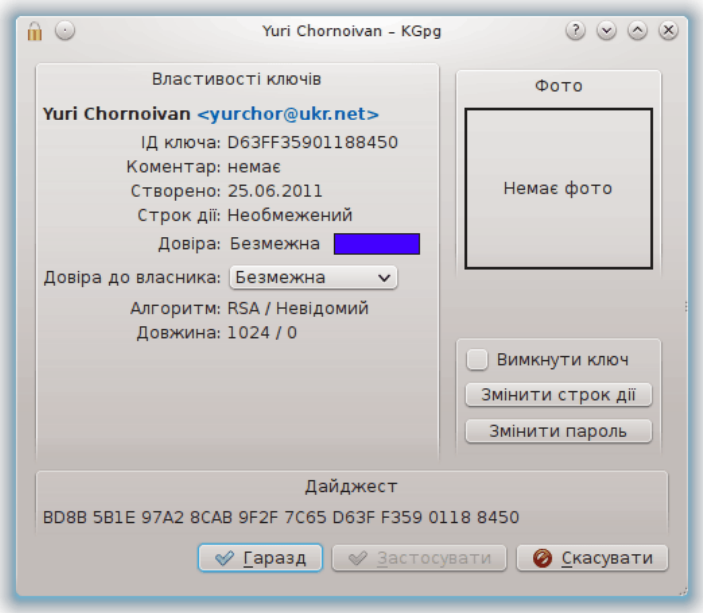
3.5.1 Засіб для керування ключами



На цьому прикладі ви можете спостерігати за групою ключів, у якій міститься два ключі, дві пари ключів і три відкриті ключі. У третьому стовпчику таблиці показано рівень довіри до цих ключів. До першої пари ключів встановлено необмежений рівень довіри, вона є типовою парою ключів (виділено напівжирним шрифтом), а строк дії другої пари ключів минув. До двох з відкритих ключів встановлено повну довіру, а до останнього ключа — обмежену. Дані останнього ключа розгорнуто, серед них видно його підключ EIGamal, додатковий ідентифікатор користувача, обидва з обмеженим рівнем довіри, а також декілька з підписів цього ключа.

Підписи надають вам змогу пересуватися вашим набором ключів. Наведення вказівника на підпис або ключ, показаний як елемент групи, з наступним подвійним клацанням лівою кнопкою миші миттєво відкриє відповідний головний ключ.

3.5.2 Властивості ключів



Вікно засобу керування ключами надає вам змогу виконувати загальні дії з одним або декількома ключами, групами ключів або підписами, а вікно властивостей ключів надає вам доступ до окремого ключа. Відкрити це вікно можна за допомогою натискання клавіші enter у засобі керування ключами або наведенням вказівника миші на запис ключа з наступним подвійним клацанням лівою кнопкою.

У цьому вікні ви зможете змінити пароль або строк дії ваших закритих ключів. Крім того, ви можете встановити рівень довіри до власника ключа.

Це значення визначає те, наскільки ви довіряєте власнику цього ключа щодо перевірки ідентичності ключів, якими він чи вона підписує повідомлення. Беручи до уваги рівні довіри до власників ключів, gpg створює вашу власну мережу довіри. Ви довіряєте ключам, які ви підписали. Якщо ви призначаєте рівень довіри до цих осіб, ви також довіряєте ключам, якими вони підписуються: вам не потрібно спочатку також підписувати ці ключі.

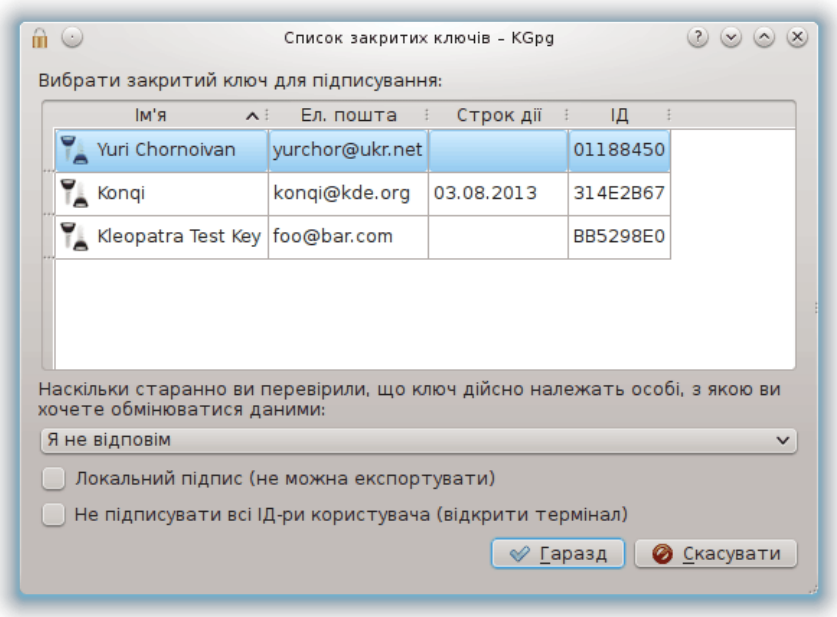
3.5.3 Підписування ключів

Якщо ви підписуєте ключ іншої особи (наприклад якоїсь Аліси), ви підтверджуєте, що ви впевнені у тому, що цей ключ насправді належить відповідній особі і що вважаєте цей ключ надійним. Звичайно ж, все це треба спочатку перевірити. Це має означати, що ви повинні зустрітися з Алісою, перевірити її особу хоча б за одним документом і отримати повний відбиток ключа або копію її ключа. Після цього ви можете підписати її ключ. Зазвичай,

пізніше підписаний ключ слід вивантажити на сервер ключів, щоб всі могли перевірити, чи можна довіряти цьому ключу і чи надійним є його власниця. Аліса, ймовірно, може виконати ті самі дії щодо вашого ключа, отже ваші ключі буде обопільно підтверджено. Якщо у когось з вас не виявиться документа, що підтверджує особу, можна обмежитися одностороннім підписуванням.

Але що робити, якщо Аліса живе у іншому кінці світу? Ви регулярно спілкуєтеся з нею, але особиста зустріч найближчим часом є малоймовірною. Як можна вважати її ключ надійним?

Після вибору її ключа з наступним використанням пункту Підписати ключ... програма відкриє діалогове вікно з параметрами підписування ключа.



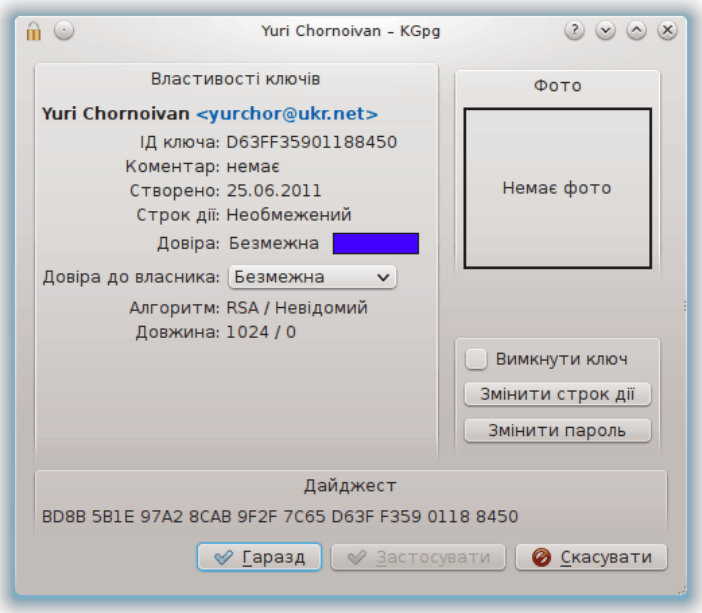
Спочатку вам слід вибрати ключ, який буде використано для підписування іншого ключа. Після цього ви маєте вказати, наскільки ретельно ви перевірили ідентичність особи власника ключа. Вказані відомості буде збережено разом з підписом, отже може допомогти будь-кому, кому може знадобитися відповідний підпис (докладніше про це нижче). Нижче буде наведено пункт, який допоможе вам, якщо ви не зустрічалися з Алісою особисто: Локальний підпис (не можна експортувати). Якщо ви позначите цей пункт, буде створено особливу версію підпису, яка ніколи, навіть випадково, не вийде за межі вашого сховища ключів.

Але чому так важливо з відповідальністю ставитися до перевірки особи Аліси? Можливо, слід забути про обережність? Існує ще один спосіб розв'язати нашу проблему з Алісою. Якщо ви не можете особисто зустрітися з Алісою, можна скористатися послугами, скажімо, Віктора. Вам відомо, що у Віктора теж є пара ключів (закритий і відкритий). Віктор подорожує по світу, буває на інших континентах принаймні двічі на місяць. Можливо, він невдовзі відвідуватиме якесь з місць, розташованих неподалік від місця проживання Аліси. Отже ви можете зустрітися з Віктором і підписати ключі один одного. Після цього ви можете повідомити Алісу, що Віктор невдовзі перебуватиме у відрядженні неподалік від місця, де вона живе, і попросити її зустрітися з Віктором і підписати ключі один одного. Після виконання відповідних процедур ви знатимете, що ключ Віктора є надійним, а Віктор знатиме, що надійним є ключ Аліси. Якщо ви впевнені, що Віктор ретельно перевірив особу Аліси, ви можете вважати ключ Аліси надійним.

Подібні співвідношення надійності ключів та їх власників формують так звані мережі довіри. У такій мережі довіри існують важливі параметри, які визначають ступінь надійності окремих ключів. Першим з них є ступінь ретельності перевірки, яку пройшов власник ключа. Значення цього параметра можна бачити над записом ключа у вікні вибору закритого ключа. Наприклад, ви з легкістю можете перевірити достовірність паспорта вашої країни, але таку перевірку буде важко виконати іноземцеві. Отже можна сказати, що ви дуже ретельно перевірили особу Віктора, оскільки його посвідчення особи дуже подібне до вашого. Але Віктор, хоча він і бачив посвідчення особи та водійське посвідчення Аліси, може сказати, що

було виконано лише поверхневу перевірку особи, оскільки йому не відома можлива ступінь довіри до документів відповідної країни.

Наступним важливим параметром є ступінь довіри до особи, яка перевіряла документи. Наприклад, вам може бути відомо, що Віктор виконує перевірку дуже ретельно, але на Ярослава не можна покластися у подібних питаннях (він не став перейматися перевіркою ваших документів, коли ви підписували ключі один одному). Ви впевнені, що Ярослав є саме тією людиною, за яку себе видає, оскільки ретельно перевірили його документи, але, здається, самому Ярославові такі перевірки видаються зайвими. Отже ступінь довіри до ключа Ярослава має бути високою, але ступінь довіри до підписів Ярослава — дуже низькою. Якщо ви відкриєте вікно властивостей ключа Ярослава, ви побачите поле з назвою Довіра до власника. За допомогою цього поля ви можете вказати ступінь довіри до власника, у разі підписування ним чи нею інших ключів. Значення цього поля не експортуватиметься, його значення є лише вашим особистим враженням щодо власника ключа.



Отже тепер вам відома основна ідея, на якій побудовано мережу довіри, для чого призначено параметри надійності ключа і його власника і чому вам завжди слід ретельно перевіряти особу власників: інші люди не зможуть покластися на вас, якщо ви цього не робитимете. Але залишається ще один елемент у процесі, який ми ще не перевіряли: адреса електронної пошти у ключах, які ви підписуєте. Для створення для вашого ключа нового запису користувача з адресою електронної пошти Аліси або Віктора достатньо декількох клацань кнопками миші. Віктор підтверджує, що ви є власником вашого ключа. Але ніхто не перевіряв, чи справді ви контролюєте адресу електронної пошти, пов'язану з вашим профілем користувача.

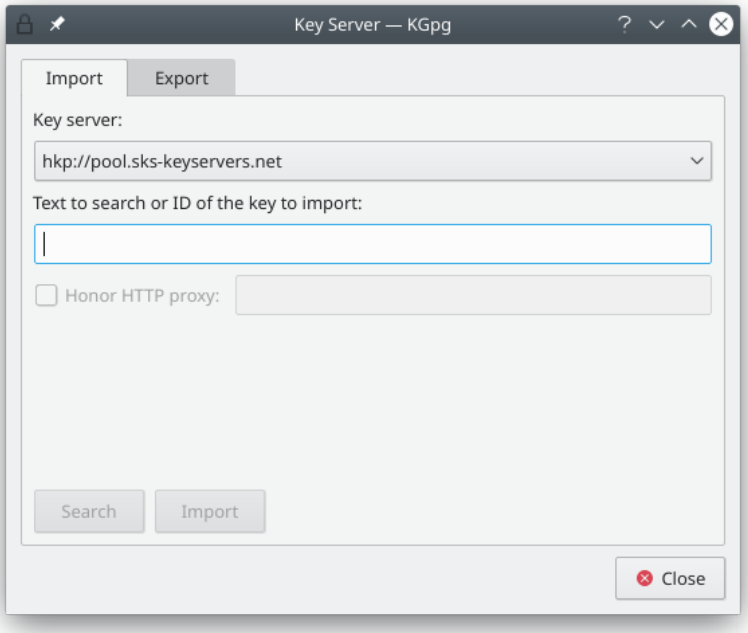
Якщо ви скористаєтеся пунктом меню Підписати і надіслати ІД користувача..., і цей недолік можна усунути. Ідея полягає у тому, що ви підпишете ключ у звичайному режимі, а потім підпис буде розбито на частини. Кожна з частин міститиме лише один профіль користувача ключа Віктора і ваш підпис цього ключа. Їх буде зашифровано за допомогою ключа Віктора і надіслано на адресу електронної пошти, вказану у профілі. Віктор зможе імпортувати підпис до власного сховища ключів, лише якщо отримає відповідне повідомлення електронної пошти і розшифрує його. Ви не будете вивантажувати ваш підпис на сервер: Віктор має зробити це самостійно. Якщо ваш підпис з'явиться на сервері ключів, ви можете бути певні, що Віктор контролює свій ключ і відповідну адресу електронної пошти. Створені вами протягом процедури підписи також не буде додано до вашого сховища ключів. Отже після підписування ключа Віктора, його буде показано у вашому сховищі як ненадійний. Після отримання Віктором вашого повідомлення електронної пошти та імпортування вашого підпису до сховища ключів, він може вивантажити відповідні дані на сервер ключів. Після оновлення ключа Віктора з сервера ключів ви отримаєте нові підписи. Загалом все це може видатися незручним, але таким чином ви можете убезпечитися від визнання надійним ключа, адресу електронної пошти якого власник ключа не контролює. Лише поява підписів на

сервері ключів надасть певності кожному, зокрема і вам, у тому, що власник ключа справді контролює адресу електронної пошти, пов'язану з ключем.

3.6 Робота з серверами ключів

3.6.1 Обмін інформацією з серверами ключів

Відкриту частину пари ключів, зазвичай, зберігають на сервері ключів. Ці сервери надають змогу всім знаходити ключі, що належать певній особі або адресі електронної пошти. Підписи також зберігаються на цих серверах.

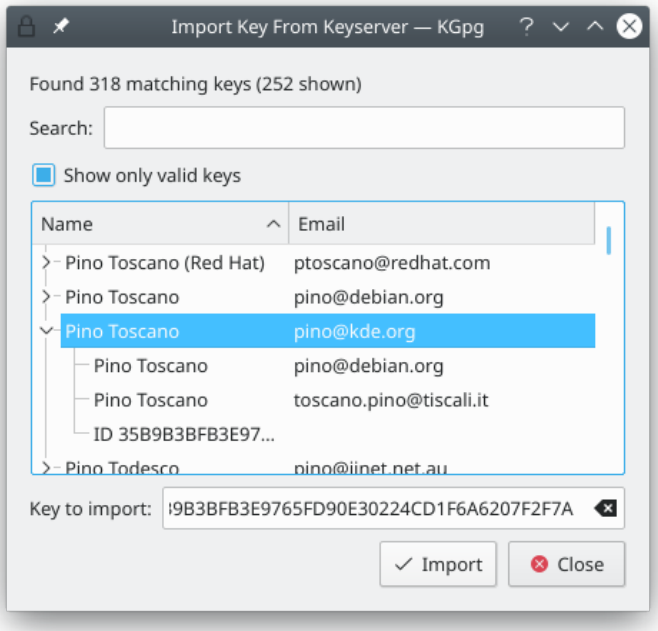


Це діалогове вікно надає вам доступ до цих серверів ключів. За його допомогою ви можете шукати та імпортувати ключі з сервера ключів, а також експортувати ключі на сервер. Прикладом пошуку і імпортування може бути випадок, коли вам слід написати листа якійсь новій особі. Якщо ви бажаєте зашифрувати ваш лист до цього контакту, ви можете пошукати його чи її ключ на серверах ключів. Якщо ви створити нову пару ключів або підписали чужий ключ, ви можете експортувати відкритий ключ (можливо з новими підписами) на сервер ключів.

Більшість серверів ключів синхронізують свої дані один з одним, отже, ви отримаєте однакові результати пошуків на кожному з таких серверів. Оскільки з цього правила існують і винятки, у цьому діалоговому вікні ви можете обрати сервер ключів, який слід використовувати програмі. Зазвичай, непогано було б обрати типовий сервер ключів так, щоб його було розташовано якомога ближче до вашого місця перебування (тобто у вашій країні або на вашому континенті), оскільки такі сервери, зазвичай, швидше відповідають на запити, які ви до них надсилаєте.

Будь ласка, зауважте, що все, що ви вивантажуєте на сервер ключів, зазвичай, залишається там назавжди. Ось причина того, що вам слід обмежувати строк дії ваших ключів. Крім того, слід пам'ятати, що сервери ключів іноді скануються особами, що розсилають небажану кореспонденцію, для пошуку адрес електронної пошти.

3.6.2 Результати пошуку на сервері ключів



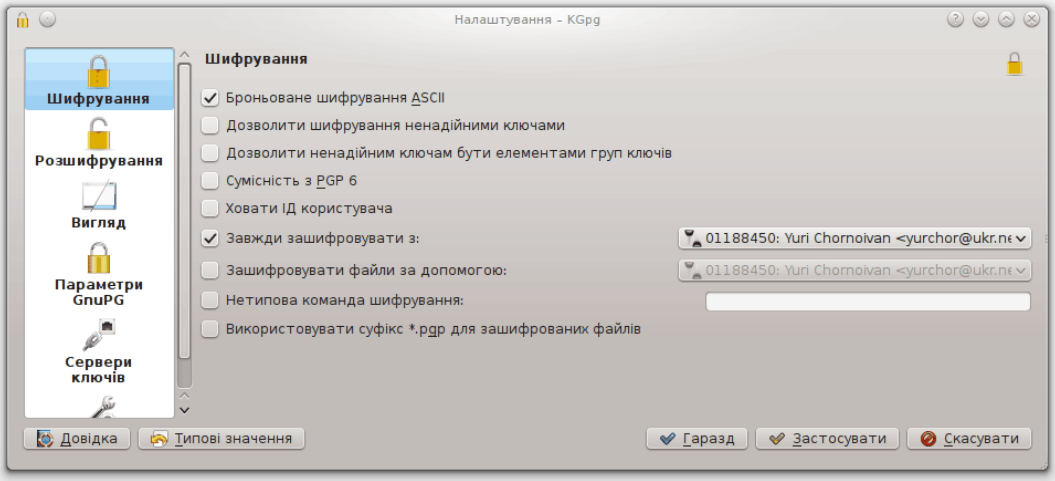
У цьому вікні буде показано всі результати пошуків. На знімку показано результат пошуку адрес ″@kde.org″ (244 результати). За допомогою поля пошуку можна звузити результати до одного ключа. Цей ключ має два відповідники: основний ідентифікатор користувача відповідає рядку пошуку разом з одним з ідентифікаторів іншого користувача.

Ви можете обрати для імпортування один або декілька ключів. Ідентифікатори цих ключів буде показано у полі Ключі для імпорту, розташованому у нижній частині вікна. Після натискання кнопки Імпортувати програма знову встановить зв'язок з сервером ключів і отримає ключі до вашого сховища ключів.

3.7 Налаштовування KGpg

Доступ до налаштувань можна отримати за допомогою меню аплету KGpg (наведіть вказівник миші на аплет і клацніть правою кнопкою) або за допомогою головного меню (пункту меню Параметри → Налаштувати KGpg). Ви можете встановити типові параметри для шифрування, розшифрування, інтерфейсу користувача і аплету. Більшість параметрів шифрування напряму пов'язана з gpg, довідку з цих параметрів можна знайти на сторінці довідника (man) програми gpg.

3.7.1 Шифрування



Тут ви можете налаштувати особливі параметри, які буде передано GnuPG для зміни поведінки програми під час шифрування. Докладний опис цих параметрів ви можете знайти у підручнику з GnuPG.

- Броньоване шифрування ASCII: використання цього параметра призведе до того, що зашифровані файли складатимуться лише з символів ASCII, призначених для друку, і матимуть короткі рядки. Файли, які зберігаються у такому форматі мають більший розмір, ніж файли у двійковому форматі, але такі файли легше надсилати, наприклад, електронною поштою.
- Дозволити шифрування ключами без довіри: цей параметр надасть вам змогу шифрувати файли ключами, яким ви не довіряєте.
- Сумісність з PGP 6: зашифровані файли будуть сумісні з застарілим стандартом PGP6. Використання цього параметра вимикає деякі з можливостей, отже, користуватися ним слід, лише якщо вам насправді потрібна така сумісність.
- Ховати ідентифікатор користувача: використання цього параметра вилучить всі відомості про отримувача з зашифрованого файла. У разі перехоплення цього файла ніхто не зможе отримати інформацію про отримувача з цього файла. Якщо у отримувача є декілька ключів, йому доведеться спробувати під час розшифрування декілька з них, щоб визначити потрібний для розшифрування.
- Завжди зашифровувати з: всі зашифровані дані додатково шифруються цим ключем. Якщо ви встановите значенням цього параметра один з ваших закритих ключів, це забезпечить можливість читання вами всіх зашифрованих даних ціною збільшення розмірів повідомлень.
- Зашифровувати файли з: встановлює поведінку, подібну до Завжди зашифровувати з, але для шифрування файлів.
- Нетипова команда шифрування: якщо вам потрібно передати якісь нетипові параметри до GnuPG, ви можете вказати тут відповідний командний рядок. Більшості користувачів цей параметр ніколи не знадобиться.
- Використовувати суфікс *.pgp для зашифрованих файлів: якщо ви залишите позначку поряд з цією міткою, зашифровані файли буде названо за вхідним файлом з додаванням суфікса .pgp, якщо ж позначки не буде програма використовуватиме суфікс .gpg.

3.7.2 Розшифрування

Тут ви можете вказати власну команду розшифрування. Потреба у цьому параметрі виникає рідко, він корисний лише для досвідчених користувачів, яким відомі параметри командного рядка GnuPG.

3.7.3 Вигляд

Тут ви можете налаштувати вигляд KGpg. Можна налаштувати кольори, якими відображатимуться різні рівні довіри до ключів у засобі керування ключами, а також параметри шрифту у редакторі.

3.7.4 Параметри GnuPG

Тут ви можете вказати назву виконуваного файла gpg, назву файла налаштувань і домашню теку програми. Ці значення буде автоматично визначено під час першого запуску програми, вони мають працювати без додаткового налаштування.

Використання агента GnuPG робить роботу з GnuPG комфортнішою: вам не потрібно для кожної дії знову вводити пароль. Пароль певний час зберігається у пам'яті, отже, будь-яка з дій, для якої потрібен пароль, виконується негайно. Зауважте, що використання цієї можливості може призвести до того, що інші особи можуть скористатися вашими закритими ключами, якщо ви залишите ваш сеанс доступним для них.

3.7.5 Сервери ключів

Тут ви можете створити список серверів ключів, які буде показано вам у діалоговому вікні серверів ключів. Якщо ви запустите GnuPG з командного рядка буде використано лише сервер ключів, вказаний як типовий.

Протокол, який використовується для обміну інформацією з серверами ключів, засновано на HTTP, отже у деяких середовищах є сенс За наявності використовувати проксі сервер HTTP.

3.7.6 Інше

У цьому розділі ви можете налаштувати декілька додаткових можливостей, які не увійшли до інших розділів. Наприклад, ви можете налаштувати можливість Запускати KGpg автоматично при вході до системи. Параметр Замість кишені використовувати позначене мишкою надає змогу увімкнути або вимкнути використання середньої кнопки миші для вставляння тексту до програми.

Крім того, ви можете увімкнути або вимкнути показ піктограми KGpg у системному лотку, а також змінити дію, яку буде виконано після наведення вказівника миші на піктограму і клацання лівою кнопкою. Якщо показ аплету увімкнено, вікно KGpg після закриття мінімізуватиметься до системного лотка. Якщо ж ви вимкнете показ піктограми у лотку, після закриття вікна програми KGpg її роботу буде завершено.

Розділ 4

Подяки і ліцензія

KGpg

Авторські права на програму (c) 2002-2003 Jean-Baptiste Mardelle bj@altern.org.

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

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

Переклад українською: Юрій Чорноіван yurchor@ukr.net

Цей документ поширюється за умов дотримання GNU Free Documentation License.

Ця програма поширюється за умов дотримання GNU General Public License.