uaToken®

Электронные идентификаторы

uaToken

для PGP версии 9.0 и выше

Руководство пользователя

2006

Пользователи PGP могут надежно защитить свои ключи шифрования, разместив их в памяти электронных идентификаторов uaToken.

В 9-ой версии PGP Desktop использование uaToken для хранения ключей шифрования стало более удобным и функциональным. Предварительные настройки 9-ой PGP Desktop претерпели некоторые и изменения, равно как и интерфейс системы при использовании созданных ключей.

Хранение ключей PGP в защищенной памяти uaToken позволяет пользователям быть уверенными, что в их отсутствие никто не сможет получить доступ к их конфиденциальной информации.

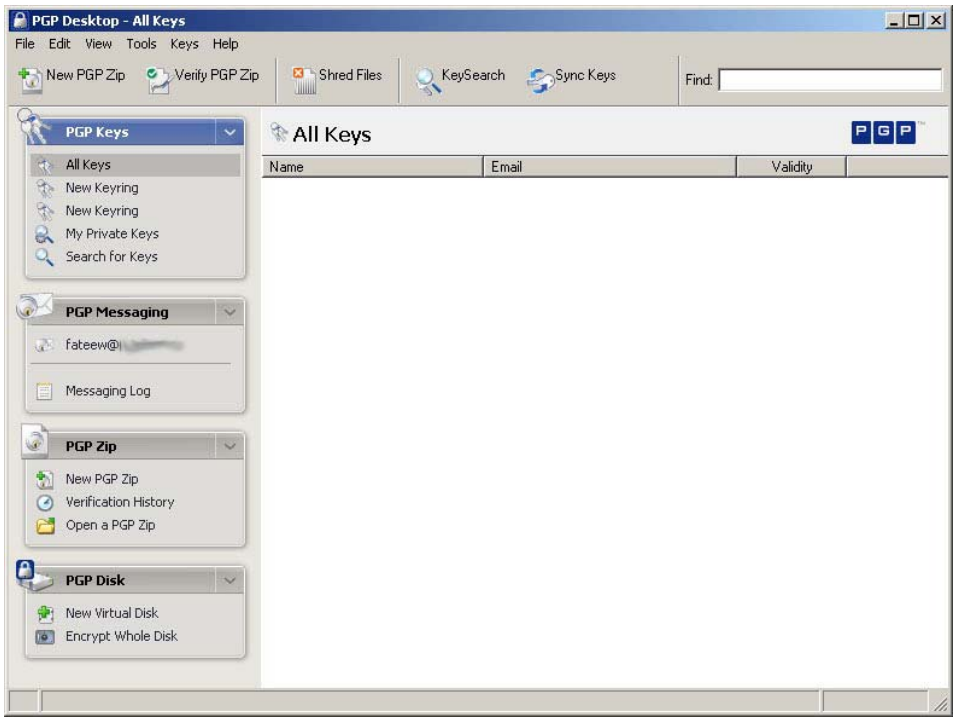
Для использования uaToken совместно с PGP достаточно приобрести сам идентификатор, установить драйверы и выполнить несложные настройки PGP.

Допускается использование идентификаторов uaToken для совместного хранения ключей PGP
и ключевой информации других приложений.

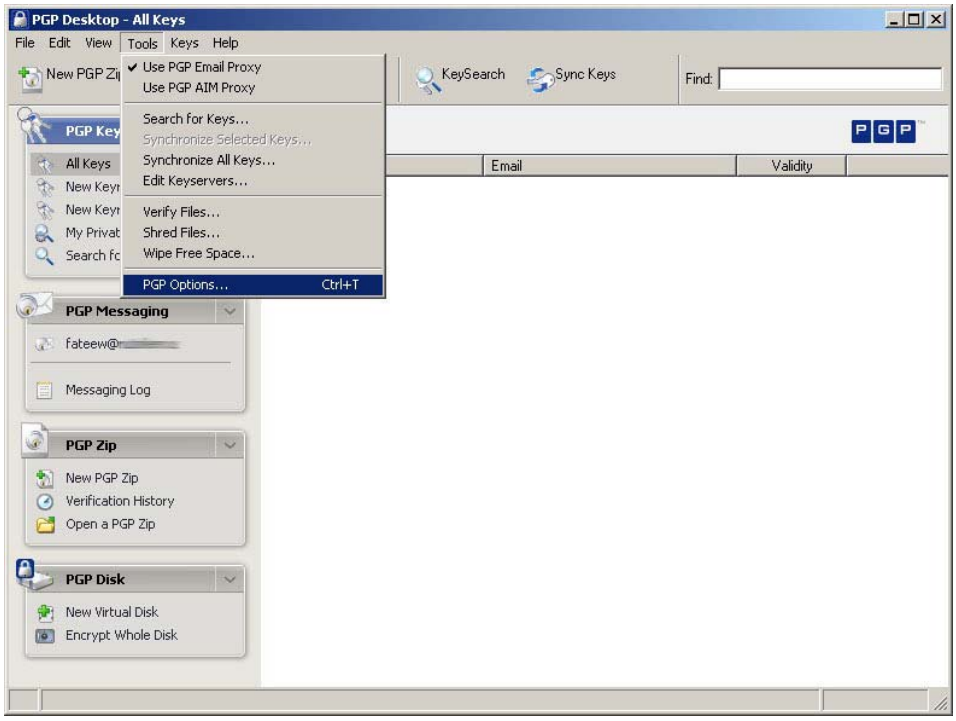
I. Настройка поддержки uaToken

Для того чтобы иметь возможность хранить ключи PGP в защищенной памяти uaToken, сначала необходимо настроить поддержку смарт-карт.

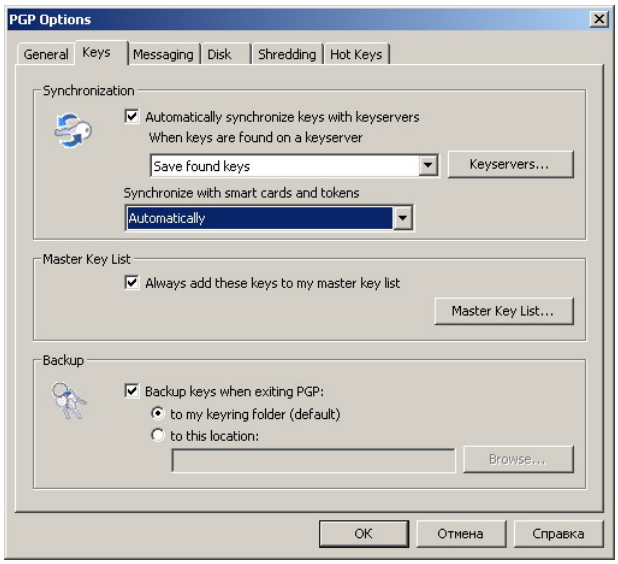
1. Запустите утилиту **PGP Desktop**:



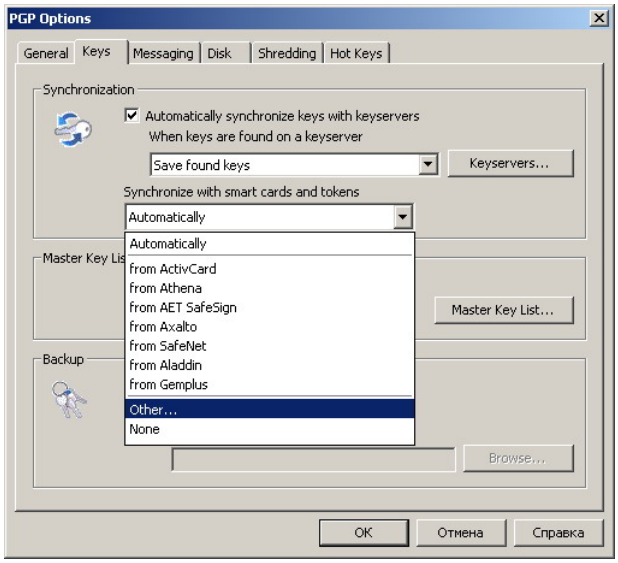
2. В меню **Tools** выберите пункт **PGP Options...**:



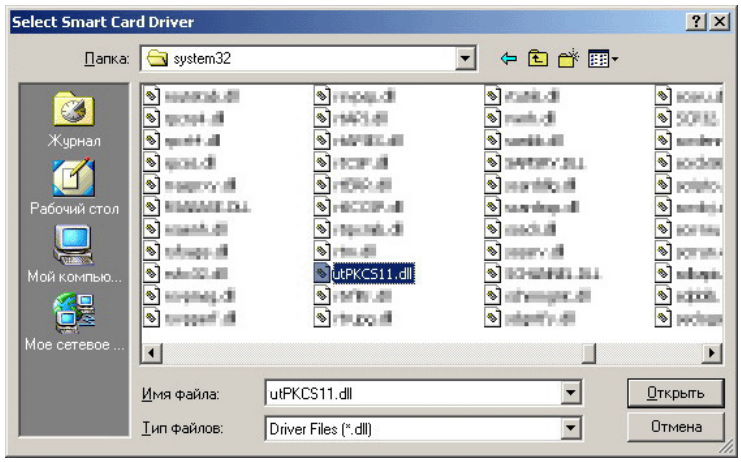
3. Перейдите на закладку **Keys**:



4. В выпадающем списке **Synchronize with smart cards and tokens** выберите пункт **Other...**:



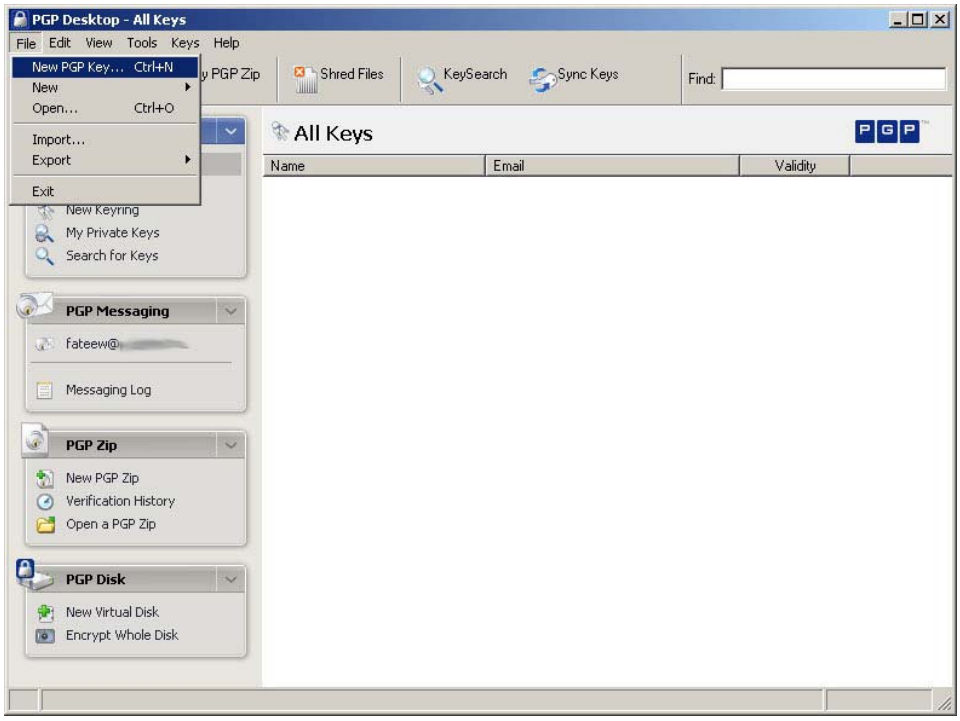
5. И укажите путь к библиотеке PKCS#11 - файл **utPKCS11.dll** (по умолчанию библиотека находится
в папке **%SYSTEMROOT%\SYSTEM32**), нажмите кнопку **Открыть**:



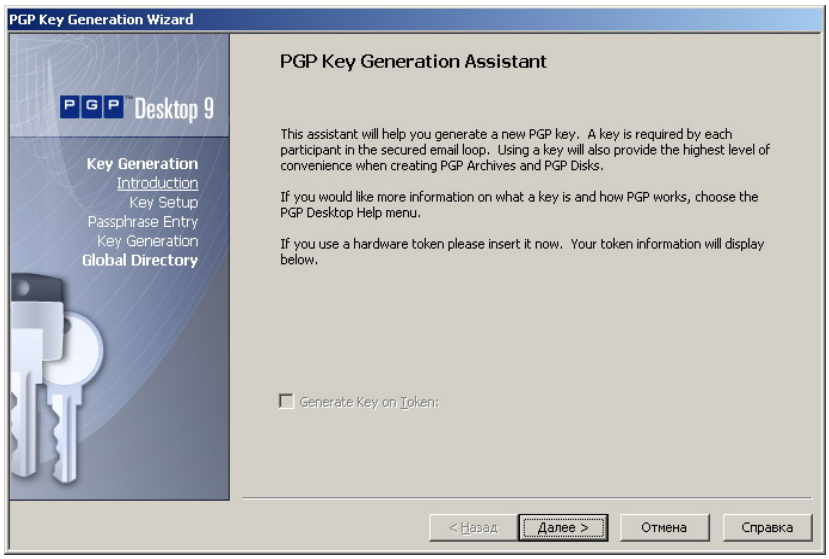
6. Закройте окно **PGP Options**, нажав на кнопку **Ok**. На этом настройка поддержки uaToken завершена:

II. Создание ключевой пары в памяти uaToken

1. Для создания ключевой пары и размещения ее в защищенной памяти токена в утилите **PGP Desktop**,
в меню **File** выберите пункт **New PGP Key...**:

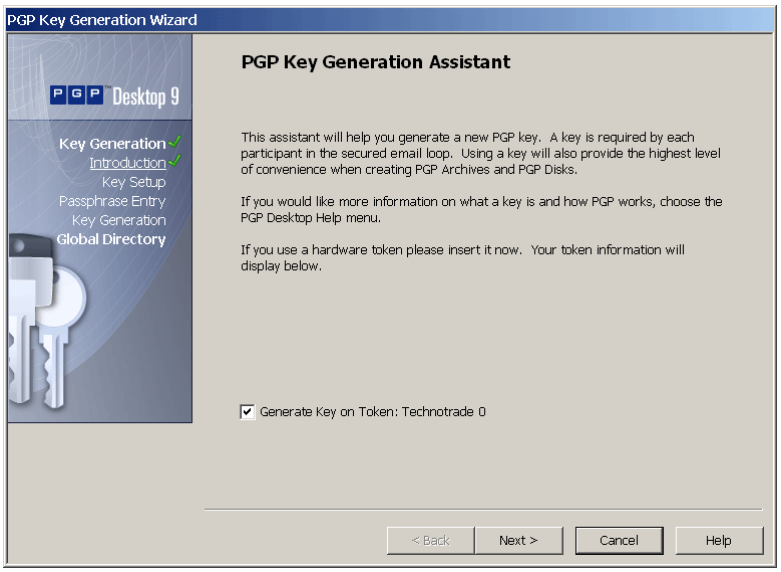


2. Откроется мастер генерации ключей:

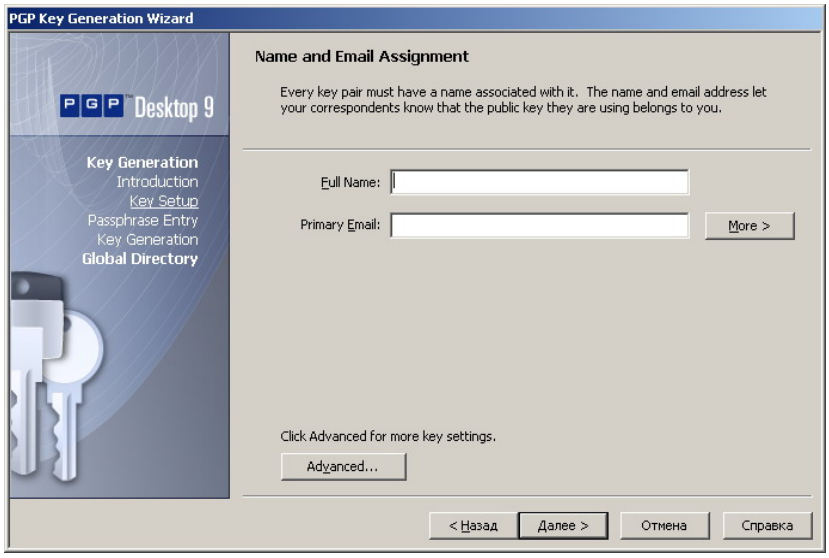


3. Подключите uaToken, в памяти которого будут записаны ключи шифрования. Дождитесь, пока светодиод перестанет мигать.

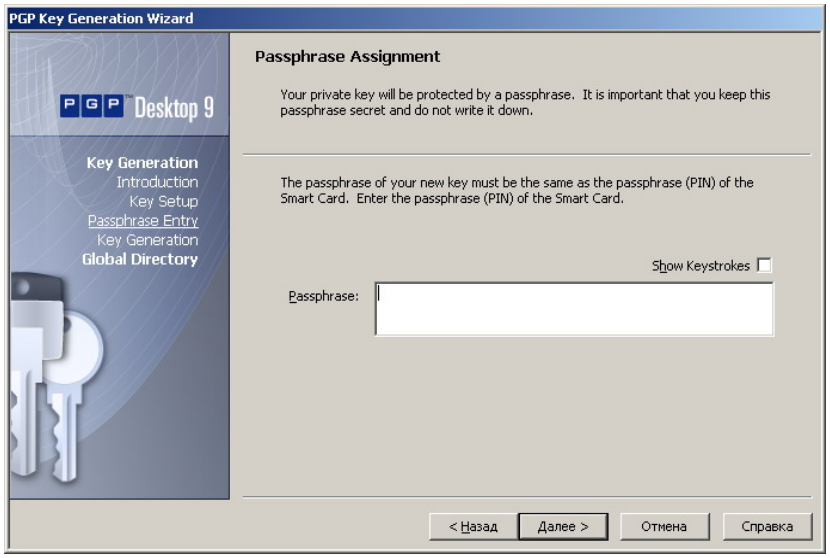
4. После этого станет доступной опция **Generate Key on Token**. Отметьте ее галочкой и нажмите кнопку **Далее**:



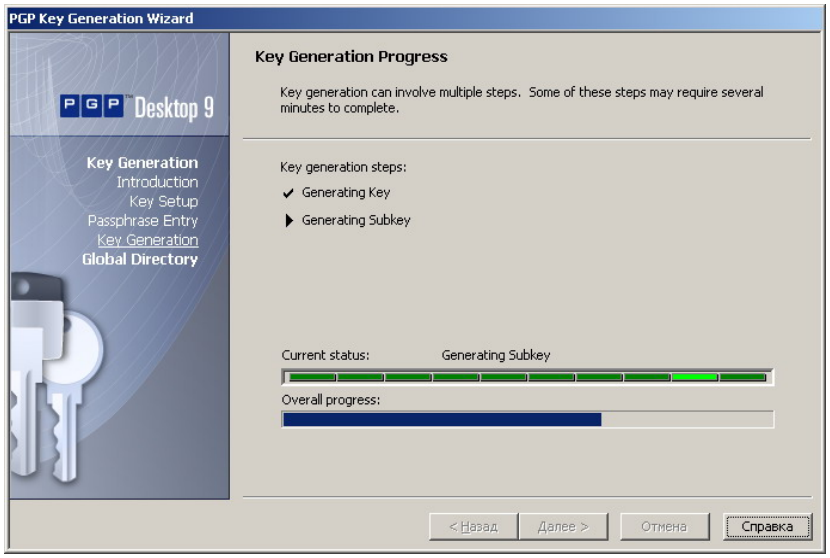
5. Заполните поля **Full Name** и **Primary Email**, при необходимости задайте дополнительные параметры для ключей шифрования, нажав кнопку **Advanced**. Нажмите кнопку **Далее**:



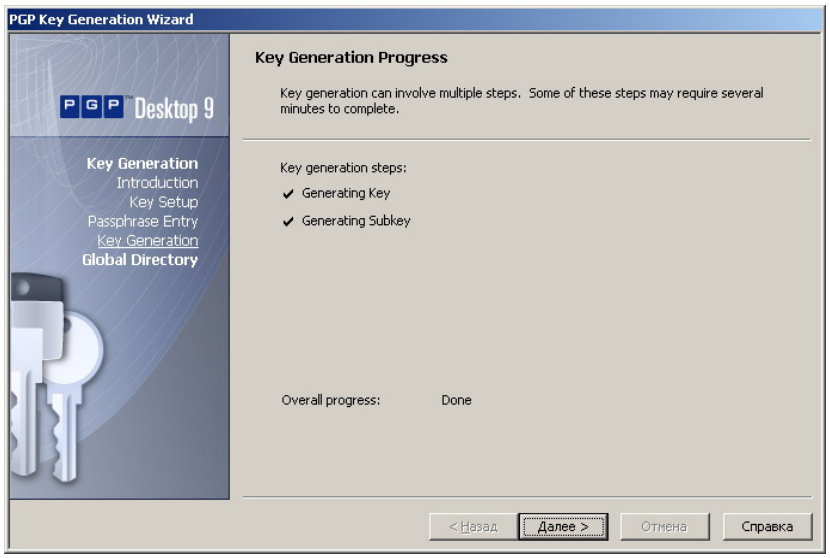
6. Вам предложат ввести PIN-код для доступа к памяти uaToken. Введите текущий PIN-код Пользователя uaToken и нажмите кнопку **Далее**:



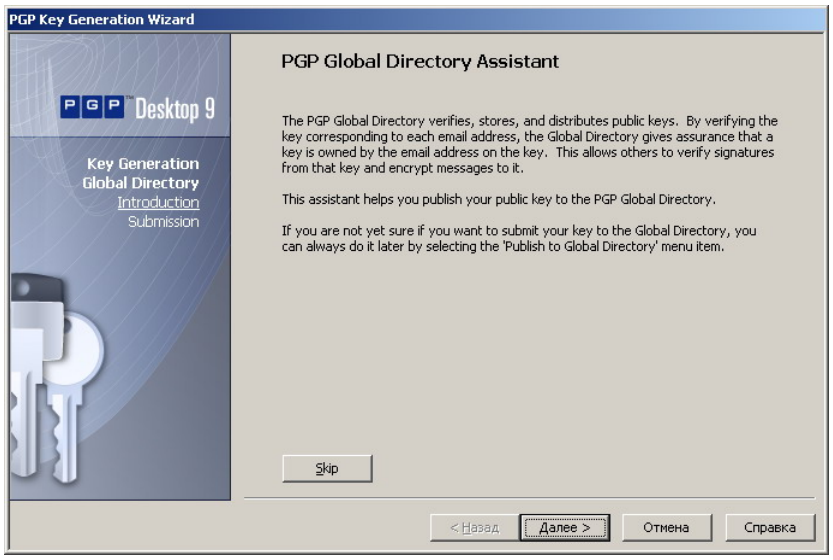
7. Начнется процесс создания ключей и записи их в защищенную память uaToken. Процесс может занять 1 - 3 минуты.



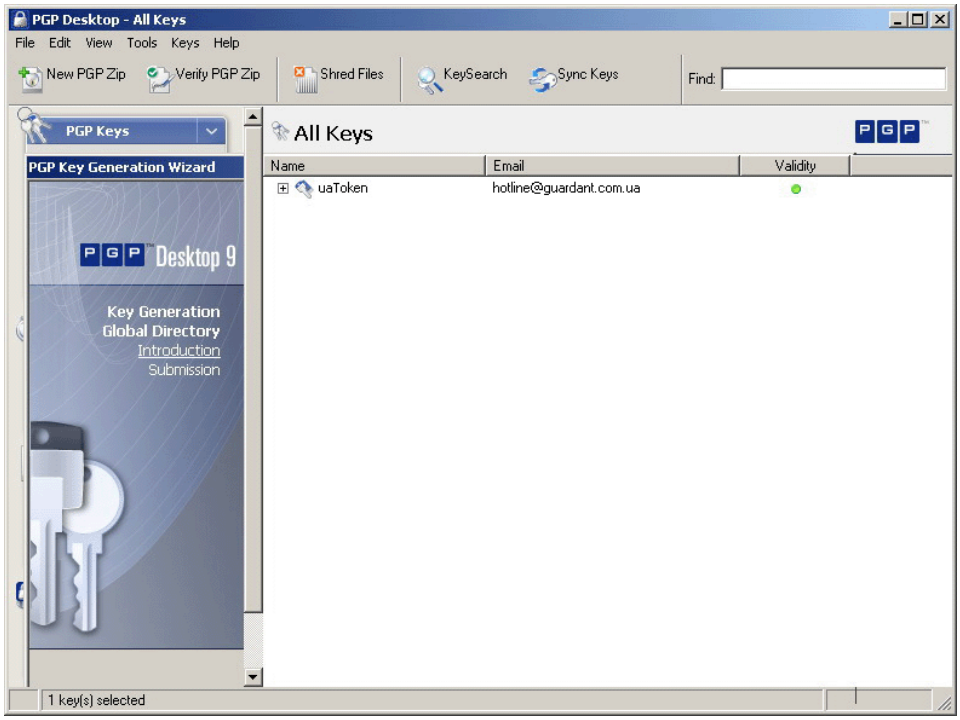
8. По окончании процесса генерации и записи ключей нажмите кнопку **Далее**:



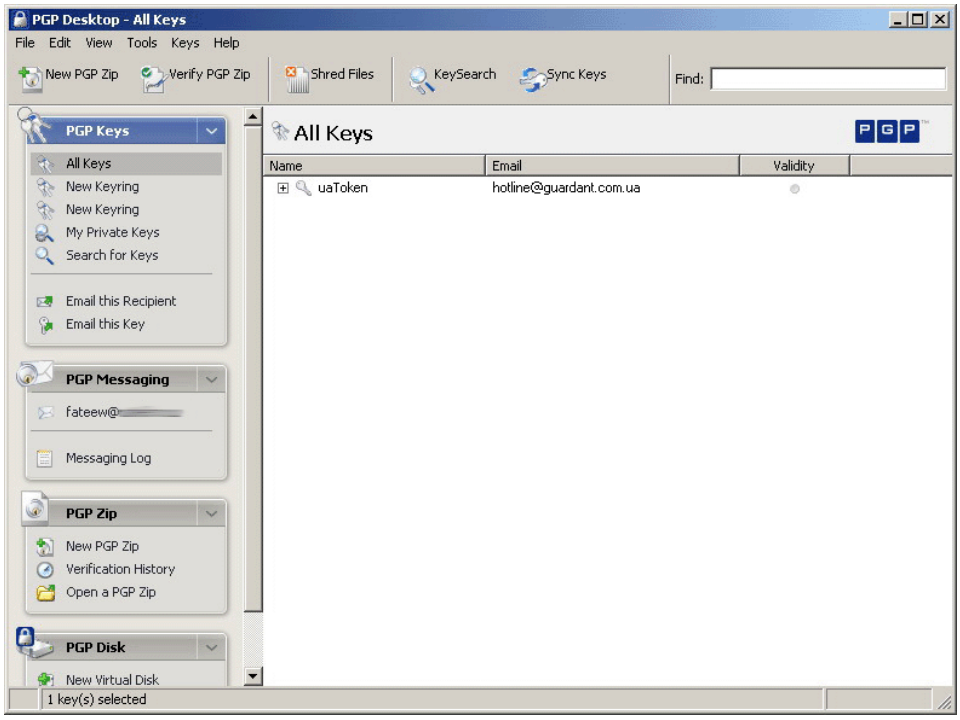
9. Появится окно публикации открытого ключа в **PGP Global Directory**. В случае необходимости публикации нажмите кнопку **Далее** и следуйте указаниям Мастера. Иначе нажмите кнопу **Skip**:



10. Вы вернетесь в основной экран утилиты **PGP Desktop**. В случае успешной генерации и записи ключевой пары в окне **All Keys** будет отображаться запись, соответствующая сгенерированной ключевой паре
и индикатор **Validity** будет зеленым:



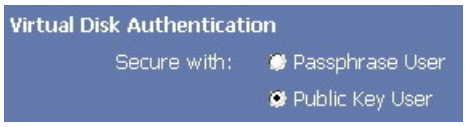
11. При отключении токена индикатор **Validity** становится серым, что указывает на отсутствие доступа
к ключевой паре.


PGP Desktop - All Keys
File Edit View Tools Keys Help
New PGP Zip
Verify PGP Zip
Shred Files
KeySearch
Sync Keys
Find:
PGP Keys
All Keys
New Keyring
New Keyring
My Private Keys
Search for Keys
Email this Recipient
Email this Key
PGP Messaging
fateew@
Messaging Log
PGP Zip
New PGP Zip
Verification History
Open a PGP Zip
PGP Disk
New Virtual Disk
All Keys
Name
Email
Validity
uaToken
hotline@guardant.com.ua
1 key(s) selected

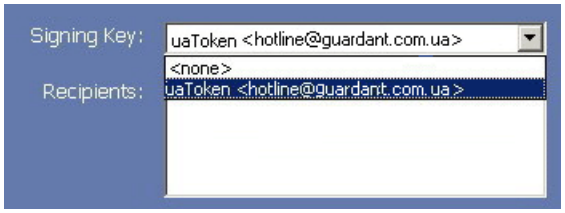
III. Использование ключей шифрования, хранящихся в памяти uaToken

1. В дальнейшем, для использования ключей требуется предварительно подключить uaToken.

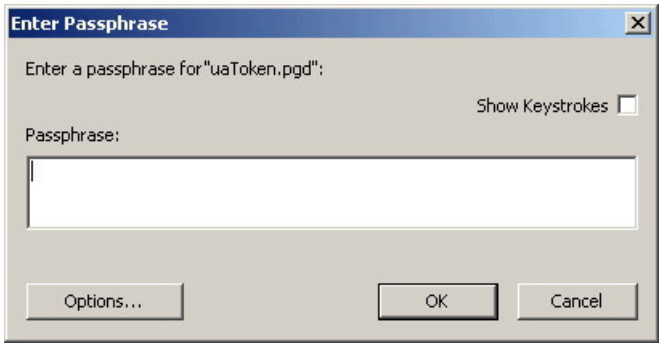
2. При выборе типа ключа (там, где это требуется) выбирать **Public Key User**:



3. Из списка ключей шифрования выбрать требующийся:



4. Ввести PIN-код Пользователя* и нажать кнопку OK:



* **PIN-код Пользователя по умолчанию: 12345678**