Tutorial de instalação e configuração do utilitário de gerenciamento de chaves pública/privada, para criptografia de arquivos

Este tutorial visa explicar os procedimentos para a instalação do programa **gpg4win.exe**, que instala um conjunto de utilitários para Windows, cuja função é criar e gerenciar chaves públicas e privadas em um computador, e usá-las para criptografar, descriptografar e assinar arquivos, garantindo o sigilo na troca de informações que trafegam pela Internet.

Passo 1:

Obter o programa **gpg4win-1.1.3.exe** e executá-lo no Windows.

Será aberta a seguinte janela :

O procedimento de instalação é bastante simples. Basta prosseguir escolhendo a opção **Next**, até concluir a instalação.

Passo 2:

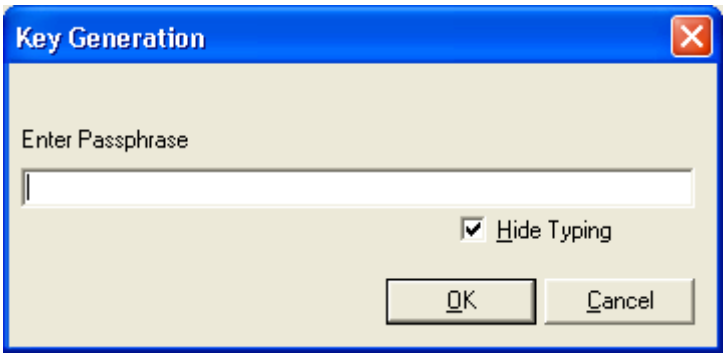
Após a conclusão da instalação, acessar o menu **Iniciar**, do Windows, e escolher **GnuPg for Windows**, na relação de programas instalados. Escolher **WinPT** no menu.

O único programa que iremos usar é o **WinPT**, que é o utilitário de criação e gerenciamento de chaves. Na primeira vez que é executado, é aberto uma janela com 3 opções de operação. Deve-se escolher a primeira (**Generate a Gnu PG key pair**) , que cria um par de chaves pública e privada, para o computador onde foi feita a instalação.

O sistema pede para informar um **Real Name** e um **endereço de e-mail**, conforme a figura abaixo:

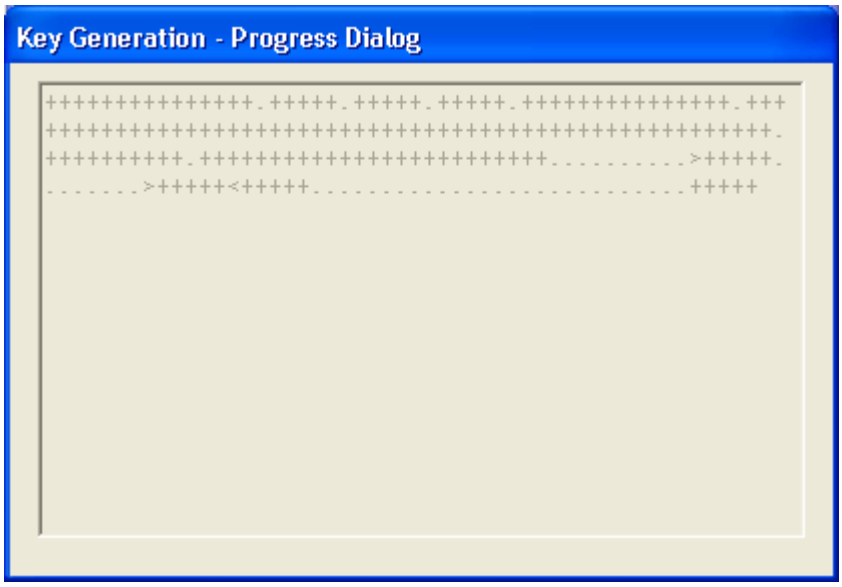
Após informar o dois campos, clicar em **OK**.

Para continuar, deve-se entrar com um **Passphrase** (com pelo menos 8 dígitos), que é uma senha para a criação das chaves:

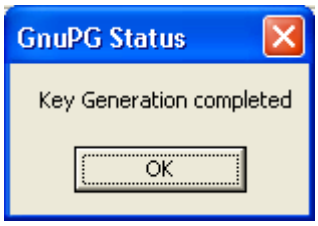


Após clicar em **OK**, deve-se informar novamente a mesma senha, para garantir que não houve erro de digitação.

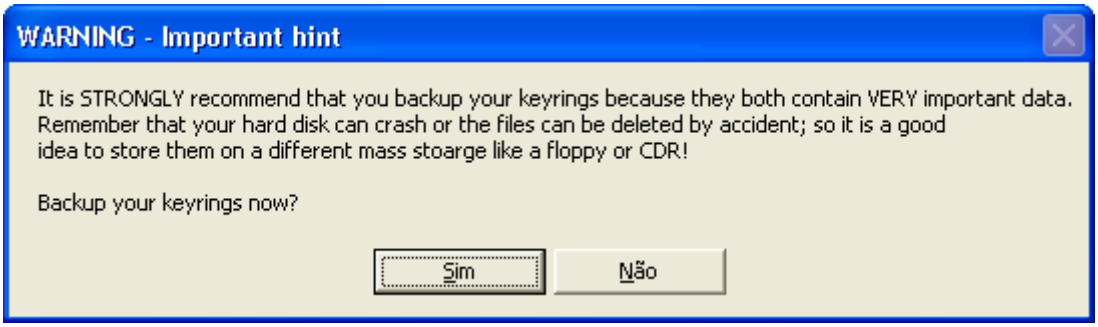
A janela de criação das chaves aparece, conforme a figura abaixo:



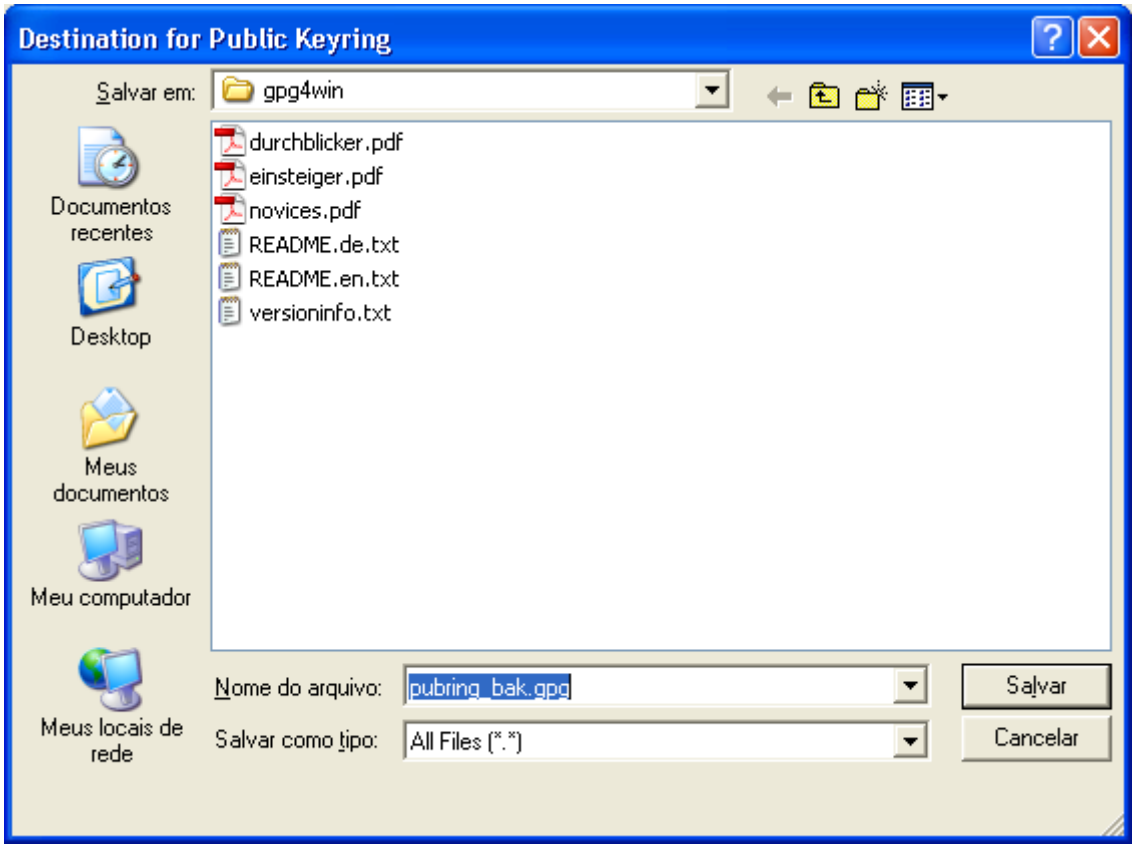
Após o término, deve aparecer a janela abaixo. Clicar em OK.



O sistema pergunta se deseja fazer backup das chaves criadas. É aconselhável que se responda **Sim**.

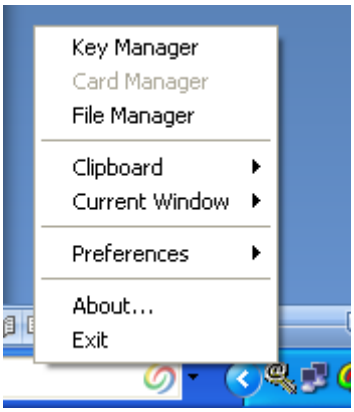


Informar um caminho para armazenar o backup. Este pode ser um disquete ou pen drive onde será gravado o backup das chaves.

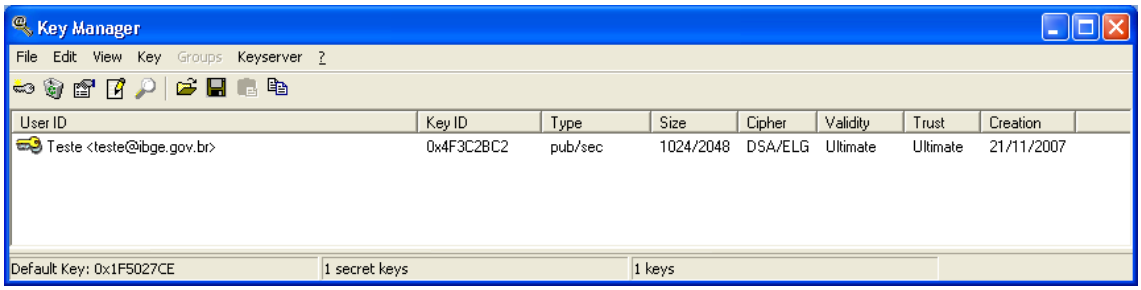


A janela acima será exibida duas vezes, na primeira para gravar a chave pública (**pubring_bak.gpg**) e na segunda para gravar a chave privada (**secring_bak.gpg**).

Finalmente, a janela principal do **Key Manager** será exibida. Pode-se também exibir esta janela a qualquer momento, clicando no ícone da **barra de tarefas do Windows** e escolhendo **Key Manager**.



A janela do **Key Manager** é a seguinte:



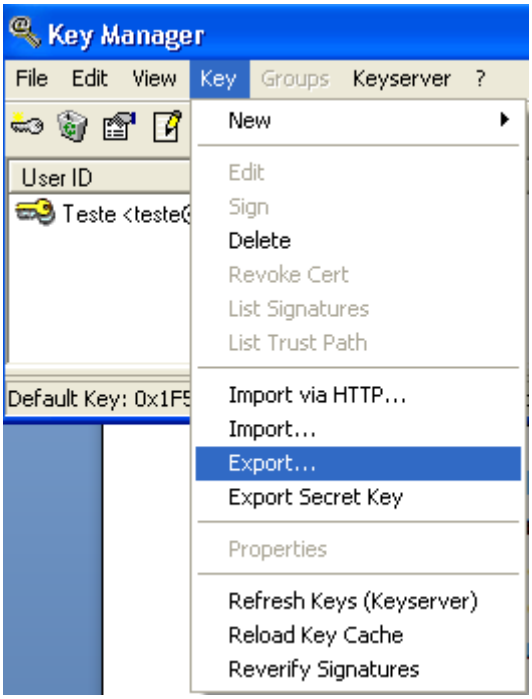
Pode-se ver o par de chaves pública e privada, criado para um usuário **Teste** (observe a coluna Type).

Passo 3:

Para exportar a chave pública para um outro usuário, que deseja enviar um arquivo criptografado, seguir os passos a seguir.

> **Observação!!**
>
> Lembrando o funcionamento do princípio das chaves:
>
> Usuário A : tem chave privada A e chave pública A
>
> Usuário B : tem chave privada B e chave pública B
>
> O usuário A deseja enviar um arquivo criptografado para B. O usuário B deve primeiramente enviar sua chave pública para A. Em seguida, o A criptografa o arquivo com a chave pública de B e envia o arquivo criptografado para B. Somente B, com sua chave privada, conseguirá descriptografar o arquivo e ler seu conteúdo.

Inicialmente, selecionar o usuário, na coluna **User ID** (no nosso exemplo: Teste). Em seguida, no menu **Key**, do **Key Manager**, escolher a opção **Export...**



Atenção!! Não escolher **Export Secret Key**, pois não queremos exportar a chave privada, mas sim a pública!

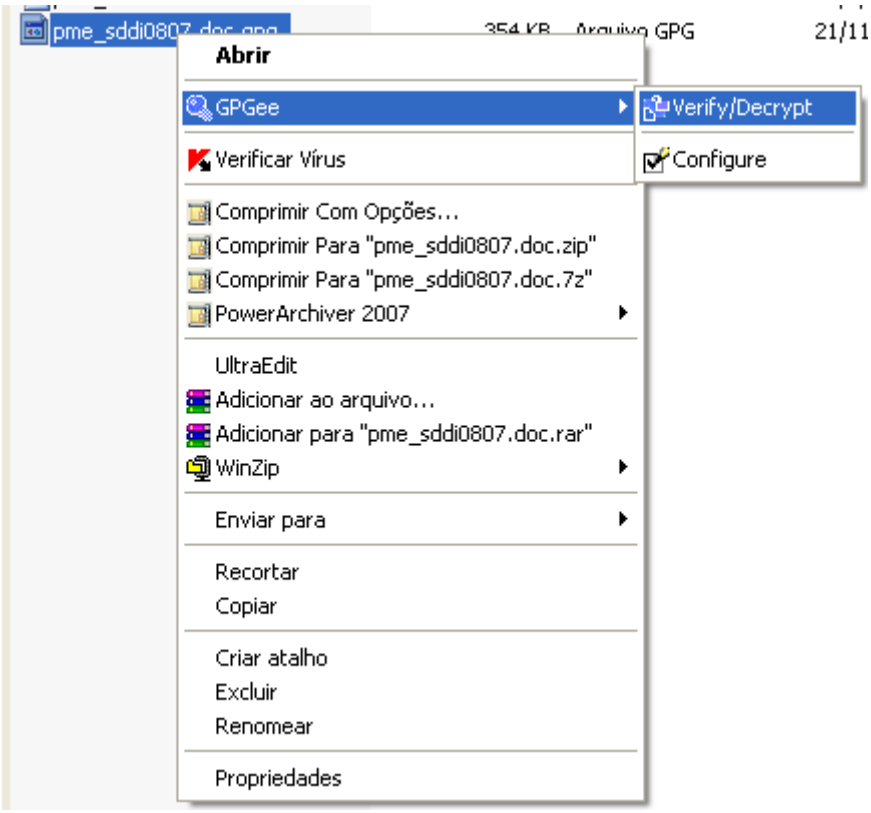
Escolher o caminho onde se deseja salvar o arquivo com extensão .asc.

Após salvar a chave pública (extensão *.asc), este deve ser enviado, por e-mail, para a pessoa que vai criptografar os arquivos. Os arquivos que forem criptografados com esta chave pública somente poderão ser descriptografados em computadores que tenham instalada a chave privada correspondente.

Caso seja necessário que mais de um computador possa descriptografar um arquivo, deve-se exportar a chave privada (Opção **Key/Export Secret Key**) para um disquete ou pen drive e importá-la no outro computador, com o procedimento do **Passo 1** instalado. Desta forma, teremos uma cópia da chave instalada em outro computador.

Passo 4:

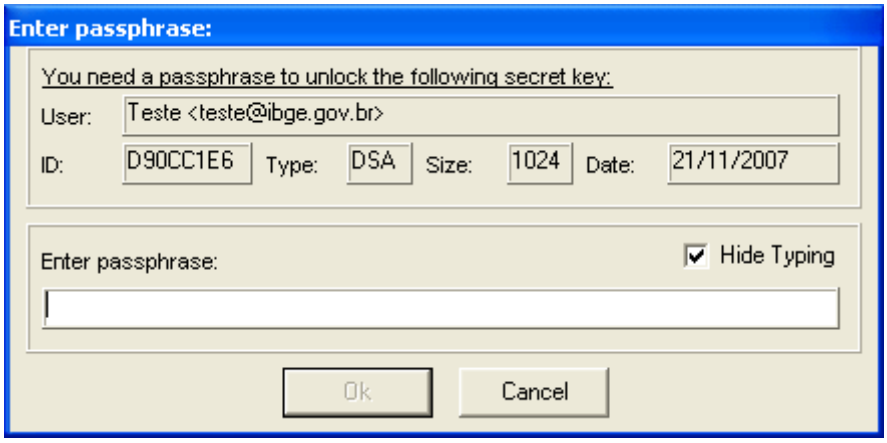
Para descriptografar um arquivo criptografado, recebido por e-mail, deve-se desanexá-lo (o arquivo criptografado tem uma extensão .gpg). Em seguida, clicar com o botão direito do mouse, sobre o arquivo desanexado. Será apresentado um menu, conforme a figura a seguir:



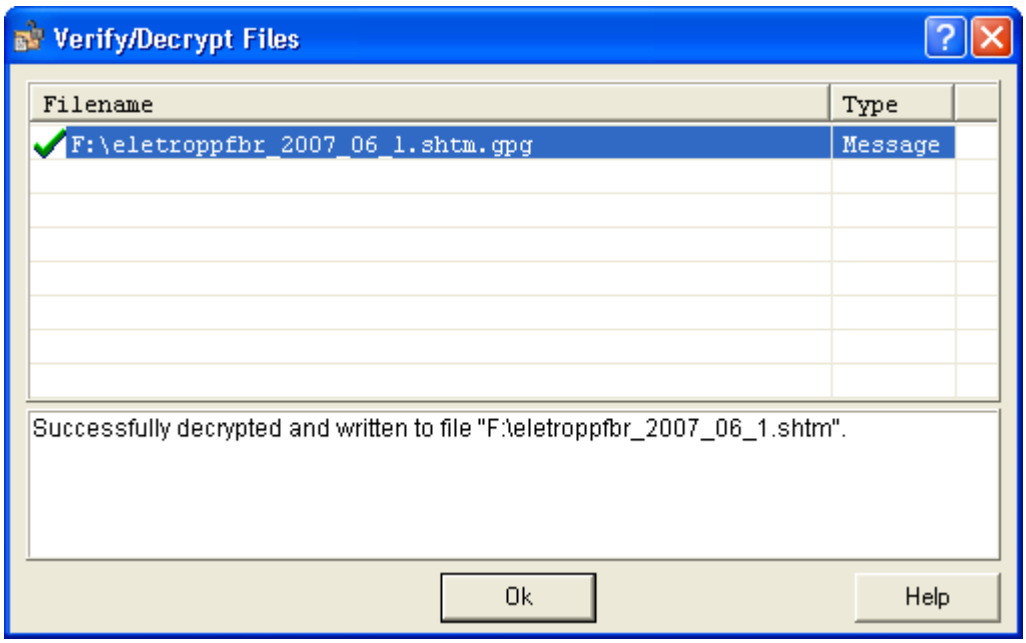
Clicar em **Verify/Decrypt**.

Se o computador possuir a chave privada necessária para descriptografar o arquivo, será exibida uma janela perguntando pela **senha** informada no **Passo 2**. Somente com a **chave privada** e a **senha** pode-se descriptografar o arquivo.

Sempre que se faz qualquer acesso à chave privada, o usuário é perguntado pela senha, inclusive quando se exporta a chave privada.

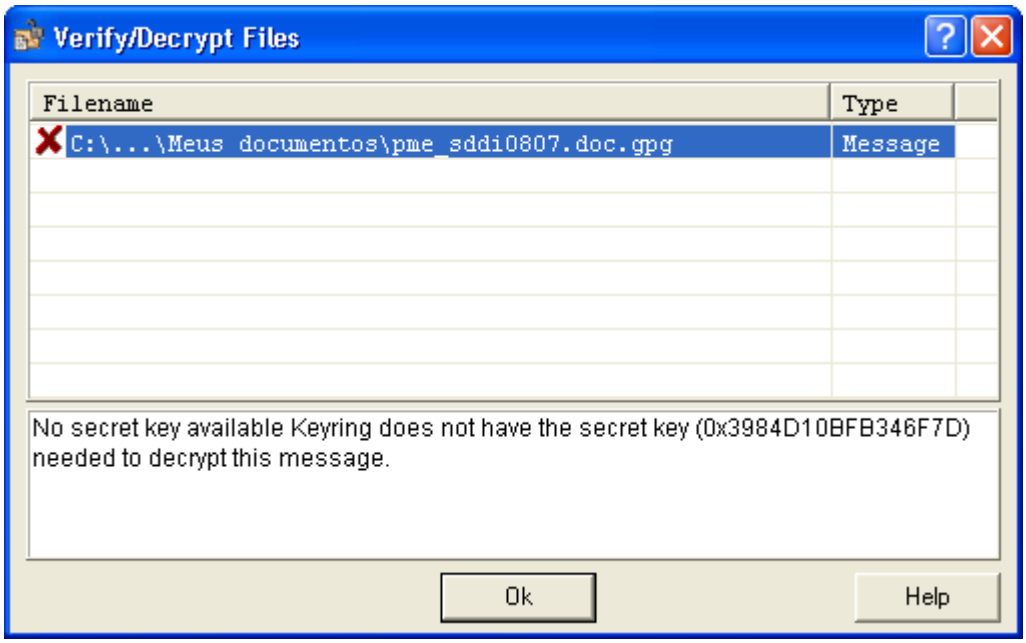


Após informar a senha, a janela seguinte é exibida informando que o arquivo foi descriptografado com sucesso:



O arquivo é descriptografado na mesma pasta onde se encontra o arquivo criptografado (*.gpg).

Caso o computador onde se deseja descriptografar o arquivo não possua a chave privada correspondente à chave pública usada na criptografia, a seguinte mensagem é exibida:

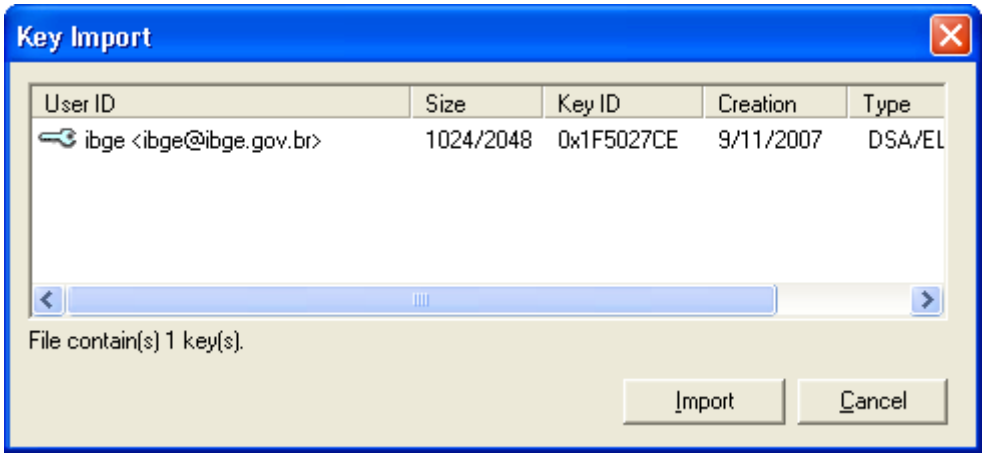


Passo 5:

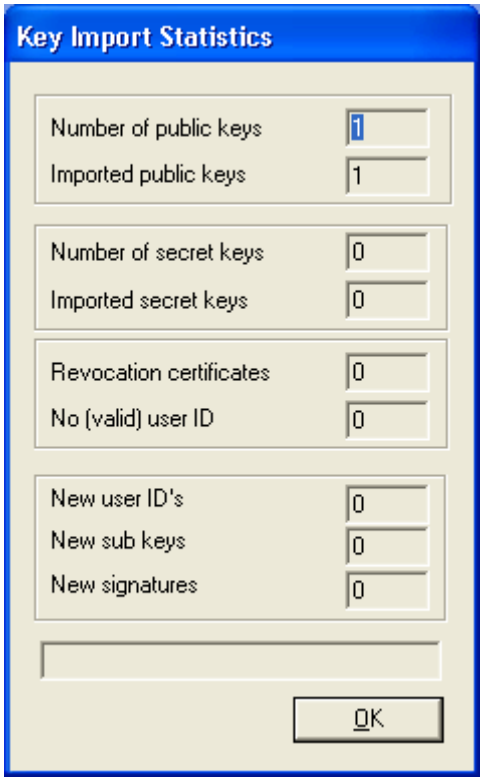
Para criptografar um arquivo, deve-se ter a chave pública do destinatário. Para isto, uma vez recebido o arquivo com a chave pública do destinatário, escolher **Import...**, na opção **Key**, do **Key Manager**.

Localizar o arquivo **.asc** com a chave pública.

No nosso exemplo, estamos importando uma chave pública. Aparecerá a seguinte janela:



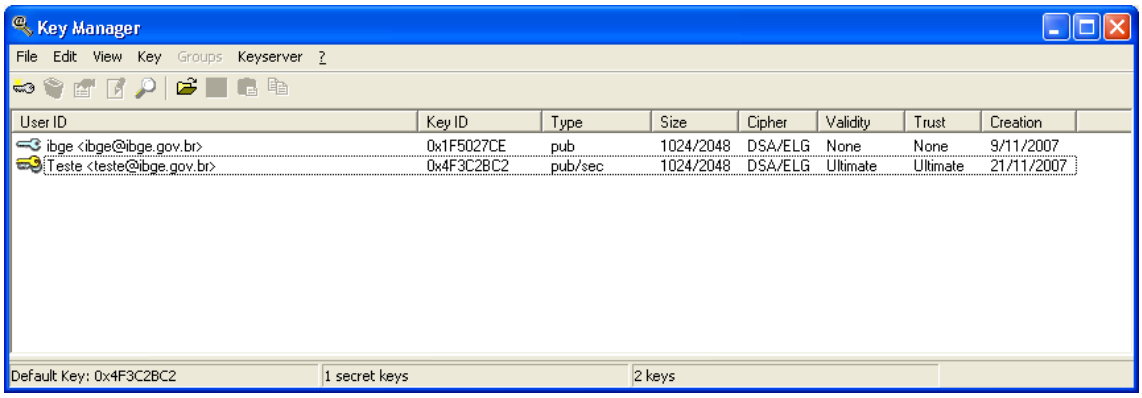
Selecionar o usuário (no nosso exemplo, ibge) e clicar em **Import**. A seguinte janela vai aparecer:



Basta clicar em **OK**.

Atenção!! Se na figura anterior, aparecer no campo **No (valid) user ID**, um valor diferente de zero, significa que a chave pública não foi corretamente gerada pelo destinatário. A chave, neste caso, não será importada. Deve-se entrar em contato com o mesmo, para proceder uma nova geração.

Após clicar em **OK**, se a chave pública estiver correta, a janela do **Key Manager** irá exibir a nova chave pública instalada. Devemos instalar uma chave pública para cada destinatário de nossos arquivos.

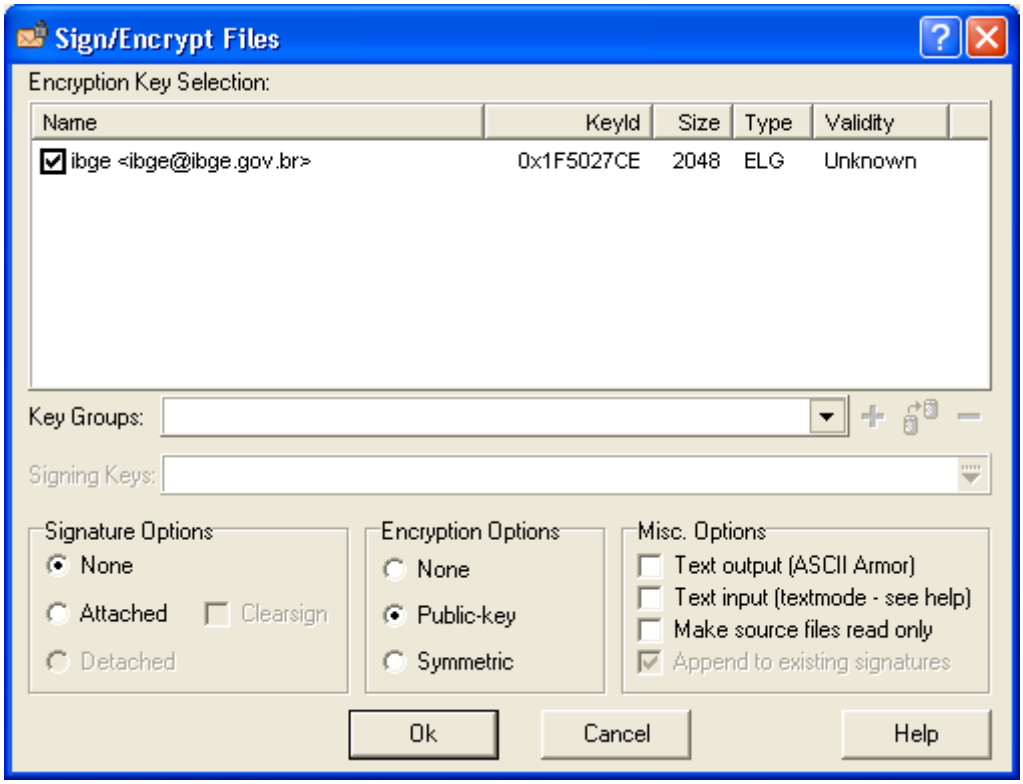


Observe na figura acima a chave importada (chamada IBGE) e a coluna **Type**, que contém a informação **pub** (indicando que é apenas uma chave pública).

Agora podemos criptografar qualquer arquivo para envio da seguinte forma:

Clicar com o botão direito do mouse no arquivo e escolher **GPGee/Encrypt(PK)**

Aparecerá a seguinte janela:



Devemos escolher a chave pública que será usada para criptografar o arquivo. No nosso exemplo, temos apenas uma chave pública (IBGE) e é esta que será usada. Bastar marcar e clicar em **OK**.

No mesmo diretório onde está o arquivo que se deseja criptografar, é criado um novo arquivo com o mesmo nome, porém com extensão .gpg (arquivo criptografado).

Agora é possível enviar este arquivo, por e-mail, para que apenas o destinatário que possui a chave privada possa descriptografá-lo, conforme visto no **Passo 4**.