# Практическое занятие № 9

## Управление ключами криптографической защиты электронной почты в комплексе программных средств PGP.

По заказу ФГУ ГНИИ ИТТ «Информика»
Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

# Цель:

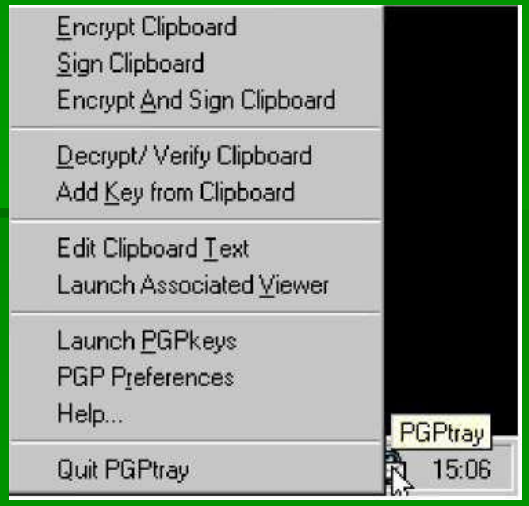
- Изучить технологию управления ключами криптографической защиты электронной корреспонденции на примере программы PGPkeys .

# Запуск PGP

- ***PGP*** основана на технологии «криптография с открытыми ключами», в которой для поддержания защищенной коммуникации используются два взаимодополняющих ключа. Один из ключей – закрытый, доступ к которому должны иметь только вы, а другой – открытый, который нужно свободно распространить среди пользователей *PGP*. Оба этих ключа, закрытый и открытый, хранятся в файлах, называемых «связками», доступ к которым производится из окна программы *PGPkeys*. В этом окне выполняются все функции управления ключами.

# Существует три основных способа запуска PGP:

- • из области индикаторов Панели задач;
- • из поддерживаемого пакета электронной почты;
- • из меню Файл (File) Проводника (Explorer).

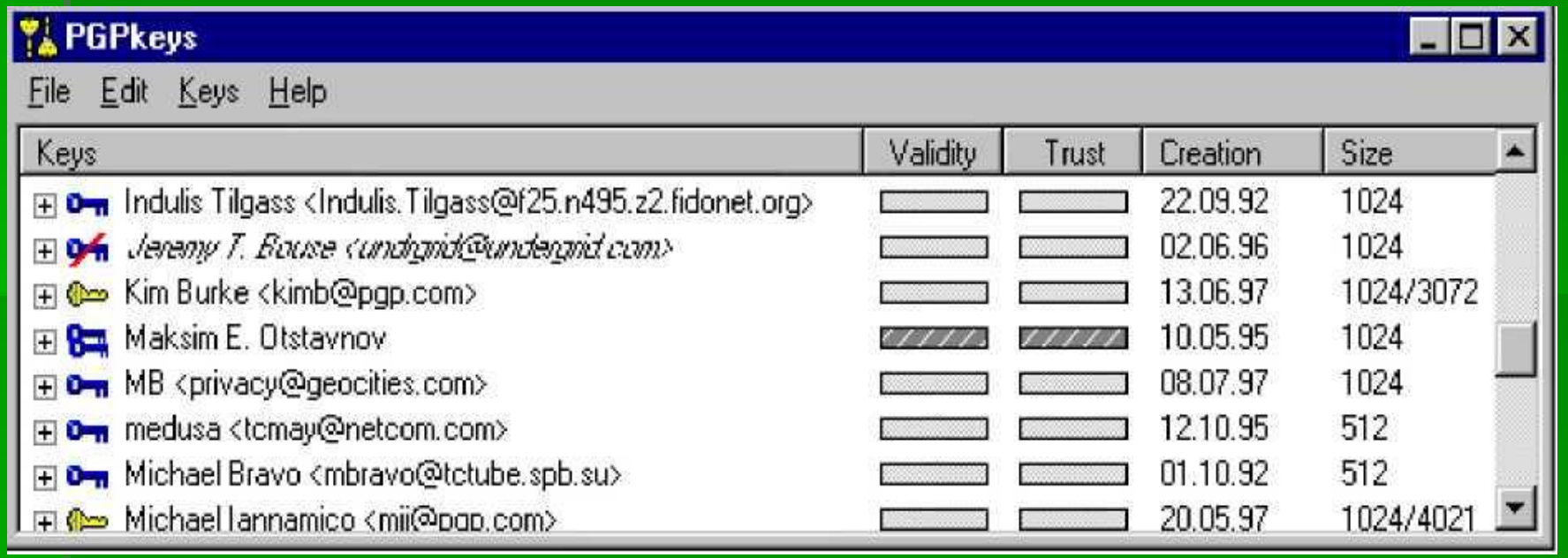


## Теоретическая часть



- Вы можете выполнить большинство основных функций, вызвав меню щелчком на значке, обычно расположенном в Области индикаторов Панели задач (если этого значка нет, следует запустить PGPtray из меню Пуск (Start)), выбрав соответствующий пункт.

- Выбрав из меню PGPtray пункт Launch PGPkeys, вы открываете окно *PGPkeys*, в котором представлены пары ваших открытых/закрытых ключей, а также все открытые ключи, которые есть у вас на связках. Если вы не создали себе пару ключей, *Мастер ключей (PGP Key Wizard)* проведет вас через необходимый для ее создания процесс.



По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

- В окне ***PGPkeys*** вы можете создавать новые пары ключей и управлять всеми ключами, находящимися на ваших связках. Например, именно здесь вы можете исследовать атрибуты каждого ключа, указывать степень уверенности в том, что ключ действительно принадлежит номинальному владельцу и степень доверия к владельцу ключа в отношении его способности быть поручителем за подлинность ключей других лиц.

# Управление ключами

- Ключи, которые вы генерируете, а также открытые ключи, получаемые от других, хранятся на связках, которые, в сущности, представляют собой файлы на жестком или гибком диске. Обычно связка закрытых ключей хранится в файле ***secring.skr***, а связка открытых – в ***pubring.pkr***. Эти файлы, как правило, располагаются в той же папке, в которую установлена ***PGP***. Для символизации файлов со связками ключей используются два особых значка, благодаря которым их можно легко обнаружить при просмотре содержимого папок.

связка закрытых ключей

связка открытых ключей

По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

- Иногда Вам может понадобится изменить атрибуты какого-либо ключа. Например, когда Вы получаете чей-либо открытый ключ, вы можете захотеть определить его тип *(**RSA** или **DSS/Diffie-Hellman**),* проверить его отпечаток или определить действительность на основе сертифицирующих его подписей. Вы можете также захотеть подписать чей-либо открытый ключ, чтобы дать знать, что вы уверены в его действительности, присвоить ключу определенный уровень надежности или изменить пароль доступа к своему закрытому ключу. Все эти функции управления ключами доступны из окна ***PGPkeys***.

По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

- Значки с двойным ключом символизируют пары из закрытого и открытого ключей, сгенерированные вами, а одиночные ключи обозначают открытые ключи, полученные вами от других. Если у вас есть ключи разных типов, вы заметите, что ***RSA-ключи*** символизируются синими значками, а ***DSS/DH*** – желтыми.

- Щелкнув два раза на любом ключе, вы раскроете список, в котором будут отображены имена (и адреса) владельца, каждое из которых символизируется значком с человечком. Щелкнув два раза на этом значке, вы увидите подписи всех тех, кто сертифицировал этот ключ. Каждая из них отображается значком с изображением пера. Если вам не нравятся двойные щелчки как способ перехода от одного уровня информации к другому, просто пометьте интересующие вас ключи и выберите пункт ***Expand Selection*** из меню ***Edit.***

# Вдоль верха главного окна расположены метки (labels), соответствующие атрибутам каждого ключа.

- ***Keys (Ключи)*** – символическое представление ключа, сопровождаемое именем и адресом его владельца.

- ***Действительность (Validity)*** – отображает степень уверенности в том, что ключ принадлежит номинальному владельцу. Действительность ключа вычисляется исходя из того, кто сертифицировал ключ и насколько вы доверяете ручательствам этих лиц. Открытый ключ, который Вы сертифицировали сами, обладает наибольшим уровнем действительности. Это основывается на допущении, что Вы подпишите чей-либо ключ лишь тогда, когда будете полностью уверены в том, что он принадлежит номинальному владельцу.

По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

- ***Надежность (Trust)*** – указывает уровень доверия, которое вы присвоили владельцу ключа в смысле его способности быть посредником при сертификации ключей третьих лиц. Вы можете указать уровень надежности *(Надежный (**Complete**), Отчасти надежный (**Marginal**)* или *Ненадежный (**Untrusted**))* в окне диалога ***Properties**).*
- ***Создание (Creation)*** – показывают дату генерации ключа.
- ***Длина (Size)*** – показывает количество бит, составляющих ключ.

## *Ниже приведены значки, используемые в окне PGPkeys, и описание того, что они обозначают.*

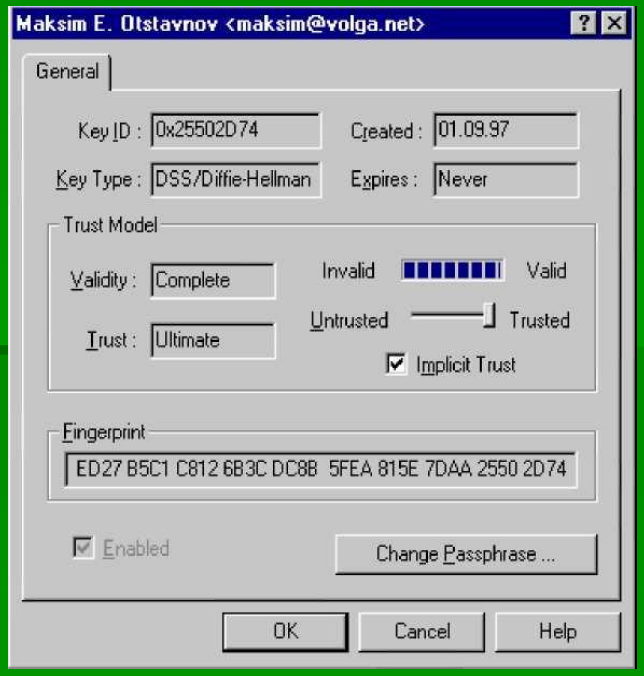
- ***Пара желтых ключей*** символизирует вашу пару ключей типа ***DSS/DH***.
- ***Одиночный желтый ключ*** символизирует открытый ключ типа ***DSS/DH***.
- ***Пара синих ключей*** символизирует вашу пару ключей типа ***RSA***.
- ***Одиночный синий ключ*** символизирует открытый ключ типа ***RSA***.
- ***Ключ или пара ключей серого цвета*** означает, что их использование временно запрещено.
- ***Изображение ключа, перечеркнутое красной линией***, означает, что ключ отозван.
- ***Изображение ключа, перечеркнутое двумя красными линиями***, означает, что ключ неправильный.
- ***Изображение ключа с часами*** означает, что срок действия ключа завершился.

По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

- ***Улыбающаяся рожица*** символизирует владельца ключа и список имен и адресов, связанных с ключом.
- ***Перо*** обозначает подпись третьего лица, ручающегося за его подлинность. Перечеркнутая красной линией подпись – это отозванная подпись, а перечеркнутая двумя красными линиями – недействительная или испорченная.
- ***Пустой прямоугольник*** означает недействительный ключ или ненадежного пользователя.
- ***Наполовину заполненный прямоугольник*** означает отчасти действительный ключ или отчасти надежного пользователя.
- ***Заполненный прямоугольник*** означает действительный ключ или надежного пользователя.
- ***Полосатый прямоугольник*** означает имплицитно действительный ключ и имплицитно надежный ключ. Эти значения присваиваются только сгенерированным вами самим парам ключей.

По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

- Кроме общих атрибутов, отображаемых в главном окне ***PGPkeys***, вы можете исследовать и изменять другие свойства ключей. Чтобы добраться до свойств конкретного ключа, пометьте его и выберите пункт ***Key Properties*** из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши.



## Теоретическая часть



- ***Идентификатор ключа (Key ID)*** – уникальное число, связанное с ключом. Идентификатор ключа нужен для того, чтобы различать разные ключи, носящие одинаковое имя пользователя и почтовый адрес.
- ***Создан (Created)*** – дата, когда был создан ключ.
- ***Тип ключа (Key Type)*** – тип ключа может быть ***RSA*** или ***DSS/DH***.
- ***Срок действия (Expires)*** – дата, когда истекает срок годности ключа.
- ***Модель доверия (Trust Model)*** – отображает действительность ключа, основываясь на сертифицирующих его подписях и уровне надежности, приданном тем, кто эти подписи наложил.
- ***Отпечаток (Fingerprint)*** – уникальный идентификационный номер, генерируемый при создании пары и являющийся основным средством контроля подлинности ключа. **Разрешен (Enabled)** – это поле указывает, разрешено ли использование этого ключа. Для того чтобы разрешить или запретить использование ключа, пометьте или очистите поле ***Enable***, или выберите соответствующую опцию (***Enable*** – разрешить, ***Disable*** – запретить) из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши.
- ***Изменить пароль (Change Passphrase)*** – изменить пароль доступа к закрытому ключу.

# Указание пары ключей, используемой по умолчанию

- Когда Вы подписываете сообщение или ключ, используется ваш ключ по умолчанию. Если Вы обладаете более чем одной парой ключей, вам может понадобиться явно обозначить одну пару, которая будет использоваться по умолчанию. Текущая пара по умолчанию выделяется в окне ***PGPkeys*** жирным шрифтом для того, чтобы ее можно было отличить от остальных пар.

# Последовательность действий:

- 1. Пометьте пару ключей, которую вы хотите использовать по умолчанию. Выберите из меню ***Keys*** пункт ***Set As Default Key***.
- Помеченная пара станет выделена жирным шрифтом, что указывает на ее использование по умолчанию.

# Добавление нового имени или адреса

- В некоторых случаях Вам может понадобиться более чем одно имя или адрес, которые Вы захотите связать с одной и той же парой ключей. После того как пара ключей сгенерирована, вы можете добавить к ней дополнительные имена или адреса. Добавить новое имя или адрес вы можете только в случае, если обладаете обоими ключами, составляющими пару.

# Последовательность действий:

- 1. Выберите пару ключей, к которой Вы хотите добавить новое имя или адрес.

- **2**. Выберите из меню **Keys** (или из контекстного меню, доступного при щелчке правой кнопкой мыши) пункт ***Add Name***. Появится окно Диалога ввода нового имени (**New User Name**).
- **3**. Введите новое имя, затем нажатием ***Tab*** переместите курсор в следующее поле.
- **4**. Введите новый адрес.
- **5**. После ввода имени и адреса щелкните **ОК**. Появится окно Диалога ввода пароля (**Enter Passphrase**).
- **6**. Введите свой пароль и щелкните **ОК**.

По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

- Новое имя будет добавлено в конец списка имен, связанных с ключом. Если вы захотите сделать это имя и адрес первичным идентификатором, пометьте его и выберите пункт ***Set As Primary User ID*** из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши.

# Проверка отпечатка ключа

- Трудно быть уверенным, что ключ принадлежит определенному лицу, если Вы не получили этот ключ непосредственно от него на дискете. Для проверки отпечатка ключа существуют разные способы, но наиболее надежно позвонить владельцу и попросить его прочитать отпечаток по телефону. Крайне маловероятно, что звонок кто-либо перехватит и сумеет сымитировать голос вашего собеседника. Вы также можете сравнить отпечаток вашей копии чьего-либо открытого ключа с отпечатком копии, хранящейся на сервере.

# Последовательность действий:

- **1**. Пометьте ключ, отпечаток которого вы хотите проверить.
- **2**. Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт ***Key Properties.***
- **3**. Посмотрите на отпечаток ***(Fingerprint)*** и сравните его с оригиналом.

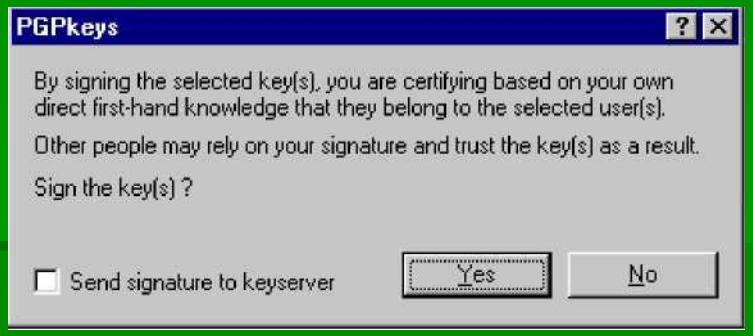
# Сертификация чужого открытого ключа

- Когда Вы генерируете пару ключей, она автоматически подписывается с помощью вашего закрытого ключа. Точно так же после того как Вы убедились, что открытый ключ принадлежит его номинальному владельцу, Вы можете подписать (сертифицировать) этот ключ, указывая, что Вы уверены в действительности оного.

# Последовательность действий:

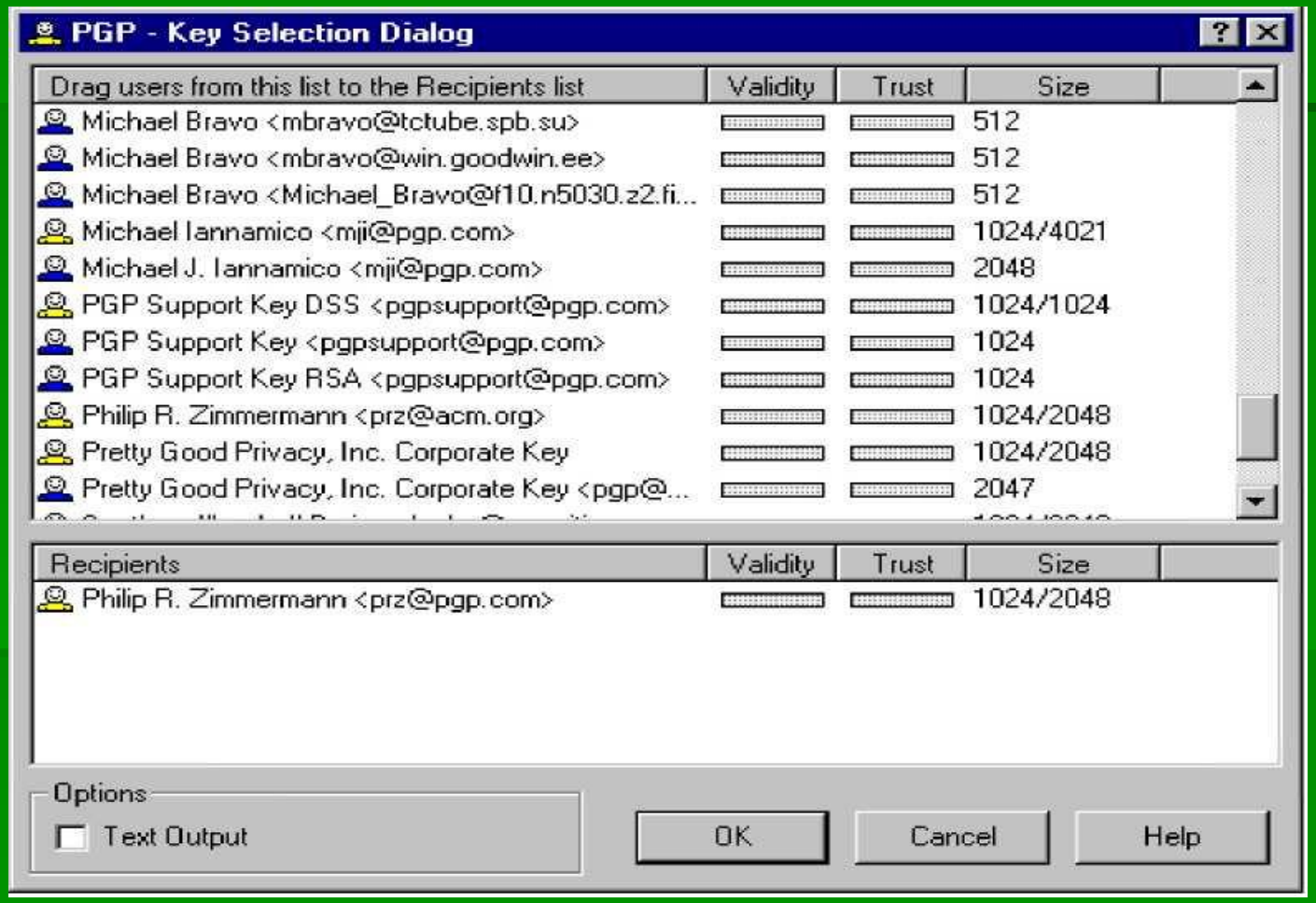
- 1. Пометьте ключ, который хотите подписать.
- 2. Выберите из меню Keys или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт Sign.

- ***Появится окно предупреждения (Alert Box).***




- 3. Щелкните Yes, чтобы подтвердить, что Вы действительно уверены в том, что ключ принадлежит номинальному владельцу.

## Появится окно Диалога ввода пароля (Enter Passphrase).



По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

- 4. Введите свой пароль и щелкните ОК. Если у Вас есть другая пара ключей и Вы хотите подписать ключ с ее помощью, вы можете нажать на стрелку и выбрать нужный ключ.
- 5. После того как Вы сертифицировали ключ, в списке сопровождающих его подписей появится строчка со значком пера и Вашим именем.

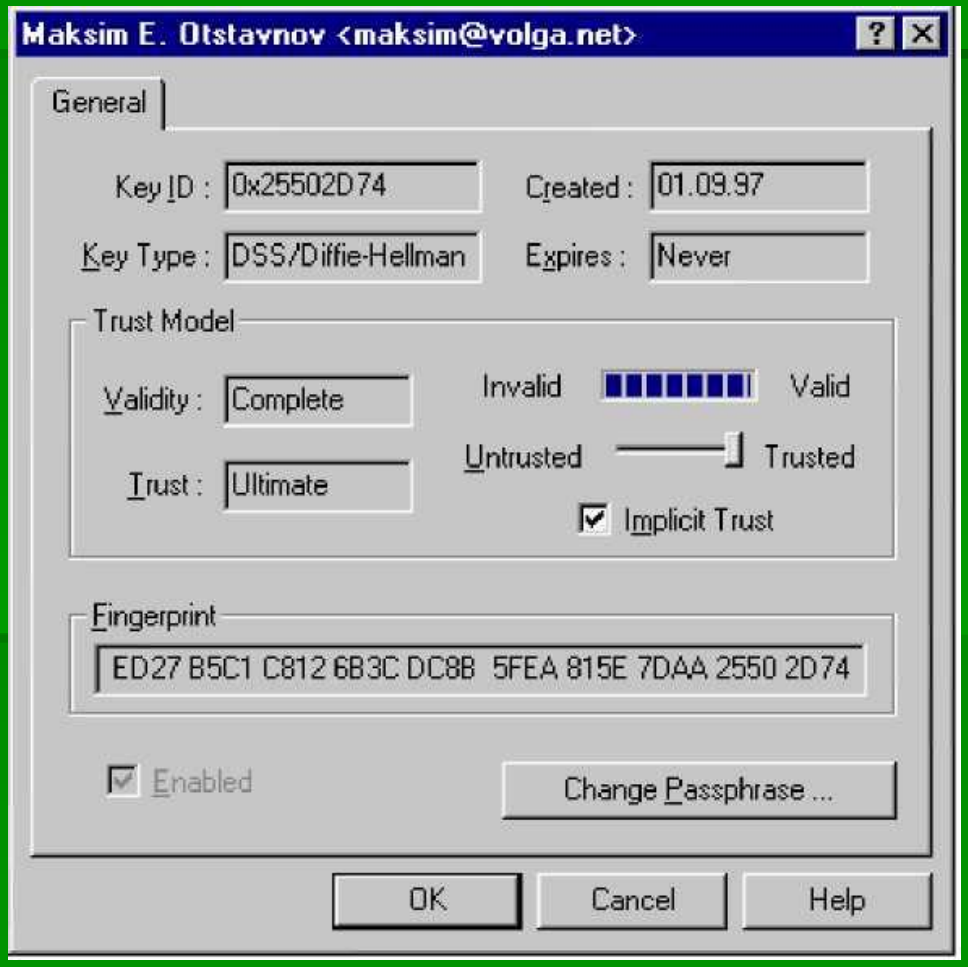
# Указание уровня доверия

- Кроме сертификации принадлежности ключа владельцу, Вы можете присвоить его владельцу определенный уровень доверия, указывающий, насколько вы доверяете ему выступать в качестве посредника, ручающегося за целостность ключей, которые Вы можете получить в будущем.

# Последовательность действий:

- **1**. Пометьте ключ, уровень доверия к владельцу которого вы хотите изменить.
- **2**. Выберите из меню Key или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт ***Key Properties***

# Появится окно Диалога свойств ключа (Properties).



По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

- **3**. Используйте движок уровня доверия *(**Trust Level**)* для установки соответствующего уровня доверия. Вы можете выбрать между уровнями *(Надежный (**Complete**), Отчасти надежный (**Marginal**)* или *Ненадежный (**Untrusted**))* в окне диалога ***Properties***).
- **4**. Для завершения операции щелкните **ОК**.

# Запрет и разрешение использования ключей

- Иногда Вам может понадобиться временно запретить использование ключа. Эта возможность полезна, когда вы хотите сохранить ключ для использования в будущем, но не хотите, чтобы лишние ключи загромождали окно Диалога выбора получателя каждый раз при отправке почты.

# Последовательность действий при запрещении:

- **1**. Пометьте ключ, использование которого хотите запретить.
- **2**. Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Disable.**
- Ключ станет отображаться серым цветом и будет временно запрещен к использованию.

# Последовательность действий при разрешении:

- **1**. Пометьте ключ, использование которого хотите разрешить.
- **2.** Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Enable.**
- Ключ станет отображаться обычным цветом и будет разрешен к использованию.

# Удаление ключа, подписи или идентификатора пользователя

- В какой-то момент Вам может понадобиться удалить ключ, сертифицирующую его подпись или идентификатор пользователя, связанный с конкретным ключом.

# Последовательность действий:

- **1.** Пометьте ключ, подпись или идентификатор пользователя, который хотите удалить.
- **2.** Выберите из меню ***Edit*** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт ***Delete.***

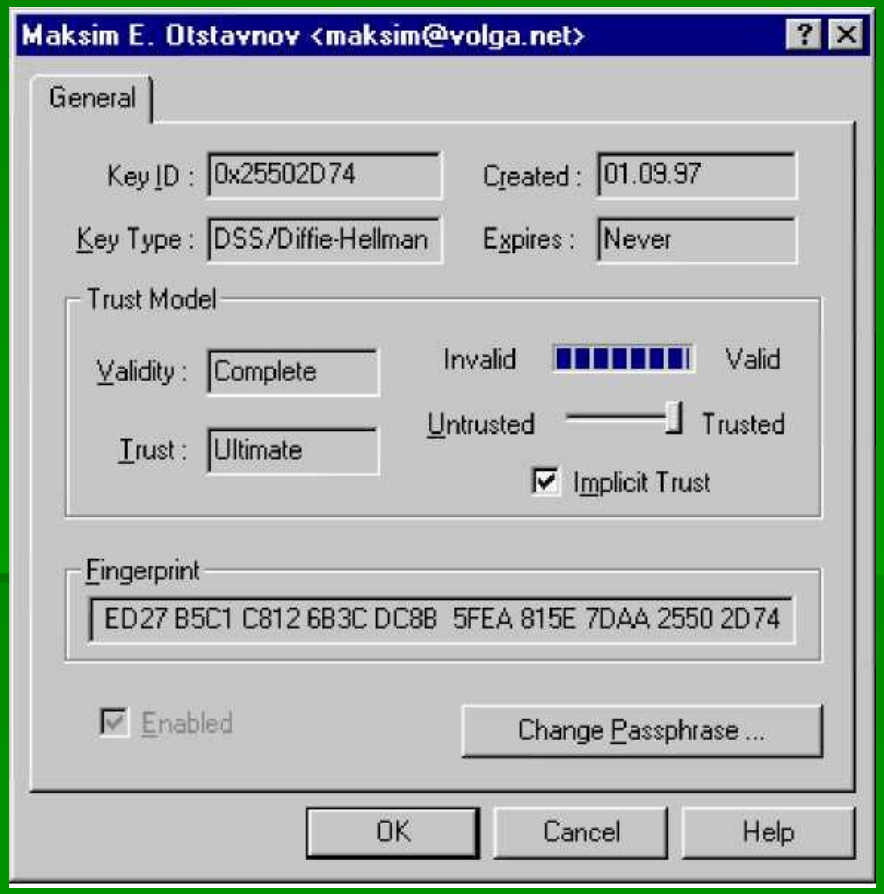
# Изменение пароля доступа

- Периодически менять пароль доступа к закрытому ключу – неплохая идея. Если вы хотите изменить пароль, сделать это очень просто.

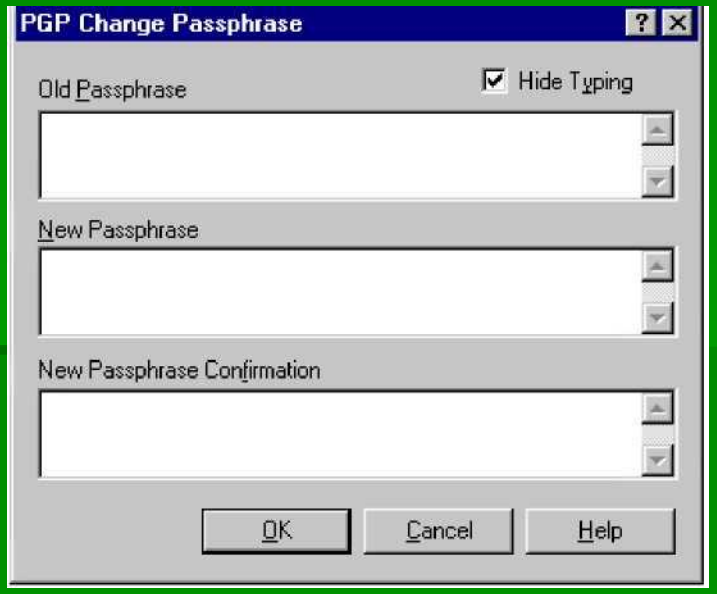
# Последовательность действий:

- **1.** Пометьте пару ключей, пароль доступа к которой хотите изменить.
- **2.** Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Key Properties.**

# Появится окно Диалога свойств ключа (Properties).



3. Щелкните на кнопке изменения пароля ***Change Passphrase.*** Появится окно Диалога смены пароля (Change Passphrase).



По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

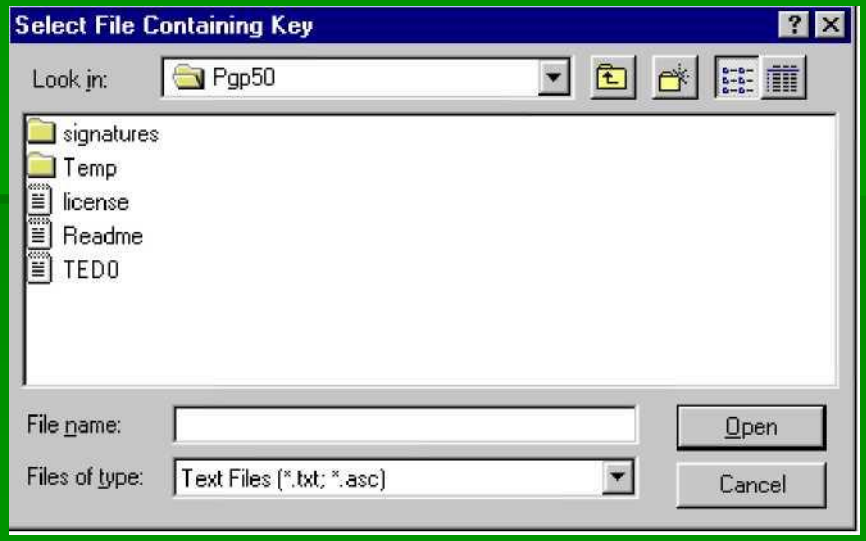
- **4.** Введите свой старый пароль в верхнем поле и нажмите ***Tab*** для перехода к следующему полю.
- **5.** Введите свой новый пароль в среднем поле и нажмите ***Tab*** для перехода к нижнему полю.
- **6.** Подтвердите новый пароль, введя его в нижнем поле еще раз.
- **7**. Щелкните **ОК**.

# Импорт и экспорт ключей

- Хотя Вы чаще распространяете свой открытый ключ и получаете открытые ключи других посредством сервера открытых ключей, обмениваться ключами можно также импортируя и экспортируя их в виде текстовых файлов.

# Последовательность действий для импорта ключа:

- **1.** Выберите пункт ***Import*** из меню **Keys**.
- *Появится окно Диалога выбора файла, содержащего ключ (**Select File Containing Key**).*



По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

- **2.** Выберите файл, содержащий ключ, который вы хотите импортировать, и щелкните Open.
- В окне ***PGPkeys*** появится вновь импортированный ключ, который теперь можно использовать для шифрования данных и верификации подписи его владельца.

# Последовательность действий для экспорта ключа:

- **1.** Пометьте ключ, который хотите экспортировать в файл.
- **2.** Выберите из меню **Keys** или из контекстного меню, доступного при щелчке правой кнопкой мыши, пункт **Export.**

# Появится окно Диалога выбора файла (Export Key to File).

По заказу ФГУ ГНИИ ИТТ «Информика» Северо-Кавказский государственный технический университет Кафедра защиты информации, zik@ncstu.ru

- **3.** Введите имя файла, в который хотите экспортировать ключ, и щелкните **Save.**
- Экспортированный ключ будет помещен в файл с заданным именем и указанным местоположением.

# Отзыв ключа

- Если когда-либо возникнет ситуация, в которой Вы не сможете больше доверять своей персональной паре ключей, вы можете выпустить сертификат отзыва ключа, сообщающий всем, что Ваш соответствующий открытый ключ не должен более использоваться. Лучший способ распространить сертификат отзыва – это поместить его на сервер открытых ключей.

# Практическая часть

- **Создайте новую пару ключей и выполните шифрование данных**

- **Результат:** Изучив материал, вы научитесь пользоваться технологией шифрования данных с использованием открытых и закрытых ключей.