Электронная цифровая подпись «для чайников». Часть 4

http://habrahabr.ru/blogs/infosecurity/99038/

В предыдущих частях мы приблизительно разобрались, что же именно мы собираемся есть. Теперь, наконец, перейдем непосредственно к выбору блюда нам по вкусу. Здесь мы рассмотрим цели использования цифровой подписи, к какому лагерю примкнуть и в чем особенности использования каждого из вариантов, а также коснемся юридической подоплеки использования цифровых подписей. Параллельно, мы будем рассматривать возникающие в процессе вопросы и углублять те познания о работе механизма, которыми на данный момент обладаем.

Допустим, у вас возникло непреодолимое желание, а, может быть, насущная необходимость использовать цифровую подпись. Первый же всеобъемлющий вопрос, который вы должны себе задать: зачем? Если вы не можете более-менее однозначно на этот вопрос ответить, то подумайте дважды перед тем, как идти по пути использования этой технологии дальше. Ведь внедрение, а главное, использование цифровой подписи в любой ее ипостаси — достаточно трудоемкий процесс, поэтому если четкого понимания поставленных целей нет, лучше даже не браться.

Пусть, вы все же понимаете, что цифровая подпись вам просто необходима. И необходима она вам, естественно, для защиты вашей информации. Теперь рассмотрим ситуации, в которых возможно применять цифровую подпись и шифрование в порядке усложнения.

Начнем со сравнительно простого варианта: вы — частное лицо и хотите защитить отсылаемую вами по электронным источникам информацию от подмены, а также, может быть, и от прочтения посторонними людьми. Информацию вы отсылаете такому же обыкновенному человеку, с которым вы всегда можете договориться о том, как же будете защищать вашу информацию. Что же вам для этого необходимо?

Рассмотрение начнем с S/MIME. Сделаем это, во-первых, потому, что данный формат, как я уже говорил, существенно более распространен, а главное: он поддерживается на уровне Windows (а Windows, как ни крути, самая распространенная операционная система), а также многими программами, которые под Windows работают. Ну а во-вторых — данный формат с юридической точки зрения позволяет (в рамках нашего государства, естественно) существенно больше.

Какой самый простой и распространенный способ передать информацию другому человеку? Конечно же, это — электронная почта. Берем письмо, цепляем к нему файлы и отправляем. И тут нам с цифровой подписью в формате S/MIME особенно везет: все

распространенные почтовые клиенты умеют как принимать сообщения с цифровой подписью, так и отправлять их. При этом подписывается все письмо целиком, включая присоединенные к письму файлы.

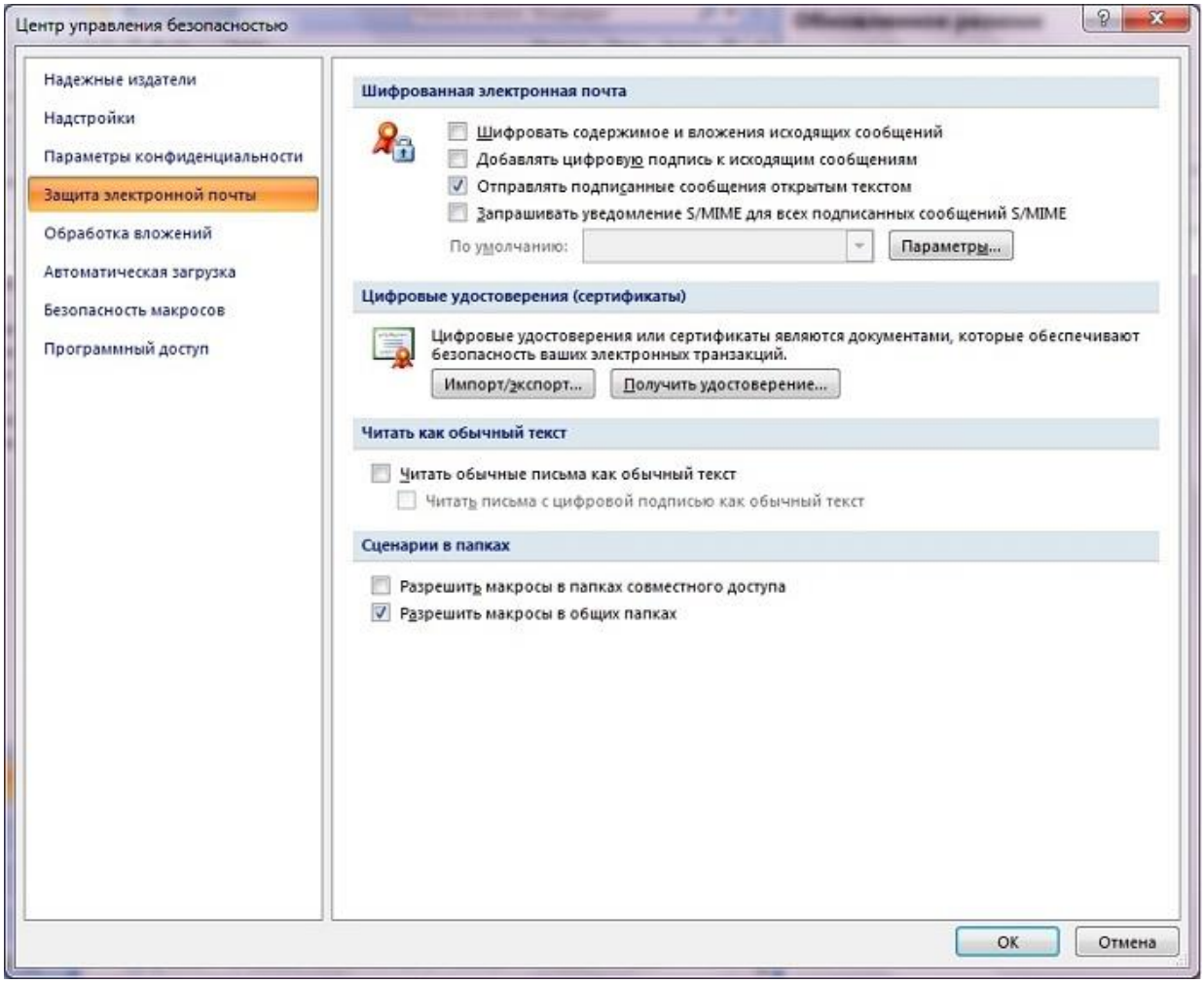


Рисунок 1. Страница центра управления безопасностью Outlook 2007

И все бы хорошо, вот только для того, чтобы отправить письмо с подписью надо иметь программу, которая осуществляет работу с криптографией (криптопровайдер или cryptographic service provider, CSP), и сертификат определенного назначения и связанный с ним закрытый ключ. Назначение сертификата — это та область, в которой он может быть использован. Подробнее о назначениях сертификатов мы поговорим позже, а для текущей задачи нам, собственно говоря, нужен сертификат для защиты электронной почты (email protection certificate).

Но вернемся к нашим потребностям. Где взять эту самую программу, криптопровайдер? На наше счастье, операционная система Windows не только поддерживает сам формат, но и содержит в себе набор криптопровайдеров, которые идут в комплекте с любой из версий системы абсолютно бесплатно, то есть даром. А значит, самое очевидное решение для данной ситуации — использовать именно их.

Итак, с криптопровайдером мы разобрались, но что же делать с сертификатом? В предыдущей части я говорил, что в процессе выдачи сертификатов участвует некая третья сторона — удостоверяющий центр, которая и осуществляет выпуск, непосредственно, сертификатов и удостоверение их содержимого и актуальности. Остановлюсь на этом моменте несколько подробнее, так как эти знания понадобятся нам в дальнейшем.

Подтверждением, что данный конкретный пользовательский сертификат корректен, и что содержимое в нем не было изменено является все та же самая цифровая подпись, только подписывается уже удостоверяющий центр.

У удостоверяющего центра, также, как и у пользователей, есть собственный сертификат. И вот именно с его помощью он подписывает выдаваемые им сертификаты. Эта процедура, во-первых, защищает выдаваемые удостоверяющим центром сертификаты от изменения (о чем я уже сказал выше), а во-вторых однозначно показывает, какой именно удостоверяющий центр данный сертификат выдал. Как следствие, нехороший человек, конечно, может сделать полную копию вашего сертификата, с вашими именем, фамилией, даже любой дополнительной информацией, вот только подделать цифровую подпись удостоверяющего центра, не имея его закрытого ключа, для него будет практически невыполнимой задачей, а значит и распознать эту подделку будет не просто легко, а очень легко.

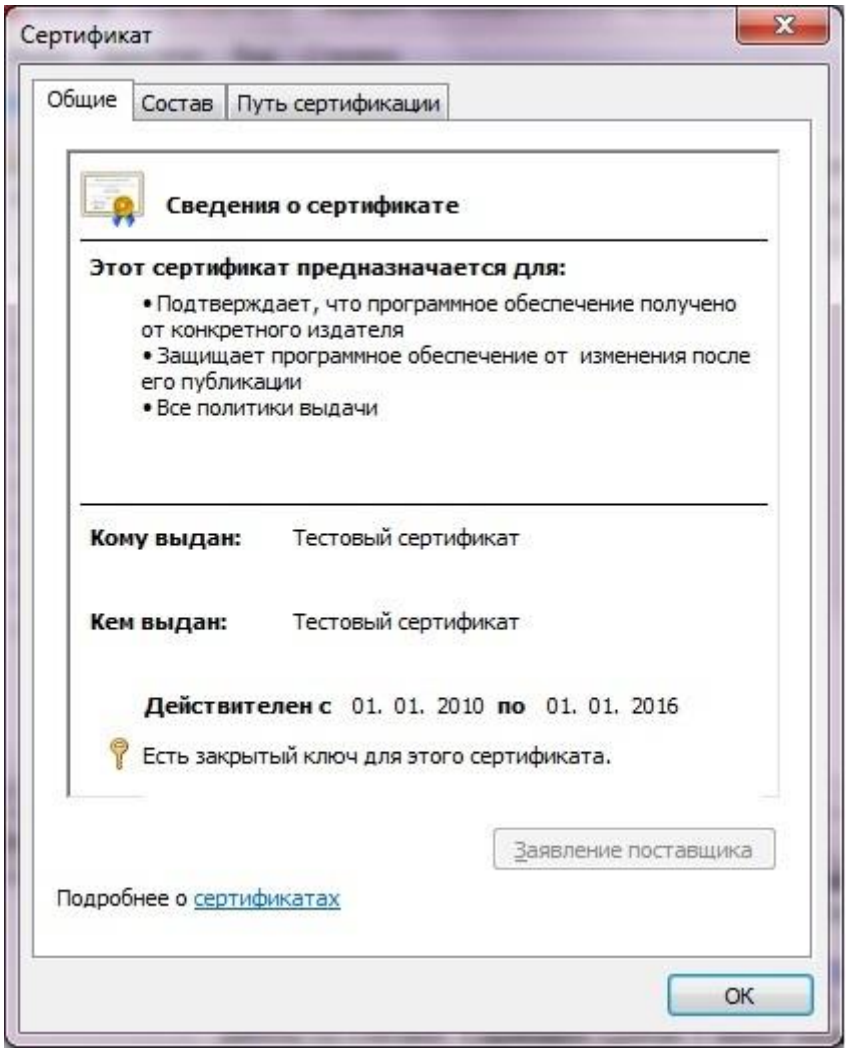
Сам же сертификат удостоверяющего центра, по-хорошему, тоже должен быть защищен. А значит, и подписан. Кем? Более высоко стоящим удостоверяющим центром. А тот, в свою очередь, еще более вышестоящим. И такая цепочка может быть очень длинной. Чем же она заканчивается?

А заканчивается она самоподписанным сертификатом удостоверяющего центра. Такой сертификат подписан закрытым ключом, связанным с ним же. Приводя аналогию, это как справка о занимаемой должности и зарплате генерального директора. «Данной справкой Иванов И.И., генеральный директор ООО „Одуванчик“ удостоверяет, что Иванов И.И. занимает в данной организации должность генерального директора и получает зарплату в размере ####### рублей». Чтобы данной справке верить, вы должны верить самой фирме ООО «Одуванчик», причем вера эта не подкрепляется никакой третьей стороной.

Так же и с корневыми сертификатами (т.е. сертификатами удостоверяющих центров). Самоподписанные сертификаты тех удостоверяющих центров, которым вы доверяете, должны лежать в специальном хранилище в системе, которое называется «Доверенные корневые центры сертификации». Но перед тем, как попасть туда, их надо как-то получить. И это — самое слабое звено в системе. Сам самоподписанный сертификат подделать, так же, как и пользовательский, не получится, зато замечательно получится

подменить при передаче. Значит, передача должна осуществляться по защищенному от подмены каналу.

Чтобы избежать, по возможности, подобных трудностей, Microsoft выбрала несколько удостоверяющих центров и включила их сертификаты прямо в установку Windows (это Thawte, VeriSign и другие). Они уже есть у вас на компьютере и их не надо ниоткуда получать. А значит и подменить их можно только, если у вас на компьютере живет троян (или у нехорошего человека должен быть администраторский доступ к вашему компьютеру), а говорить об использовании цифровой подписи в таком случае несколько бессмысленно. Кроме того, эти удостоверяющие центры широко известны и много кем используемы, и простая подмена их сертификатов приведет к множеству ошибок в работе, скажем, сайтов, чьи сертификаты выданы этими удостоверяющими центрами, что, в свою очередь, достаточно быстро наведет на мысль о том, что что-то здесь не чисто.



Кстати, о самоподписанных сертификатах: такой сертификат можно создать и для собственного пользования, а не только для удостоверяющего центра. Естественно, такой сертификат наследует все минусы сертификатов подобного типа, но для проверки того,

стоит ли использовать цифровую подпись в переписке, или лучше так обойтись он отлично подходит. Для создания подобных сертификатов можно использовать программу, входящую в состав средств Microsoft Office (Цифровой сертификат для проектов VBA), или же, для лучшей настройки назначения и прочих полей данного сертификата, программу стороннего производителя, например КриптоАрм, который даже в бесплатной своей версии позволяет такие сертификаты создавать.

Рисунок 2. Просмотр самоподписанного сертификата средствами системы Windows

Итак, мы выбираем некий устраивающий нас обоих удостоверяющий центр, получаем на нем сертификаты (для чего заполняем форму на сайте, предоставляем необходимые документы и платим деньги, если потребуется), или создаем себе самоподписанный сертификат и… Собственно говоря, все. Теперь мы можем с помощью нашего почтового клиента (того же Outlook'a) отправлять и принимать подписанные и зашифрованные сообщения.

Для использования стандарта OpenPGP все и проще и сложнее. Для использования данного стандарта все так же необходимы криптопровайдер, пара из открытого и закрытого ключа и программа, осуществляющая непосредственно подписание и шифрование. Для OpenPGP все эти компоненты могут быть как платными, так и бесплатными. С бесплатными больше мороки по установке, а с платными меньше, но принципы и у тех, у тех одинаковы.

Следуя уже использованной последовательности описания, начнем с программы, с которой вы и будете контактировать больше всего: почтовым клиентом. Использование чистого Outlook'a здесь уже невозможно, по причине незнания им о стандарте OpenPGP, а значит надо либо переходить на клиент, который стандарт знает, либо использовать плагины к Outlook'у, или же даже осуществлять работу с подписями и шифрованием через копирование информации во внешние программы. Как пример почтовых клиентов, работающих со стандартом OpenPGP, можно привести Mozilla Thunderbird к которому, кстати, все равно нужен плагин или же The Bat!, умеющий в версии Profissional работать со стандартом OpenPGP сам по себе.

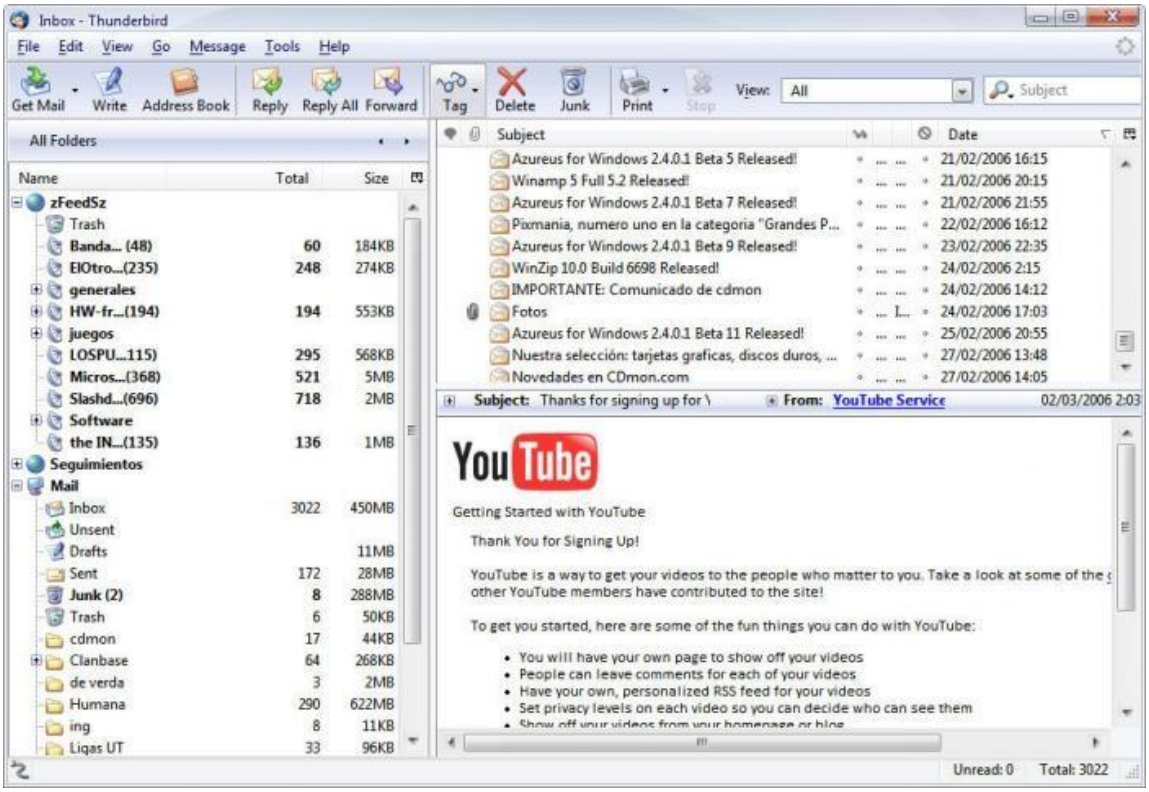


Рисунок 3. Экран почтового клиента Thunderbird

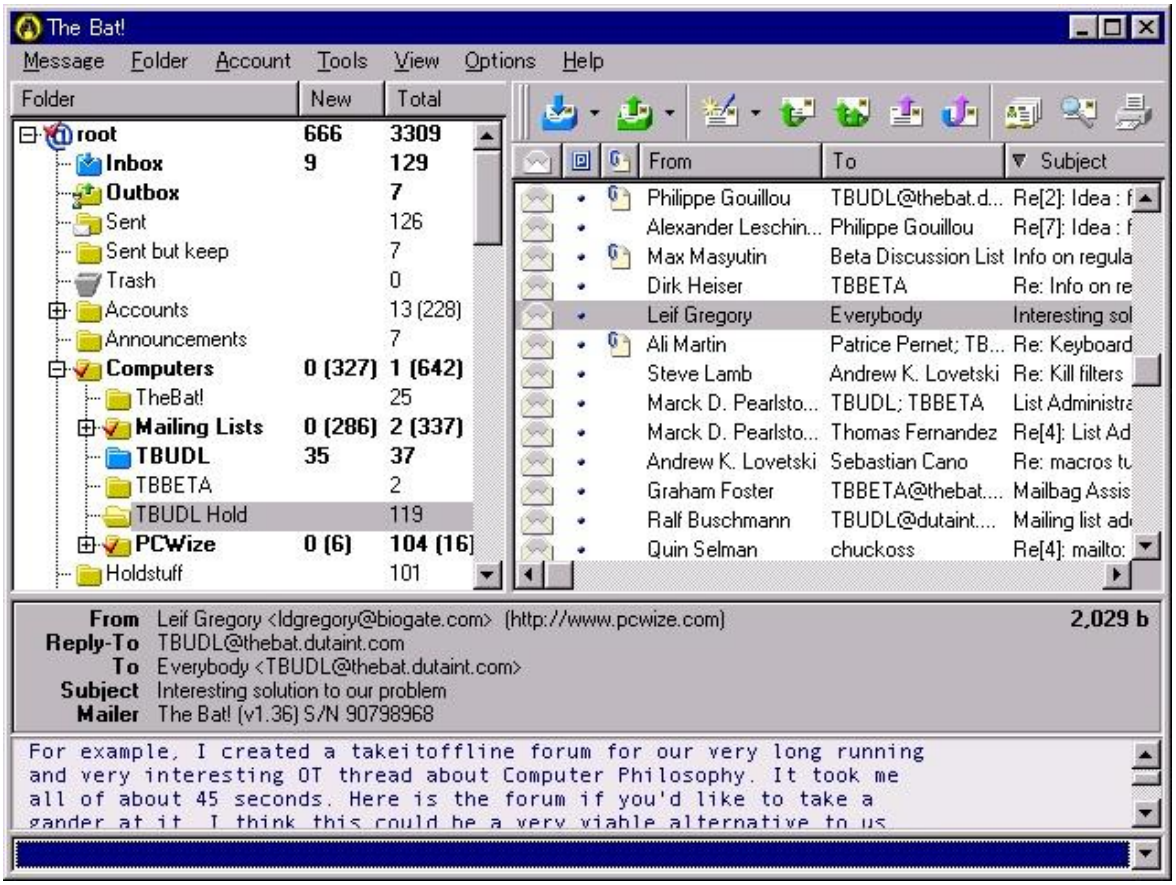


Рисунок 4. Экран почтовой программы The Bat.

Плагины, необходимые для работы со стандартом OpenPGP в почте, также можно найти как платные, так и бесплатные. Платные плагины поставляются вместе с платными же версиями программы PGP, а как пример бесплатного плагина можно привести плагин Enigmail для все того же Thunderbird.

Рисунок 5. Дополнения, появляющиеся в почтовом клиенте после установки Enigmail

Криптопровайдеры же здесь все так или иначе бесплатные. Можно использовать криптопровайдер, поставляющийся в составе даже бесплатной версии программы PGP, а можно использовать GnuPG.

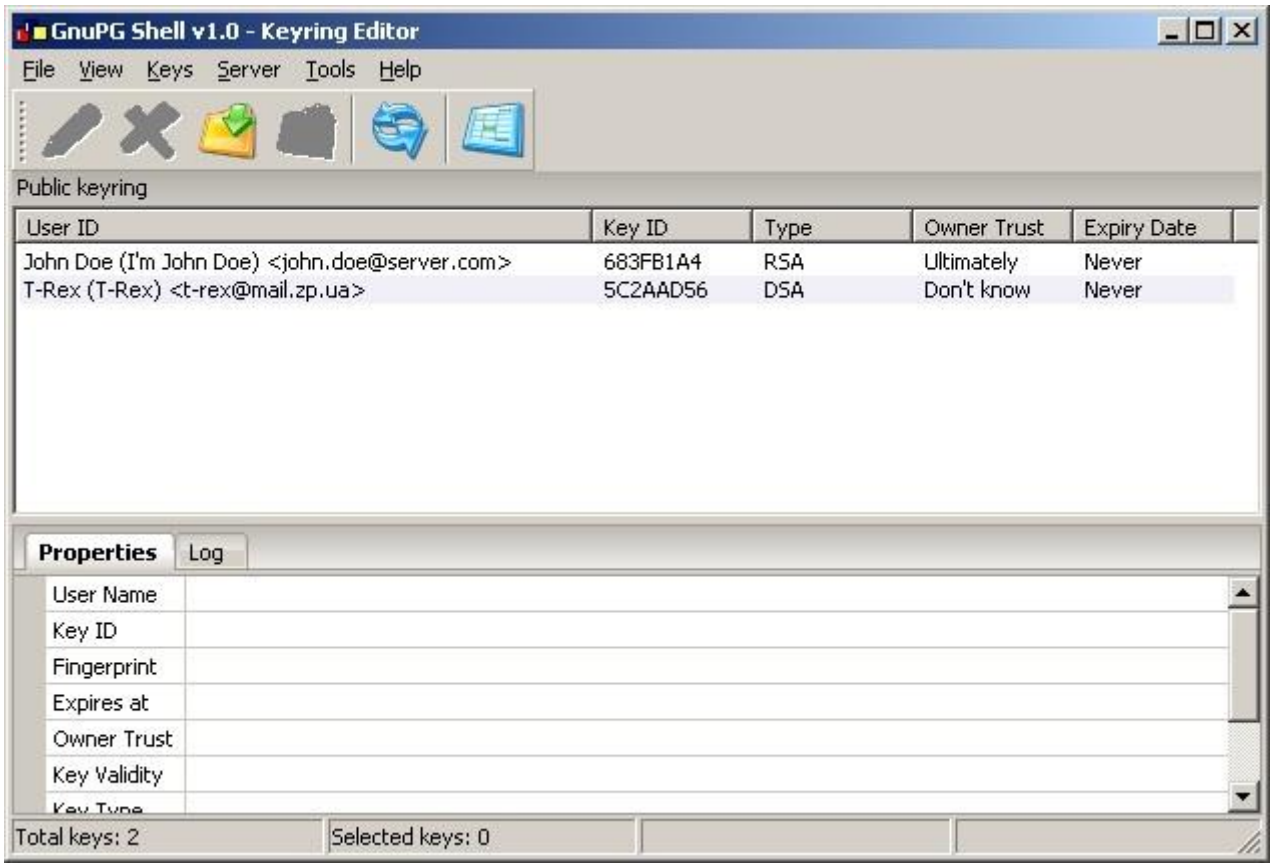


Рисунок 6. Страница управления ключами GnuPG

Здесь, пожалуй, стоит немного предостеречь тех, кто погонится за бесплатностью и открытостью кода. Большинство подобных приложений действительно работают и выполняют свои функции, но есть ряд проблем, характерных для всех них. И особенно весомо звучит проблема недостаточного тестирования и проблема проработки пользовательских интерфейсов. Обе эти проблемы коренные для свободного ПО по самой его сути: разработка ведется «всем миром» (или отдельной группой), а значит у проектов в большинстве случаев нету общего идеолога, нету общего конструктора, дизайнера и т.п. В итоге, зачастую получается ситуация «что выросло — то выросло», а это не всегда удобно чисто с функциональной точки зрения. Тестирование тоже, как правило, ведется «всем миром», а не профессиональными тестировщиками, над которыми нависает злой руководитель, поэтому багов в итоговую версию попадает больше. Кроме того, если обнаружен баг, который может привести к потере вашей информации, спросить бывает некого: ПО-то бесплатное и открытое, и финансовой или юридической ответственности перед вами точно никто не несет. Впрочем, не стоит обольщаться, с платным ПО ситуация ровно такая же, хотя в редких случаях возможны варианты. К сожалению, эти случаи относятся, скорее, к компаниям-партнерам и корпоративным клиентам, поэтому для нас, простых пользователей, можно с тем же успехом считать, что вариантов нет.

При этом я ни в коей мере не хочу умолять достоинства такого рода софта. Вообще-то, рассматривая и платные, и бесплатные программы, работающие с криптографией, можно заметить, что первой проблеме — багам — данный софт практически (за редким исключением, которым просто не надо пользоваться) не подвержен. А вот вторая — ужасающие с точки зрения пользователя интерфейсы — касается, как ни странно, почти всех. И если причиной такой ситуации для свободного ПО может быть принято как раз «что выросло — то выросло» (скажем, у замечательной во всех отношениях программы TrueCrypt, являющейся де-факто стандартом в области шифрования данных, интерфейс ужасающ для человека, не очень глубоко разбирающегося в вопросе), то аналогичную ситуацию с платным ПО можно объяснить, пожалуй, только тем, что криптография, как направление разработки, обычно рассматривается по остаточному принципу. Исключения из этих правил встречаются и там, и там, но большее число исключений лично мне, все же, встречалось в лагере платного ПО.

Но, вернемся к нашей почте. Остался нерешенным вопрос сертификата. «Проще и сложнее» живет именно здесь. Создать его вы можете прямо у себя на компьютере, не прибегая к услугам внешнего удостоверяющего центра, что, согласитесь, проще, чем отправлять запрос в какой-то удостоверяющий центр. Но отсюда и проблемы с данными сертификатами: они все самоподписанные, а значит на них распространяются те же

вопросы, которые мы рассматривали с самоподписанными сертификатами удостоверяющих центров. Второй пункт, собственно говоря и является тем самым «сложнее».

Проблема доверия к сертификатам в данном лагере решается с помощью сетей доверия, принцип которых можно вкратце описать следующим образом: чем больше человек знают вас (ваш сертификат), тем больше оснований для доверия. Кроме того, облегчить решение проблемы передачи сертификата получателю могут публичные банки сертификатов, в недрах которых покопаться нехорошему человеку несколько сложнее, чем в передаваемой почте. В данный банк можно загрузить сертификат при его создании, а получателю просто передать, откуда ему следует этот сертификат забрать.

Сертификаты хранятся в некоторых хранилищах, которые создают на вашей машине программы для работы со стандартом OpenPGP, они обеспечивают доступ к ним. Об этом тоже не стоит забывать, ведь это означает, что получить доступ к этим сертификатам только лишь силами операционной системы без использования данных программ не получится.

Все, как и в случае S/MIME, вышеописанного набора действий вам уже хватит для достижения поставленной нами цели: обмена подписанной и зашифрованной почтой.

Итак, начало положено. Мы уже можем употребить первое, достаточно простое блюдо с приправой в виде цифровых подписей, но оно хорошо лишь для затравки и останавливаться на нем, естественно, не стоит. В дальнейших статьях мы будем разбирать все более и более сложные ситуации, и все больше и больше узнавать про особенности этой технологии.