Московский Физико-Технический Институт
Факультет Радиотехники и Кибернетики

***Эссе*: "Цифровая подпись для физического адреса(почтового ящика)"**

***Предмет*:** Защита информации
***Преподаватель*:** Обернихин В.В.
***Автор*:** Кудрявцев А.С., студент 911 гр.

2003 г.

Введение.

Рукописные подписи издавна используются как доказательство авторства документа или, по краеней мере, согласия с ним. Что же такого притягательного в подписи:

1. Подпись достоверна. Она убеждает получателя документа в том, что подписавший сознательно подписал документ.
2. Подпись неподдельна. Она доказывает, что именно подписавший, и никто иной сознательно подписал документ.
3. Подпись не может быть использована повторно. Она является частью документа, жулик не сможет перенести подпись на другой документ.
4. Подписанный документ нельзя изменить. После того, как документ подписан, его невозможно изменить.
5. От подписи невозможно отречься. Подпись и документ материальны. Подписавший не сможет впоследствии утверждать, что он не подписывал документ.

Достаточно важный элемент современного использования электронной почты, особенно в сфере бизнеса, - это применение шифрования текста писем и защита сообщений с помощью цифровой подписи. В случае шифрования вы будете уверены, что никто, кроме вашего адресата, не сможет познакомиться с содержимым вашего письма, а цифровая подпись гарантирует, что если кто-то по пути открывал файл с вашим письмом и изменял содержимое, то это не останется незамеченным.

Сообщение e-mail по пути следования от вашего компьютера до конечного адресата проходит через несколько почтовых серверов и в принципе, на любом из них оно может быть прочитано персоналом провайдеров, отредактировано или даже подменено на ложное сообщение. Разумеется, через почтовые серверы проходят в день тысячи, если не миллионы писем, и прочитать их все просто невозможно. Вдобавок положение о провайдерах Интернета в любой стране запрещает персоналу читать электронные письма клиентов. Поэтому, если вы пишете самое обычное письмо своему приятелю, то можете быть на "на все сто" уверены, что его вряд ли кто прочтет. Но... любители чужих секретов могут в

принципе поставить на поток проходящих через почтовый сервер писем некие программы-фильтры, которые отлавливают определенные адреса e-mail или слова или сочетания символов в тексте писем (такие как 16-значные номера кредиток) и далее отсортированная таким образом почта может подвергнуться уже ручному просмотру.

Поэтому шифрование сообщений и применение цифровой подписи - основная мера, которая может на многие порядки снизить вероятность прочтения электронного письма и его подмену на письмо с другим содержанием.

Правовые аспекты.

Документ, исходящий от организации, должен отвечать определенным требованиям, в том числе иметь соответствующие реквизиты и быть подписан компетентным должностным лицом. Что касается подписей лиц, уполномоченных распоряжаться счетом, то при их отсутствии ни один расчетно-кассовый документ не может считаться оформленным надлежащим образом. Однако если документ изготовлен в электронной форме, он не может быть подписан обычным способом (физическая подпись). Практика выработала иную систему подписи - электронную цифровую подпись (ЭЦП). В соответствии с п.2 ст.160 УК РФ использование при совершении сделок ЭЦП допускается в случаях и порядке, предусмотренных законом, иными правовыми актами или соглашением сторон.

ЭЦП представляет собой набор байтов, который является результатом работы программы генерации цифровой подписи ЭЦП. ЭЦП является аналогом физической подписи и обладает двумя основными свойствами: воспроизводима только одним лицом, а подлинность ее может быть удостоверена многими; она неразрывно связана с конкретным документом и только с ним. ЭЦП предназначена для обеспечения подлинности, целостности и авторства документов, обрабатываемых с помощью вычислительной техники. ЭЦП жестко увязывает в одно целое содержание документа и секретный ключ подписывающего и делает невозможным изменение документа без нарушения подлинности этой подписи.

Суть процедуры использования ЭЦП состоит в том, что каждый пользователь программного обеспечения имеет возможность изготовить пару индивидуальных ключей: секретного - для формирования цифрового аналога подписи под документом и парного с ним, открытого - для проверки достоверности цифровых подписей, вычисленных с помощью данного секретного ключа. С помощью открытого ключа пользователя можно гарантированно подтверждать подлинность и авторство электронных документов, что именно данная последовательность бит была передана и подписана обладателем секретного ключа, соответствующего открытому ключу проверки.

Секретный ключ для электронной цифровой подписи может храниться в виде файла на дискете или на специальном устройстве - "таблетке" (Touch-Memory). Их называют носителями секретного ключа.

Для обеспечения целостности и достоверности сообщений, циркулирующих в системе Центрального банка Российской Федерации, приказом ЦБ РФ от 21 сентября 1993 г. N 02-159 был введен в действие стандарт Центрального банка Российской Федерации "Подпись цифровая электронная".

Для обеспечения безопасности электронных платежей наряду с использованием ЭЦП может дополнительно применяться шифрование электронных документов. Для этой цели используются специальные ключи для шифрования (дешифрования), изготавливаемые, как правило, банком.

Поскольку применение ЭЦП в современном деловом обороте Российской Федерации стало реальностью, закономерно поставить вопрос о доказательственной силе заверенных ЭЦП документов. В связи с использованием таких документов на практике могут возникать споры, в процессе рассмотрения которых такие документы будут представляться сторонами в качестве доказательств по делу. Сейчас можно достаточно уверенно признать за документами в электронной форме, подписанными с помощью ЭЦП, доказательственную силу.

Первым в России использовал электронную подпись Межбанковский финансовый дом. Летом 1993 года юридическая фирма ЮКОН по заказу МФД разработала методику заключения финансовых сделок с использованием модема и электронной подписи. Договор об оплате заказа также был заключен с использованием электронной подписи. Далее заказчик отказался оплатить услуги партнера, тем самым спровоцировав передачу дела в арбитражный суд г.Москвы. Появился первый прецедент рассмотрения судом финансового спора по электронному договору. 28 июля того же года арбитражный суд завершился определением в пользу истца, признанием договора с электронной подписью правомочным. МФД, с которого по постановлению суда взыскали 100 тыс.рублей, трактует это как доказательство законности электронной подписи.

Подпись документа с помощью криптографии с открытыми ключами.

Существуют алгоритмы с открытыми ключами, которые можно использовать для цифровых подписей. В некоторых алгоритмах – примером является RSA – для шифрования может быть использован или открытый, или закрытый ключ. Зашифровав документ своим закрытым ключом, вы получите надёжную цифровую подпись. В других случаях – примером является DSA – для цифровых подписей используется отдельный алгоритм, который невозможно использовать для шифрования. Эта идея была впервые изобретена Диффи и Хеллманом и в дальнейшем была расширена и углублена в других работах.

В цифровые подписи часто включают метки времени. Дата и время написания добавляется к документу и подписываются вместе со всем содержанием сообщения.

Возможности шифрования популярных почтовых программ .

Последние версии многих популярных программ по работе с электронной почтой включают способность посылать и получить зашифрованную электронную почту и подписывать письма цифровыми подписями. Программы Microsoft Outlook, Microsoft Outlook Express, и Netscape Messenger могут посылать сообщения и подписывать их от пользователей, у которых имеется цифровое свидетельство, например VeriSign Digital ID. Они могут также использоваться, чтобы посылать зашифрованные сообщения другим пользователям, если они имеют такое

свидетельство. Цифровые удостоверения часто бывают бесплатными на испытательный срок, но после этого пользователям потребуется платить небольшую ежегодную плату. Другая программа - Eudora light и Eudora Pro - доступна со встроенным PGP. Поскольку пользователи могут генерировать свои собственные PGP ключи, им нет необходимости в приобретении цифрового удостоверения.

Поддержка PGP может быть включена другим программам по работе с электронной почтой, включая Microsoft Outlook, Microsoft Outlook Express, Microsoft Exchange, Lotus Notes, Netscape Messenger, Pegasus Mail, Claris Emailer, Elm, Pine, Zmail, и Emacs.

Стандарт S/MIME.

"***Secure/Multipurpose Internet Mail Extensions***" является стандартом, позволяющим использовать X.509 - сертификаты для защиты e-mail-обмена. X.509 - сертификаты широко применяются также для защиты других электронных коммуникаций, таких как HTTP и др. Таким образом, один и тот же сертификат используется в различных целях и разным програмным обеспечением.

S/MIME представляет собой реализацию криптографической системы с асимметричным ключом. Система может быть использована как для внедрения так называемой digital signature (электронной подписи) в ваши почтовые сообщения, так и для шифрования последних. Поддерживается также комбинация двух вышеперечисленных методов. Система с асимметричным ключом отличается от традиционной (работающей с симметричным ключом), в первую очередь, тем, что вам не придется сообщать вашему корреспонденту по телефону или каким-либо иным методом пароль, который вы использовали для пересылки ему секретных сведений: система с асимметричным ключом сделает это за вас. Все, что надо иметь, чтобы послать такие сведения - это публичную часть S/MIME-сертификата адресата, т.е. ту его часть, которая ни в коем случае секретом не является. Разумеется, ваш корреспондент должен иметь и **секретную** часть своего S/MIME-сертификата, иначе он не сможет дешифровать тот текст, что вы ему пошлете (как не сможет этого сделать и никто другой, не имея секретной части его S/MIME-сертификата).

В случае применения электронной подписи подписанное сообщение передается в "читабельной" форме, т.е. в нешифрованном виде, однако получатель письма имеет возможность убедиться в том, что автором сообщения и в самом деле являетесь вы, а главное - возможность убедиться в том, что данное сообщение никем не было изменено "по дороге". При этом получателю письма для подобной проверки не требуется никакой дополнительной информации, так как публичная часть S/MIME-сертификата отправителя подписанного письма (необходимая для процесса "сверки" подписи) передается вместе с подписанным письмом. Такие электронным образом подписанные сообщения уже на протяжении нескольких лет принимаются судами ряда западных стран в качестве свидетельских показаний и т.д., по имеющейся информации в ближайшее время аналогичный закон должен быть принят и в России (что позволит, в частности, принимать налоговые декларации от граждан по электронной почте).

В случае использования шифрованных сообщений прочитать текст письма сможет лишь тот человек (те люди), кому вы в момент написания шифрования явно предоставляется такое право (те, кому шифруется сообщение). Наконец, применение комбинации обоих методов означает, что прочитать сообщение сможет лишь тот, кому оно предназначено, и он же сможет убедиться в том, что сообщение и в самом деле написано вами.

Для использования возможностей S/MIME, прежде всего, необходимо получить "сертификат", состоящий из двух частей: секретного ключа и публичного ключа. Должна быть защита сертификата от несанкционированного доступа, и уж в любом случае нельзя сообщать никому пароль, которым защищен сертификат.

Источники:

1. http://www.spb.osi.ru/ic/distant/oemail
2. http://www.nobat.ru/smime.html
3. Брюс Шнайер “Прикладная криптография”