Электронная подпись

и пространство доверия

С 1 июля 2012 года утрачивает силу Федеральный закон «Об электронной цифровой подписи» [1], действовавший немногим более 10 лет. Однако выданные ранее сертификаты будут продолжать действовать в соответствии с установленными для них сроками. Новый закон «Об электронной подписи» [2] предусматривает три вида электронных подписей (ЭП): одну простую и две усиленные (квалифицированную и неквалифицированную), идентичные описанным в директиве Европейского Союза [3]. Рассмотрим виды ЭП и приведем некоторые возможные примеры их построения и применения.

А.П. Баранов

Прежде всего поясним, что представляет собой ЭП. Это некоторая дополнительная к основной информации часть электронного документа, которая, как правило, добавляется в цифровом виде, хотя может иметь и различные формы графического представления.

Виды и основные характеристики ЭП

Как ожидается, наиболее распространенной подписью будет **простая ЭП**, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования ЭП определенным лицом [2, подп. 2 ст. 5). Примером простой ЭП, недостаток которой заключается в возможности несанкционированного повторения, может быть pin-код в карточке платежной системы или других

идентифицирующих личность или услуги электронных картах. Надежность pin-кода обеспечивается защитой канала передачи документа, невозможностью его просмотра недоверенными лицами, а также сменой разового pin-кода или пароля. Вместе с тем подобные схемы громоздки в использовании, требуют дополнительного канала связи с центром выдачи разовых паролей, а также определенной подготовки клиентов. Более перспективной представляется схема выработки разового пароля на основе шифрования синхропосылки по известному только удостоверяющему центру (УЦ) и пользователю ключу подписи. Желающий проверить соответствие подписи пользователю может получить подтверждение в УЦ.

Самым простым и наиболее уязвимым является графический образ реальной подписи, который, как печать, проставляется в конце графического (полученного из электронного) образа документа. Единожды получив подобный документ, получатель имеет возможность воспроизводить его многократно, в том числе без ведома легитимного владельца.

Неквалифицированная усиленная подпись [2, подп. 3 ст. 5]:

- должна обеспечивать обнаружение факта внесения изменения в документ после его подписания;
- позволяет определить личность подписанта;
- является результатом криптографического преобразования с ключом подписи;
- создается с использованием средств ЭП.

Наиболее распространенным видом неквалифицированной ЭП в нашей стране является электронная цифровая подпись (ЭЦП), реализованная в продуктах фирмы Microsoft, которая имеет, с одной стороны, все признаки ЭЦП и создана, как утверждают авторы, по одному из международно-признанных алгоритмов. С другой стороны, этот продукт не проходил соответствующей сертификации в ФСБ России, и его реализация не подтверждена заключениями экспертного сообщества. Ключ подписи от Microsoft выдается по Интернету пользователю, купившему легальную версию Windows от не сертифицированного в России удостоверяющего центра фирмы Microsoft. Таким образом, мы имеем все признаки усиленной неквалифицированной подписи, доверие к которой зиждется на уверенности в качественности программного продукта этой известной фирмы.

Постановлением Правительства РФ от 09.02.2012 № 111 установлено требование к ЭП, используемой при оказании государственных и муниципальных услуг. В данной сфере будет использоваться только усиленная квалифицированная подпись, т.е. ЭЦП.

Вместе с тем сфера применения простой и усиленной неквалифицированной подписи остается неурегулированной. Повышению ответственности применения этих видов подписей могли бы служить требования и стандарты, разработанные соответствующими государственными организациями.

komment

» «Размытость» и «неопределенность» ситуаций, в которых возможно применение различных видов ЭП, создают предпосылки к использованию, в том числе в преступных целях, некачественных ЭП.

Квалифицированная усиленная ЭП с небольшими изменениями фактически соответствует ранее использовавшейся сертифицированной ЭЦП. Дополнительно к требованиям, предъявляемым к неквалифицированной усиленной ЭП, она должна удовлетворять следующим двум условиям:

- ключ проверки ЭП указан в квалифицированном сертификате;
- для создания и проверки ЭП используются средства, получившие подтверждение соответствия требованиям сертифицирующих органов, уполномоченных в области криптографии. Иными словами, квалифицированным сертификатом ключа проверки ЭП является подтверждение УЦ (третьей стороны), также использующего только сертифицированные средства проверки и подтверждения подписи.

Принципы, положенные в основу ЭЦП

Главный принцип заключается в неадекватности операций над числами.

Рассмотрим для примера всем известные операции умножения числа на себя, т.е. возведения его во вторую степень, и извлечения корня второй степени. Перемножение двузначных чисел легко произвести на бумаге, а извлечь корень из четырехзначного числа уже очень трудно. Это можно сделать либо подбором, либо по таблицам. В этом и заключается идея использования неадекватных операций в ЭЦП.

Для работы с ЭЦП создаются два ключа: ключ подписи — хранимый пользователем втайне, и ключ проверки подписи, который может быть известен любому лицу, работающему с документом.

Особенность этих двух ключей состоит в их неразрывной связи — ключ проверки подписи получен по формуле возведения в степень исходного ключа подписи. Таким образом, ключ проверки есть прямое формульное следствие ключа подписи и с ним связан. При этом вычисление ключа проверки ЭЦП по задаваемому пользователем ключу подписи или вырабатываемому генератором чисел для пользователя ключу подписи производится на любой доступной в настоящее время персональной ЭВМ.

В то же время, и это регулярно проверяется криптографами и математиками всего мира, получение по ключу проверки подписи исходного ключа подписи ЭЦП требует гигантски трудоемкой работы ЭВМ и невозможно для реализации в течение ближайших 50–100 лет.

Процедура учета ключей подписи и ключей проверки подписи, а также их фиксации сертификатом возлагается на УЦ, главная функция которого состоит в ведении реестра выданных и аннулированных ключей проверки подписи, а также подтверждении действительности ключей при обращении заявителей в электронном или в письменном виде [2, ст. 13]. Это подтверждение УЦ, снабженное ЭЦП, и является сертификатом.

Таким образом, произвольная смена ключа подписи пользователем, не учтенная УЦ, будет непременно обнаружена.

Из изложенного следует, что все участники взаимодействия с использованием ЭЦП доверяют определенному УЦ, и в этом смысле участники создают определенное **пространство доверия**. Вместе с тем ясно, что один УЦ, каким бы разветвленным он ни был, не справится с обслуживанием запросов многомиллионной массы пользователей. К тому же ЭЦП пользователей, как правило, связана с определенным видом деятельности, и организации – владельцы УЦ оказывают дополнительные услуги по аутсорсингу этого вида деятельности, например по правильному формированию налоговой отчетности, ведению электронных счетов-фактур и т. д. Наличие различных УЦ порождает множество пространств доверия, объединить которые призван **головной удостоверяющий центр**, создание которого ожидается в ближайшее время. Отдельные же пространства доверия функционируют потому, что являются по сути корпоративными системами в рамках корпоративных договоров, что позволяет в случае возникновения конфликтных ситуаций разрешать споры в судебном порядке. Объединение отдельных корпоративных пространств доверия в единую систему должно сопровождаться установлением соответствующих юридически значимых отношений.

Способ образования и проверки ЭЦП

Для образования ЭЦП документ переводится в электронную форму и представляется в виде последовательности чисел. Такое представление возможно как для текстовых, так и для графических документов. При этом обязательным требованием к средствам ЭП является отображение документов в естественно воспринимаемом пользователем виде. Преобразование документа осуществляется специальной программой, входящей в состав средств ЭП. Полученная последовательность цифр сжимается до 256 бит с помощью специального преобразования, называемого хешированием. Очевидно, что после такого сжатия обратное преобразование в исходную последовательность цифр

или восстановление документа невозможно. Сжимающее преобразование устроено таким образом, что изменение любого бита в исходном документе приводит к полному изменению результирующих 256 бит. Ключ подписи в хешировании не участвует, это преобразование описано математическими формулами и зафиксировано в виде ГОСТа, т. е. его применяют все пользователи и УЦ. Число возможных хеш-образов составляет число 10 в 77-й степени.

Для сравнения: число атомов во Вселенной равно 10 в 78-й степени, т. е. на каждые 10 атомов приходится один хеш-образ, а на каждый документ требуется более 10 атомов. Следовательно, у каждого документа будет свой хеш-образ, т. е. два документа со своими хеш-образами не совпадут никогда.

Полученный хеш-образ документа как число смешивается в пользовательской программе с секретным ключом подписи по специальной математической формуле, из которой получается значение ЭЦП. Особенность этого преобразования состоит в том, что по значению ЭЦП и хеш-образа невозможно восстановить секретный ключ подписи, сколько бы различных хеш-образов и ЭЦП ни рассматривалось. Естественно, возможность перебора секретного ключа ЭП не учитывается как нереализуемая на практике. Таким образом, получается ЭЦП документа, которая фиксирует само содержание документа с точностью до бита и с помощью УЦ не дает возможности пользователю отказаться от подписи, поскольку секретный ключ может находиться только у него. При этом должны соблюдаться правила работы УЦ, при которых выработанный и переданный пользователю ключ подписи должен быть сразу уничтожен. В таком случае пользователь не может сослаться на возможность подделки ЭЦП со стороны УЦ. Имя пользователя с помощью ЭЦП гарантированно связывается с документом и его содержанием.

При проверке правильности ЭЦП проверяющий самостоятельно вычисляет на своем экземпляре ПО хеш-образ документа и смешивает его, пользуясь другой (в отличие от подписанта) формулой, с ключом проверки подписи. Особенность этого процесса заключается в том, что при «правильных» ЭЦП и ключе проверки подписи, соответствующем ключу подписи, использованному для получения этого значения ЭЦП, получается заведомо известный результат, не зависящий от ЭЦП и ключа подписи, который и подтверждает неизменность исходного документа.

■ ■ ■

Изложенное показывает, что программный продукт, реализующий всю процедуру ЭЦП, является непростым и весьма ответственным изделием. Достаточно небольших погрешностей в работе программ, чтобы открылись бреши для злонамеренного использования ЭЦП. Например, если остались неучтенные поля в стандартном документе, т.е. хеш-функция не учитывает значение этих полей, то документ может быть подделан с изменением этих полей, при этом ЭЦП будет правильно проверяться, и найти ошибку можно будет только после скрупулезного анализа программного обеспечения, реализующего ЭЦП. Этим объясняется законодательное требование необходимости сертификации квалифицированной ЭП компетентной организацией, несущей ответственность и дающей гарантию надежности работы комплекса ЭЦП. НП

komment

» Число возможных хеш-образов равно 1077, что сравнимо с числом атомов во Вселенной – 1078, а значит, два документа со своими хеш-образами никогда не совпадут.

Литература

1. Об электронной цифровой подписи: федер. закон Рос. Федерации от 10 янв. 2002 г. № 1-ФЗ (с изм. и доп.).

2. Об электронной подписи: федер. закон Рос. Федерации от 6 апр. 2011 г. № 63-ФЗ (с изм. и доп.).

3. Об общих принципах электронных подписей: директива ЕС от 13 дек. 1999 г. № 1999/93/ЕС .

об авторе

А.П. Баранов
заместитель генерального директора ГНИВЦ ФНС России,
доктор физико-математических наук,
академик Академии криптографии России
baranov@gnivc.ru