АЛЬТЕРНАТИВНЫЕ МЕТОДЫ ПОДПИСИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Трунов Д.Н., магистр, d.n.trunov@gmail.com
КИИ ДонНТУ, Красноармейск, Украина

Электронные цифровые подписи (ЭЦП) в настоящее время имеют широкое распространение и в ряде случаев являются полноценной заменой собственноручных подписей. Более того, применение ЭЦП иногда оказывается даже более удобным по сравнению с собственноручными подписями, если речь идёт о подписании документов дистанционно. Например, сделки в системах электронной торговли подписываются электронной подписью.

Однако поскольку ЭЦП создаётся с помощью личного ключа, попадание такого ключа «не в те руки» может привести к его несанкционированному применению, а далее – к отмене сертификата ключа, что сделает все ранее созданные с помощью него подписи недействительными. Это предъявляет повышенные требования как к владельцу ключа, так и к центру сертификации ключей [1].

Поэтому сертификат электронной подписи имеет ограниченный срок действия, обычно не превышающий двух лет, и не очень подходит для создания подписей длительного хранения (от пяти лет и выше). Кроме того, документооборот с участием внешнего центра сертификации в масштабах отдельной организации или учреждения может оказаться непрактичным. В таких случаях, видимо, нужны иные механизмы подписи документов.

Алгоритмы асимметричного шифрования считаются достаточно надёжными, а электронные подписи на их основе – практически единственным эффективным инструментом подписи электронных документов [2, 3]. При этом проблемы безопасного использования и хранения закрытых ключей решаются путём применения технических [4] и организационных мер [1]. Что касается ограниченного срока действия ЭЦП, то для электронных документов длительного хранения предлагается, например, добавление к документу новых временных штемпелей, когда срок действия предыдущих закончится [5]. По сути, это добавление новой технической подписи, которая подтверждает все предыдущие с истёкшим сроком действия.

Поскольку проблема безопасного хранения закрытых ключей и низкого срока действия ЭЦП не решена полностью (если такое решение вообще возможно), ставится задача: найти альтернативный механизм подписи электронных документов, имеющей длительный срок действия (в идеале – неограниченный) и не требующей работы с секретными ключами.

Механизм подписи документов без ключей шифрования давно применяется для обычных документов и выглядит в виде собственноручных

подписей и мокрых печатей. Считается, что на электронный документ собственноручную подпись не поставить – его нужно вначале распечатать, что во множестве случаев и делается. Однако это не всегда обязательно, поскольку и электронный документ можно заверить обычной подписью (или печатью).

Чтобы понять, как это происходит, вернёмся к принципам ЭЦП. Для вычисления электронной подписи документ нужно зашифровать закрытым ключом и отправить получателю вместе с оригиналом и соответствующим закрытому открытым ключом. Получатель должен расшифровать документ открытым ключом и сравнить с оригиналом. Если они полностью совпадают, подпись считается действительной.

На практике, вместо шифрования всего электронного документа, для него вычисляется так называемая хэш-функция [3], которая и подлежит шифрованию и расшифровке. Хэш-функция возвращает результат в виде цепочки бит фиксированной и часто небольшой длины, независимо от размера самого документа. Кроме того, она очень чувствительна к содержимому документа, и малейшие изменения в нём исказят её до неузнаваемости. Вот эту-то цепочку бит и предлагается подписывать собственноручной подписью вместо вычисления ЭЦП.

Если хэш-функции подходят для ЭЦП, то почему нельзя их использовать и без ЭЦП? Для этого результирующую цепочку бит нужно представить в удобном для чтения формате и перенести на бумажный носитель (лист формата А4, А5 или запись в специальном журнале), а далее – подписать обычными подписями или заверить любыми другими современными средствами, позволяющими подтвердить личность подписанта и дату подписи.

Подпись под хэш-функцией электронного документа будет эквивалентна подписи под самим документом. Для проверки документа нужно всего лишь повторно вычислить для него такую функцию и сравнить её с ранее заверенной. Если они совпадают – подпись действительна, а документ подлинный. При этом не нужны никакие закрытые ключи шифрования, которые требовалось бы хранить в секрете.

Данный метод, конечно, не может заменить ЭЦП в случаях подписания электронных документов дистанционно, например, те же сделки в системе электронной торговли. В остальных случаях, когда предполагается печать электронного документа и его последующее собственноручное подписание, вместо всего документа можно обойтись печатью только его хэш-функции, которую и следует подписывать. Это тем более актуально, если сам документ состоит из десятков или даже сотен страниц.

Чтобы отличить данный вид подписей от обычных ЭЦП, предлагается называть сами цепочки бит хэш-подписями или криптоподписями [6], поскольку сама хэш-функция предполагает криптографическую обработку исходного документа. Если алгоритм вычисления такой подписи будет до-

статочно надёжным, чтобы исключить возможность подделки документа даже в отдалённой перспективе, срок её действия может быть потенциально неограниченным.

Таким образом, преимущества хэш-подписей (или криптоподписей) в их понятности, простоте и удобстве. Их можно понимать и воспринимать как «усиленную» контрольную сумму электронного документа, позволяющую выявлять в нём изменения и исключать его подделку. Кроме того, хэш-подписи нескольких электронных документов можно подписывать целым списком (одна собственноручная подпись на список хэш-подписей), что практически невозможно в случае применения только ЭЦП или только обычных подписей. И, в отличие от ЭЦП, хэш-подписи не требуют применения ключей шифрования и обладают потенциально неограниченным сроком действия.

Литература

1. Закон Украины «Об электронной цифровой подписи»

2. Ерош И.Л. Дискретная математика. Математические вопросы криптографии: Учеб. пособие / СПбГУАП. СПб, 2001. – 56с.

3. Баричев С. Криптография без секретов // Бюро научно-технической информации [Электронный ресурс]: http://www.bnti.ru/dbtexts/ipks/old/analmat/1_2002/crypto4.pdf

4. Абашев А.А, Жуков И.Ю., Иванов М.А., Метлицкий Ю.В., Тетерин И.И. Ассемблер в задачах защиты информации. – М.: КУДИЦ-ОБРАЗ, 2004. – 544 с.

5. Мелащенко А.О., Перевозчикова О.Л., Скарлат О.С. «Складові стенду валідації архівних електронних документів». // Проблеми програмування. – 2012 – №1. – С. 91-98

6. Трунов Д.Н. Компьютерная программа CryptoSignature: описание, назначение и принципы работы [Электронный ресурс]: https://sites.google.com/site/publicworkstrunov

Анотація

Представлено короткий опис методу підпису електронних документів, заснованого на обчисленні та завіренні їх хеш-функцій. Розглянуті переваги таких підписів у порівнянні зі звичайними електронними цифровими підписами.

Ключові слова: хеш-функція, електронний цифровий підпис.

Аннотация

Представлено краткое описание метода подписи электронных документов, основанного на вычислении и заверке их хэш-функций. Рассмотрены преимущества таких подписей в сравнении с обычными электронными цифровыми подписями.

Ключевые слова: хэш-функция, электронная цифровая подпись.

Abstract

The research represents a brief description of the method of electronic documents' signature based on calculation and verification of hash-functions. Also there were considered the advantages of such signatures in comparison with conventional digital signatures.

Keywords: hash-function, electronic digital signature.