УДК 004

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Ашурок Е.В., Разоренов Н.А.
Белорусский национальный технический университет, г. Минск

Цифровые подписи могут использоваться для распространения сообщения в виде открытого текста, когда получатели должны идентифицировать и проверить отправителя сообщения. Подписание сообщения не меняет сообщение, оно просто генерирует строку цифровой подписи, которую вы можете связать с сообщением или передать отдельно. Цифровая подпись - это короткий фрагмент данных, зашифрованный с помощью закрытого ключа отправителя. Расшифровка данных подписи с использованием открытого ключа отправителя доказывает, что данные были зашифрованы отправителем или кем-то, кто имел доступ к личному ключу отправителя.

Цифровые подписи генерируются с использованием алгоритмов подписи с открытым ключом. Закрытый ключ производит подпись, и соответствующий открытый ключ должен использоваться для проверки подписи.

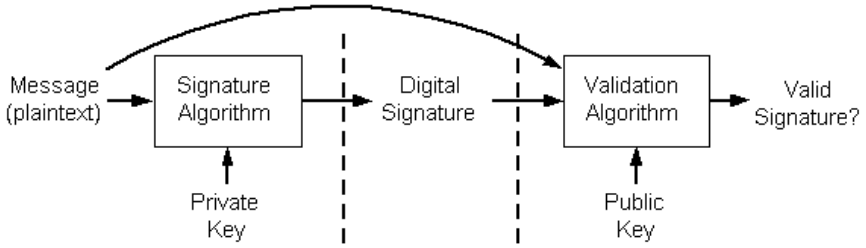

Рисунок 1 – Генерация электронной подписи

Для создания пар ключей асимметричного шифрования использовалася следующая функция CryptoAPI:BOOL CryptGenKey(HCRYPTPROV hProv, ALGJD Algid, DWORD dwFlags, HCRYPTKEY *phKey). Эта функция позволяет :создание в контейнере ключей с дескриптором hProv пары ключей ЭЦП (Algid=AT_SIGNATURE) или обмена сеансовыми ключами (Algid=AT_KEYEXCHANGE) и запись дескриптора открытого ключа созданной пары в *phKey; если закрытый ключ созданной пары должен иметь возможность экспорта из CSP, то dwFlags=CRYPT_EXPORTABLE (открытые ключи всегда являются экспортируемыми).

Получение дескриптора открытого ключа *phUserKey из соответствующего контейнера ключей hProv возможно с помощью следующей функции: BOOL CryptGetUserKey(HCRYPTPROV hProv, DWORD dwKeySpec, HCRYPTKEY *phUserKey), где параметр

dwKeySpecопределяет тип запрашиваемого ключа — обмена (AT_KEYEXCH AN GE) или ЭЦП (AT_SIGNATURE).

Создание цифровой подписи из сообщения состоит из двух этапов. Первый шаг включает создание значения хеша (также известного как дайджест сообщения) из сообщения. Это хэш-значение затем подписывается с использованием закрытого ключа.

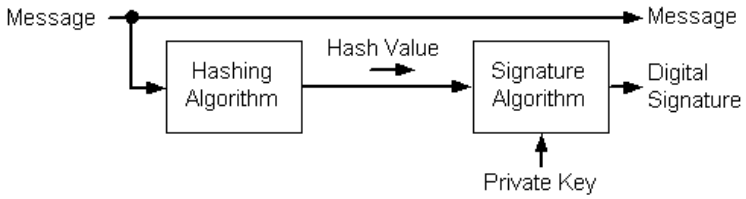

Рисунок 2 – Иллюстрация этапов создания цифровой подписи.

Для проверки подписи требуется как сообщение, так и подпись. Во-первых, из сообщения должно быть создано хеш-значение так же, как была создана подпись. Затем это значение хеш-функции проверяется на соответствие подписи с использованием открытого ключа подписавшего. Если значение хеш-функции и подпись совпадают, вы можете быть уверены, что сообщение действительно является тем, которое подписавший подписал первоначально, и что оно не было подделано.

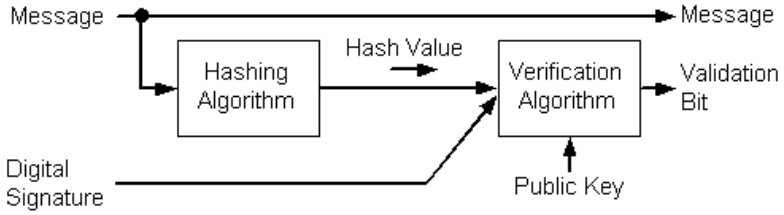

Рисунок 3 - Процесс поверки цифровой подписи.

Для проверки электронной цифровой подписи вначале также необходимо вычислить хеш-значение для электронного документа, чьи аутентичность и целостность проверяются. После этого вызывается функция CryptoAPI, выполняющая проверку ЭЦП: BOOL CryptVerifySignature(HCRYPTHASH hHash, BYTE *pbSignature, DWORD dwSigLen, HCRYPTKEY hPubKey, LPCTSTR sDescription, DWORD dwFlags). Проверка ЭЦП из буфера*pbSignature длины dwSigLen для хеш-значения с дескриптором hHash с помощью открытого ключа hPubKey (sDescription=NULL или строка с описанием проверяемого документа, dwFlags=0); если данные, хеш-значение которых содержится в hHash, были после получения ЭЦП изменены или открытый ключ hPubKey не соответствует закрытому ключу ЭЦП, то эта функция возвращает FALSE с кодом ошибки NTEBADSIGNATURE от функции GetLastError[1].

Значение хеша состоит из небольшого количества двоичных данных, обычно около 160 бит. Это производится с использованием алгоритма хеширования. Ряд этих алгоритмов перечислены ниже в этом разделе.

Все хэш-значения имеют следующие свойства независимо от используемого алгоритма.

Длина значения хеш-функции определяется типом используемого алгоритма, а его длина не зависит от размера сообщения. Наиболее распространенные значения хеш-значений составляют 128 или 160 бит.

Каждая пара неидентичных сообщений преобразуется в совершенно разные значения хеш-функции, даже если два сообщения отличаются только одним битом. Используя сегодняшнюю технологию, невозможно обнаружить пару сообщений, которые преобразуются в одно и то же значение хэша, не нарушая алгоритм хэширования.

Каждый раз, когда конкретное сообщение хэшируется с использованием одного и того же алгоритма, создается одно и то же значение хеш-функции.

Все алгоритмы хеширования являются односторонними. Учитывая значение хеш-функции, невозможно восстановить исходное сообщение. Фактически, ни одно из свойств исходного сообщения не может быть определено только с помощью значения хеш-функции.

С 18 февраля 2019 года вступил в силу Закон Республики Беларусь от 8 ноября 2018 г. № 143-З «О внесении изменений и дополнений в Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи». Изменение закона обеспечит правовое поле для более широкого использования электронного документа в Беларуси. Дополнительные возможности появятся у организаций и физлиц, в том числе ИП. Законом предусмотрено, что ЭЦП является аналогом собственноручной подписи. Электронный документооборот обеспечивает с технической стороны Национальный центр электронных услуг. Получить сертификат открытого ключа можно в его подразделении — Республиканском удостоверяющем центре государственной системы управления открытыми ключами (Минск, проспект Машерова, 25). Он начал работать летом 2014 года. Есть региональные представительства в крупных городах. Ожидается, что в стране будет создана система, позволяющая человеку получить сертификат открытого ключа единого образца. Узнать, как сделать ЭЦП, можно на сайте Национального центра удостоверяющих услуг[2].

Литература

1.Официальный сайт Microsoft [Электронный ресурс]. − Режим доступа: https://docs.microsoft.com/en-us/windows/win32/seccrypto/digital-signatures. − Дата доступа 10.10.2019г.

2. Сайт Национального центра удостоверяющих услуг [Электронный ресурс]. − Режим доступа:https://nces.by/pki/. − Дата доступа 5.11.2019г.