

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ И ЕЁ ПРИМЕНЕНИЕ

Войнилко В.А.

Научный руководитель: Ковалькова И.А.

Белорусский национальный технический университет

На сегодняшний день используется большой набор различных аналогов собственноручной подписи (АСП) – биометрические, PIN-коды, факсимильные и т.д. В том числе широко используются системы цифровой подписи (ЦП).

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронная подпись предназначена для идентификации лица, подписавшего электронный документ.

Кроме этого, использование электронной подписи позволяет осуществлять:

- *контроль целостности передаваемого документа:* при любом случайном или преднамеренном изменении документа подпись становится недействительной, потому что вычислена она на основании исходного содержания документа и соответствует лишь ему;

- *защиту от изменений (подделки) документа:* гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев;

- *невозможность отказа от авторства:* так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец не может отказаться от своей подписи под документом;

- *доказательно подтверждение авторства документа:* так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец пары ключей может доказать своё авторство под подписью под документом.

В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т.д.

Все эти свойства электронной подписи позволяют использовать её для следующих целей:

- декларирование товаров и услуг (таможенные декларации);
- регистрация сделок по объектам недвижимости;

- использование в банковских системах;
- электронная торговля и госзаказы;
- контроль исполнения государственного бюджета;
- в системах обращения органов власти;
- для обязательной отчетности перед государственными учреждениями;
- организация юридически значимого электронного документооборота;
- в расчётных и рейтинговых системах.

Виды электронных подписей:

- простая электронная подпись (ПЭП);
- усиленная электронная подпись (УЭП);
- усиленная неквалифицированная электронная подпись (НЭП);
- усиленная квалифицированная электронная подпись (КЭП).

Существует несколько схем построения цифровой подписи:

1. На основе алгоритмов симметричного шифрования.

Данная схема предусматривает наличие в системе третьей стороны – арбитра, пользующегося доверием обеих сторон.

Авторизацией документа является сам факт шифрования его секретным ключом и передача его арбитру.

2. На основе алгоритмов асимметричного шифрования.

На данный момент такие схемы электронной подписи наиболее распространены и находят широкое применение.

3. Кроме этого, существуют другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись), которые являются модификациями описанных выше схем.

Их появление обусловлено разнообразием задач, решаемых с помощью электронной подписи.

Социальные атаки направлены на взлом алгоритмов цифровой подписи, а на манипуляции с открытым и закрытым ключами. Злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа. Злоумышленник может обманом заставить владельца подписать какой-либо документ, например, используя протокол слепой подписи; подменить открытый ключ владельца на свой собственный, выдавая себя за него. Использование протоколов обмена ключами и защита закрытого ключа от несанкционированного доступа позволяют снизить опасность социальных атак.

Важной проблемой всей криптографии с открытым ключом, в том числе и с тем электронной подписи, является управление открытыми ключами. Так как открытый ключ доступен любому пользователю, то необходимо механизм проверки того, что этот ключ принадлежит именно своему владельцу. Необходимо обеспечить доступ любого пользователя к подлинному открытому ключу любого другого пользователя, защитить эти ключи от подмены злоумышленником, атаке же организовать отзвучивание ключа в случае его компрометации.

Задача защиты ключей от подмены решается с помощью сертификатов. Сертификат позволяет удостовериться в заключённых в нём данных о владельце и его открытый ключ подписью какого-либо доверенного лица.

С 2014 года таможенное декларирование товаров при пересечении границы РБ производится в электронном виде. Это делает процедуру ВЭД проще и удобнее. Подключаясь к системе электронного декларирования через Интернет, компания значительно снижает затраты времени и уменьшает финансовые расходы на оформление документов ВЭД. Электронная декларация на любые товары проходит значительно быстрее и требует значительно меньше усилий на оформление.

Чтобы таможенная декларация в электронном виде имела юридическую силу, она должна сопровождаться электронной подписью.

Среди преимуществ, которые предоставляет электронная таможенная декларация, необходимо отметить: высокую скорость обработки документов и таможенного оформления; безбумажный документооборот; возможность осуществить документальный контроль до фактического поступления товара на склад; доступ к интеграции документов в информационную систему других стран; возможность использовать электронные документы других государств при таможенном оформлении.

В Республике Беларусь 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. Он начал работать летом 2014 года. Есть региональные представительства в крупных городах.

Индивидуальные предприниматели, желающие подавать декларации в налоговую службу дистанционно, могут заказать ЭЦП в Удостоверяющем центре РУП «Информационно-издательский центр по налогам и сборам». Сейчас работают 4 филиала в Минске. Также заказать ЭЦП для подписи электронной декларации можно в Бресте, Гродно, Гомеле, Могилёве, Витебске, Борисове, Слуцке, Пинске, Барановичах, Полоцке, Лиде, Мозыре и Бобруйске.

Удостоверяющий центр Министерства финансов работает в системе названного министерства и также выпускает сертификаты и ключи.