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).

Электроннаяцифроваяподпись(ЭЦП)– реквизитэлектронногодокумента,предназначенныйдлязащитыданногоэлектронногодокументаотподделки,полученныйврезультатекриптографическогопреобразованияинформациисиспользованиемзакрытогоключаэлектронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электроннаяподписьпредназначенадляидентификациилица,подписавшегоэлектронныйдокумент.

Кромеэтого,использованиеэлектроннойподписипозволяетосуществить:

- *контрольцелостностипередаваемогодокумента*: прилюбомслучайномилипреднамеренномизмененииидокументаподписьстанетнедействительной,потомучтовычисленаонанаосновании исходного состояниядокументаисоответствуетлишьему;
- *защитуотизменений (подделки) документа*: гарантиявыявленияподделкиприконтролецелостностиделаетподделывание нецелесообразнымвбольшинствеслучаев;
- *невозможностьотказаотавторства:*таккаксоздатькорректнуюподпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец не может отказаться от своей подписи под документом;
- *доказательноеподтверждениеавторстваdокумента*: таккаксоздатькорректнуюподписьможно,лишьзнаязакрытыйключ,аондолженбытьизвестентольковладельцу,товладелецпарыключейможетдоказатьсвоёавторствоподписиподдокументом.

Взависимостиотделейопределениядокументамогутбытьподписанытакие поля,как«автор»,«внесённыеизменения»,«меткавремени»и т.д.

Всеэтисвойстваэлектронной подписипозволяютиспользоватьеёдлясследующихцелей:

- декларированиетоваровиуслуг (таможенныедекларации);
- регистрациясделокпообъектамнедвижимости;

- использованиевбанковскихсистемах;
- электроннаяторговляигосзаказы;
- контрольисполнениягосударственногобюджета;
- всистемахобращениякорганамвласти;
- дляобязательнойотчётностипередгосударственнымиучреждениями;
- организацияюридическизначимогоэлектронногодокументооборота;
- врасчётныхитрейдинговыхсистемах.

Видыэлектронныхподписей:

- простаяэлектроннаяподпись (ПЭП);
- усиленнаяэлектроннаяподпись (УЭП);
- усиленнаянеквалифицированнаяэлектроннаяподпись (НЭП);
- усиленнаяквалифицированнаяэлектроннаяподпись (КЭП).

Существуетнесколькосхемпостроенияцифровойподписи:

1. Наоснове*алгоритмовсимметричногошифрования*.

Даннаясхемапредусматриваетналичиевсистеметретьеголица–арбитра,пользующегосядовериемобеихсторон.
Авторизацийдокументаявляетсясамфактзашифрованияегосекретнымключомипередачаегоарбитру.

2. Наоснове*алгоритмовасимметричногошифрования*.

Наданныймоменттакиесхемыэлектронной подписинаиболеераспространеныинаходятширокоеприменение.

3. Кромеэтого,существуютдругиеразновидностицифровыхподписей (групповаяподпись,неоспоримаяподпись,доверенная подпись), которыеявляютсямодификациямиописанныхвышесхем.

Ихпоявлениеобусловленоразнообразиемзадач,решаемыхспомощьюэлектронной подписи.

Социальныеатакинаправленыненавзломалгоритмовцифровойподписи,а наманипуляцииоткрытымизакрытымключами.Злоумышленник,укравший закрытыйключ,можетподписатьлюбойдокументотименивладельцаключа.Злоумышленникможетобманомзаставитьвладельцаподписаткакой-либодокумент,например,используяпротоколслепойподписи; подменитьоткрытыйключвладельцанасвойсобственный,выдаваясебязанего.Использованиепротоколовобменаключамиизащитазакрытогоключаотнесанкционированногодоступапозволяетснизитьопасностьсоциальныхатак.

Важнойпроблемойвсейкриптографиисоткрытымключом,втомчислеисистемэлектронной подписи,являетсяуправлениеоткрытымиключами. Таккакоткрытыйключдоступенлюбомупользователю,тонеобходиммеханизмпроверкитого,чтоэтотключпринадлежитименносвоемувладельцу. Необходимообеспечитьдоступлюбогопользователякподлинномуоткрытомуключулюбогодругогопользователя,защититьэтиключиотподменызлоумышленником,атакжеорганизоватьотзывключавслучаеегокомпрометации.

Задачазащитыключейотподменырешаетсяспомощьюсертификатов. Сертификатпозволяетудостоверитьзаключённыевнёмданныеовладельцеиег ооткрытыйключподписьюкакого-либодоверенноголица.

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.