Сертификат и Электронная цифровая подпись

ЭЦП

- Электронная цифровая подпись — комбинация знаков или паролей, которая служит эквивалентом обычной подписи на бумаге.
- Главная необходимость ЭЦП заключается в подписи цифровых документов, дать подтверждение о том что абонент ознакомлен и согласен с содержимым документа, так же ЭЦП можно дать еще одно определение
- ЭЦП это информация связанная с электронным документом и позволяющее идентифицировать лицо подписавшее этот документ

Требования ЭЦП

- Требуемые свойства подписываемых документов:
- целостность;
- достоверность;
- аутентичность (подлинность; «неотрекаемость» от авторства информации).

Преимущества ЭЦП

- **Надежность -**Обычную подпись просто подделать, а электронная имеет высокий уровень защиты от фальсификаций
- **Экономия времени** - Можно подавать документы в государственные инстанции, заключать соглашения с контрагентами, не присутствуя при этом лично
- **Доступ к электронным торгам** -Наличие электронной подписи — обязательное условие участия в торгах о государственных закупках и других

Виды ЭЦП

- Есть 3 вида электронных подписей. Они отличаются сферой применения и степенью надёжности
- **Простая электронная подпись**
- **Неквалифицированная электронная подпись**
- **Квалифицированная электронная подпись**

Простая ЭЦП

- Это комбинация цифровых данных, с помощью которых можно идентифицировать личность. Простой пример — логин и пароль, которые вводим на сайтах для авторизации, или смс-код, который присылают на телефон для входа в личный кабинет. Это электронная подпись для повседневной жизни

Простую ЭЦП можно применять

- Для регистрации или авторизации на интернет-сайтах.
- В качестве ключа доступа к файлам и базам данных, защищенным паролем.
- Для заверения электронных документов

недостатки

- Простая электронная подпись не имеет юридической силы. Её нельзя использовать для подачи документов в государственные инстанции, а также для участия в торгах по 44-ФЗ и 223-ФЗ.
- Чтобы при помощи ПЭП можно было подписывать обычные документы (например, договоры с контрагентами), нужно составить соглашение о простой электронной подписи. Такое соглашение должно содержать пункты об обязанности соблюдать конфиденциальность сведений и правила определения подписавшего лица — подлинности подписи.
- И подписывать его придётся всем сторонам, участвующим в электронном взаимодействии. Иначе все документы, подписанные ПЭП, закон признает недействительными

Неквалифицированная электронная подпись

- Неквалифицированная электронная подпись (НЭП) — чаще всего это ключ, хранящийся на USB-носителе. Иногда НЭП может создать программа, в которой работаете (только она и опознает эту подпись). Функционал такой подписи тоже частично ограничен, но, по сравнению с ПЭП, она обладает рядом преимуществ
- Применятся в
- В рамках внутреннего документооборота компании.
- Для взаимодействия с контрагентами, если заключено соглашение с указанием условий использования НЭП (аналогично ПЭП).

Недостатки

- НЭП подходит скорее физлицам. Юридическим лицам и ИП неквалифицированная электронная подпись подойдёт только при внушительном объёме внутреннего или внешнего документооборота, в других ситуациях её функционала может быть недостаточно.

Усиленная квалифицированная подпись

- Наиболее совершенный вид электронной подписи — усиленная квалифицированная подпись (КЭП). Это ключ, сформированный с помощью сертифицированных криптографических средств, который записывается на USB-носитель
- Ключ электронной подписи указан в сертификате, который выдаёт удостоверяющий центр, аккредитованный в Минкомсвязи.
- КЭП состоит из двух частей:
- проверочного сертификата для ключа подписи (USB-носитель);
- лицензированного дистрибутива — установочного пакета специальной программы, который можно использовать в течение ограниченного периода действия ключа.
- КЭП способна обеспечить надёжную защиту информации от посторонних лиц, а степень конфиденциальности данных владелец устанавливает сам. Данные будут защищены даже когда срок действия ключа истечёт

Где применяются

- Если коротко — везде.
- Для (пере)регистрации онлайн-кассы в ФНС.
- Для удалённой подачи документов.
- Для работы с государственными порталами, включая ФНС, ПФР и другие.
- Для участия в коммерческих и государственных торгах или покупки имущества банкротов на множестве площадок

Недостатки

- У КЭП существует один недостаток: нужно ежегодно оплачивать сертификат электронной подписи

Сертификат

- Сертификат электронной подписи — это бумажный или электронный документ, позволяющий проверить подлинность электронной подписи, он подтверждает принадлежность ключа проверки электронной подписи владельцу сертификата

- Сертификат ключа электронной подписи состоит из нескольких компонентов:
- — Открытого ключа. Он же называется ключ проверки электронной подписи. Ключ проверки электронной подписи содержит уникальный код, с помощью которого можно проверить подлинность электронной подписи. Сертификат открытого ключа содержит сведения о подписанте (ФИО, СНИЛС и др.), об удостоверяющем центре, который выдал ЭП и срок действия ключа. Благодаря открытому ключу проверки получатель электронного документа может убедиться, что документ не менялся, а сертификат электронной подписи является действующим.
- — Закрытого ключа проверки электронной подписи. В отличие от открытого ключа проверки закрытый ключ, как следует из названия, содержит конфиденциальную информацию, получив которую злоумышленники могут скомпрометировать подпись. Для хранения закрытого ключа, как правило, используется отдельный носитель – токен. Ответственность за хранение такого носителя лежит на владельце подписи

- Пара закрытый ключ + сертификат открытого ключа надёжно обеспечивают безопасность ЭЦП и одновременно считываемость всей информации, которую содержит сертификат ключа ЭЦП, а именно:
- — уникальный номер сертификата ключа проверки электронной подписи;
- — реквизиты компании или человека, на имя которого выдан сертификат;
- — код ключа проверки электронной подписи для идентификации;
- — стандарты этого вида сертификата;
- — наименование и адрес удостоверяющего центра;
- — страховой номер лицевого счёта и ИНН владельца;
- — дату выдачи и срок действие сертификата, как правило, электронная подпись выдаётся сроком на 12 месяцев.

Состав поставки ЭП

- Как правило для использования ЭП физическому или юридическому лицу необходимо обеспечить комплект поставки ЭП в данный комплект входит
- Сертификат электронной подписи
- Средство криптографической защиты информации (СКЗИ, криптопровайдер)
- Защищенный носитель

СКЗИ

- Криптопровайдер - это независимое программное обеспечение которое обеспечивает связь между операционной системой и операциями криптографического преобразования используемые при работе с электронной подписью без него ЭП не работает

Поставки СКЗИ

- Существует 2 вида поставок
- Поставка на рабочее место
- В составе ЭП
- **Поставка на рабочее место ,**предлагается в виде бланка лицензии с указанием кода активации при использовании такого вида лицензии, вводится код активации лицензии и она будет действительна на данном рабочем месте, на том месте где установлено ПО там и будет использоваться ЭП (ограничение по рабочему месту)
- **В составе сертификата ЭП,** данный вид поставки предполагает что удостоверяющий центр при создании сертификата указывает код активации лицензии в самом сертификате который выдается , данный метод позволят использовать сертификат на любом компьютере без ввода кода лицензии (достигается мобильность)

Защищенный носитель

- Защищенный носитель (Токен) предлагаемый носитель обеспечивает защиту и хранение сертификатов пользователя поставляется в виде Flash - накопителя или смарт карт
- Обеспечивает защиту от доступа третьих лиц
- Обеспечивает защиту от случайного удаления
- Обеспечивает защиту от вредоносного ПО

Виды токенов

- Актив
- РУТОКЕН
- ЕТОКЕН