Электронно-цифровая подпись и криптография

Основные сведения

Первые активные попытки использования электронных документов в коммерческих информационных системах, прежде всего банковских, начались еще в конце 60-х годов. Они привели к появлению новой технологии оформления документа в электронном виде - так называемой **"цифровой или электронной подписи« (ЭЦП)**.

Для чего нужна ЭЦП

Электронно-цифровая подпись (ЭЦП) ставится под электронным документом с теми же целями, что и обычная ручная подпись под бумажным документом:

- Для проверки, что электронный документ создан именно лицом, поставившим под ним свою ЭЦП;
- Для гарантии, что электронный документ не изменялся после его подписания.

При этом:

- Цифровая подпись имеет такую же юридическую силу, как и обычная.
- Признана в качестве доказательства Высшим Арбитражным судом РФ.
- Электронные документы, подписанные программой, соответствуют всем законам России и положениям Центрального Банка.

Основные определения

Закрытый ключ – строка символов, сгенерированная для конкретного пользователя (уникальная строка). Хранится у пользователя.

Открытый ключ – строка символов, сгенерированная для конкретного человека (уникальная строка), и связанная с Закрытым ключом. Хранится в БД. Открытый ключ работает только в паре с закрытым ключом. На открытый ключ выдается сертификат, который автоматически передается вместе с письмом, подписанным ЭЦП.

Нужно обеспечить наличие своего открытого ключа у всех, с кем Вы собирается обмениваться подписанными документами. Дубликат открытого ключа направляется в Удостоверяющий Центр, где создана библиотека открытых ключей ЭЦП. В библиотеке Удостоверяющего Центра обеспечивается регистрация и надежное хранение открытых ключей во избежание попыток подделки или внесения искажений.

Результат проверки подписи – утверждение Да/Нет, полученное в результате криптопреобразования из Файла с ЭЦП и Открытого ключа

Принцип создания ЭЦП

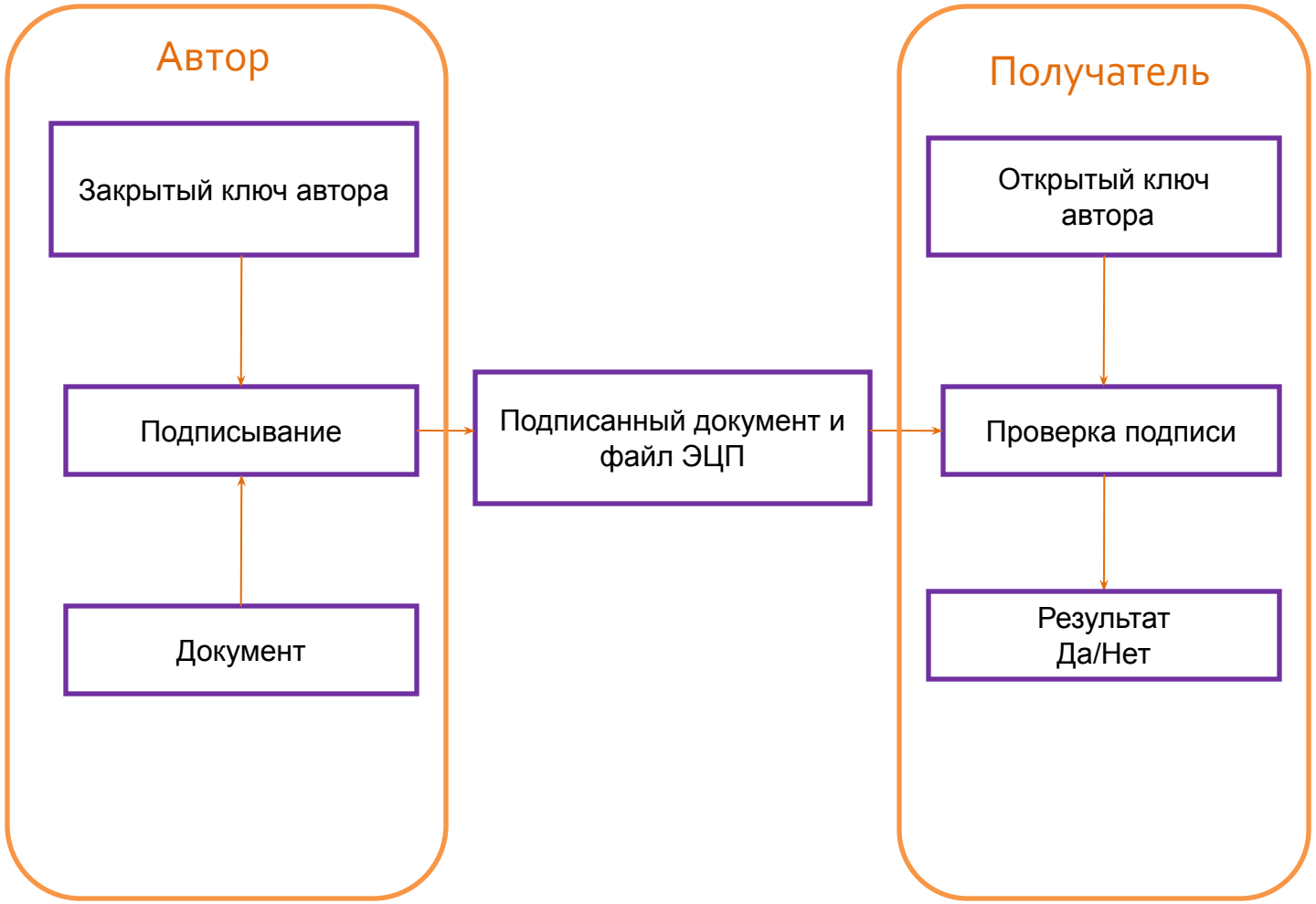
В работе ЭЦП используются два ключа – **секретный и открытый, принадлежащие автору.**

Электронный документ подписывается автором с использованием своего секретного ключа. В результате получается подписанный электронный документ, т.е. комплект из исходного документа и ЭЦП автора к этому документу.

Секретный ключ хранится на компьютере автора в зашифрованном виде. Как ясно из названия, свой секретный ключ автор не должен сообщать никому. При любом подозрении об утере секретности ключа (его компрометации) автор должен немедленно заменить свой комплект ключей.

Открытый ключ автора передается получателям, и используется ими для проверки подлинности ЭЦП.

Принцип создания ЭЦП



Принцип создания ЭЦП

Положительным результатом сверки является подтверждение авторства документа и отсутствия изменений в нем. Если сверка дала отрицательный результат, то либо документ был подписан не автором, либо содержание документа было изменено после его подписания. В обоих случаях такому документу верить нельзя.

Подписать документ от имени автора с использованием открытого ключа невозможно. Поэтому свой открытый ключ автор может сообщать любому лицу, с которым он собирается обмениваться электронными документами.

Дополнительная защита от подделки обеспечивается сертификацией Удостоверяющим центром открытого ключа подписи. Кроме того по желанию клиента Удостоверяющий центр может застраховать ЭЦП клиента

Принцип создания ЭЦП

Для исключения повторений одной и той же цифровой подписи пользователя под одним и тем же документом при повторном его подписывании в каждую цифровую подпись автоматически добавляется случайное число, которое затем "замешивается" с секретным ключом и содержимым документа.

Принципиальным моментом в системе цифровой (электронной) подписи является невозможность практического подделывания подписей пользователя без знания его секретного ключа подписывания.

2. Криптография (шифрование)

Основные сведения

Современная криптография включает в себя:

- асимметричные криптосистемы,
- системы электронной цифровой подписи (ЭЦП),
- хеш-функции,
- управление ключами,
- получение скрытой информации,
- квантовую криптографию.

Основные понятия

- **Открытый (исходный) текст** — данные (не обязательно текстовые), передаваемые с использованием криптографии.
- **Шифрованный (закрытый) текст** — данные, полученные после применения криптосистемы с указанным ключом.
- **Ключ** — параметр шифра, определяющий выбор конкретного преобразования данного текста.
- **Зашифрование** — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа в результате которого возникает шифрованный текст.
- **Расшифрование** — процесс нормального применения криптографического преобразования шифрованного текста в открытый.
- **Имитозащита** — защита от навязывания ложной информации. Имитозащита достигается обычно за счет включения в пакет передаваемых данных имитовставки.
- **Имитовставка** — блок информации, применяемый для имитозащиты, зависящий от ключа и данных. В частном случае обеспечивается ЭЦП.

Механизм шифрования документов

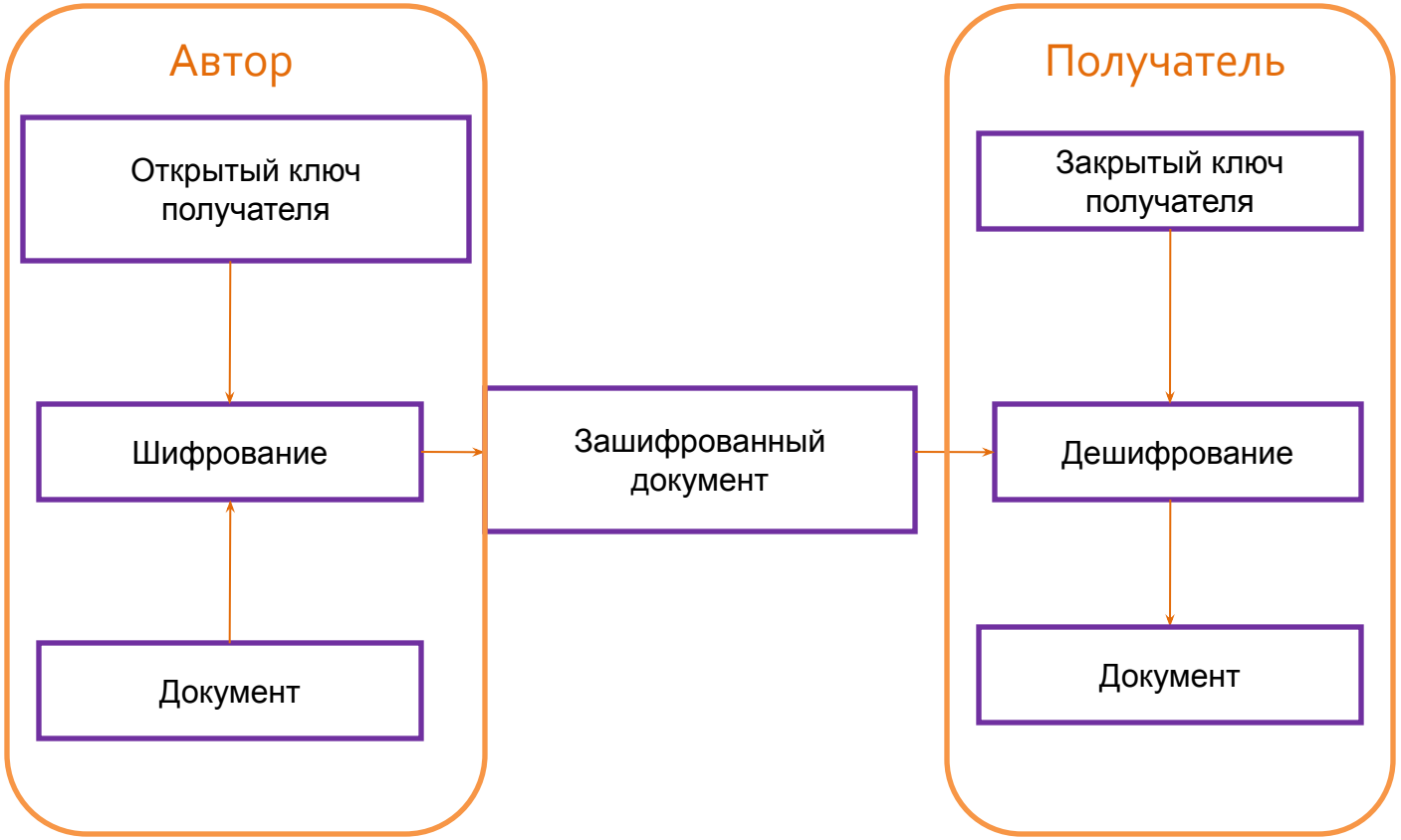
Шифрование - это процесс преобразования открытых данных в закрытые по определенному криптографическому алгоритму с использованием секретного ключевого элемента – ключа шифрования.

В данной презентации рассмотрим ассиметричное шифрование, использующее взаимосвязанные пары ключей:

- **закрытого** – хранящегося только у владельца для цели расшифрования данных и их цифрового подписания,
- **открытого,** который не нуждается в защите, может быть широко распространен и используется для зашифрования и сличения цифровых подписей.

Механизм шифрования

Принципиальным отличием шифрования документов от подписывания их с помощью ЭЦП является то, что шифрование происходит с использованием открытого ключа получателя, а не автора.



Программное обеспечение

Существует достаточно большое количество программных пакетов, выполняющих функции подписывания документов ЭЦП и их шифрования. Некоторые примеры:

- Крипто Офис ЛАН Крипто (РФ)
- ВербаМО ПНИЭИ (РФ)
- PGP Network Associates inc. (США)
- Priva Seal Aliroo Inc. (США)