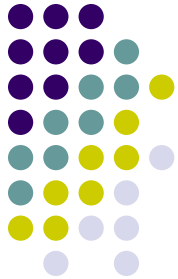
ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ (ЭЦП)

Что такое ЭЦП

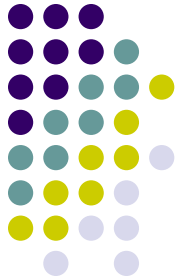


Электронная подпись (Электронная цифровая подпись, ЭП, ЭЦП) - реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий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

Отношения в области использования электронных подписей регулируются Федеральным законом N 63-ФЗ от 6 апреля 2011 года «Об электронной подписи».

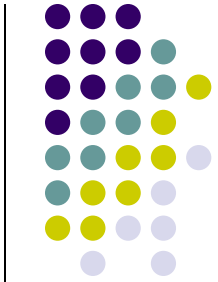
Электронная подпись предназначена для идентификации лица, подписавшего электронный документ, и является полноценной заменой (аналогом) собственноручной подписи в случаях, предусмотренных законом.

Основные направления применения ЭЦП



- **В электронной торговле и госзаказе.** Поставщик может подписать ЭЦП предложение на торгах и это гарантирует юридическую значимость его предложения, заказчик может подписать ЭЦП размещенное в системе электронных торгов предложение о закупке. ЭЦП по 223-ФЗ
- **В организации юридически значимого электронного документооборота.** Многие до сих пор считают, что юридически значимый документ (удостоверение, справка, выписка и т.д.) это бумага, оформленная по определенным правилам, заверенная подписью и печатью уполномоченной организации. Но технологические возможности развиваются, и сегодня электронные документы также могут быть юридически значимыми, если в них используется электронная цифровая подпись – электронный аналог собственноручной подписи.
- **В бухгалтерской и налоговой отчётности.** Законодательная база РФ предусматривает технологию сдачи налоговой и бухгалтерской отчетности по телекоммуникационным каналам связи с использованием электронной цифровой подписи.
- **Получение доступа к информационным системам** Росреестра (для кадастровых инженеров), ЕИАС ФСТ России, а также другим ведомств.

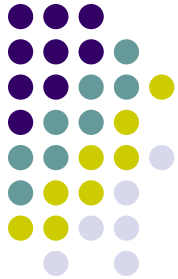
Порталы госзакупок



Владельцы сертификатов ЭЦП ekey.ru могут принимать участие в электронных торговых процедурах:

- Единая электронная торговая площадка (Федеральный заказ) - www.roseltorg.ru
- Система электронных торгов ГУП Агентства по госзаказу РТ - www.zakazrf.ru
- Автоматизированная система торгов sberbank-ast.ru
- ЭТП ММВБ "Госзакупки" www.etp-micex.ru
- Электронная торговая площадка www.rts-tender.ru

Как это работает



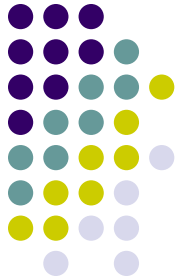
Необходимо 2 сертификата: личный и удостоверяющего центра

Личный сертификат состоит из двух частей - открытого ключа и закрытого ключа. Открытый ключ свободно распространяется, закрытый - хранится в безопасности и никому не дается. После установки сертификата, закрытый ключ автоматически помещается в специальное хранилище компьютера, обеспечивающее его недоступность для посторонних. Файл сертификата больше не нужен и его необходимо удалить или хранить в сейфе.

Открытый и закрытый ключ связаны друг с другом, дополняют друг друга, и подходят только друг для друга. Нельзя взять открытый ключ из одной пары, а закрытый ключ из другой пары ключей.

Как открытый, так и закрытый ключ служат для шифрования и дешифрования. При этом все, что зашифровано открытым ключом, может быть расшифровано только закрытым ключом. А все, что зашифровано закрытым ключом, может быть расшифровано только открытым ключом.

Когда Вы подписываете свое письмо происходит следующее:

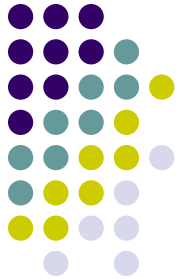


1. Программа получает некий набор символов (иначе ее называют контрольной суммой, хэшем или дайджестом сообщения), который точно соответствуют тексту вашего письма. Если письмо будет изменено, то этот набор (контрольная сумма) тоже должен измениться.

2. Затем полученная контрольная сумма шифруются Вашим закрытым ключом. Теперь ее можно расшифровать только Вашим открытым ключом.

3. Вместе с письмом отправляются контрольная сумма и Ваш открытый ключ.

4. Когда Ваше письмо получено, программа получателя берет ваш открытый ключ, присланный с письмом, и с его помощью расшифровывает полученную контрольную сумму. Затем она сама генерирует контрольную сумму для текста письма и сверяет обе контрольные суммы. Если присланная контрольная сумма и вторично полученная программой контрольная сумма совпадают, значит письмо не изменялось.



5. Предположим, кто-то перехватил ваше письмо и поменял его содержимое. Он должен сгенерировать новую контрольную сумму, соответствующие новому содержанию письма, но он не сможет зашифровать эту новую контрольную сумму Вашим закрытым ключом за его отсутствием. Если он зашифрует ее другим закрытым ключом, ему придется заменить и открытый ключ. При этом получатель получит не Ваш открытый ключ, выданный "чужим" центром сертификации. И если пользователь не установил сертификат этого центра в свой компьютер как доверенный центр, при получении "чужого" сертификата пользователь будет оповещен об этом.


ПРИНЦИП ДЕЙСТВИЯ ЭЛЕКТРОННОЙ ПОДПИСИ
Подготовка ключей
Закрытый ключ
Программно-технический комплекс
Открытый ключ
Остаётся у владельца подписи
Передаётся адресату
001100 110011 100
Хеш-функция (Идентификатор документа, математически рассчитываемый на основании текста самого документа, позволяющий сравнивать документ на соответствие)
Подписание
Электронный документ
Создание хеш-функции
Шифрование хеш-функции закрытым ключом
Создание электронной подписи
Соединение подписи с документом
Проверка
Подписанный электронный документ, переданный адресату
Считывание документа
Расшифровка хеш-функции открытым ключом
Создание хеш-функции
Восстанов-ление хеш-функции
Сравнение хеш-функций, если они одинаковые, электронная подпись верна
Источник: uc.credos.ru
ТАСС Телеком
ИТАР ТАСС

Подписывание

Проверка