# Электронная подпись

Свойства собственноручной подписи

- согласие

- аутентичность подписанта

- авторство

- непереносимость

- целостность

Договор 1969

- открытость

- подлинность

DSA

Подписание

M, E, D

H(M)

ЭП = Шифрование (Н(М), Е)

Проверка подписи

M,ЭП,D

H(M)

H’= Расшифровка (ЭП,D)

? Н=Н’

63-ФЗ

Виды подписи

- простая

- усиленная

- квалифицированная

- неквалифицированная

Модели

- децентрализованная (PGP)

- централизованная (+арбитр: сертификация открытых ключей) - PKI

Certification Authority (CA)

Удостоверяющий центр (УЦ)

Шаги:

- пользователь создает пару ключей

- запрос в УЦ на сертификацию открытого ключа

- выпуск сертификата

X.509

- версия и алгоритм подписания

- реквизиты УЦ

- срок действия сертификата

- данные владельца закрытого ключа (соответствующего открытому)

- открытый ключ

Certificate Revocation List (CRL)