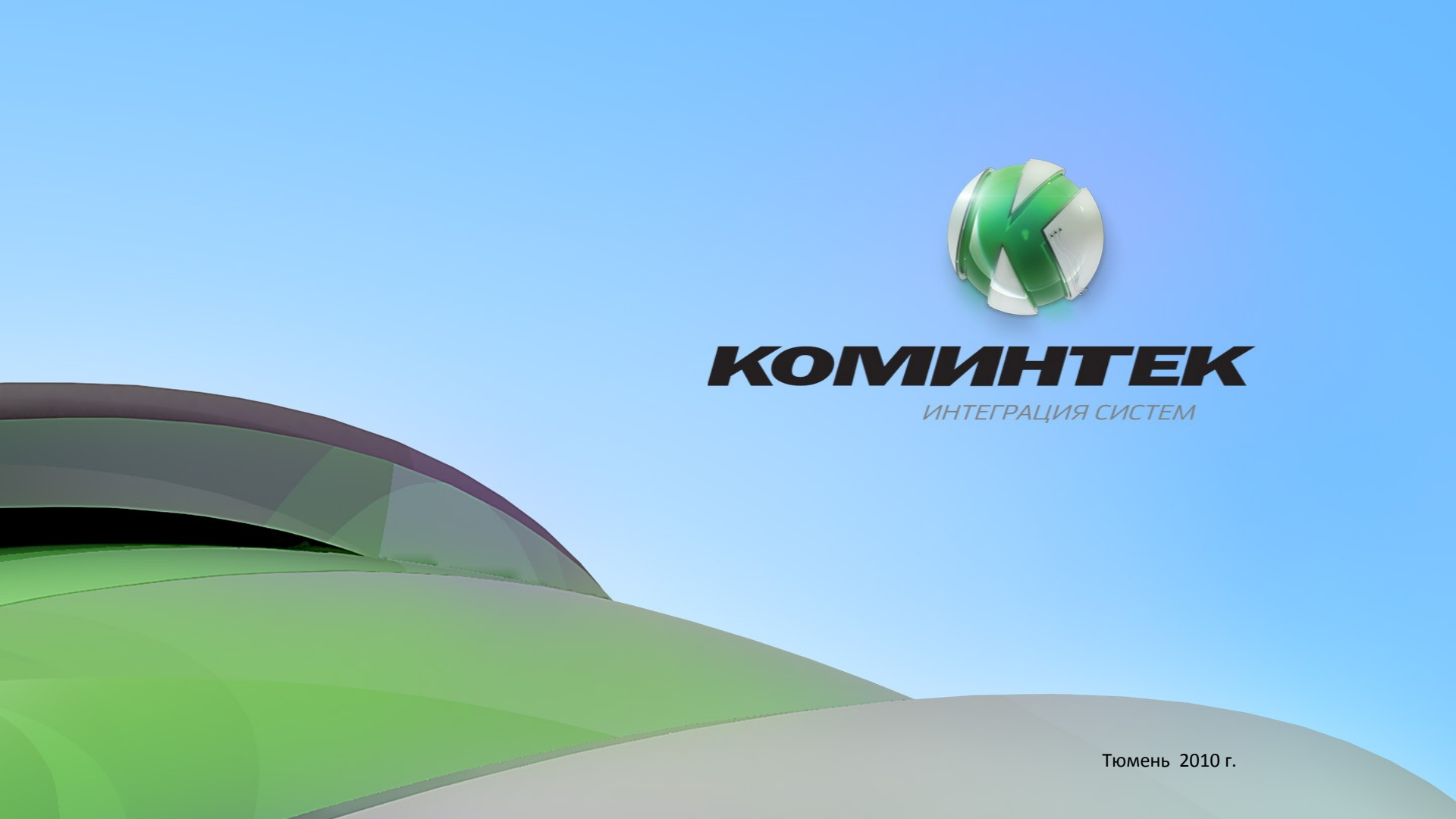


Тюмень 2010 г.

ЭЦП

электронная
цифровая
подпись

Бондарев Евгений Алексеевич
Менеджер активных продаж
ООО «КОМИНТЕК»

КОМИНТЕК

ПРЕДПОСЫЛКИ ПОЯВЛЕНИЯ ЭЦП

- Повсеместное применение электронных сообщений
- Необходимость обеспечения юридической значимости электронных сообщений
- Необходимость обеспечения достоверности электронных сообщений

ПРОБЛЕМЫ БУМАЖНОГО ДОКУМЕНТООБОРОТА

- низкая скорость обмена документами
- высокие накладные расходы

ФУНКЦИИ ЭЦП

- Контроль целостности передаваемого документа
- Защита от изменений (подделки) документа
- Невозможность отказа от авторства
- Доказательное подтверждение авторства документа

ОПРЕДЕЛЕНИЕ ЭЦП

(согласно федерального закона от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»)

«**Электронная цифровая подпись** — реквизит электронного документа, предназначенный для защиты данного 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»

ЗАКОНОДАТЕЛЬНЫЕ НОРМЫ

- Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»
- Приказ Министерства по налогам и сборам РФ от 2 апреля 2002 г. N БГ-3-32/169 «Порядок представления налоговой декларации в электронном виде по телекоммуникационным каналам связи»

ИСТОРИЯ ВОЗНИКНОВЕНИЯ

1976, Уитфилд Диффи и Мартин Хеллманом - предложено понятие «электронная цифровая подпись»

1977, Рональд Ривест, Ади Шамир и Леонард Адлеман - разработан криптографический алгоритм RSA, примитивные цифровые подписи

1984, Шафи Гольдвассер, Сильвио Микали и Рональд Ривест - определены требования безопасности к алгоритмам цифровой подписи, выявлены методы атак

1994, Главное управление безопасности связи Федерального агентства правительственной связи и информации - разработан первый российский стандарт ЭЦП — ГОСТ Р 34.10-94

2002 - введен стандарт ГОСТ Р 34.10-2001 вместо устаревшего ГОСТ Р 34.10-94

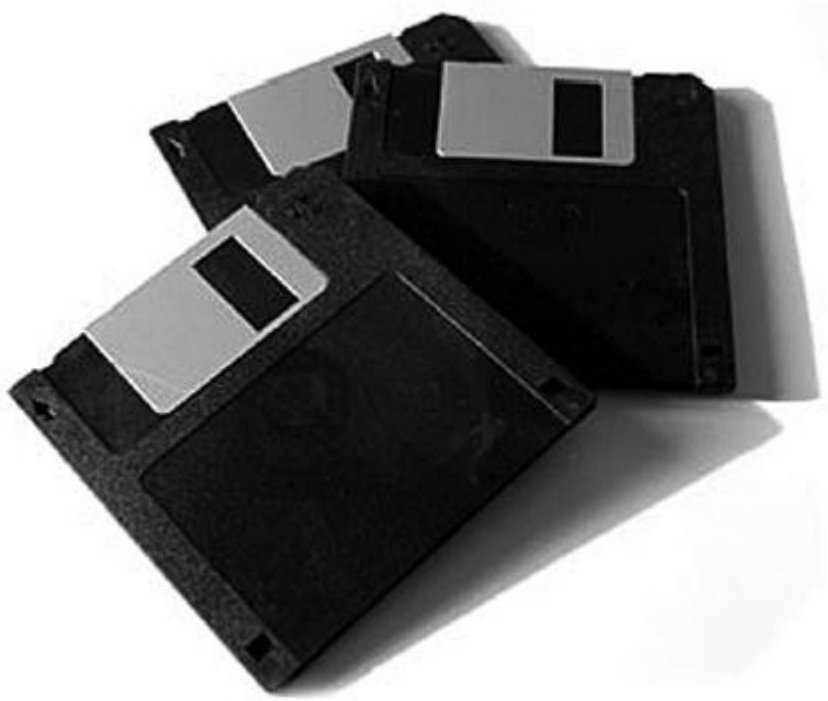
АЛГОРИТМЫ ПОСТРОЕНИЯ ЭЦП

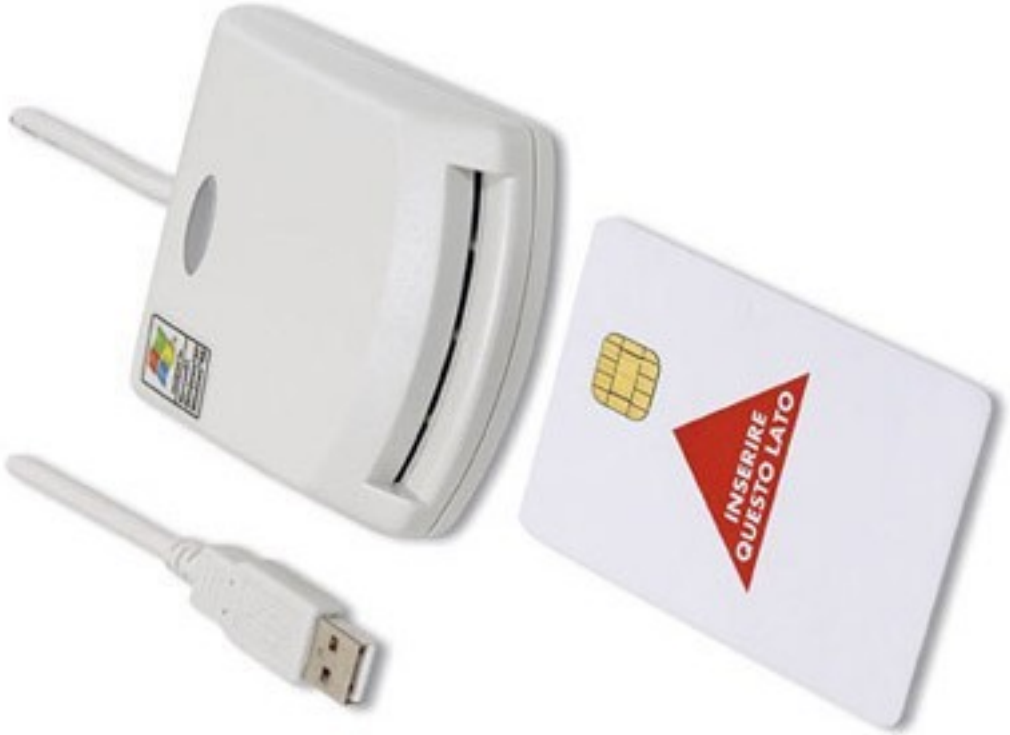
- Алгоритмы симметричного шифрования
- Алгоритмы асимметричного шифрования
- Другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись и т.д.)

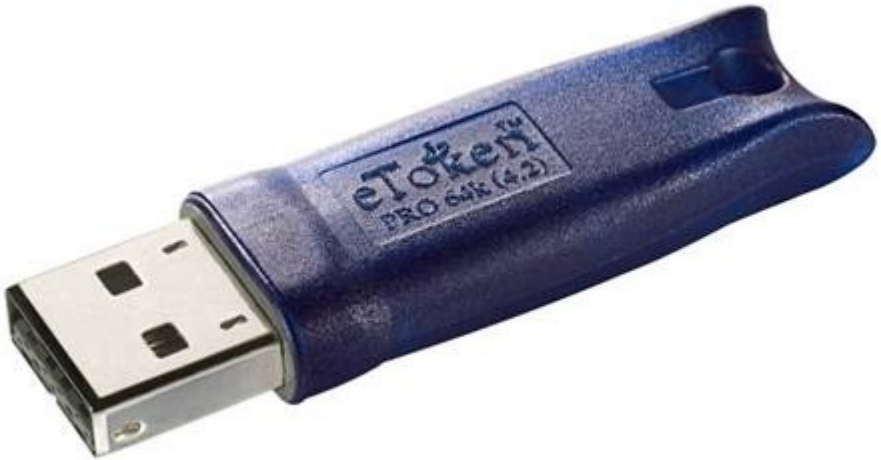
ХРАНЕНИЕ ЭЦП

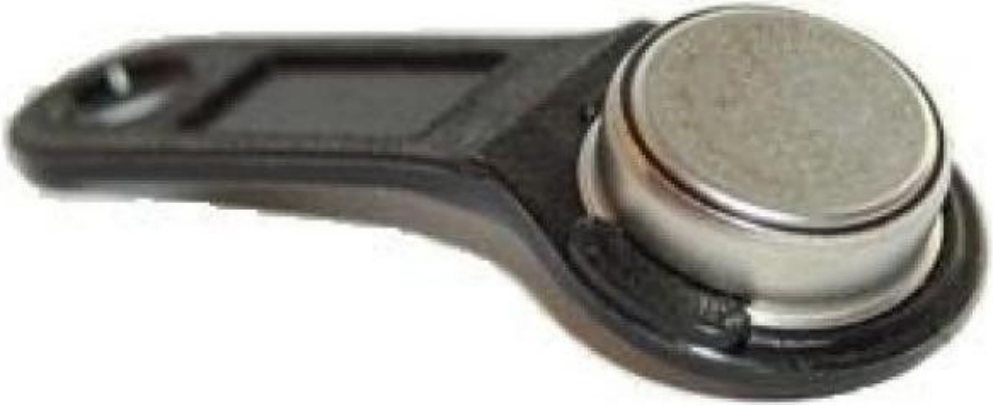
- Дискета
- Смарт-карта
- USB-брелок
- Таблетки Touch-Memory

В соответствии с законом «ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ», ответственность за хранение закрытого ключа владелец несет сам.




INSERIRE
QUESTO LATO

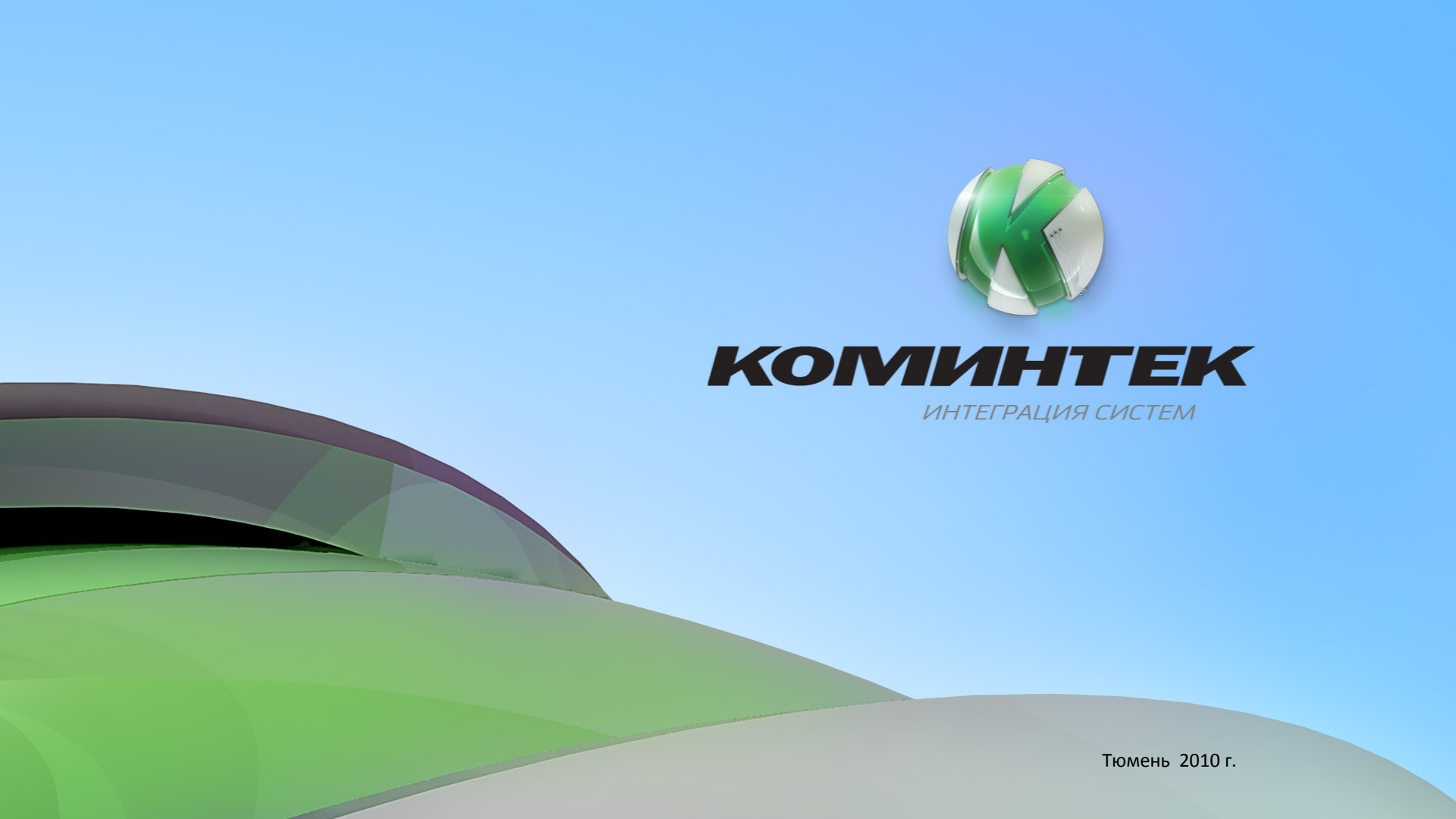

eToken
PRO 64k (4.2)



ЭЦП В ЭЛЕКТРОННЫХ ТОРГАХ

- Торговая площадка Сбербанк-АСТ
- Торговая площадка правительства Москвы
- Торговая площадка Республики Татарстан
- Торговая площадка ММВБ
- Торговая площадка РТС

ВОПРОСЫ



Тюмень 2010 г.