ЭЛЕКТРОННАЯ ПОДПИСЬ

Советы и рекомендации

Часть

1

ЭП и законодательство

Принципы использования юридически значимой электронной подписи в РФ

1

Классическая подпись на бумажном документе

- Однозначно идентифицирует подписавшего
- Не требует специального оборудования
- Не нужно изучать законодательство и пользоваться дополнительными устройствами
- Легко и быстро повторяется подписывающим
- Эталон подписи находится в паспорте
- Проверить сложно и дорого – почерковедческая экспертиза

2

Электронная подпись…

- **Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;**
- **Регламентируется законом 63-ФЗ «Об электронной подписи»**
- **При соблюдении ряда требований - полный аналог обычной подписи на бумажном документе**

3

Преимущества ЭП

- Позволяет реализовать электронный документооборот и снизить его стоимость
- Для КЭП и УНЭП:
  - Доказывает авторство электронного документа – нельзя сказать «это подписал не я»
  - Обеспечивает целостность документа – любые изменения в нем приведут к недействительности ЭП, поэтому нельзя как в бумажном договоре заменить страницу или исправить текст

4

Законодательство и нормативные акты

- N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г.
- № 44-ФЗ «О контрактной системе…» от 5 апреля 2013 г.
- Приказ ФСБ РФ от 27 декабря 2011 года N 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»
- Приказ ФСБ от 27 декабря 2011 года № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра»
- 382П положение центрального банка РФ
- 152 федеральный закон – О персональных данных

Часть

2

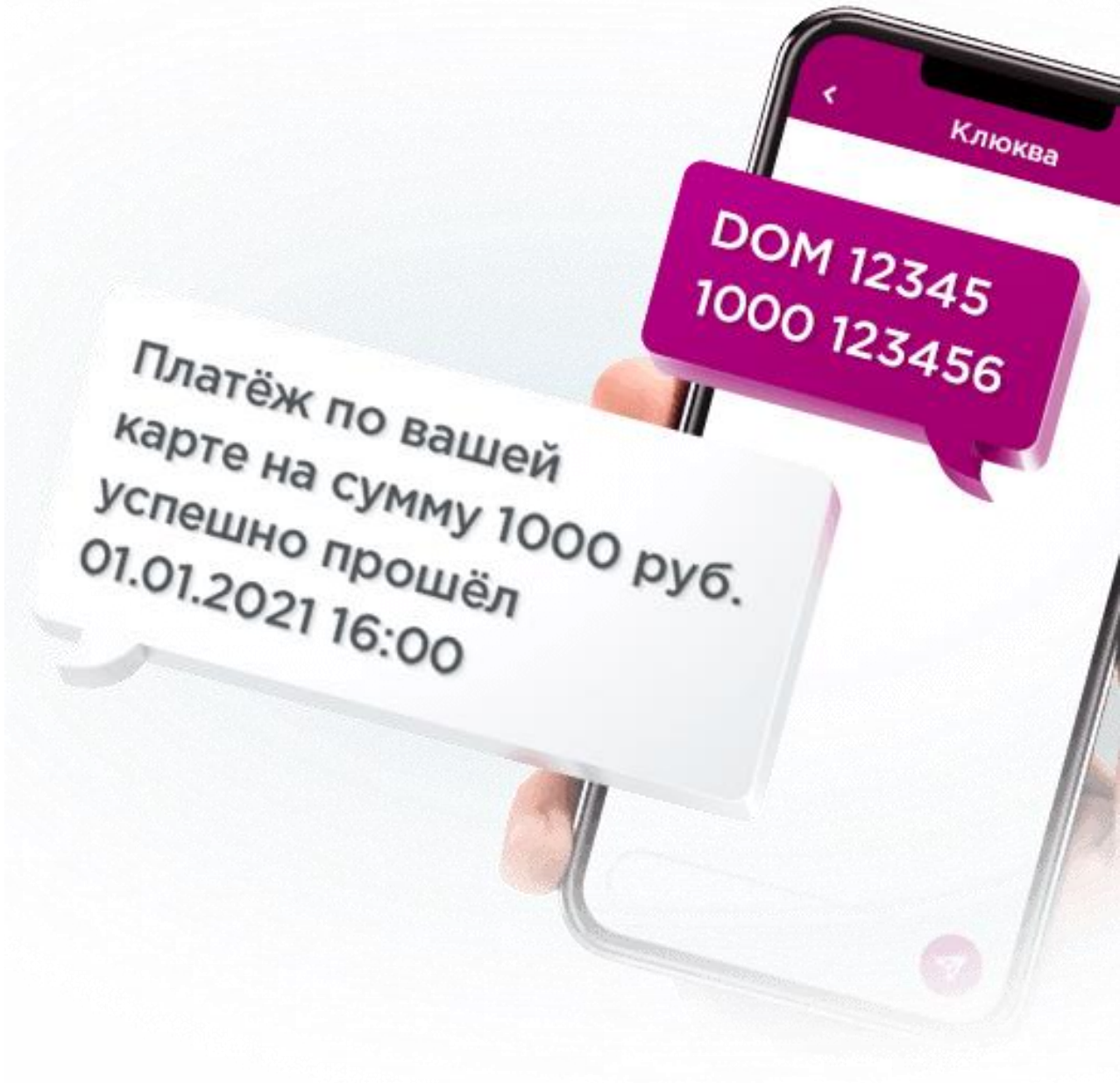
Виды электронной подписи

Простая, усиленная и квалифицированная

1

Простая электронная подпись

- Посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом
- Применяется, например, на Госуслугах, личном кабинете физического лица ФНС, в банковском обслуживании физических лиц



2

Усиленная неквалифицированная

- Получена в результате криптографического преобразования информации с использованием ключа электронной подписи
- Позволяет определить лицо, подписавшее электронный документ
- Позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания
- Создается с использованием средств электронной подписи

3

Усиленная квалифицированная

- Соответствует всем признакам НЭП и следующим дополнительным признакам:
- Ключ проверки электронной подписи указан в квалифицированном сертификате (а значит выдан акредитованным УЦ)
- Для создания и проверки ЭП используются средства ЭП, имеющие подтверждение соответствия требованиям 63-ФЗ

4

Обязанности участников электронного взаимодействия при использовании КЭП и УНЭП

- Обеспечивать конфиденциальность ключей электронных подписей
- Уведомлять УЦ и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи
- Не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена

Часть

3

Устройство и компоненты усиленной ЭП

Ключи, сертификаты, криптопровайдеры и ключевые носители

2

Сертификат ключа проверки электронной подписи

- Ключ проверки ЭП доступен всем
- Любой человек должен доверять ключу проверки ЭП
- Сертификат – электронный документ, подтверждающий принадлежность ключа проверки ЭП конкретному человеку
- Сертификат заверяется (подписывается) удостоверяющим центром
- Удостоверяющему центру (и его сертификату) доверяют по умолчанию

3

Виды удостоверяющих центров

- Обычный УЦ:
  - Выдаваемые сертификаты используются для УНЭП
  - Может установить кто угодно
  - Можно использовать любое ПО, в том числе бесплатный MS Certification Service
- Аккредитованный УЦ:
  - Выдаваемые сертификаты используются для КЭП
  - УЦ получает аккредитацию в Минкомсвязи РФ и работает по утвержденным регламентам
  - Используемое ПО сертифицировано

4

Где хранить ключи ЭП

- В файловой системе, на обычных Flash-накопителях, в реестре операционной системы
  - Очень низкий уровень защиты
  - Ключи могут быть скопированы
  - Факт копирования / компрометации ключей не может быть обнаружен
- Токен / смарт-карта
  - Высокий уровень защиты
  - Соответствует требованиям законодательства

5

Что произойдет в случае кражи ключей ЭП

- Злоумышленник сможет скопировать ключи на свой носитель
- Он сможет в любое время подписать любой документ от имени легального владельца
- Владелец не сможет узнать, что его ключами обладает кто-то другой
- Владелец не сможет узнать, что его ключом что-то подписали
- Владелец не сможет доказать, что документ подписывал не он
- 63-ФЗ будет нарушен

6

Как токен / смарт-карта защищает ключи ЭП

- Доступ к памяти токена защищен PIN-кодом
- При попытке подбора PIN-кода (от 3 до 10 попыток) токен будет заблокирован
- Извлечь информацию путем разбора токена невозможно
- При краже токена сертификат отзывается
- Если токен оснащен криптографическим процессором, то можно создавать ***неизвлекаемые*** ключи

7

С помощью чего вычисляется ЭП

- Программный криптопровайдер
- Для КЭП используются:
  - КриптоПро CSP – платный + тест
  - VipNet CSP - бесплатный
  - Signal-COM CSP – платный
- Токены и смарт-карты оснащенные криптографическим процессором
- Например, линейка Рутокен ЭЦП (2100, 3000, 3.0)

8

Требования УЦ ФНС

- Обязательно личное присутствие
- Предоставляемый ключевой носитель должен быть сертифицирован
  - Носитель без криптоядра – сертификация ФСТЭК
  - Носитель с криптоядром – сертификация ФСБ
- Один сертификат ЭП – один ключевой носитель

Часть

4

Безопасность ЭП

Как хранить и чем защищать

1

Что даст аппаратный ключевой носитель

- Ключи становятся материальным объектом и факт кражи можно отследить
- PIN-код защищает доступ к ключам
- При попытке подбора PIN-кода доступ блокируется

2

Преимущества использования неизвекаемых ключей

- Экспортируемые и неэкспортируемые ключи могут быть скопированы, если известен PIN-код
- Неизвлекаемые ключи не могут быть скопированы
- Может существовать только одна копия ключа на единственном ключевом носителе

3

Требования к использованию неизвлекаемых ключей

- Ключевой носитель (токен или смарт-карта) с криптографическим ядром
- Например, линейки Рутокен ЭЦП 2.0 и Рутокен ЭЦП 3.0
- Создание ключа с помощью специального программного обеспечения:
  - ПО с поддержкой интерфейса программирования токена, например PKCS#11
  - Программный криптопровайдер, работающий в режиме «активного токена» (КриптоПро версии 5)

4

Безопасное хранение и использование

- Не хранить PIN-код вместе с токеном
- PIN-код лучше вообще не записывать
- Но забытый PIN-код восстановить невозможно, ключи ЭП на токене – тоже
- Токен никому не передавать, даже на время, особенно токен с извлекаемыми ключами
- При любом подозрении в копировании ключей – обратиться в УЦ
- Не существует способов блокировать использование токена на любом ПК при знании PIN-кода

Игнатов Андрей Евгеньевич

- +7 968 813 49 28
- andrey@ignatov.email