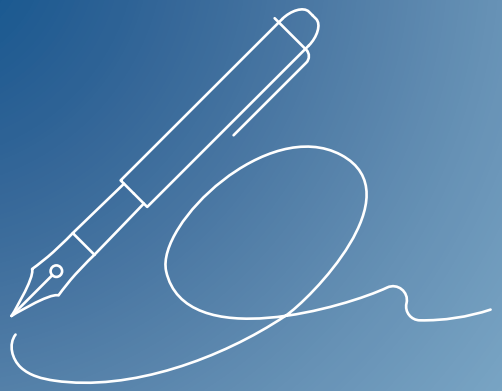
ИНФОТЕКС ТРАСТ

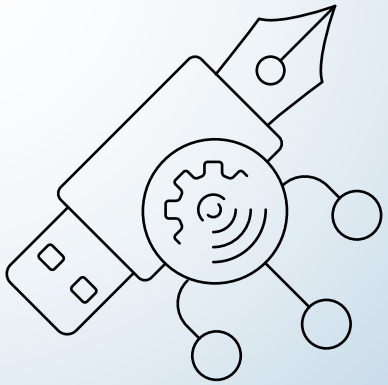
Кто прошлое помянет

Проблематика проверки электронной подписи документов с учётом времени

Проблемы прогресса

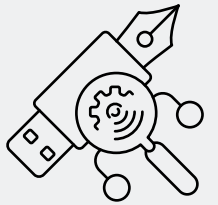


Собственноручные подписи проверяются глазами и не имеют срока действия,
а документы с собственноручной подписью могут храниться вечно и проверяться многократно.



Электронные подписи – напротив.
Их проверка сопряжена с множеством вопросов, а устойчивость ограничена по времени: сроком действия сертификатов подписи.

Подписанные документы **требуется хранить и иметь возможность проверить (в том числе, в течение длительного времени)**, невзирая на электронный формат.



Проблемы проверки электронных подписей **не существуют для бумажных** документов.
Для их решения нужны новые подходы.

Буква закона

По закону, квалифицированная подпись верна в случае, если:

1

«<...> сертификат выдан <...> аккредитованным УЦ, **аккредитация которого действительна на день выдачи указанного сертификата**»;

2

«<...> сертификат **действителен на момент подписания** <...> (при наличии достоверной информации о моменте подписания <...>) или **на день проверки** <...>, если **момент подписания** <...> не определён»;

3

«<...> **срок действия ключа ЭП**, <...> **не истёк на момент подписания** <...> (при наличии достоверной информации о моменте подписания <...>) или **на день проверки** <...> , если **момент подписания** <...> не определён»;

4

«<...> **положительный результат проверки принадлежности владельцу** <...> сертификата <...> , и подтверждено отсутствие изменений, внесённых в этот документ <...> **проверка осуществляется с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям**».

Аккредитованность УЦ

На текущий момент есть два реестра:

1

TSL Головного УЦ

2

Таблица на сайте Минцифры

Эти списки **не синхронизированы друг с другом** и обновляются не одновременно с принятием решений правительственной комиссией (например, о приостановлении аккредитации).

В итоге – не ясно, на что правильно ориентироваться:
На один из списков или решение Правительственной комиссии.

Не предусмотрено механизма, отвечающего потребностям автоматизированной массовой проверки подписей (например, операторами ЭДО), являющегося юридически корректным.

Из-за описанных проблем
подход к определению аккредитованности
каждый выбирает сам, на свой страх и риск

ИНФОТЕКС ТРАСТ

Дата формирования подписи

Поскольку мы говорим про архивные подписи, то задача – понять, когда такая подпись была сформирована:

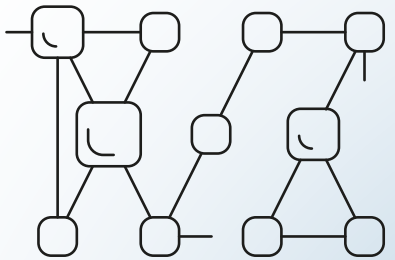
1

Первый и очевидный подход строгий – **использование метки времени (timestamp)**

2

Нестрогий и активно применяемый подход – **определение времени подписания по косвенным факторам**, таким как записи в базе данных, даты документов и т.д.

3



Относительно новый строгий подход – **использование цепного реестра (блокчейна)**, в котором записаны сведения о сформированных электронных подписях

Метки времени: проблемы

1

Не ясно, где нужно получать сертификаты для TSA: обезличенные сертификаты на организацию с необходимыми полями не выдает УЦ ФНС России, а АУЦ не имеют права их выдавать

2

Без использования архивного формата (CAdES-A) метки лишь **незначительно продлевают «срок жизни» подписи** (на срок жизни сертификата подписи метки)

3

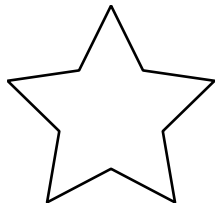
Существующая норма, предусматривающая, использование меток времени, **не учитывает** архивный формат меток (CAdES-A)

4

Рост количества электронных документов, которые одновременно нужно долго хранить, приводит к **стремительному росту необходимой для регулярного формирования новых меток вычислительной мощности**

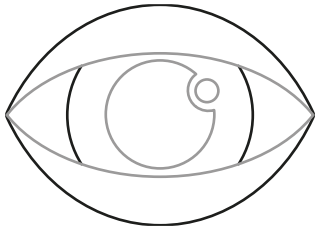
(объём меток, который нужно регулярно формировать, увеличивается с ростом числа хранимых документов, что потенциально приводит к необходимости создания криптофермы для регулярного переподписания всех хранимых меток)

Проверка по косвенным признакам



1

На текущий момент **наиболее распространённая практика**



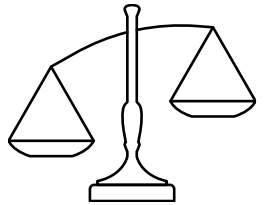
2

При росте числа документов и переводе всё более критичных процессов в электронный вид **возрастёт и интерес мошенников к эксплуатации нестрогости такого подхода**

3

Текущая практика рано или поздно **может привести к реализации той или иной мошеннической схемы**

(отказ от реально подписанного документа по причине недействительности подписи)

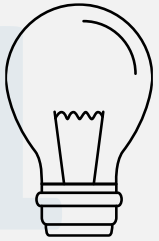


4

Формально, применяемая практика **не соответствует требованиям законодательства** и опирается на решения судей и общечеловеческую логику

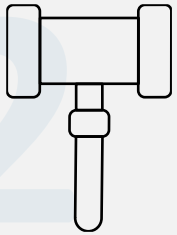
Цепной реестр с записями о сформированных ЭП

1



На текущий момент **есть только идея**, готовых реализаций нет

2



Не существует юридической основы для признания действительности подписей на основе наличия записей в цепном реестре

3

Не существует готовой технической реализации, учитывающей особенности документооборота

Основное преимущество:

в теории, **позволяет обеспечить техническую строгость** за счёт применения технологии цепного реестра **при сравнительно невысоких требованиях по производительности** – при росте числа хранимых документов требуемая вычислительная мощность не растёт, она растёт при ускорении роста их числа

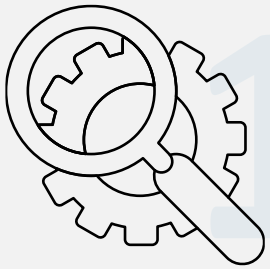
«Недостоверная» информация о времени формирования подписи

Если у нас **нет информации о времени формирования подписи**, то проверка осуществляется с учётом времени осуществления проверки.
Действовать в этом случае должен не только сертификат ключа проверки ЭП, но и ключ ЭП, который, как правило, действует меньше чем сертификат.

Таким образом, без использования хоть какой-нибудь технологии достоверного определения времени формирования подписи **срок «проверяемости» подписей документов сократится ещё больше** и сделает крайне сложным реальное использование технологии электронной подписи для подписания значимых документов с учётом буквы закона.

Определение соответствия средства подписи требованиям

1

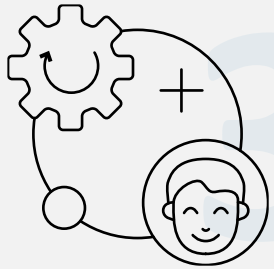


Нет строгих методов контроля того, что использовано конкретное средство, **опора только на SST**

2

Нет никаких методов **контроля соблюдения на стороне подписанта требований** к использованию применяемого средства

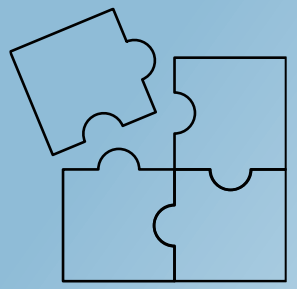
3



Проверка сводится к **проверке соответствия подписи стандарту и принятию риска** того, что на стороне подписанта может быть что-то не так со средством подписи

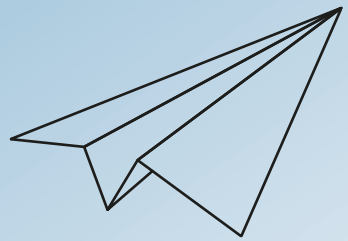
Норма, фактически, сформулирована так, что **не может быть реализована на проверяющей стороне** и не ясно, как принимающей стороне управлять рисками использования несертифицированных средств пользователями

Выводы и предложения



1

Существующее законодательство имеет ряд лакун, которые **вынуждают при решении практических задач ориентироваться на практику и гипотезы**,
а не на нормы и требования



2

Практический **вопрос хранения (в том числе долговременного) и проверки документов с электронной подписью сложен** и, поскольку опереться на опыт бумажных документов не получится, **должно быть найдено** в первую очередь **технологическое решение этого вопроса** и после этого закреплено нормой

3

Часть обозначенных проблем **актуальна уже сегодня** и требует решения. В то же время, пока **объём** подписанных электронных документов в чувствительных сферах жизни **только начинает расти**, проблема хранения и проверки подписей не стала критической, у рынка и регуляторов **есть время сформировать и закрепить подход**. И подход этот может стать не унаследованным от бумажного документооборота, а **по-настоящему электронным**.

ИНФОТЕКС ТРАСТ

ИНФОТЕКС ТРАСТ

Спасибо за внимание!

Никита Александрович Вылегжанин
Руководитель ДРУП

АО «Инфотекс Интернет Траст»

8 800 250-8-265
litrust.ru