"... в настоящее время доверие основано на репутации учреждения – это доверие к «вывеске» ... предлагается перейти к технологической поддержке этого доверия ... чтобы криптографически гарантировать происхождение, неизменность и, следовательно, целостность сохраненных в архивах документов."

Джон Колломоссе
(Проект ARCHANGEL)

Сохранность цифровых активов

Обеспечение юридической значимости электронных документов размещенных на хранение

Главный тезис

Заниматься хранением информации, которая не отражает какую либо деловую активность, не несет в себе юридическую, историческую значимость, аналитическую или культурную ценность – БЕССМЫСЛЕННО!!!

По любому хранимому документу из прошлого необходимо иметь состоятельные ответы на вопросы:

- кто его автор и его полномочия по созданию такого рода документов
- время создания, откуда он поступил и кто его разместил на хранение
- кто им пользовался
- какие события происходили с документом в период хранения
- И т.д. и т.п. ….

Любые электронные хранилища это:

1. **Регламентирующее организационно-распорядительное сопровождение процесса хранения.**
   - - обследование и понимание в целом ЖЦ ключевых документов и роли тех, кто их порождает и использует
   - - общая конструкция НПА и организационно-распорядительных документов
   - - описание орг. изменений, которые потребуются для внедрения Э-хранилища и НПА,
   - - обсуждение и в целом согласование (Минтруд ….)
   - - детальный план с горизонтом 2-3-4 года
   - - проекты НПА
   - - внедрение (включая организационные изменения и утверждение НПА)

2. **Прикладная составляющая с задачами:**
   - **общие инфраструктурные задачи:**
     - Идентификация и аутентификация субъектов информационного обмена, инфраструктура открытых ключей, УЦ, методы разграничения доступа ...
     - Инфраструктура управления полномочиями (PMI), назначение/обработка полномочий авторам ЭП …
     - Синхронизация времени аппаратных платформ, эталон маркеров доверенного времени.
   - **интеграции с ЭДО, размещение ЭД на хранение и формирование «выписок» (методы осуществления аутентичности: повторное получение одного и того же или валидатор актуальности «выписки»)**
   - **администрирование и аудит процедур**

3. **Организация бизнес-процесса непосредственного хранения с обеспечением целостности**
   - **Выбор носителей - WORM (Write Once, Read Many) однократная запись, многократное считывание**
   - **Исходно предусмотреть миграцию на новые поколения носителей и программно-аппаратных сред**
   - **Техническая реализация обеспечения целостности - аппаратные, деревья хэшей …**

4. **Обеспечение юридической значимости размещенных на хранение ЭД в исторической перспективе.**

Обеспечение юридической значимости

Юридическая значимость (**ГОСТ** Р 7.0.8-2013 Свойство документа выступать в качестве подтверждения деловой деятельности либо событий личного характера) – это комплексная задача, проходящая через все стадии жизненного цикла ЭД, обеспечивающая ЭД необходимыми характеристиками.

ГОСТ Р ИСО 15489-2007, среди таких характеристик, определяет:

- Достоверность (Обеспечивается на ранних стадиях жизненного цикла ЭД).

  Достоверным является документ, содержание которого можно считать полным и точным представлением подтверждаемых операций, деятельности или фактов и которому можно доверять в последующих операциях или в последующей деятельности.

- Целостность (Обеспечивается средствами хранения и частично Компонентами обеспечения ЮЗ).

  Целостность документа определяется его полнотой и неизменностью.

- Пригодность для использования (Обеспечивается средствами создания и хранения).

  ЭД, который можно локализовать, найти, воспроизвести и интерпретировать.

Аутентичность документа

Документ аутентичен, если он:

а) **является тем, чем должны быть (соответствует установленным правилам)**

Определяется на этапе создания ЭД и фиксируется личной ЭП автора ЭД, в последующим должна быть обеспечена непрерывность доверия к ЭП во времени, включая смену криптографических алгоритмов и формата представления хранимого ЭД

б) **был создан или отправлен лицом, уполномоченным на это**

Определяется автором ЭД, включая инфраструктуру управления полномочиями в организации

в) **был создан или отправлен в то время, которое обозначено в документе**

Определяется на этапе создания ЭД и фиксируется личной ЭП автора ЭД с учетом обеспечения непрерывности доверия к ЭП во времени

Аутентичность - выливается во внедрение и документальную фиксацию политики и процедур контроля над созданием, получением, передачей, сохранением и отбором документов, что должно гарантировать, что создатели документов уполномочены на это и идентифицированы, а документы защищены от несанкционированного дополнения, удаления, изменения, использования.

Осознать объем организационно технической задачи могут в чём то помочь:

- Перечень профильных стандартов:
  - ГОСТ Р ИСО 15489-2007 «Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования»
  - ГОСТ Р ИСО 13008—2015 Информация и документация ПРОЦЕССЫ КОНВЕРСИИ И МИГРАЦИИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ.
  - ГОСТ Р 54989-2012 /ISO TR 18492:2005 Обеспечение долговременной сохранности электронных документов
  - ГОСТ Р ИСО 23081-1–2008 «Система стандартов по информации, библиотечному и издательскому делу. Процессы управления документами. Метаданные для документов. Часть 1. Принципы»
- Методические и регламентирующие документы, которых крайне мало
  - Технологическая концепция хранения и использования электронных документов с обеспечением их юридической силы для финансового рынка
  - Росархив. Проект. Типовые функциональные требования к системам электронного документооборота и системам хранения электронных документов в архивах государственных органов
  - Приказ Минкомсвязь от 2 сентября 2011 г. N 221 "Об утверждении Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения"

Способы обеспечения доверия к характеристикам ЭД во времени

Это концептуальный вопрос, который может «отправить под откос» все последующие усилия.

Основная проблема - что делать с ЭП во времени? Действительность открытого ключа ограничена, смена легитимной криптографии и смена формата хранимого ЭД делает ЭП недействительной.

Различные бизнес процессы, с учетом приемлемых для них рисков, используют различные подходы, среди которых можно выделить:

1. «Снятие» ЭП.
2. Переподписание «служебной» ЭП как способ обеспечения аутентичности при хранении.
3. Исходно использовать сертификаты ключа проверки электронной подписи продолжительного действия.
4. Использование специальных форматов ЭП.
5. «Снятие» ЭП через оформление электронного Акта (служебного ЭД) представленного в виде метаданных о достоверности, целостности и аутентичности хранимого ЭД.

«Снятие» исходной ЭП

Самый простой способ, но с очень неприятным допущением - всё что попало и находится в хранилище ЭДО аксиоматично заслуживает доверия и ни каких доказательств не требует.

Некоторой разновидностью является добавление к ЭД хэш-функции, но надо помнить, что этот факт аутентичность ЭД не обеспечивает.

Очевидно, что такого рода допущения применимы далеко не во всех процессах. Как только в Модели угроз процесса организации хранения появляется «внутренний нарушитель», то такой подход использовать нельзя.

Под «снятием» понимается не удаление/уничтожения данного реквизита, а прекращение поддержания его аутентичности ввиду экономической нецелесообразности или технической сложности.

Переподписание «служебной» ЭП

Наиболее «опасный» способ, поскольку провоцирует на ложные иллюзии обеспечения аутентичности ЭД во временной перспективе и безопасности при кажущейся простоте.

1. В НПА отсутствует определение такой сущности как «служебная» ЭП.
2. При формировании «служебной» ЭП потребуются не тривиальные правовые конструкции, которые должны разорвать связь авторства между контентом ЭД и автора «служебной» ЭП (помним, что авторство – это ключевое свойство подписи ГОСТ Р 34.10-2012 п.4), очевидно, что автор «служебный» ЭП не имеет никакого отношения к содержанию хранимого ЭД.
3. Не отменяет выполнение аудита аутентичности исходного ЭД перед выработкой «служебной» ЭП что потребует разработки/использования протоколов взаимодействия с сервисами валидации и сохранения где то доказательной базы с разработкой формата метаданных для размещения этой информации, потому что сам формат ЭП не предназначен для указания статуса выполнения валидации, размещения и сохранения доказательной базы проведения процедур проверки.
4. Следом ставится еще более сложная задача – каким образом сохранить процедуры аудита во времени в аутентичном виде, в противном случае появляются реальные риски не признания служебной ЭП существенным доказательство, например, в суде.
5. Не предоставляет инструментов обработки событий конверсии криптоалгоритмов и конверсии формата представления исходного ЭД, которые неизбежно будут происходить в период хранения ЭД особенно длительного.

Использование сертификатов ключа проверки ЭП продолжительного действия

Один из простых способов для краткосрочных хранилищ, но с учетом ряда особенностей:

1. Авторы ЭД должны использовать СКЗИ, допускающих период действия открытого ключа более года с прекращением использования закрытого ключа в момент времени когда разница между моментом подписания и завершением действия открытого ключа меньше или равно периоду хранения ЭД в хранилище.

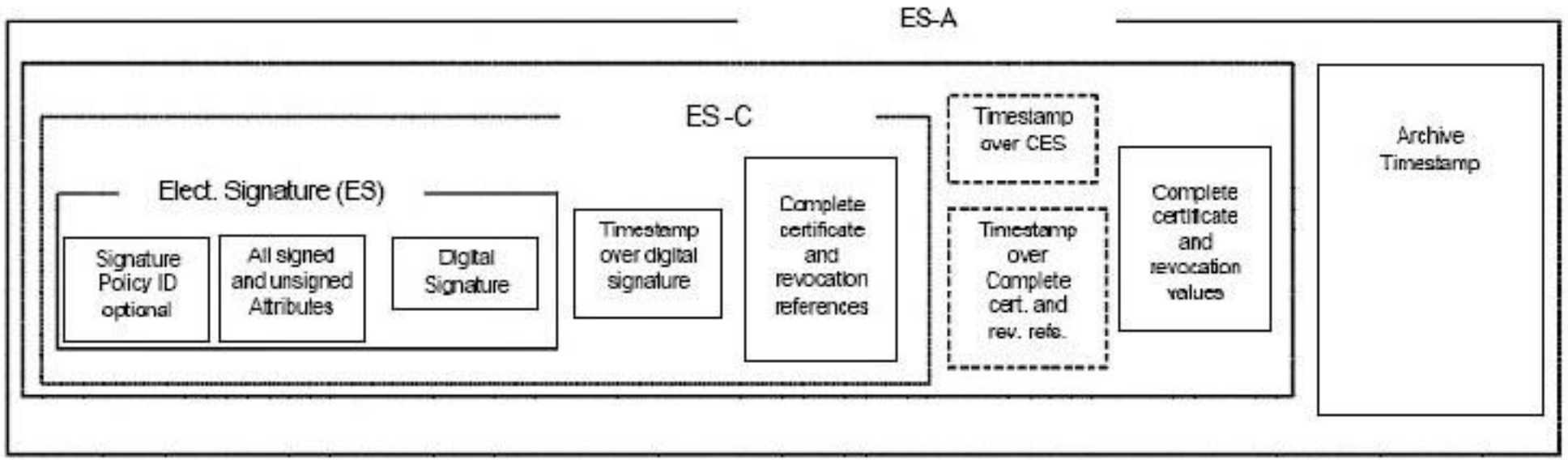
   Срок хранения <= «not After» - Момент подписания (внутри «Private Key Usage Period»)

2. Увеличение срока действия сертификата более 3-5 лет требует использования более сложных и дорогих СКЗИ (в том числе и на стороне пользователя!), а также увеличивает риск не продления сертификата на СКЗИ регулятором каждые 3 года по любым причинам.

3. Существенное допущение: в период хранения не происходит конверсии формата представления хранимого ЭД и легитимный криптоалгоритм не изменяется.

Использование специальных форматов ЭП. Усиление электронной подписи.

Используют так называемое «усиление» («улучшение»/«усовершенствование») подписи в соответствии, например, со стандартами принятыми в ЕС для CAdES. Смысл «усиления» заключается в том, что в ЭП добавляются атрибуты содержащие всю доказательную базу для последующей локальной проверки исходной ЭП и на всю эту информацию создаётся «штамп» времени.



Некоторые особенности практического использования «усиления» подписи

1. Исходно предполагается, что ЭП уже присутствует на ЭД, что на практике не всегда так.

2. Факт того, что перед созданием штампа времени, исходная подпись вообще проверялась с каким либо результатом ни где не фиксируется и документально в составе «усиленной» ЭП не указывается.

3. Технология «усиления» сильно зависит от формата представления ЭД, например, помимо CAdES, существуют еще и PAdES для ЭД в формате PDF и XAdES для XML ЭД, соответственно поддержка всех этих форматов значительно усложнит техническую составляющую хранилища.

4. Семейство AdES не предлагает никаких инструментов для обеспечения аутентичности хранимых ЭД при конверсии формата ЭД и/или криптографических алгоритмов, которая неизбежно будет происходить при длительном хранении ЭД.

5. Выработка очередного «штампа» предполагает доступность исходного ЭД, например, при размещении хранилища в шкафах на магнитных лентах, автоматизировать процедуру выработки очередного «штампа» времени будет крайне затруднительно. Если же выделить хэш (атрибут messagedigest), то дополнительно придется через какие то процедуры обеспечить контроль связки хэш – исходный ЭД и результат как тои где то фиксировать.

«Снятие» ЭП через оформление электронного Акта – наиболее приемлемый способ

Любое событие с ЭД оформляется через создание электронного Акта, представленного в вид метаданных. Чтобы обеспечить доверие к создаваемому электронному Акту необходимо криптографически связать его с хранимым ЭД, зафиксировать факт, время и статус проверки ЭП исходного ЭД, а также правомочность уполномоченного лица хранилища на подписание и создание такого электронного Акта. Фактически создаются процессные метаданные, поддерживающие аутентичность хранимых ЭД во времени.

Если размещаемый на хранение ЭД не имеет ЭП, то создаваемый электронный Акт должен фиксировать существование данного документа на момент времени размещения ЭД на хранение.

Подход аналогичен изложенному в пункте 15 Приказа Минкомсвязи РФ от 02.09.2011 № 221

15. Для проверки аутентичности, целостности и достоверности электронных документов СЭД ФОИВ должна обеспечивать:

- проверку и сохранность электронных подписей, связанных с ними сертификатов ключей проверки электронной подписи;
- хранить результат проверки электронной подписи в виде метаданных электронного документа;
- информировать пользователя СЭД ФОИВ о результатах проверки электронной подписи.

Процессные метаданные связанные с хранимым ЭД

Процессные метаданные используются для документирования следующих событий в процессе хранения ЭД:

- Размещение ЭД на хранение (с учетом версионности). Проверка исходной ЭП или фиксирование факта существования ЭД (если нет ЭП) на конкретный момент времени.
- (*) Обеспечение доверия к факту проверки исходной ЭП или факту существования ЭД в исторической перспективе через цепочку связанных электронных Актов.
- (*) Ввод в действие новых стандартов на хэш-функцию и/или электронную цифровую подпись.
- (*) Ввод в действие новых форматов представления ЭД размещенного на хранение.
- Создание выписки. Выгрузка хранимого ЭД из хранилища с добавленными процессными метаданными для обеспечения достоверности, целостности, аутентичности и **актуальности** с учетом возможной версионности ЭД. Последующая проверка метаданных может осуществляться без непосредственного обращения к хранилищу внешним сервисом по аналогии правил работы с реестром CRL при проверке сертификата на отзыв.

(*) – При этом цепной список электронных Актов оформляется в блоки. Самая близкая аналогия (именно аналогия, а не сама технология) – процедура оформления блока из цепочки транзакций в **Blockchain**.

Ввод в действие новых криптоалгоритмов

Уметь документировать данное событие очень важно! Причём документировать таким образом, чтобы:

- Сохранить связь с исходным ЭД.
- Зафиксировать действительность цепного списка на «старых» криптоалгоритмах.
- Зафиксировать получившейся цепной список вновь созданными процессными метаданными на «новых» криптоалгоритмах.

Следует напомнить, что в начале марта 2019г. специалисты из Франции и Сингапура **продемонстрировали атаку(*)** на хэш-функцию SHA-1 стоимостью менее 100 000$ - это уже уровень интересов малого и среднего бизнеса.

Другими словами за эти деньги можно подобрать "новый" контент ЭД для которого ЭЦП от "старого" ЭД будет сходиться и тут даже "штампы времени" не спасут.

Разумеется и наша отечественная хэш-функция тоже будет со временем не стойкой и двигаться в сторону того, что просто храним ЭД и «старинную» ЭП и не предпринимаем ни какие дополнительные технические меры будет уже крайне опасно.

(*) https://eprint.iacr.org/2019/459.pdf

https://www.securitylab.ru/news/499062.php?fbclid=IwAR2rsjv1cbpluw_NLbz1R_6MtniIACN4b6XrAgCCTA4QnJ_aGMWHOIq__Es

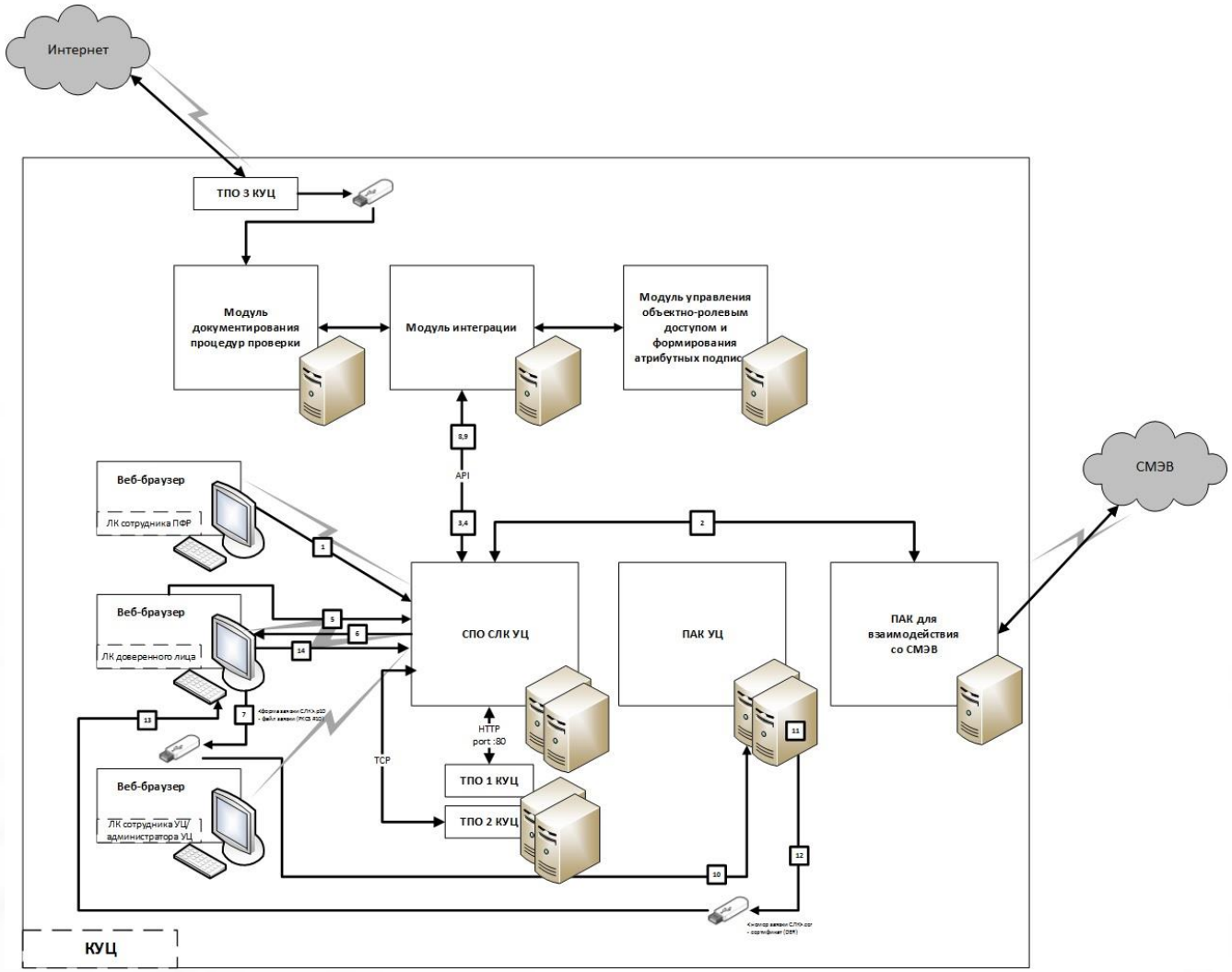
Пилотный проект ПФР 2016 г.

Задача: создать условия по переводу выплатных пенсионных дел в электронный вид с сохранением их юридической значимости при длительных сроках размещения в ведомственном хранилище.

Основные выводы:

- зафиксирована технологическая состоятельность работы с процессными метаданными
- электронные хранилища требуется рассматривать в неразрывной связи с процессами создания и захвата ЭД в системе ЭДО
- опережающими темпами по отношению к технологии должны развиваться организационные и нормативные обеспечения

2018 г. Вторая очередь работ проекта ПФР



Задача: создать условия для обеспечения юридической значимости информации в Реестре выданных сертификатов ключа проверки подписи в течении всего времени существования ведомственного УЦ ПФР.

Вывод: Техническое решение Модулей обеспечения юридической значимости – имеет очень слабую зависимость от специфики контента хранимых ЭД и может использоваться фактически в любых бизнес-процессах.

Вопросы?

Муругов Сергей Михайлович
msm@top-cross.ru