

Организация архивного хранения документов, подписанных усиленной электронной подписью: Как все-таки это делать?

Храмцовская Наталья Александровна

к.и.н., ведущий эксперт по управлению документацией
компании «Электронные Офисные Системы», эксперт ИСО, член МСА
ТК 459/ПК6 «Жизненный цикл электронного документооборота»

Что считать длительным хранением?

- Для документов, подписанных УЭП, длительное хранение фактически начинается с момента, когда **требуется дополнительные действия** для обеспечения юридической значимости и пригодности к использованию – обычно с истечения срока действия любого из сертификатов
- В традиционном российском делопроизводстве и архивном деле к документам длительного хранения относят документы со сроками хранения от 10 лет и более

Что представители разных профессий считают «длительным хранением»

- Представители деловых подразделений - 5 лет
- ИТ- подразделения - 5-10 лет
- Юристы и архивисты - 100 лет
- В ядерной энергетике – от 1 до 100 тысяч лет

Для решения задачи в краткосрочной (5-10 лет) перспективе существуют опробованные на практике решения

- В общем случае они не поддерживаются российским законодательством, но
- Ими можно пользоваться в корпоративной среде

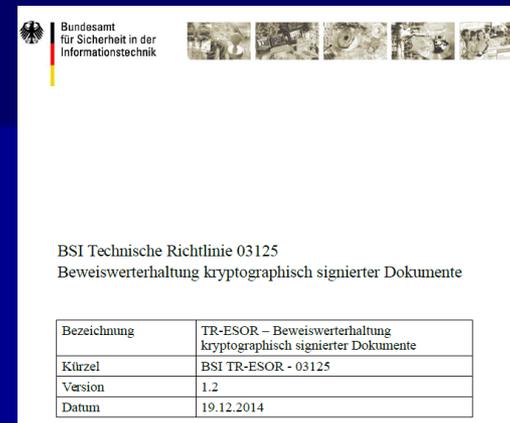
Существующие технологии

- Перепроверка УЭП удостоверяющим центром (в качестве доверенной третьей стороны)
- Создание государственных регистров электронных документов и «точек проверки» подлинности электронных документов
- Переподписание
- Использование услуг доверенной третьей стороны по долговременному хранению электронных документов
- Ряд частичных решений – использование отметок времени, носителей однократной записи, отдельное сохранение хешей и т.д.

Существующие технологии: Европа

■ Переподписание ЭД (Германия)

- Требования TR 03125 «Сохранение доказательной силы документов, подписанных с использованием криптографических методов» v 1.2 (декабрь 2014) – особого восторга не вызвали



■ Использование сертифицированных информационных систем (Франция)

- Системы (собственные и третьих сторон) должны соответствовать стандарту NF Z 42-013 при работе с электронными документами, а также международному стандарту OAIS при создании электронных архивов. Создана система сертификации
- Декрет 2009 года разрешил государственным органам Франции, передавать свои документы на внеофисное хранение поставщикам, аккредитованным Министерством культуры

Существующие технологии: Европа

Draft ETSI EN 319 122-2 V1.0.0 (2015-06)



Electronic Signatures and Infrastructures (ESI);
CAAdES digital signatures;
Part 2: Extended CAAdES signatures

Использование специальных форматов (Евросоюз):

- Евросоюз: Использование специальных вариантов форматов УЭП XAdES, CAAdES, PAdES помогает решать проблему в кратко- и среднесрочной перспективе
- По завершении процесса пересмотра CEN / ETSI, данные варианты могут быть официально признаны решением Еврокомиссии

Решение Национальных архивов США, август 2015 года

- Бюллетень 2015-03 Национальных архивов США
- Перепроверкой электронных подписей Национальные архивы США заниматься не будут. На архивное хранение будут принимать только сами документы, без поддерживающей документации (сертификаты, списки отозванных сертификатов и т.д.)
- Ответственность за подлинность сдаваемых документов несут источники комплектования (контролируется в процессе передачи на архивное хранение). Национальные Архивы выполняют роль доверенного хранителя

От чего зависит решение

- На каком временном периоде решается проблема
 - В атомной отрасли временные рамки – от 1 тыс. лет и более
- Особенности национального законодательства
 - Удобное (например, англосаксонское)
 - Неудобное – континентальное (в т.ч. российское)
 - Очень неудобное – Франция, Германия

Текущая позиция электронных архивистов

- Мы не можем предложить конкретную технологию для столь длительного периода времени
- Мы не знаем, какими будут технологии и право через 50 лет
- Наша задача – сделать то, что в наших силах, и передать электронные документы в приличном состоянии тем, кто придёт после нас через ~40 лет

Главная проблема - правовая

- Все проблемы технического плана решаемы. Нехватку функциональных возможностей обычно можно компенсировать с помощью организационных мер
- Правовые проблемы – самые неприятные
 - Когда за документами стоят деньги и имущество, они обязательно будут оспариваться, даже если противная сторона на самом деле не сомневается в их подлинности. Для этого будут использованы любые, даже самые смехотворные «зацепки»
 - В настоящее время в российском праве нет иной общей концепции доказывания подлинности документов с УЭП, помимо перепроверки подписей. Нет четкого общего порядка представления электронных доказательств

Текущая ситуация в России: где и что можно сделать уже сегодня

- В текущих условиях не может быть 100% уверенности в достаточности принимаемых мер по сохранению ЭД, даже если есть установившееся судебная практика (которая в любой момент может измениться)
- Важно продемонстрировать добросовестность действий организации и принятие ею разумных мер
- В корпоративной среде и во внутренней работе государственных органов и организаций можно использовать практически любые подходы
- В случае, когда деловые документы представляют интерес для государственных регуляторов, можно и нужно договариваться с регуляторами

Путь первый: Архив как доверенный хранитель документов

- Архив объявляется доверенным учреждением (контроль и сертификация)
- Задача архива убедиться в том, что документы были целостными, аутентичными, пригодными к использованию в момент передачи на архивное хранение
- В дальнейшем целостность, аутентичность и пригодность к использованию документов обеспечивает и удостоверяет доверенный хранитель, которому законодательство должно предоставить право гибко использовать как известные, так и новые технологии для обеспечения сохранности электронных документов – как это сейчас делается в бумажном архивном деле

Путь второй: Централизованные реестры электронных документов

- Возвращение к истокам регистрационной системы
- Создание системы, в рамках которой каждый выпускаемый в обращение электронный документ (или его хеш, если содержание документа раскрывать нежелательно) должен регистрироваться уполномоченным органом
- Ведущий реестр орган должен иметь достаточно широкие полномочия по выбору технологий

Путь третий: делать то, что возможно и поси́льно для организации

- Используется подход систем менеджмента
- Регламентируется порядок хранения и подтверждения подлинности электронных документов. Далее организация действует в строгом соответствии с этим порядком, документируя свои действия. Выявляются и устраняются недостатки, обеспечивается цикл непрерывного улучшения. Проводится обучение персонала
- Важно быть не хуже других в своей отрасли

Приглашаю Вас на мой блог: <http://rusrim.blogspot.com/>

КТО НЕ ИДЁТ ВПЕРЕД, ТОТ ИДЁТ НАЗАД

DR NATASHA KHRAMTSOVSKY



ОБО МНЕ: НАТАША ХРАМЦОВСКАЯ / DR

ПЯТНИЦА, 11 СЕНТЯБРЯ 2015 Г.

Евросоюз определился с форматами электронных подписей и печатей, используемых при получении государственных электронных услуг

Недавно Евросоюз обновил своё законодательство по вопросам электронных подписей и услуг в области доверия, выпустив вместо реализуемых каждой страной через национальное законодательство европейской Директивы 1999/93/ЕС законодательный акт (Регламент) прямого действия (см. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG).

Теперь опубликован ещё один из предусмотренных регламентом подзаконных нормативных актов – «Исполнительное решение Еврокомиссии 2015/1506 от 8 сентября 2015 года, устанавливающее требования к форматам усиленных электронных подписей и усиленных печатей, признаваемых учреждениями и организациями государственного сектора в соответствии со ст. 27(5) и 37(5) утвержденного Европейским Парламентом и Советом Регламента № 910/2014 относительно электронной идентификации и услуг в области доверия для электронных транзакций на внутреннем рынке» (Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_235_R_0006&from=EN).

а также на мои каналы на Slideshare и YouTube

