Эффективный документооборот власти и информационное общество

27-29 апреля 2011 года

Проблемы длительного архивного хранения электронных документов с ЭЦП

КОМПАНИЯ КРИПТО-ПРО
ключевое слово в защите информации

www.cryptopro.ru

Общие положения

В данной презентации не будут рассматриваться все проблемы архивного хранения документов в электронной форме

Не будут рассматриваться вопросы технического обеспечения работы с электронным документом (включая средства ЭЦП), находящемся на длительном архивном хранении.

Будут рассматриваться проблемы и способы их решения, связанные с ЭЦП, являющейся реквизитом электронного документа, находящемся на длительном архивном хранении.

О чем нам говорит 1-ФЗ «Об электронной цифровой подписи»?

Статья 4 «Условия признания равнозначности электронной цифровой подписи и собственноручной подписи»

Часть 1

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания
- подтверждена подлинность электронной цифровой подписи в электронном документе (а значит и средство ЭЦП на момент проверки или на момент подписания электронного документа должно быть сертифицировано согласно статьи 3 1-ФЗ)
- …

А теперь проблемы:

Проблема 1: Обеспечить, что бы сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки ЭЦП

Максимально разрешенный срок действия сертификата ключа подписи – 15 лет.
Максимальный срок действия сертификата соответствия на средство ЭЦП – 3 года.

Выводы:

Максимальный срок хранения = не более «срок действия сертификата ключа подписи» минус «срок действия закрытого ключа, соответствующего сертификату ключа подписи»

На протяжении архивного хранения в течении этого срока нужно обеспечить наличие сертификата соответствия на средство ЭЦП, которое используется для проверки ЭЦП

А теперь проблемы:

Проблема 2: Обеспечить наличие доказательств, определяющих момент подписания электронного документа

Использование штампов времени позволяет создавать доказательство факта существования документа на определённый момент времени. Штамп времени (time-stamp) - это подписанный ЭЦП документ, которым Служба штампов времени удостоверяет, что в указанный момент времени ей было предоставлено значение хэш-функции от другого документа. Само значение хэш-функции также указывается в штампе. Служба штампов времени (Time Stamping Authority - TSA) - доверенный субъект ИОК, обладающий точным и надёжным источником времени и оказывающий услуги по созданию штампов времени.

Выводы:

Сохранение в электронном документе штампа времени, полученного сразу после создания ЭЦП обеспечит доказательство, что документ был подписан не позднее времени, указанного в штампе времени

А теперь проблемы:

Проблема 3: Обеспечить наличие доказательств действия сертификата ключа подписи на момент подписания электронного документа

Использование службы OCSP для распространения информации о статусах сертификатов клиентам имеет следующие преимущества по сравнению со списками отзыва сертификатов (CRL):

- Актуальность информации о статусе. Служба может получать информацию об изменении статусов сертификатов в реальном времени и распространять её клиентам.
- Меньший объём OCSP-ответа. Объём ответа службы фиксирован и сравнительно мал, тогда как списки отзыва сертификатов могут иметь большой объём.

Выводы:

Сохранение в электронном документе CRL или OCSP-ответов, полученных сразу после создания ЭЦП обеспечит доказательство, что документ был подписан действующим сертификатом ключа подписи

Наиболее оптимально – использовать формат усовершенствованной ЭЦП:

Данный формат включает в себя:

- Подписываемый документ (может храниться отдельно от всех остальных полей).
- Подписываемые атрибуты.
- Электронную цифровую подпись.
- Штамп времени, полученный на значение ЭЦП.
- Хэш-коды доказательств подлинности.
- Внешний штамп времени, полученный на все вышеперечисленное.
- Доказательства подлинности (значения сертификатов и информация об отзыве).