PKI-FORUM
РОССИЯ

XI международная конференция «PKI-FORUM Россия 2013»

г. Санкт-Петербург, 17–19 сентября 2013 г.

Некоторые технологии реализации применения электронной подписи

Маслов Юрий
Коммерческий директор
ООО «КРИПТО-ПРО»

Зачем нужен этот доклад?

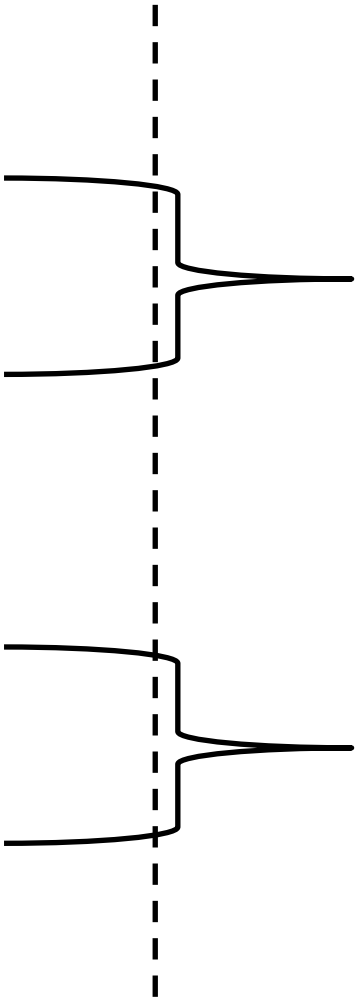
- Может использоваться при выборе технологии реализации электронной подписи
- Узнать про ещё одну нетрадиционную технологию реализации электронной подписи

Угрозы как следствие наличия неопределённостей

Уменьшение неопределённостей уменьшает вероятность возникновения угрозы

Неопределённости

- Возможно не получится доказать, что подпись не могла быть сделана посторонним лицом
- Возможно не получится доказать, что документ был неизменён после подписания
- Возможно не получится доказать, что лицо могло определить действительность электронной подписи
- Возможно не получится доказать, что действительность электронной подписи является неизменяемым во времени



Угрозы

Лицо может принять к исполнению электронный документ, удостоверенный «недействительной» электронной подписью, а подписант может отказаться от факта подписания этого документа

Лицо может не принять к исполнению документ, удостоверенный «действительной» электронной подписью

Мера неопределённости - вероятность наступления событий, от которых зависит возникновение угрозы

Меру неопределённости определим как произведение вероятностей событий:

Перечень событий (независимых и совместных)
Лица, подписавшее электронный документ, определено однозначно:
- ключ подписи и ключ проверки подписи являются уникальными
- существует однозначная связь между ключом подписи и ключом проверки подписи
- существует однозначная связь между ключом проверки подписи и его владельцем
Доказано отсутствие изменения в документе после подписания:
- однозначность механизма контроля целостности подписи документа и подписи
Доказана действительность электронной подписи на любой момент времени:
- однозначность механизма информирования участников системы о факте аннулирования ключа проверки подписи
- однозначность механизма определения статуса ключа проверки подписи на момент времени (создания и/или проверки ЭП)

В связи с невозможностью использования объективных методов определения вероятности исхода в неопределённости (нет статистики), используется субъективный метод оценки (на суждениях и личном опыте) вероятности исхода неопределённости

Неопределённости	Без криптографических средств (для простой ЭП)	Криптографические неГОСТ средства ЭП без СКПЭП	Криптографические ГОСТ средства ЭП без СКПЭП	Криптографические неГОСТ средства ЭП с СКПЭП	Криптографические ГОСТ средства ЭП с СКПЭП	Сертифицированные средства ЭП и УЦ
Однозначность определения лица, подписавшего электронный документ:	**0.125**	**0.32**	**0.45**	**0.512**	**0.81**	**1**
- уникальность ключа подписи и ключа проверки подписи	0.5	0.8	0.9	0.8	0.9	1
- однозначная связь между ключом подписи и ключом проверки подписи	0.5	0.8	1	0.8	1	1
- однозначная связь между ключом проверки подписи и его владельцем	0.5	0.5	0.5	0.8	0.9	1
Доказуемость отсутствия изменения в документе после подписания:	**0.5**	**0.8**	**1**	**0.8**	**1**	**1**
- однозначность механизма контроля целостности подписи документа и подписи	0.5	0.8	1	0.8	1	1
Доказуемость действительности электронной подписи на любой момент времени	**0.25**	**0.25**	**0.25**	**0.64**	**0.9**	**1**
- однозначность механизма информирования участников системы о факте аннулирования ключа проверки подписи	0.5	0.5	0.5	0.8	1	1
- однозначность механизма проверки статуса ключа проверки подписи на момент времени	0.5	0.5	0.5	0.8	0.9	1
Мера неопределённости	**0.016**	**0.064**	**0.113**	**0.262**	**0.729**	**1**

Что нужно пользователю технологии ЭП?

КРИПТО ПРО

Безопасность

Любые устройства

Любые платформы

Любые браузеры

«Традиционная» технология реализации применения ЭП

КРИПТО ПРО

“Каждая система безопасна настолько, насколько безопасно ее самое слабое звено.”

Б.Шнайер, Н.Фергюсон “Практическая криптография” (2003)

- утрата и кража ключевых носителей;
- невозможность контроля среды функционирования криптосредства на рабочем месте клиента.

«Облачная» технология реализации применения ЭП

КРИПТО ПРО

Что мы от неё хотим?

Исключить установку и использование средств ЭП на рабочем месте пользователя

- Любой компьютер, в любой точке мира, на любой платформе
- Массовый, неквалифицированный пользователь
- Не требуется контроль среды функционирования криптосредства на рабочем месте клиента

Исключить хранение ключа ЭП непосредственно у владельца

- Не имею и не теряю
- Невозможность компрометации ключа ЭП владельцем

«Облачная» технология реализации применения ЭП

КРИПТО ПРО

Какие предъявляем требования?

Должна обеспечивать доверенное хранение и использование ключей электронных подписей

- Доказываемое исключение из числа нарушителей любого сотрудника оператора «облачной» технологии, включая администраторов системы
- Гарантированная защита от компрометации ключей по любым каналам атак
- Доверенная среда функционирования средства ЭП, использующего ключи ЭП пользователей

«Облачная» технология реализации применения ЭП

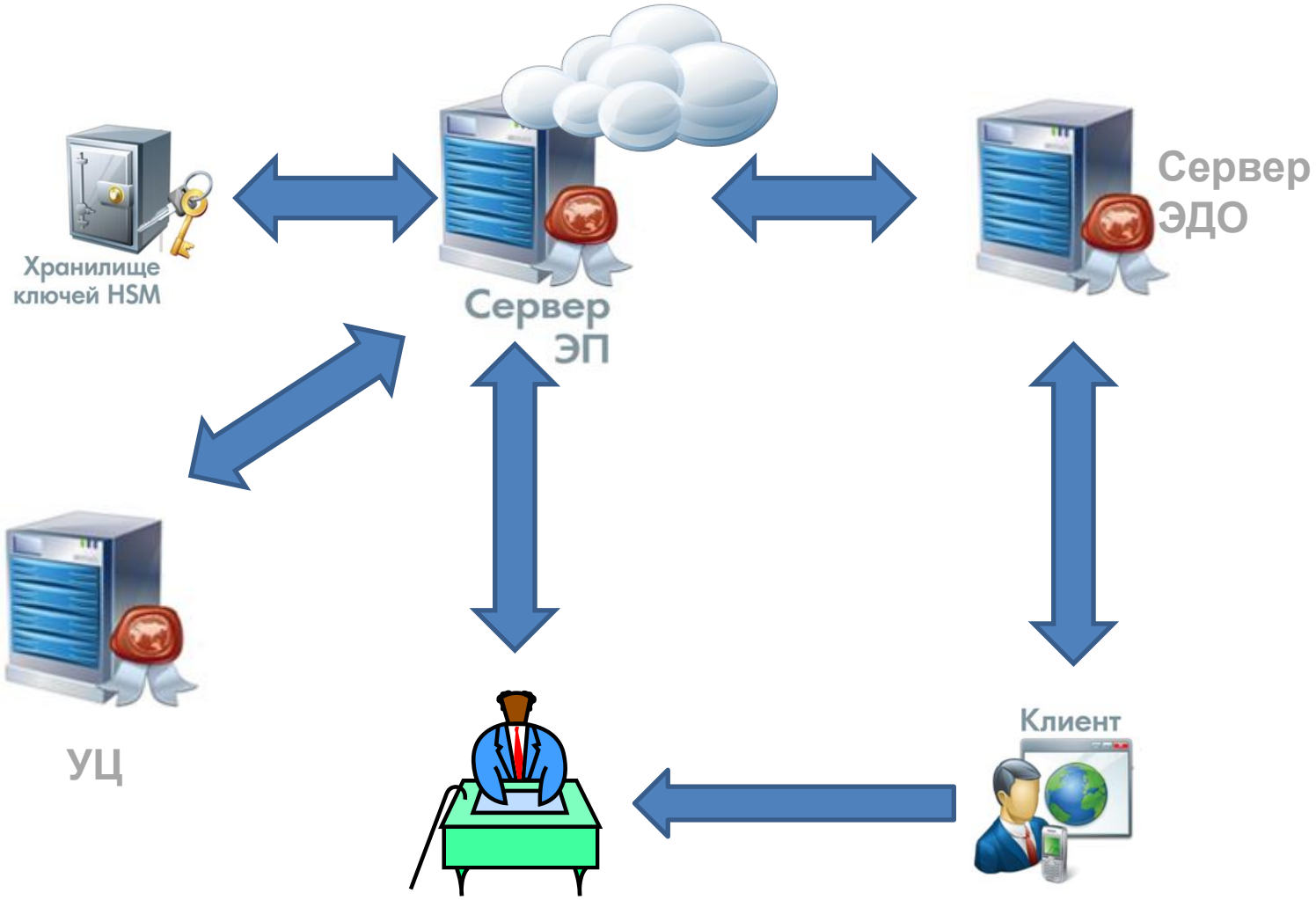
Какие предъявляем требования?

Должна реализовывать надежную и оцениваемую систему аутентификации владельца сертификата

- Доказываемая аутентификация в рамках принятой модели нарушителя и модели угроз
- Несколько способов многофакторной аутентификации владельцев ключа электронной подписи
- Использование резервных методов аутентификации

Видение реализации «облачной» технологии применения ЭП

Общая схема взаимодействия компонент



Пример реализации «облачной» технологии применения ЭП

ПАК «КриптоПро DSS» использует:

Для доверенного хранения и применения ключей электронных подписей

- ПАКМ «КриптоПро HSM»

Для аутентификации владельца сертификата

- Двухфакторная аутентификация OTP по SMS
- Двухфакторная аутентификация с Рутокен WEB и Рутокен ЭЦП

КРИПТО ПРО

СПАСИБО ЗА ВНИМАНИЕ!

Вопросы?

КРИПТО-ПРО – ключевое слово в защите информации

http://www.cryptopro.ru
info@cryptopro.ru

Тел./факс:
+7 (495) 995-48-20
+7 (495) 984-07-90