конференция
РусКрипто'2013

КРИПТО ПРО

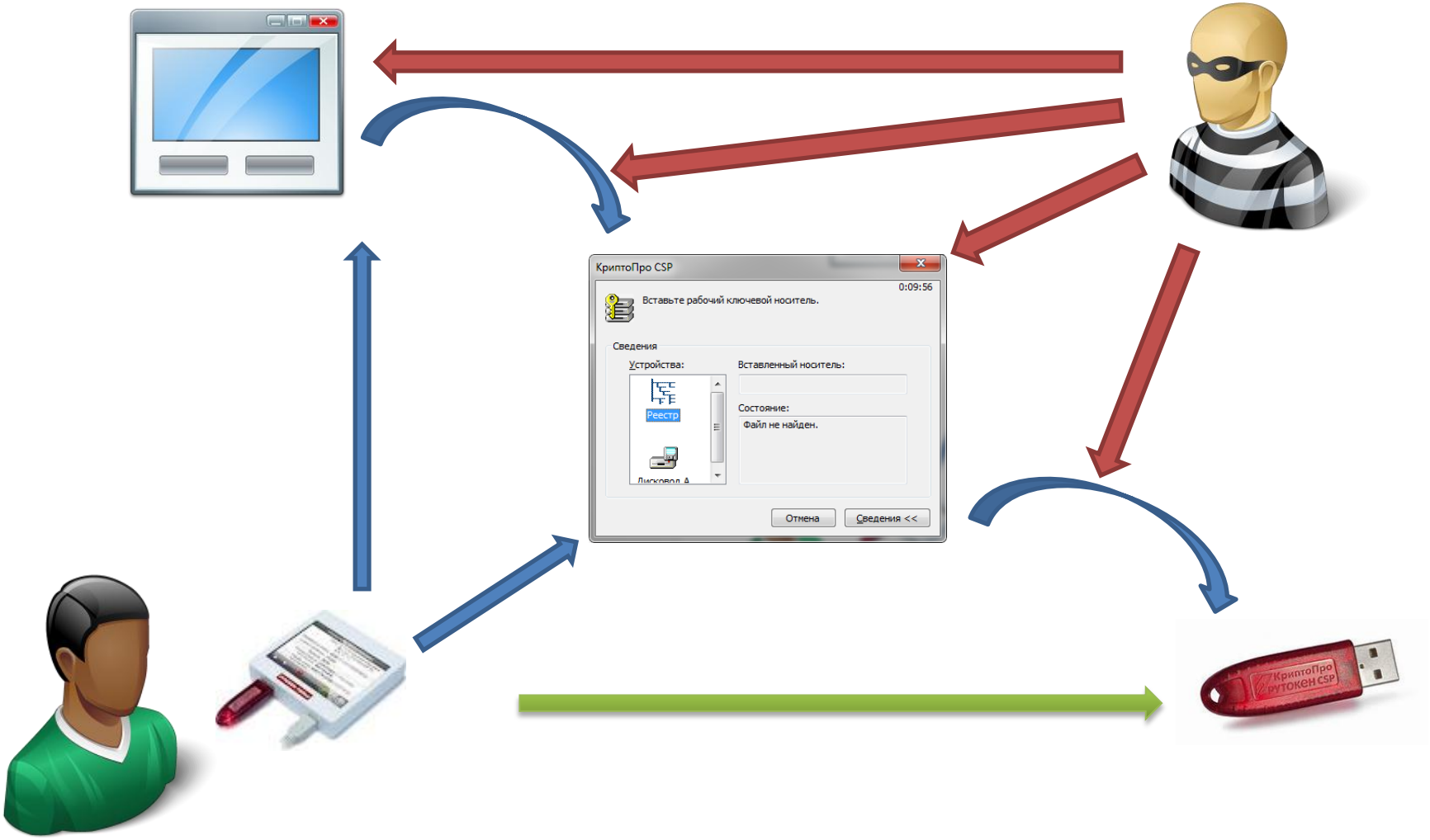
Реализация доверенного отображения подписанного документа в системах ДБО и не только

Смирнов Павел
Зам. начальника отдела разработок, к.т.н.
ООО «КРИПТО-ПРО»

План

- От чего защищаемся
- Чем защищаемся
- Недостатки существующих решений
- Как избавиться от недостатков
- Что работает сейчас

Модель нарушителя



Требования регулятора

63-ФЗ требует от средств ЭП показывать документ

- При подписании
- При проверке

В общем виде задача неразрешима

- Никакое средство ЭП не способно отобразить произвольный документ
- Письмо ФСБ: для документов MS Office и PDF, подписываемых встроенными в Adobe и Office средствами, «всё хорошо»

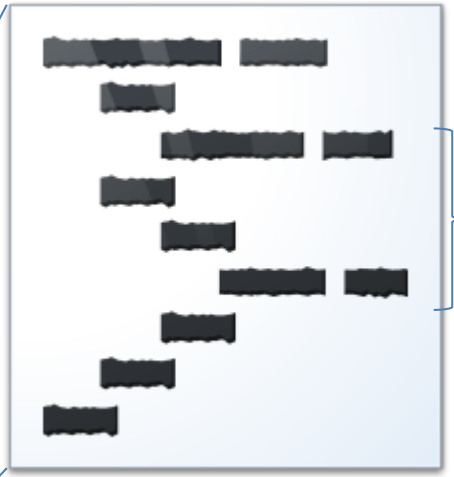
Существующие устройства

Недостатки

- Разная разметка
- Нет поддержки стандартных форматов CMS и XMLDSig
- Необходимость изменения принятого формата документа
- Разные способы встраивания для различных устройств

Предлагаемое решение

Подпись CMS или XMLDsig



Структурированная «выжимка» из документа

Подписанные атрибуты

- Идентификатор (OID) атрибута определяет формат разметки
- Middleware вызывает средство ЭП и устройство отображения, которое показывает только «выжимку»

Работает уже сейчас

Подпись CMS через CryptoAPI

- КриптоПро eToken CSP + SafeTouch
- Магистра CSP + SafeTouch

Ближайшее будущее: подтверждение подписания документа в КриптоПро DSS

- «Выжимка» из документа отправляется в SMS вместе с одноразовым паролем
- Эта же информация попадает в специальный атрибут подписанного документа

СПАСИБО ЗА ВНИМАНИЕ!

КРИПТО-ПРО – ключевое слово в защите информации

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

Тел./факс:
+7 (495) 780-48-20
+7 (495) 660-23-30