



конференция
РусКрипто'2013



Реализация доверенного отображения подписанного документа в системах ДБО и не только

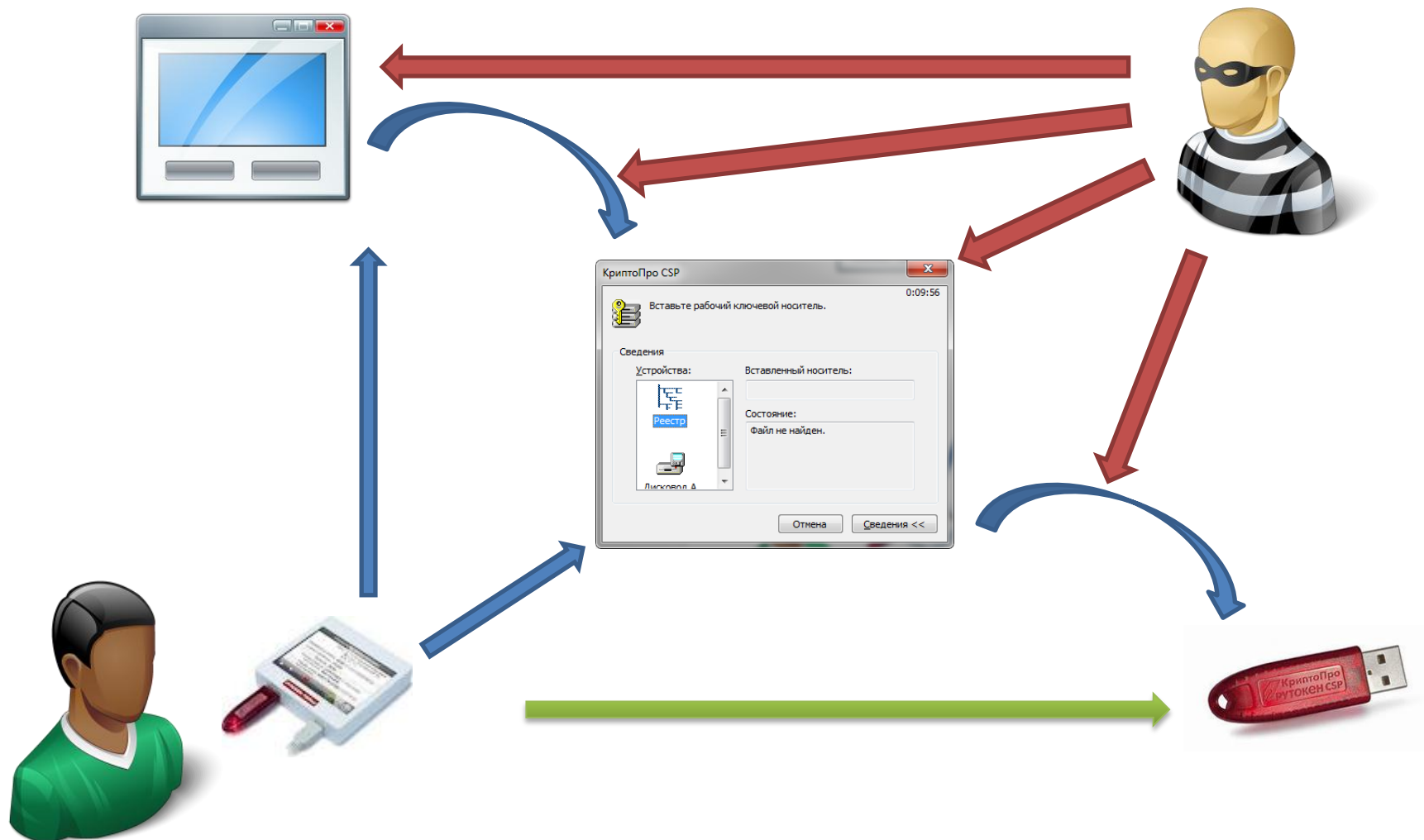
Смирнов Павел
Зам. начальника отдела разработок, к.т.н.
ООО «КРИПТО-ПРО»

© 2000-2013 КРИПТО-ПРО



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

Модель нарушителя



Существующие устройства

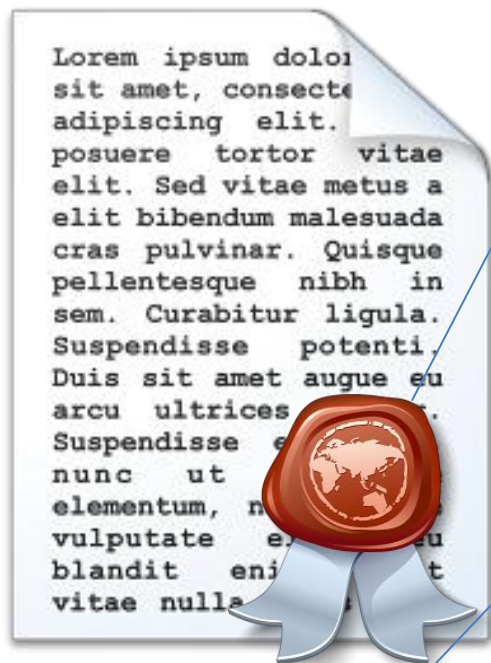




Недостатки

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

Предлагаемое решение



Структурированная
«выжимка» из
документа

Подписанные
атрибуты

Подпись CMS
или XMLDsig

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

Работает уже сейчас



Подпись CMS через CryptoAPI

- КристоПро eToken CSP + SafeTouch
- Магистра CSP + SafeTouch

Ближайшее будущее: подтверждение подписания документа в КристоПро 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