Новые инициативы Европейского союза в области электронной подписи

Смирнов Павел
ведущий специалист, к.т.н.
ООО «КРИПТО-ПРО»

Содержание

- Проверка сертификата и электронной подписи в сложной системе PKI
- Форматы электронной подписи
- Трансграничная аутентификация
- Выводы

Цифровая повестка дня для Европы

Основные действия по электронной подписи

1. Рационализация стандартов по электронной подписи
2. Переработка Решения 2003/ 511 /EC
3. Доверенный список провайдеров квалифицированных сертификатов
4. Форматы электронной подписи
5. Надзор за издателями квалифицированных сертификатов
6. Исследования, пилотные проекты: PEPPOL

Основные действия по электронной идентификации

1. STORK
2. Исследования

Проблемы проверки подписи

- Можно ли доверять сертификату ключа подписи?
- Подходит ли регламент УЦ?
- Надёжен ли алгоритм хэширования?
- Надёжен ли алгоритм подписи?
- Достаточен ли размер ключа подписи?

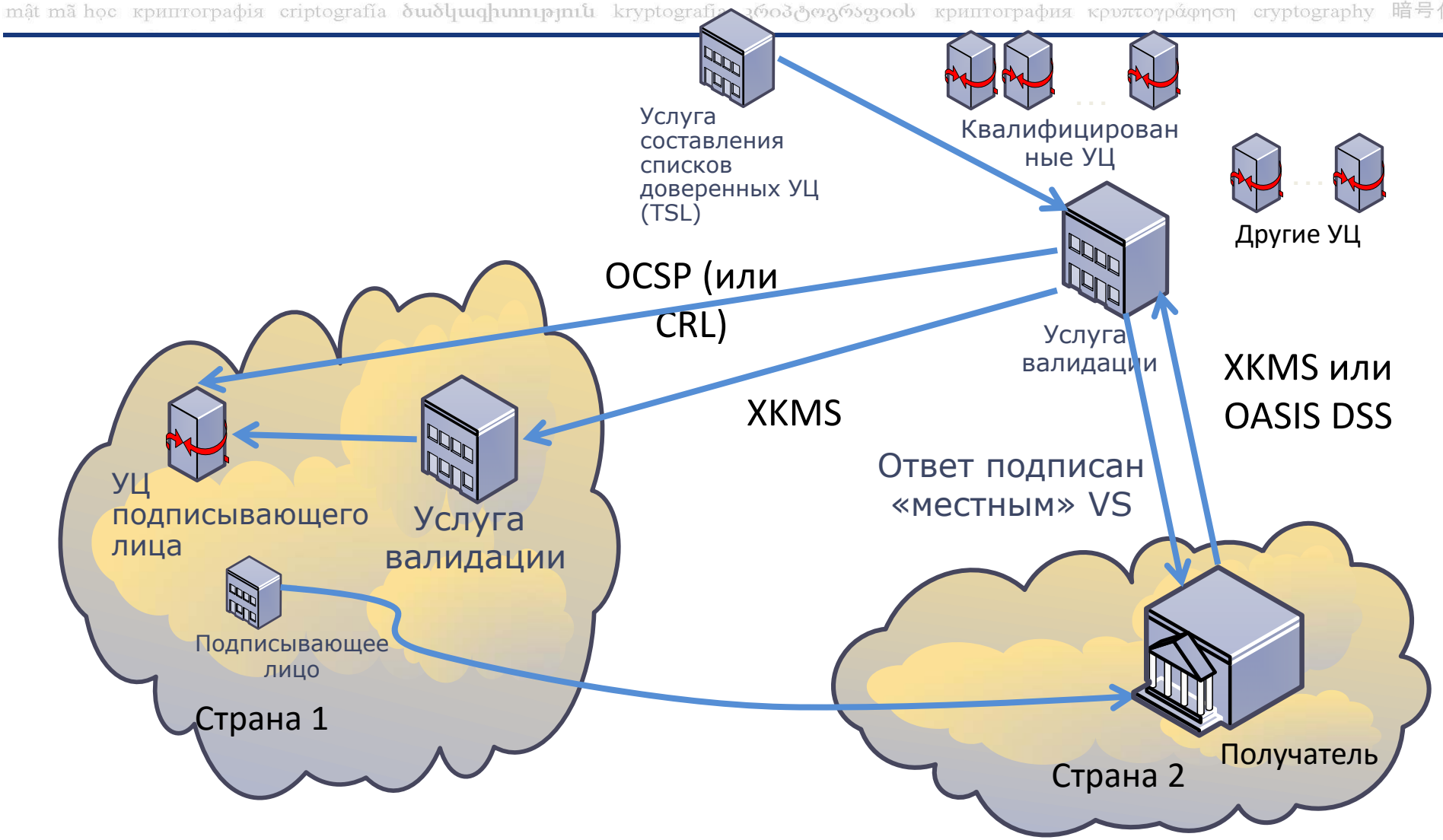
Проект PEPPOL

Функциональные спецификации трансграничного использования электронной подписи на электронных торгах:

Часть 1. Предпосылки и объем исследования
Часть 2. Спецификации пилотного проекта системы электронных торгов
Часть 3. Политика в области подписи
Часть 4. Архитектура и доверенные модели
Часть 5. Спецификация интерфейса XKMS v2
Часть 6. Спецификация интерфейса OASIS DSS
Часть 7. Классификация качества электронной личности и электронной подписи

http://www.peppol.eu/deliverables/wp-1

Проверка подписи как сервис



PEPPOL: Качество подписи

- Качество подписи (0-6)
  - 6 – уровень политики квалифицированной подписи
  - 5 – уровень политики квалифицированного сертификата
- Уровень доверия к сертификату (0-7)
  - 6-7 – контролируемый/аккредитованный УЦ, выдающий квалифицированные сертификаты
- Стойкость алгоритма хэширования (0-5)
  - 1 – SHA-1 (до 3 лет в перспективе)
  - 2/3/4/5 – SHA-224/256/384/512
- Стойкость закрытого ключа подписи (0-5)
  - 1 – RSA-1024
  - 2 – RSA-2048

Совместимость форматов ЭЦП

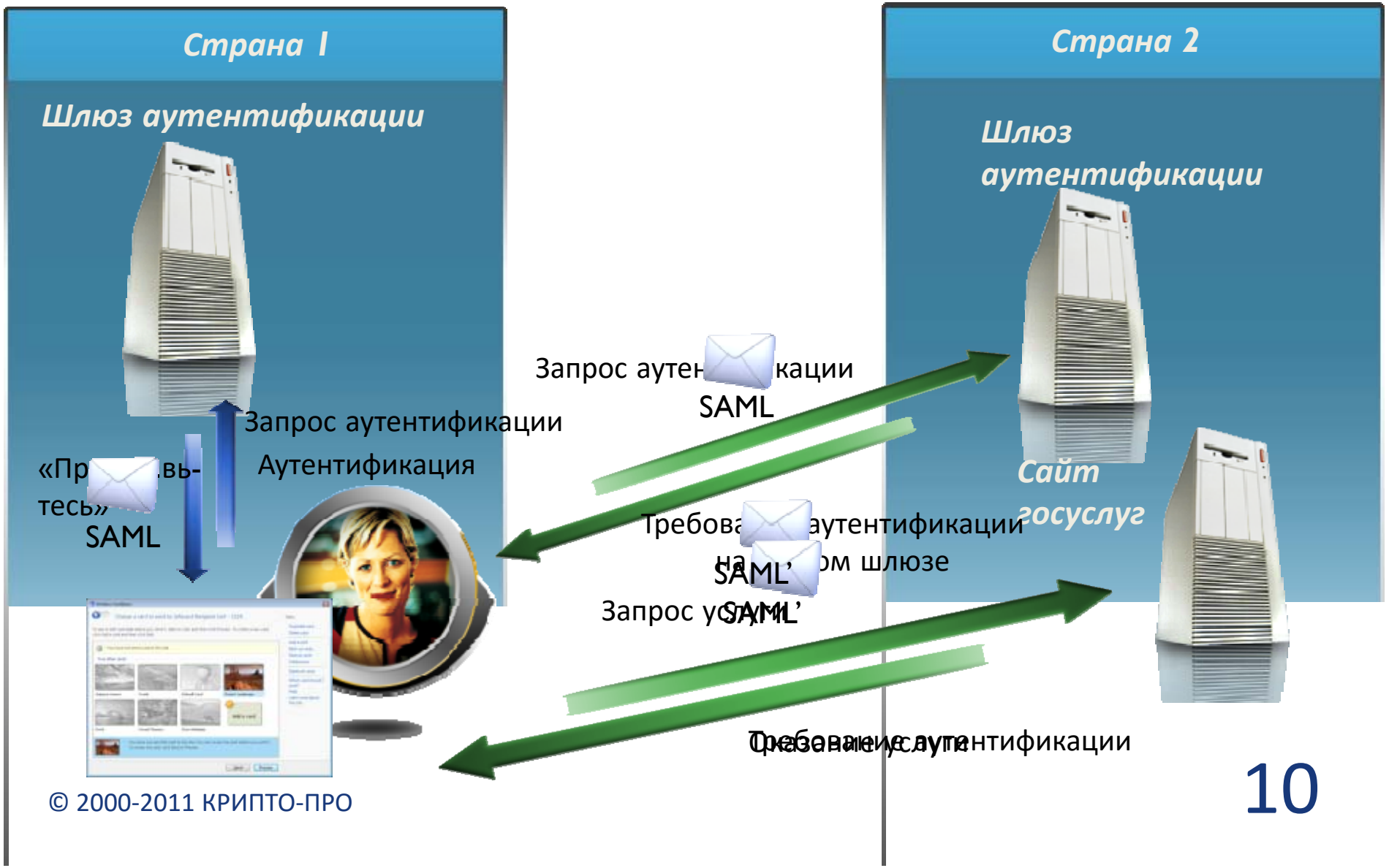
- Решение Еврокомиссии 2011/130/EU от 25.02.2011:
  - Электронные сервисы должны уметь обрабатывать документы, подписанные компетентными органами, в форматах C/X/PaDES-BES (EPES)
  - Подпись должна включать подписанный атрибут, содержащий время подписи

Совместимость электронных идентификаторов

Из Цифровой повестки дня для Европы:

- Ключевое действие 3. В 2011 предложено провести переработку Директивы по электронной подписи с целью обеспечения законодательной основы для трансграничного признания и интероперабельности безопасных систем электронной аутентификации
- Ключевое действие 16. В 2012 предложено принять Решение Совета и Правительства о гарантии взаимного признания электронной идентификации и аутентификации в ЕС на основе ”услуг аутентификации“ онлайн, которые будут предложены всем странам-участницам (с возможным использованием официальных гражданских документов, выпущенных государственным или частным сектором)

Проект STORK



Выводы

- Для решения сложной задачи проверки подписи можно использовать услугу доверенной третьей стороны, работающей в соответствии с рекомендациями PEPPOL
- Форматы электронной подписи должны быть едиными и основываться на C/X/PAdES
- Задачи интегрированной аутентификации – универсальная электронная карта
- Юридические нормы в области ЭЦП должны быть подкреплены техническими нормами – стандартами

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